

SGP.23 RSP Test Specification Version 1.4 18 December 2018

This is a Change Request of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2018 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy

V1.4 Page 1 of 777

Table of Contents

1	Intro	duction	7
	1.1	Overview	7
	1.2	Scope	7
	1.3	Definition of Terms	8
	1.4	Abbreviations	12
	1.5	Document Cross-references	15
	1.6	Conventions	16
2	Testi	ng Rules	16
	2.1	Applicability	16
	2.1.1	Format of the Optional Features Table	16
	2.1.2	Format of the Applicability Table	16
	2.1.3	Applicability and Notations	17
	2.1.4	Optional Features Table	17
	2.1.5	Applicability Table	19
	2.2	General Consideration	27
	2.2.1	Test Case Definition	27
	2.2.2	Test Cases Format	28
	2.2.3	General Rules for eUICC Testing	32
	2.2.4	General Rules for Device Testing	33
	2.2.5	Pass Criteria	35
	2.2.6	Future Study	35
3	Testi	ng Architecture	35
	3.1	Testing Scope	35
Fiç	gure 1:	Scope of the Tests	36
	3.2	Testing Execution	37
	3.2.1	eUICC - Test Environment	38
	3.2.2	SM-DP+ and SM-DS - Test Environment	38
	3.2.3	Device/LPAd - Test Environment	40
	3.2.4	End-to-End Testing	42
4	Inter	ace Compliance Testing	42
	4.1	General Overview	42
	4.2	eUICC Interfaces	43
	4.2.1	ATR and ISD-R Selection	43
	4.2.2	ES6 (Operator eUICC): UpdateMetadata	43
	4.2.3	ES8+ (SM-DP+ eUICC): InitialiseSecureChannel	52
	4.2.4	ES8+ (SM-DP+ eUICC): ConfigureISDP	55
	4.2.5	ES8+ (SM-DP+ eUICC): StoreMetadata	58
	4.2.6	ES8+ (SM-DP+ eUICC): ReplaceSessionKeys	69
	4.2.7	ES8+ (SM-DP+ eUICC): LoadProfileElements	71
	4.2.8	ES10a (LPA eUICC): GetEuiccConfiguredAddresses	80
	4.2.9	ES10a (LPA eUICC): SetDefaultDpAddress	81
	4.2.1	D ES10b (LPA eUICC): PrepareDownload	84

V1.4 Page 2 of 777

4.2.11	ES10b (LPA eUICC): LoadBoundProfilePackage	90
4.2.12	ES10b (LPA eUICC): GetEUICCChallenge	101
4.2.13	ES10b (LPA eUICC): GetEUICCInfo	101
4.2.14	ES10b (LPA eUICC): ListNotification	106
4.2.15	ES10b (LPA eUICC): RetrieveNotificationsList	120
4.2.16	ES10b (LPA eUICC): RemoveNotificationFromList	148
4.2.17	ES10b (LPA eUICC): LoadCRL	155
4.2.18	ES10b (LPA eUICC): AuthenticateServer	155
4.2.19	ES10b (LPA eUICC): CancelSession	176
4.2.20	ES10c (LPA eUICC): GetProfilesInfo	184
4.2.21	ES10c (LPA eUICC): EnableProfile	193
4.2.22	ES10c (LPA eUICC): DisableProfile	216
4.2.23	ES10c (LPA eUICC): DeleteProfile	238
4.2.24	ES10c (LPA eUICC): eUICCMemoryReset	250
4.2.25	ES10c (LPA eUICC): GetEID	255
4.2.26	ES10c (LPA eUICC): SetNickname	256
4.2.27	ES10b (LPA eUICC): GetRAT	260
4.3 S	M-DP+ interfaces	262
4.3.1	ES2+ (Operator SM-DP+): DownloadOrder	262
4.3.2	ES2+ (Operator SM-DP+): ConfirmOrder	262
4.3.3	ES2+ (Operator SM-DP+): CancelOrder	262
4.3.4	ES2+ (Operator SM-DP+): ReleaseProfile	262
4.3.5	ES2+ (Operator SM-DP+): HandleDownloadProgressInfo	262
4.3.6	ES2+ (Operator SM-DP+): TLS, Mutual Authentication, Server,	
	Session Establishment	262
4.3.7	ES8+ (SM-DP+ eUICC): InitialiseSecureChannel	262
4.3.8	ES8+ (SM-DP+ eUICC): ConfigureISDP	263
4.3.9	ES8+ (SM-DP+ eUICC): StoreMetadata	263
4.3.10	ES8+ (SM-DP+ eUICC): ReplaceSessionKeys	263
4.3.11	ES8+ (SM-DP+ eUICC): LoadProfileElements	263
4.3.12	ES9+ (LPA SM-DP+): InitiateAuthentication	264
4.3.13	ES9+ (LPA SM-DP+): GetBoundProfilePackage	270
4.3.14	ES9+ (LPA SM-DP+): AuthenticateClient	308
4.3.15	ES9+ (LPA SM-DP+): HandleNotification	341
4.3.16	ES9+ (LPA SM-DP+): CancelSession	359
4.3.17	ES9+ (LPA SM-DP+): TLS, Server Authentication, Session	
	Establishment	379
4.3.18	ES12 (SM-DP+ SM-DS): RegisterEvent	379
4.3.19	ES12 (SM-DP+ SM-DS): DeleteEvent	379
4.3.20	ES12 (SM-DP+ SM-DS): TLS, Mutual Authentication, Client, Session	
	Establishment	379
	PAd Interfaces	380
4.4.1	ES10a (LPA eUICC): GetEuiccConfiguredAddresses	380
4.4.2	ES10a (LPA eUICC): SetDefaultDpAddress	380
4.4.3	ES10b (LPA eUICC): PrepareDownload	380

V1.4 Page 3 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

4.4.4	ES10b (LPA eUICC): LoadBoundProfilePackage	380
4.4.5	ES10b (LPA eUICC): GetEUICCChallenge	380
4.4.6	ES10b (LPA eUICC): GetEUICCInfo	380
4.4.7	ES10b (LPA eUICC): ListNotification	380
4.4.8	ES10b (LPA eUICC): RetrieveNotificationsList	380
4.4.9	ES10b (LPA eUICC): RemoveNotificationFromList	380
4.4.10	ES10b (LPA eUICC): LoadCRL	380
4.4.11	ES10b (LPA eUICC): AuthenticateServer	381
4.4.12	ES10b (LPA eUICC): CancelSession	381
4.4.13	ES10c (LPA eUICC): GetProfilesInfo	381
4.4.14	ES10c (LPA eUICC): EnableProfile	381
4.4.15	ES10c (LPA eUICC): DisableProfile	381
4.4.16	ES10c (LPA eUICC): DeleteProfile	381
4.4.17	ES10c (LPA eUICC): eUICCMemoryReset	381
4.4.18	ES10c (LPA eUICC): GetEID	381
4.4.19	ES10c (LPA eUICC): SetNickname	381
4.4.20	ES10b (LPA eUICC): GetRAT	381
4.4.21	ES9+ (LPA SM-DP+): InitiateAuthentication	381
4.4.22	ES9+ (LPA SM-DP+): GetBoundProfilePackage	387
4.4.23	ES9+ (LPA SM-DP+): AuthenticateClient	395
4.4.24	ES9+ (LPA – SM-DP+): HandleNotification	409
4.4.25	ES9+ (LPA – SM-DP+): CancelSession	417
4.4.26	ES9+ (LPA – SM-DP+): HTTPS	432
4.4.27	ES11 (LPA – SM-DS): InitiateAuthentication	437
4.4.28	ES11 (LPA – SM-DS): AuthenticateClient	442
4.4.29	ES11 (LPA SM-DS): HTTPS	450
4.5 S	M-DS Interfaces	454
4.5.1	ES12 (SM-DP+ SM-DS): RegisterEvent	454
4.5.2	ES12 (SM-DS SM-DP+): DeleteEvent	463
4.5.3	ES15 (SM-DS SM-DS): RegisterEvent	472
4.5.4	ES15 (SM-DS SM-DS): DeleteEvent	474
4.5.5	ES11 (LPA SM-DS): InitiateAuthentication	476
4.5.6	ES11 (LPA SM-DS): Authenticate Client	477
4.5.7	ES15 (SM-DS SM-DS): TLS, Mutual Authentication, Client, Session	
	Establishment	498
4.5.8	ES12 (SM-DS SM-DP+): TLS, Mutual Authentication, Server, Session	
	Establishment	499
4.5.9	ES15 (SM-DS SM-DS): TLS, Mutual Authentication, Server, Session	
	Establishment	499
4.5.10	ES11 (LPA SM-DS): TLS, Server Authentication, Session	
	Establishment	500
	LS Interface	500
4.6.1	TLS, Mutual Authentication, Client, TLS Establishment	500
4.6.2	TLS, Mutual Authentication, Server, TLS Establishment	509
4.6.3	TLS, Server Authentication, TLS Establishment	517

Non-confidential

V1.4 Page 4 of 777

	4.7	LPAe Interfaces	521
5	Proce	dure - Behaviour Testing	522
	5.1	General Overview	522
	5.2	eUICC Behaviour	522
	5.2.1	Retry mechanism	522
	5.2.2	Forbidden PPRs	528
	5.2.3	eUICC's RAT	530
	5.2.4	eUICC File Structure	531
	5.2.5	eUICC Delete Profile Process	532
	5.2.6	eUICC Enable Profile Process	533
	5.2.7	eUICC Disable Profile Process	535
	5.2.8	eUICC Notifications	536
	5.3	Platform Procedures	537
	5.3.1	Profile Download and Installation Procedure	537
	5.3.2	Common Mutual Authentication Process	537
	5.3.3	Profile Download and Installation Process	537
	5.4	Device Procedures	541
	5.4.1	Local Profile Management - Add Profile	541
	5.4.2	Local Profile Management - ListProfiles	553
	5.4.3	Local Profile Management - SetNickname	554
	5.4.4	Local Profile Management - Delete Profile	558
	5.4.5	Local Profile Management - Enable Profile	563
	5.4.6	Local Profile Management - Disable Profile	568
	5.4.7	Local eUICC Management - Retrieve EID Process	571
	5.4.8	Local eUICC Management - eUICC Memory Reset Process	572
	5.4.9	Local eUICC Management - eUICC Test Memory Reset Process	577
	5.4.10	Local eUICC Management – Set/Edit Default SM-DP+ Address Process	577
	5.4.11	Device Power On – Profile Discovery	579
6	End-t	o-End Testing	582
7	Exter	nal Test Specifications	583
	7.1	SIMAlliance eUICC Profile Package Test Specification	583
An	nex A	Constants	584
	A.1	Generic Constants	584
	A.2	Test Certificates and Test Keys	593
An	nex B	Dynamic Content	602
An	nex C	Methods and Procedures	612
	C.1	Methods	612
	C.2	Procedures	626
An	nex D	Commands And Responses	643
	D.1	ES8+ Requests And Responses	643
		ES8+ Requests	643
		ES9+ Requests And Responses	660
	D.2.1	ES9+ Requests	660
	D.2.2	ES9+ Responses	691

V1.4 Page 5 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

D.3	ES10x Requests And Responses	705
D.3.1	ES10x Requests	705
D.3.2	ES10x Responses	717
D.4	APDU	743
D.4.1	APDU Commands	743
D.4.2	R-APDU Chaining	744
D.5	ES6 Requests And Responses	745
D.5.1	ES6 Requests	745
D.6	ES11 Requests And Responses	746
D.6.1	ES11 Requests	746
D.6.2	ES11 Responses	753
D.7	ES12 Requests And Responses	754
D.8	ES15 Requests And Responses	754
D.9	Common Server Responses	754
Annex E	Profiles	762
Annex F	IUT Settings	768
F.1	eUICC Settings	768
F.2	Platforms Settings	768
F.3	Device Settings	769
F.4	Common Settings	770
Annex G	Initial States	771
G.1	Device	771
G.1.1	Device (default)	771
G.1.2	Companion Device connected to a Primary Device	771
G.1.3	Test eUICC Settings	771
G.2	eUICC	772
G.2.1	Common Initial States	772
G.2.2	For eUICC supporting NIST P-256	773
G.2.3	For eUICC supporting BrainpoolP256r1	773
G.2.4	With default RAT configuration	773
G.2.5	With Additional PPARs in the RAT	773
G.2.6	• •	774
G.3	SM-DP+ and SM-DS	774
Annex H	Icons and QR Codes	775
Annex I	Requirements	776
Annex J	Document Management	777
J.1	Document History	777

V1.4 Page 6 of 777

GSM Association
Official Document SGP.23 - SGP.23 RSP Test Specification

Non-confidential

1 Introduction

1.1 Overview

The main aim of the GSMA Remote SIM Provisioning specifications [2] & [3] is to provide solution for the Remote SIM Provisioning of Consumer Devices. The adoption of this technical solution will provide the basis for global interoperability between different Operator deployment scenarios, for example network equipment (e.g. Subscription Manager Data Preparation (SM-DP+)) and various eUICC platforms.

This Test Plan provides a set of test cases to be used for testing the implementations of the provisioning system specifications documents [2] & [3]. This document offers to the involved entities an unified test strategy and ensures interoperability between different implementations.

1.2 Scope

This document is intended for:

- · Parties which develop test tools and platforms
- Vendors (Device and eUICC Manufacturers, SM-DP+ and SM-DS Providers)
- Operators

The Test Plan consists of a set of relevant test cases for testing all entities involved in the eUICC remote provisioning system. The Implementations Under Test (IUT) are:

- the eUICC
- the LPAd for a Standalone and Companion Device
- the SM-DP+
- the SM-DS

The testing scopes developed in this document are:

- Interface compliance testing: Test cases to verify the compliance of the interfaces within the system.
- System behaviour testing: Test cases to verify the functional behaviour of the system.

Each test case specified within this Test Plan refers to one or more requirements.

The Test Plan contains test cases for the following versions of SGP.22:

- GSMA RSP Technical Specification V2.1 [2a]
- GSMA RSP Technical Specification V2.2 [2b]
- GSMA RSP Technical Specification V2.2.1 [2]

This document includes an applicability table providing an indication whether test cases are relevant for a specific entity.

V1.4 Page 7 of 777

1.3 Definition of Terms

Term	Description
Activation Code	Information issued by an Operator/Service Provider to an End User. It is used by the End User to request the download and installation of a Profile.
Activation Code Token	A part of the Activation Code information provided by the Operator/Service Provider to reference a Subscription.
Alternative SM-DS	SM-DS used in cascade mode with a Root SM-DS to redirect Event Registration from a SM-DP+ to the Root SM-DS.
Authenticated Confirmation	A mechanism by which the End User confirms their action through a method involving the input of personalised information (e.g. PIN, fingerprint).
Bound Profile Package	A Protected Profile Package that has been cryptographically linked to a particular eUICC.
Certificate Authority	A Certificate Authority is an entity that issues digital certificates.
Companion Device	A Device that relies on the capabilities of a Primary Device for the purpose of Remote SIM Provisioning.
Confirmation Code	A code entered by an End User required by the SM-DP+ to confirm the download of a Profile.
Confirmation Code Required Flag	A parameter to indicate whether the Confirmation Code is required.
Device	User equipment used in conjunction with an eUICC to connect to a mobile network. E.g. a tablet, wearable, smartphone or handset.
Disabled (Profile)	The state of a Profile where all files and applications (e.g. NAA) present in the Profile are not selectable.
Enabled (Profile)	The state of a Profile when its files and/or applications (e.g., NAA) are selectable.
End User	The person using the Device.
eUICC	A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way. NOTE: The term originates from "embedded UICC".
eUICC Certificate	A certificate issued by the EUM for a specific eUICC. This Certificate can be verified using the EUM Certificate.
eUICC Memory Reset	An action that returns the eUICC to a state equivalent to a factory state.
eUICC Test Memory Reset	An action that deletes all post-issuance Test Profiles on an eUICC.
EUM Certificate	A certificate issued by a GSMA CI to a GSMA accredited EUM which can be used to verify eUICC Certificates.
Event	A Profile download which is set by an SM-DP+ on behalf of an Operator, to be processed by a specific eUICC.
EventID	Unique identifier of an Event for a specific EID generated by the SM-DP+ / SM-DS.

V1.4 Page 8 of 777

Term	Description
Event Record	The set of information stored on the SM-DS for a specific Event, via the Event Registration procedure. This information consists of either: • the Event-ID, EID, and SM-DP+ address or
	the Event-ID, EID, and SM-DS address.
Event Registration	A process notifying the SM-DS on the availability of information on either a specific SM-DP+ or a specific SM-DS for a specific eUICC.
GSMA Certificate Issuer	A Certificate Authority accredited by GSMA.
Integrated Circuit Card ID	Unique number to identify a Profile in an eUICC as defined by ITU-T E.118 [10].
International Mobile Subscriber Identity	Unique identifier owned and issued by Mobile Operators as defined in 3GPP TS 23.003 [12] section 2.2.
Issuer Identifier Number	The first 8 digits of the EID identifying the EUM issuing the eUICC.
Issuer Security Domain	A security domain on the UICC as defined by GlobalPlatform Card Specification [6].
Local Profile Assistant	A functional element in the Device or in the eUICC that provides the Local Profile Download (LPD), Local Discovery Services (LDS) and Local User Interface (LUI) features. When the LPA is located in the Device, they are called LPAd, LPDd, LUId, LDSd. When the LPA is located in the eUICC, they are called LPAe, LPDe, LUIe, LDSe. Where LPA, LPD, LDS or LUI are used, they apply to the element independent of its location in the Device or in the eUICC.
Local Profile Management	Local Profile Management are operations that are locally initiated on the End User (ESeu) interface.
Local Profile Management Operation	Local Profile Management Operations include enable Profile, Disable Profile, Delete Profile, query Profile Metadata, eUICC Memory Reset, eUICC Test Memory Reset, set/edit Nickname, add Profile and edit default SM-DP+ address.
MatchingID	Reference data for an RSP Server which could be an Activation Code Token or the EventID.
Mobile Network Operator	An entity providing access capability and communication services to its End User through a mobile network infrastructure.
Mobile Network Operator Security Domain (MNO-SD)	Part of the Profile, owned by the Operator, providing the Secured Channel to the Operator's Over The Air (OTA) Platform. It is used to manage the content of a Profile once the Profile is enabled.
Network Access Application	Application residing in a Profile providing authorisation to access a network.
Notification	A report about a Profile installation or Local Profile Management Operation processed by the eUICC.

V1.4 Page 9 of 777

Term	Description
Operational Profile	A combination of Operator data and applications to be provisioned on an eUICC for the purposes of providing services by the Operator. The Profile SHALL be in support of a Subscription with the relevant Operator and allow connectivity to a mobile network. Applications MAY be included to provide non-telecommunication services.
Operator	A Mobile Network Operator or Mobile Virtual Network Operator; a company providing wireless cellular network services.
Other Notification	Any Notification other than a Profile Installation Result.
Primary Device	A Device that can be used to provide some capabilities to a Companion Device for the purpose of Remote SIM Provisioning.
Profile	A combination of data and applications to be provisioned on an eUICC for the purpose of providing services.
Profile Component	A Profile Component is an element of the Profile, when installed in the eUICC, and MAY be one of the following: • An element of the file system like an MF, EF or DF; • An Application, including NAA and Security Domain;
	 An Application, including NAA and Security Domain, Profile Metadata, including Profile Policy Rules; An MNO-SD.
Profile Installation Result	A Notification that contains the result of a Profile installation.
Profile Management	A combination of local and remote management operations (e.g.: enable Profile, disable Profile, delete Profile, and query Profile Metadata).
Profile Management Operation	An operation related to the content and state update of a Profile in a dedicated ISD-P on the eUICC.
Profile Metadata	Information pertaining to a Profile used for the purpose of Local Profile Management.
Profile Nickname	Alternative name of the Profile set by the End User.
Profile Owner	The entity that controls the operations that can be performed upon its Profile. With the exception of Test Profiles, this is always the Operator.
Profile Package	A personalised Profile using an interoperable description format that is transmitted to an eUICC to load and install a Profile.
Profile Policy Authorisation Rule	A set of data that governs the ability of a Profile Owner to make use of a Profile Policy Rule in a Profile.
Profile Policy Rule	Defines a qualification for or enforcement of an action to be performed on a Profile when a certain condition occurs.
Protected Profile Package	A Profile Package which has been cryptographically protected for storage but not linked to a particular eUICC.

V1.4 Page 10 of 777

Term	Description
Provisioning Profile	A combination of Operator data and applications to be provisioned on an eUICC for the purposes of providing connectivity to a mobile network solely for the purpose of the provisioning of Profiles on the eUICC. NOTE: Use of Provisioning Profiles for other system services in version 3 of this specification MAY require modifications of this definition.
Remote SIM Provisioning	The downloading, installing, enabling, disabling, and deleting of a Profile on an eUICC.
Roles	Roles are representing a logical grouping of functions.
Root SM-DS	A globally identified central access point for finding Events from one or more SM-DP+(s).
Rules Authorisation Table	A set of Profile Policy Authorisation Rules that, together, determines the ability of a Profile Owner to make use of a set of Profile Policy Rules in a Profile.
RSP Server	Either an SM-DS or SM-DP+.
Service Provider	The organization through which the End User obtains PLMN telecommunication services. This is usually the network Operator or possibly a separate body.
Simple Confirmation	A mechanism by which the End User confirms their action, e.g. by selecting Yes/No, OK/Cancel
SM-DP+ Certificate	A Certificate issued by a GSMA CI to a GSMA accredited SM-DP+.
SM-DS Certificate	A Certificate used by a GSMA CI to a GSMA accredited SM-DS.
SM-DP+ OID	Identifier of the SM-DP+ that is globally unique and is included as part of the SM-DP+ Certificate.
SM-DS OID	Identifier of the SM-DS that is globally unique and is included as part of the SM-DS Certificate.
Standalone Device	A Device which provides all the capabilities to be able to be used in an RSP environment and needs no other Device for the purpose of Remote SIM Provisioning
Subscription	Describes the commercial relationship between the End User and the Service Provider.
Subscription Manager Data Preparation+ (SM-DP+)	This role prepares Profile Packages, secures them with a Profile protection key, stores Profile protection keys in a secure manner and the Protected Profile Packages in a Profile Package repository, and allocates the Protected Profile Packages to specified EIDs. The SM-DP+ binds Protected Profile Packages to the respective EID and securely downloads these Bound Profile Packages to the LPA of the respective eUICC.
Subscription Manager Discovery Server (SM-DS)	This is responsible for providing addresses of one or more SM-DP+(s) to a LDS.
Test Plan	Current document describing the test cases that allow the RSP ecosystem to be tested.

V1.4 Page 11 of 777

Term	Description
Test Profile	A combination of data and applications to be provisioned on an eUICC to provide connectivity to test equipment for the purpose of testing the Device and the eUICC. A Test Profile is not intended to store any Operator Credentials.
User Intent	Describes the direct, real time acquisition and validation of the manual End User instruction on the LUI to trigger locally a Profile download or Profile Management Operation. As defined in SGP.21 [3].

1.4 Abbreviations

Abbreviation	Description
AID	Application Identifier
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
ATR	Answer To Reset
BPP	Bound Profile Package
C-APDU	Command APDU
CASD	Controlling Authority Security Domain
CERT.CI.ECDSA	Certificate of the CI for its Public ECDSA Key
CERT.DPauth.ECDSA	Certificate of the SM-DP+ for its Public ECDSA key used for SM-DP+ authentication
CERT.DPpb.ECDSA	Certificate of the SM-DP+ for its Public ECDSA key used for Profile Package Binding
CERT.DSauth.ECDSA	Certificate of the SM-DS for its Public ECDSA key used for SM-DS authentication
CERT.EUICC.ECDSA	Certificate of the eUICC for its Public ECDSA key
CERT.EUM.ECDSA	Certificate of the EUM for its Public ECDSA key
CERT.DP.TLS	Certificate of the SM-DP+ for securing TLS
CERT.DS.TLS	Certificate of the SM-DS for securing TLS
CI	Certificate Issuer
CRL	Certificate Revocation List
CRT	Control Reference Template
DER TLV	Distinguished Encoding Rules - Tag Length Value
DH	Diffie-Hellman
ECASD	eUICC Controlling Authority Security Domain
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve cryptography Digital Signature Algorithm
ECKA	Elliptic Curve cryptography Key Agreement algorithm

V1.4 Page 12 of 777

Abbreviation	Description
EID	eUICC-ID as defined in SGP.02 [1]
ETSI	European Telecommunications Standards Institute
EUM	eUICC Manufacturer
FCP	File Control Parameters
FFS	For Future Study
FQDN	Fully Qualified Domain Name
GID1	Group Identifier 1, as defined in 3GPP TS 31.102 [18]
GID2	Group Identifier 2, as defined in 3GPP TS 31.102 [18]
GSMA	GSM Association
HW	Hardware
ICCID	Integrated Circuit Card ID
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
ISO	International Standards Organisation
ITU	International Telecommunications Union
IUT	Implementation Under Test
KVN	Key Version Number
LDS	Local Discovery Service
LDSd	Local Discovery Service when LPA is in the Device
LDSe	Local Discovery Service when LPA is in the eUICC
LPA	Local Profile Assistant
LPAd	Local Profile Assistant when LPA is in the Device
LPAe	Local Profile Assistant when LPA is in the eUICC
LPD	Local Profile Download
LPDd	Local Profile Download when LPA is in the Device
LPDe	Local Profile Download when LPA is in the eUICC
LTE	Long Term Evolution
LUI	Local User Interface
LUId	Local User Interface when LPA is in the Device
LUIe	Local User Interface when LPA is in the eUICC
MAC	Message Authentication Code
MNO	Mobile Network Operator
MOC	Mandatory, Optional or Conditional
NAA	Network Access Application
OCE	Off-Card Entity

V1.4 Page 13 of 777

Abbreviation	Description		
OTA	Over The Air		
OS	Operating System		
otPK.EUICC.ECKA	One-time Public Key of the eUICC for ECKA		
otSK.EUICC.ECKA	One-time Private Key of the eUICC for ECKA		
PE	Profile Element		
PKI	Public Key Infrastructure		
PIR	Profile Installation Result		
POR	Proof Of Receipt		
PPAR	Profile Policy Authorisation Rule		
PPK-ENC	Profile Protection Key for message encryption/decryption		
PPK-MAC	Profile Protection Key for message MAC generation/verification		
PPP	Protected Profile Package		
PPR	Profile Policy Rule		
R-APDU	Response APDU		
RAT	Rules Authorisation Table		
RSA	Rivest / Shamir / Adleman asymmetric algorithm		
RSP	Remote SIM Provisioning		
SAS	Security Accreditation Scheme		
SCP	Secure Channel Protocol		
SD	Security Domain		
S-ENC	Session key for message encryption/decryption		
S-MAC	Session Key for message MAC generation/verification		
SK.CI.ECDSA	Private key of the CI for signing certificates		
SK.DPauth.ECDSA	Private Key of the of SM-DP+ for creating signatures for SM-DP+ authentication		
SK.EUICC.ECDSA	Private key of the eUICC for creating signatures		
SK.EUM.ECDSA	Private key of the EUM for creating signatures		
SM-DP+	Subscription Manager Data Preparation (Enhanced compared to the SM-DP in SGP.02 [1])		
SP	Service Provider		
SSD	Supplemental Security Domain		
SVN	SGP.22 Specification Version Number (referred to as 'eSVN' in SGP.21 [3]).		
TAC	Type Allocation Code		
TAR	Toolkit Application Reference		
TLS	Transport Layer Security		
UPP	Unprotected Profile Package		
URI	Uniform Resource Identifier		

V1.4 Page 14 of 777

Abbreviation	Description
URL	Uniform Resource locator
USIM	Universal Subscriber Identity Module

1.5 Document Cross-references

Ref	Document Number	Title	
[1]	SGP.02	GSMA "Remote Provisioning of Embedded UICC Technical specification" V3.1	
[2]	SGP.22	RSP Technical Specification V2.2.x (x≥1)	
[2a]	SGP.22	RSP Technical Specification V2.1	
[2b]	SGP.22	RSP Technical Specification V2.2	
[3]	SGP.21	RSP Architecture V2.2	
[3a]	SGP.21	RSP Architecture V2.1	
[4]	SIMalliance	SIMalliance eUICC Profile Package: Interoperable Format Technical Specification V2.0 or later	
[5]	ETSI TS 102 221	Smart Cards; UICC-Terminal interface	
[6]	GPC_SPE_034	GlobalPlatform Card Specification v.2.3	
[7]	ISO/IEC 7816-4:2013	Identification cards – Integrated circuit cards - Part 4: Organization, security and commands for interchange	
[8]	RFC 5639	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation	
[9]	ANSSI ECC FRP256V1	Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français. JORF n°0241 du 16 octobre 2011 page 17533. texte n° 30. 2011	
[10]	ITU E.118	The international telecommunication charge card	
[11]	NIST SP 800-56A	NIST Special Publication SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revision 2), May 2013	
[12]	3GPP TS 23.003	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification	
[13]	ETSI TS 102 225	Secured packet structure for UICC based applications; Release 12	
[14]	ETSI TS 102 226	Remote APDU structure for UICC based applications; Release 9	
[15]	TS.26	GSMA NFC Handset Requirements V9.0	
[16]	ITU-T X.690 (11/2008)	ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) including Corrigendum 1 and 2	
[17]	ETSI TS 102 241	Smart cards; UICC Application Programming Interface (UICC API) for Java Card™	

V1.4 Page 15 of 777

Ref	Document Number	Title		
[18]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application		
[19]	GPC_SPE_095	GlobalPlatform Card - Digital Letter of Approval - Version 1.0		
[20]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels 2119 S. Bradner		
		http://www.ietf.org/rfc/rfc2119.txt		
[21]	SGP.11	Remote Provisioning Architecture for Embedded UICC Test Specification V3.2		
[22]	3GPP TS 23.040	Technical realization of the Short Message Service (SMS)		
[23]	SIMalliance Test	SIMAlliance eUICC Profile Package: Interoperable Format Test Specification Version 2.1.2		
[24]	RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)		
[25]	SGP.26	RSP Test Certificates Definition v1.2		

1.6 Conventions

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document SHALL be interpreted as described in RFC 2119 [20].

2 Testing Rules

2.1 Applicability

2.1.1 Format of the Optional Features Table

The columns in Table 4 have the following meaning:

Column	Meaning
Option	The optional feature supported or not by the implementation.
Mnemonic	The mnemonic column contains mnemonic identifiers for each item.

Table 1: Format of the Optional Features Table

2.1.2 Format of the Applicability Table

The applicability of every test in Table 5 is formally expressed by the use of a Boolean expression defined in the following clause.

The columns in Table 5have the following meaning:

Column	Meaning
	The "Test case" column gives a reference to the test case number detailed in the present document and is required to validate the implementation of the corresponding item in the "Name" column.

V1.4 Page 16 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

Name	In the "Name" column, a short non-exhaustive description of the test is found.
Roles	SM-DP+, SM-DS, Device, LPAd, LPAe or eUICC Entities under test that take in charge the functions used in the test case.
Version	This column indicates which test cases are applicable for the given SGP.22 version. See clause 2.1.3 'Applicability and Notations'.
Test Env.	Test environment used for executing the test case.

Table 2: Format of the Applicability Table

2.1.3 Applicability and Notations

The following notations are used for the Applicability column:

Applicability code	Meaning			
М	mandatory - the capability is required to be supported.			
N/A	not applicable - in the given context, it is impossible to use the capability.			
Ci	conditional - the requirement on the capability depends on the support of other items. "i" is an integer identifying an unique conditional status expression which is defined immediately following the table. For nested conditional expressions, the syntax "IF THEN (IF THEN ELSE) ELSE" is to be used to avoid ambiguities.			

Table 3: Applicability and Notations

2.1.4 Optional Features Table

The supplier of the implementation SHALL state the support of possible options in Table 5.

eUICC Options	Mnemonic	
The eUICC supports NIST P-256 [11] for signing and for verification (see Note 2)	O_E_NIST	
The eUICC supports brainpoolP256r1 [8] for signing and for verification (see Note 2) O_E_BRP		
The eUICC supports FRP256V1 [9] for signing and for verification (see Note 2)	O_E_FRP	
The eUICC supports Test Profiles	O_E_TEST_PROF	
The eUICC supports CRL	O_E_CRL	
The eUICC supports the LPAe	O_E_LPAe	
The eUICC stores the otPK.eUICC.ECKA / otSK.eUICC.ECKA from previous unsuccessful download attempt for future retry	O_E_REUSE_OTPK	
The eUICC can hold two PIR	O_E_2_PIR	
Device Options	Mnemonic	
The Device supports LPAd	O_D_LPAD	
The Device supports GSM/GERAN	O_D_GSM_GERAN	

V1.4 Page 17 of 777

The Device supports UMTS/UTRAN	O_D_UMTS_UTRAN		
The Device supports cdma2000 1X	O_D_CDMA2000_1X		
The Device supports cdma2000 HRPD	O_D_CDMA2000_HRPD		
The Device supports cdma2000 eHRPD	O_D_CDMA2000_EHRPD		
The Device supports LTE/E-UTRAN	O_D_LTE		
The Device supports NFC as defined in TS26	O_D_NFC_TS26		
The Device supports eUICC CRL	O_D_CRL		
Initiation of the Enable Profile procedure is allowed on a Profile that is enabled already	O_D_ENPROF		
Initiation of the Enable Profile procedure is allowed even if the currently enabled Profile has PPR1	O_D_ENPREVPPR1		
Device supports only cellular connectivity (see Note 1)	O_D_ONLY_CELLULAR_CO NNECTIVITY		
Device offers a user interface to enter a PIN for user authentication	O_D_PIN		
Device allows the End User to initiate the disabling or deletion of an enabled Profile with ppr1	O_D_DISDELPPR1		
Device allows the End User to initiate the deletion of a Profile with ppr2	O_D_DELPPR2		
Initiation of the Disable Profile procedure is allowed on a Profile that is disabled already	O_D_DISPROF		
Initiation of Disable Profile procedure is allowed even if the currently enabled Profile has PPR1	O_D_DISPPR1		
Device retries after unsuccessful CC entry attempt	O_D_CC_RETRY		
The Device provides the LUI functionality to postpone Profile Download	O_D_EU_POSTPONED		
Device supports Power-on Profile discovery	O_D_POW_ON_PROF_DISC OVERY		
Initiation of the Enable Profile procedure is allowed only if no Profile is enabled already	O_D_ENPROF1ST		
The Device provides the LUI functionality to reject Profile Download	O_D_EU_REJECT		
The Device supports Set/Edit Nickname procedure and displaying the profile's Nickname	O_D_NICKNAME		
The Device supports additional verification of TLS certificate content	O_D_TLS_FULL_VERIFICATI		
e. key usage, extended key usage and certificate policy) ON			
SM-DP+ Options	Mnemonic		
SM-DP+ reuses otPK.eUICC.ECKA from previous unsuccessful	O_P_REUSE_OTPK		
download attempt			

V1.4 Page 18 of 777

SM-DS Options	Mnemonic
SM-DS is an Alternative SM-DS. NOTE: If an SM-DS is not an Alternative SM-DS then it is a Root SM-DS.	O_S_ALT

Note 1: Devices which supports O_D_ONLY_CELLULAR_CONNECTIVITY are out of scope of the current version of this document.

Note 2: For this version of test specification:

- O_E_FRP is not applicable
- The eUICC SHALL support either O_E_NIST or O_E_BRP or both

Table 4: Options

2.1.5 Applicability Table

Table 5 specifies the applicability of each test case. See clause 2.1.2 for the format of this table.

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.	
	eUICC Interfaces Compliance Testing					
4.2.1.2.1	TC_eUICC_ATR_And_ISDR_Selection	eUICC	C006	C006	TE_eUICC	
4.2.2.2.1	TC_eUICC_ES6.UpdateMetadata	eUICC	М	М	TE_eUICC	
4.2.3.2.1	TC_eUICC_ES8+.InitialiseSecureChannel	eUICC	М	М	TE_eUICC	
4.2.4.2.1	TC_eUICC_ES8+.ConfigureISDP	eUICC	М	М	TE_eUICC	
4.2.5.2.1	TC_eUICC_ES8+.StoreMetadata	eUICC	М	М	TE_eUICC	
4.2.6.2.1	TC_eUICC_ES8+.ReplaceSessionKeys	eUICC	М	М	TE_eUICC	
4.2.7.2.1	TC_eUICC_ES8+.LoadProfileElements	eUICC	М	М	TE_eUICC	
4.2.8.2.1	TC_eUICC_ES10a.GetEuiccConfiguredAddresses	eUICC	М	М	TE_eUICC	
4.2.9.2.1	TC_eUICC_ES10a.SetDefaultDpAddress	eUICC	М	М	TE_eUICC	
4.2.10.2.1	TC_eUICC_ES10b.PrepareDownloadNIST	eUICC	C001	C001	TE_eUICC	
4.2.10.2.2	TC_eUICC_ES10b.PrepareDownloadBRP	eUICC	C002	C002	TE_eUICC	
4.2.10.2.3	TC_eUICC_ES10b.PrepareDownloadFRP	eUICC	C003	C003	TE_eUICC	
4.2.10.2.4	TC_eUICC_ES10b.PrepareDownloadErrorCases	eUICC	М	М	TE_eUICC	
4.2.11.2.1	TC_eUICC_ES10b.LoadBoundProfilePackageNIST	eUICC	C001	C001	TE_eUICC	
4.2.11.2.2	TC_eUICC_ES10b.LoadBoundProfilePackageBRP	eUICC	C002	C002	TE_eUICC	
4.2.11.2.3	TC_eUICC_ES10b.LoadBoundProfilePackageFRP	eUICC	C003	C003	TE_eUICC	
4.2.11.2.4	TC_eUICC_ES10b.LoadBoundProfilePackage_ErrorC ases	eUICC	М	М	TE_eUICC	
4.2.12.2.1	TC_eUICC_ES10b.GetEUICCChallenge	eUICC	М	М	TE_eUICC	
4.2.13.2.1	TC_eUICC_ES10b.GetEUICCInfo1	eUICC	М	М	TE_eUICC	

V1.4 Page 19 of 777

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.
4.2.13.2.2	TC_eUICC_ES10b.GetEUICCInfo2_RSP_V2.1	eUICC	М	N/A	TE_eUICC
4.2.13.2.3	TC_eUICC_ES10b.GetEUICCInfo2_RSP_V2.2.x	eUICC	N/A	М	TE_eUICC
4.2.13.2.4	TC_eUICC_ES10b.GetEUICCInfo2	eUICC	М	М	TE_eUICC
4.2.14.2.1	TC_eUICC_ES10b.ListNotification All test sequences except the sequence #5	eUICC	М	М	TE_eUICC
4.2.14.2.1	TC_eUICC_ES10b.ListNotification Only the test sequence #5	eUICC	C025	C025	TE_eUICC
4.2.15.2.1	TC_eUICC_ES10b.RetrieveNotificationsList All test sequences except the sequences #5 and #15	eUICC	М	М	TE_eUICC
4.2.15.2.1	TC_eUICC_ES10b.RetrieveNotificationsList Only the test sequences #5 and #15	eUICC	C025	C025	TE_eUICC
4.2.16.2.1	TC_eUICC_ES10b.RemoveNotificationFromList All test sequences except the sequence #5	eUICC	М	М	TE_eUICC
4.2.16.2.1	TC_eUICC_ES10b.RemoveNotificationFromList Only the test sequence #5		C025	C025	TE_eUICC
4.2.18.2.1	TC_eUICC_ES10b.AuthenticateServer_SM-DP+_NIST	eUICC	C001	C001	TE_eUICC
4.2.18.2.2	TC_eUICC_ES10b.AuthenticateServer_SM-DP+_BRP	eUICC	C002	C002	TE_eUICC
4.2.18.2.3	TC_eUICC_ES10b.AuthenticateServer_SM-DP+_FRP	eUICC	C003	C003	TE_eUICC
4.2.18.2.4	TC_eUICC_ES10b.AuthenticateServer_SM- DP+_ErrorCases	eUICC	М	М	TE_eUICC
4.2.18.2.5	TC_eUICC_ES10b.AuthenticateServer_SM-DS_BRP	eUICC	C002	C002	TE_eUICC
4.2.18.2.6	TC_eUICC_ES10b.AuthenticateServer_SM-DS_NIST	eUICC	C001	C001	TE_eUICC
4.2.18.2.7	TC_eUICC_ES10b.AuthenticateServer_SM-DS_FRP	eUICC	C003	C003	TE_eUICC
4.2.18.2.8	TC_eUICC_ES10b.AuthenticateServer_SM-DS_ErrorCases	eUICC	М	М	TE_eUICC
4.2.19.2.1	TC_eUICC_ES10b.CancelSessionNIST	eUICC	C001	C001	TE_eUICC
4.2.19.2.2	TC_eUICC_ES10b.CancelSessionBRP	eUICC	C002	C002	TE_eUICC
4.2.19.2.3	TC_eUICC_ES10b.CancelSessionFRP	eUICC	C003	C003	TE_eUICC
4.2.19.2.4	TC_eUICC_ES10b.CancelSession_ErrorCase	eUICC	М	М	TE_eUICC
4.2.20.2.1	TC_eUICC_ES10c.GetProfilesInfo		М	М	TE_eUICC
4.2.21.2.1	TC_eUICC_ES10c.EnableProfile_Case3		М	М	TE_eUICC
4.2.21.2.2	TC_eUICC_ES10c.EnableProfile_ErrorCases_Case3	eUICC	М	М	TE_eUICC
4.2.21.2.3	TC_eUICC_ES10c.EnableProfile_Case4	eUICC	М	М	TE_eUICC
4.2.21.2.4	TC_eUICC_ES10c.EnableProfile_ErrorCases_Case4	eUICC	М	М	TE_eUICC
4.2.22.2.1	TC_eUICC_ES10c.DisableProfile_Case3	eUICC	М	М	TE_eUICC

V1.4 Page 20 of 777

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.
4.2.22.2.2	TC_eUICC_ES10c.DisableProfile_ErrorCases_Case3	eUICC	М	М	TE_eUICC
4.2.22.2.3	TC_eUICC_ES10c.DisableProfile_Case4	eUICC	М	М	TE_eUICC
4.2.22.2.4	TC_eUICC_ES10c.DisableProfile_ErrorCases_Case4	eUICC	М	М	TE_eUICC
4.2.23.2.1	TC_eUICC_ES10c.DeleteProfile_Case3	eUICC	М	М	TE_eUICC
4.2.23.2.2	TC_eUICC_ES10c.DeleteProfile_ErrorCases_Case3	eUICC	М	М	TE_eUICC
4.2.23.2.3	TC_eUICC_ES10c.DeleteProfile_Case4	eUICC	М	М	TE_eUICC
4.2.23.2.4	TC_eUICC_ES10c.DeleteProfile_ErrorCases_Case4	eUICC	М	М	TE_eUICC
4.2.24.2.1	TC_eUICC_ES10c.eUICCMemoryReset	eUICC	М	М	TE_eUICC
4.2.24.2.2	TC_eUICC_ES10c.eUICCMemoryReset_ErrorCases	eUICC	М	М	TE_eUICC
4.2.25.2.1	TC_eUICC_ES10c.GetEID	eUICC	М	М	TE_eUICC
4.2.26.2.1	TC_eUICC_ES10c.SetNickname	eUICC	М	М	TE_eUICC
4.2.27.2.1	TC_eUICC_ES10b.GetRAT	eUICC	М	М	TE_eUICC
	SM-DP+ Interfaces Compliance	Testing			
4.3.12.2.1	TC_SM-DP+_ES9+.InitiateAuthenticationNIST	SM-DP+	М	М	TE_P2
4.3.12.2.2	TC_SM-DP+_ES9+.InitiateAuthenticationFRP	SM-DP+	М	М	TE_P2
4.3.12.2.3	TC_SM-DP+_ES9+.InitiateAuthenticationBRP	SM-DP+	М	М	TE_P2
4.3.13.2.1	TC_SM-DP+_ES9+.GetBoundProfilePackageNIST Test sequences #1, #2 and #5	SM-DP+	C028	C028	TE_P2
4.3.13.2.1	TC_SM-DP+_ES9+.GetBoundProfilePackageNIST Test sequences #3, #4 and #6	SM-DP+	М	М	TE_P2
4.3.13.2.2	TC_SM-DP+_ES9+.GetBoundProfilePackageFRP	SM-DP+	М	М	TE_P2
4.3.13.2.3	TC_SM-DP+_ES9+.GetBoundProfilePackageBRP Test sequence #1	SM-DP+	C028	C028	TE_P2
4.3.13.2.3	TC_SM-DP+_ES9+.GetBoundProfilePackageBRP Test sequence #2	SM-DP+	М	М	TE_P2
4.3.13.2.4	TC_SM- DP+_ES9+.GetBoundProfilePackage_RetryCases_Re useOTPK_NIST Test sequences #1, #2, #5 and #6	SM-DP+	C029	C029	TE_P2
4.3.13.2.4	TC_SM- DP+_ES9+.GetBoundProfilePackage_RetryCases_Re useOTPK_NIST Test sequences #3, #4, #7, #8 and #9	SM-DP+	C015	C015	TE_P2
4.3.13.2.7	Test sequences #3, #4, #7, #8 and #9 TC_SM- DP+_ES9+.GetBoundProfilePackage_RetryCases_Diff erentOTPK_NIST Test sequences #1 and #2	SM-DP+	C030	C030	TE_P2

V1.4 Page 21 of 777

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.
4.3.13.2.7	TC_SM-DP+_ES9+.GetBoundProfilePackage_RetryCases_DifferentOTPK_NIST	SM-DP+	C016	C016	TE_P2
	Test sequences #3 and #4				
4.3.13.2.10	TC_SM-DP+_ES9+.GetBoundProfilePackage_ErrorCasesNIST	SM-DP+	М	М	TE_P2
4.3.14.2.1	TC_SM-DP+_ES9+.AuthenticateClientNIST	SM-DP+	М	М	TE_P2
4.3.14.2.2	TC_SM-DP+_ES9+.AuthenticateClientNIST_ErrorCases	SM-DP+	М	М	TE_P2
4.3.14.2.3	TC_SM-DP+_ES9+.AuthenticateClientFRP	SM-DP+	М	М	TE_P2
4.3.14.2.5	TC_SM-DP+_ES9+.AuthenticateClientBRP	SM-DP+	М	М	TE_P2
4.3.14.2.6	TC_SM-DP+_ES9+.AuthenticateClient_RetryCases_Reuse_OTPK	SM-DP+	C015	C015	TE_P2
4.3.15.2.1	TC_SM-DP+_ES9+_HandleNotificationNIST		М	М	TE_P2
4.3.15.2.2	TC_SM_DP+_ES9+_HandleNotificationFRP	SM-DP+	М	М	TE_P2
4.3.15.2.3	TC_SM-DP+_ES9+_HandleNotificationBRP	SM-DP+	М	М	TE_P2
4.3.16.2.1	TC_SM- DP+_ES9+.CancelSession_After_AuthenticateClientNI ST		М	М	TE_P2
4.3.16.2.2	TC_SM- DP+_ES9+.CancelSession_After_GetBoundProfilePac kageNIST	SM-DP+	М	М	TE_P2
4.3.16.2.3	TC_SM_DP+_ES9+.CancelSession_After_Authenticat eClientFRP	SM-DP+	М	М	TE_P2
4.3.16.2.4	4.3.16.2.4 TC_SM_DP+_ES9+.CancelSession_After_GetBoundProfilePackageFRP	SM-DP+	М	М	TE_P2
4.3.16.2.5	TC_SM-DP+_ES9+.CancelSession_After_AuthenticateClientBRP	SM-DP+	М	М	TE_P2
4.3.16.2.6	TC_SM- DP+_ES9+.CancelSession_After_GetBoundProfilePac kageBRP	SM-DP+	М	М	TE_P2
4.3.17.1	TC_SM-DP+_ES9+_Server_Authentication_for_HTTPS_EstablishmentNIST	SM-DP+	М	М	TE_P2
4.3.17.2	TC_SM-DP+_ES9+_Server_Authentication_for_HTTPS_EstablishmentBRP	SM-DP+	М	M	TE_P2
4.3.20.1	TC_SM- DP+_ES12_Client_Mutual_Authentication_for_HTTPS _EstablishmentNIST	SM-DP+	М	M	TE_P1

V1.4 Page 22 of 777

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.				
4.3.20.2	TC_SM- DP+_ES12_Client_Mutual_Authentication_for_HTTPS _EstablishmentBRP	SM-DP+	М	М	TE_P1				
	LPAd Interfaces Compliance Testing								
4.4.21.2.1	TC_LPAd_InitiateAuthentication_Nominal	LPAd	C007	C007					
4.4.21.2.2	TC_LPAd_InitiateAuthentication_ErrorCases	LPAd	C007	C007					
4.4.22.2.1	TC_LPAd_ES9+_GetBoundProfilePackage_Nominal		C007	C007					
4.4.22.2.2	TC_LPAd_ES9+_GetBoundProfilePackage_Retry	LPAd	C005	C005					
4.4.22.2.3	TC_LPAd_ES9+_GetBoundProfilePackage_Error	LPAd	C007	C007					
4.4.23.2.1	TC_LPAd_AuthenticatClient_Nominal	LPAd	C007	C007					
4.4.23.2.2	TC_LPAd_AuthenticateClient_ErrorCases	LPAd	C007	C007					
4.4.24.2.1	TC_LPAd_ES9+_HandleNotification_Nominal	LPAd	C007	C007					
4.4.25.2.1	TC_LPAd_ES9+_CancelSession_Nominal All test sequences except the sequence #02	LPAd	C007	C007					
4.4.25.2.1	TC_LPAd_ES9+_CancelSession_Nominal Only the test sequences #02		C023	C023					
4.4.25.2.2	TC_LPAd_ES9+_CancelSession_EndUserPostponed_ Nominal		C008	C008					
4.4.25.2.3	TC_LPAd_ES9+_CancelSession_Error	LPAd	C026	C026					
4.4.25.2.4	TC_LPAd_ES9+_CancelSession_PPRs	LPAd	C0026	C026					
4.4.26.2.1	TC_LPAd_HTTPS_Nominal	LPAd	C007	C007					
4.4.26.2.2	TC_LPAd_HTTPS_ErrorCases All test sequences except the sequence #04, #05, #06	LPAd	C007	C007					
4.4.26.2.2	TC_LPAd_HTTPS_ErrorCases Only the test sequences #04, #05, #06	LPAd	C031	C031					
4.4.27.2.1	TC_LPAd_ES11_InitiateAuthentication_Nominal	LPAd	C007	C007					
4.4.27.2.2	TC_LPAd_ES11_InitiateAuthentication_ErrorCases	LPAd	C007	C007					
4.4.28.2.1	TC_LPAd_ES11_AuthenticateClient_Nominal	LPAd	C007	C007					
4.4.28.2.2	TC_LPAd_ES11_AuthenticateClient_ErrorCases	LPAd	C007	C007					
4.4.29.2.1	TC_LPAd_HTTPS_Nominal		C007	C007					
4.4.29.2.2	TC_LPAd_HTTPS_Error All test sequences except the sequence #04, #05, #06	LPAd	C007	C007					
4.4.29.2.2	TC_LPAd_HTTPS_Error Only the test sequences #04, #05, #06	LPAd	C031	C031					
	SM-DS Interfaces Compliance	Testing			1				
4.5.1.2.1	TC_ROOT_SM_DS_ES12.RegisterEvent	SM-DS	C024	C024	TE_S3				

V1.4 Page 23 of 777

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.
4.5.1.2.2	TC_ALT_SM_DS_ES12.RegisterEvent	SM-DS	C021	C021	TE_SA1
4.5.2.2.1	TC_ROOT_SM_DS_ES12.DeleteEvent	SM-DS	C024	C024	TE_S3
4.5.2.2.2	TC_ALT_SM_DS_ES12.DeleteEvent	SM-DS	C021	C021	TE_SA1
4.5.2.2.3	TC_ALT_SM_DS_ES12.DeleteEvent_Error_Nonexista nt_EventID	SM-DS	C021	C021	TE_S2
4.5.3.2.1	TC_ROOT_SM_DS_ES15.RegisterEvent	SM-DS	C024	C024	TE_SR2
4.5.4.2.1	TC_ROOT_SM_DS_ES15.DeleteEvent	SM-DS	C024	C024	TE_SR2
4.5.5.2.1	TC_SM_DS_ES11.InitiateAuthenticationNIST	SM-DS	М	М	TE_S1
4.5.6.2.1	TC_SM_DS_ES11.AuthenticateClientNIST	SM-DS	М	М	TE_S1
4.5.6.2.2	TC_SM_DS_ES11.AuthenticateClientBRP	SM-DS	М	М	TE_S1
4.5.7.1	TC_ALT_SM_DS_ES15_Client_Mutual_Authentication _for_HTTPS_EstablishmentNIST	SM-DS	C021	C021	TE_SA1
4.5.7.2	TC_ALT_SM_DS_ES15_Client_Mutual_Authentication _for_HTTPS_EstablishmentBRP		C021	C021	TE_SA1
4.5.8.1	TC_SM_DS_ES12_Server_Mutual_Authentication_for _HTTPS_EstablishmentNIST	SM-DS	М	М	TE_S2
4.5.8.2	TC_SM_DS_ES12_Server_Mutual_Authentication_for _HTTPS_EstablishmentBRP	SM-DS	М	М	TE_S2
4.5.9.1	TC_ROOT_SM_DS_ES15_Server_Mutual_Authenticat ion_for_HTTPS_EstablishmentNIST	SM-DS	C024	C024	TE_SR1
4.5.9.2	TC_ROOT_SM_DS_ES15_Server_Mutual_Authenticat ion_for_HTTPS_EstablishmentBRP	SM-DS	C024	C024	TE_SR1
4.5.10.1	TC_SM_DS_ES11_Server_Mutual_Authentication_for _HTTPS_EstablishmentNIST	SM-DS	М	М	TE_S1
4.5.10.2	TC_SM_DS_ES11_Server_Mutual_Authentication_for _HTTPS_EstablishmentBRP	SM-DS	М	М	TE_S1
	Procedure - Behaviour Tes	ting			
5.2.1.2.1	TC_eUICC_PrepareDownload_Retry_ReuseOTKeys	eUICC	C019	C019	TE_eUICC
5.2.1.2.2	TC_eUICC_PrepareDownload_Retry_NewOTKeys	eUICC	C020	C020	TE_eUICC
5.2.2.2.1	TC_eUICC_ForbiddenPPRs	eUICC	М	М	TE_eUICC
5.2.3.2.1	TC_eUICC_GetProfilesInfo_GetRAT_RSPSession	eUICC	М	М	TE_eUICC
5.2.4.2.1	TC_eUICC_Default_FileSystem	eUICC	М	М	TE_eUICC
5.2.5.2.1	TC_eUICC_DeleteProfile_ISDP_And_Components	eUICC	М	М	TE_eUICC
5.2.6.2.1	TC_eUICC_EnableProfile_Twice_Notifications	eUICC	М	М	TE_eUICC
5.2.7.2.1	TC_eUICC_DisableProfile_ApplicationManagement	eUICC	М	М	TE_eUICC
5.2.8.2.1	TC_eUICC_Enable_Disable_Delete_Notifications	eUICC	М	М	TE_eUICC
5.3.3.2.1	TC_SM-DP+_ProfileMetadata	SM-DP+	М	М	

V1.4 Page 24 of 777

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.
5.4.1.2.1	TC_LPAd_AddProfile_Manual_Entry	LPAd	C007	C007	
5.4.1.2.2	TC_LPAd_AddProfile_QRcode_scanning	LPAd	C007	C007	
5.4.1.2.3	TC_LPAd_AddProfile_ActivationCode_InvalidFormat_ QRcode	LPAd	C007	C007	
5.4.1.2.4	TC_LPAd_AddProfile_ActivationCode_InvalidFormat_ ManualEntry	LPAd	C007	C007	
5.4.1.2.5	TC_LPAd_AddProfile_ConfirmationCode_smdpSigned 2_QR	LPAd	C007	C007	
5.4.1.2.6	TC_LPAd_AddProfile_ConfirmationCode_smdpSigned 2_Manual_Entry	LPAd	C007	C007	
5.4.1.2.7	TC_LPAd_AddProfile_default_SM-DP+_address	LPAd	C007	C007	
5.4.1.2.8	TC_LPAd_AddProfile_QRCode_with_ConfirmationCod e	LPAd	C007	C007	
5.4.1.2.9	TC_LPAd_AddProfile_PPRs	LPAd	C007	C007	
5.4.1.2.10	TC_LPAd_LUI_access_protected	LPAd	C007	C007	
5.4.1.2.11	TC_LPAd_AddProfile_Security_Errors	LPAd	C007	C007	
5.4.2.2.1	TC_LPAd_ListProfiles	LPAd	C007	C007	
5.4.3.2.1	TC_LPAd_SetNickname	LPAd	C027	C027	
5.4.3.2.2	TC_LPAd_EditNickname	LPAd	C027	C027	
5.4.4.2.1	TC_LPAd_DeleteProfile_Disabled_without_PPR	LPAd	C007	C007	
5.4.4.2.2	TC_LPAd_DeleteProfile_Enabled_without_PPR	LPAd	C009	C009	
5.4.4.2.3	TC_LPAd_DeleteProfile_Error_with_PPR1	LPAd	C012	C012	
5.4.4.2.4	TC_LPAd_DeleteProfile_Error_Disabled_with_PPR2	LPAd	C013	C013	
5.4.4.2.5	TC_LPAd_DeleteProfile_Error_Enabled_with_PPR2	LPAd	C014	C014	
5.4.4.2.6	TC_LPAd_DeleteProfile_Security_Errors	LPAd	C007	C007	
5.4.5.2.1	TC_LPAd_EnableProfile	LPAd	C009	C009	
5.4.5.2.2	TC_LPAd_EnableProfile_ImplicitDisable	LPAd	C009	C009	
5.4.5.2.3	TC_LPAd_EnableProfile_Error_ProfileAlreadyEnabled	LPAd	C010	C010	
5.4.5.2.4	TC_LPAd_EnableProfile_Error_PPR1Set	LPAd	C011	C011	
5.4.5.2.5	TC_LPAd_EnableProfile_Security_Errors	LPAd	C007	C007	
5.4.6.2.1	TC_LPAd_DisableProfile	LPAd	C009	C009	
5.4.6.2.2	TC_LPAd_DisableProfile_Error_ProfileAlreadyDisable d	LPAd	C017	C017	
5.4.6.2.3	TC_LPAd_DisableProfile_Error_PPR1Set	LPAd	C018	C018	
5.4.6.2.4	TC_LPAd_DisableProfile_Security_Errors	LPAd	C007	C007	
5.4.7.2.1	TC_LPAd_RetrieveEID	LPAd	C004	C004	

V1.4 Page 25 of 777

Test case	Name	Roles	V2.1	V2.2.X (X≥0)	Test Env.	
5.4.8.2.1	TC_LPAd_eUICCMemoryReset		C007	C007		
5.4.8.2.2	TC_LPAd_eUICCMemoryResetWithPINVerification LPAd		C009	C009		
5.4.10.2.1	0.2.1 TC_LPAd_Set/Edit Default SM-DP+ Address LPAd C007 C		C007			
5.4.11.2.1	11.2.1 TC_LPAd_DevicePowerOnProfileDiscovery_SM-DP+_address		C022	C022		
5.4.11.2.2	TC_LPAd_DevicePowerOnProfileDiscovery_SM-DS		C022	C022		
	Test Specifications					
7.1	SIMAlliance eUICC Profile Package Test Specification	eUICC	М	М	See section 7.1	

Table 5: Applicability of Tests

Conditional item	Condition
C001	IF (O_E_NIST) THEN M ELSE N/A
C002	IF (O_E_BRP) THEN M ELSE N/A
C003	IF (O_E_FRP) THEN M ELSE N/A
C004	IF (O_D_LPAD) THEN M ELSE N/A
C005	IF (O_D_CC_RETRY AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C006	IF (NOT O_E_LPAe) THEN M ELSE N/A
C007	IF (O_D_LPAD AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C008	IF (O_D_LPAD AND O_D_EU_POSTPONED AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C009	IF (O_D_LPAD AND O_D_PIN AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C010	IF (O_D_LPAD AND O_D_ENPROF AND NOT O_D_ENPROF1ST) THEN M ELSE N/A
C011	IF (O_D_LPAD AND O_D_ENPREVPPR1 AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEM M ELSE N/A
C012	IF (O_D_LPAD AND O_D_DISDELPPR1 AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C013	IF (O_D_LPAD AND O_D_DELPPR2 AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C014	IF (O_D_LPAD AND O_D_PIN AND O_D_DELPPR2 AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C015	IF (O_P_REUSE_OTPK) THEN M ELSE N/A
C016	IF (NOT O_P_REUSE_OTPK) THEN M ELSE N/A

V1.4 Page 26 of 777

Conditional item	Condition
C017	IF (O_D_LPAD AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY AND O_D_DISPROF) THEN M ELSE N/A
C018	IF (O_D_LPAD AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY AND O_D_DISPPR1) THEN M ELSE N/A
C019	IF (O_E_REUSE_OTPK) THEN M ELSE N/A
C020	IF (NOT O_E_REUSE_OTPK) THEN M ELSE N/A
C021	IF (O_S_ALT) THEN M ELSE N/A
C022	IF (O_D_LPAD AND O_D_POW_ON_PROF_DISCOVERY AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C023	IF (O_D_LPAD AND O_D_EU_REJECT AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) THEN M ELSE N/A
C024	IF (NOT O_S_ALT) THEN M ELSE N/A
C025	IF (O_E_2_PIR) THEN M ELSE N/A
C026	IF ((O_D_LPAD AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY) AND (O_D_EU_POSTPONED OR O_D_EU_REJECT)) THEN M ELSE N/A
C027	IF (O_D_LPAD AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY AND O_D_NICKNAME) THEN M ELSE N/A
C028	IF (O_P_SESSION_KEYS) THEN M ELSE N/A
C029	IF (O_P_SESSION_KEYS AND O_P_REUSE_OTPK) THEN M ELSE N/A
C030	IF (O_P_SESSION_KEYS AND NOT O_P_REUSE_OTPK) THEN M ELSE N/A
C031	IF (O_D_LPAD AND NOT O_D_ONLY_CELLULAR_CONNECTIVITY AND O_D_TLS_FULL_VERIFICATION) THEN M ELSE N/A

Table 6: Conditional Items Referenced by Table 5

2.2 General Consideration

This section contains some general considerations about the test cases defined in this document. Note that some external test specifications are referred to in chapter 7. Consequently, the following sub sections SHALL only apply for test cases defined in sections 4 and 5 and 6.

2.2.1 Test Case Definition

Test descriptions are independent.

For each test described in this document, a chapter provides a general description of the initial conditions applicable for the whole test. This description is completed by specific configurations to each individual sub-case.

It is implicitly assumed that all entities under test SHALL be compliant with the initial states described in Annex G. An initial state SHALL be considered as a pre-requisite to execute all the test cases described in this Test Plan.

After completing the test, the configuration is reset before the execution of the following test.

V1.4 Page 27 of 777

2.2.2 Test Cases Format

Here is an explanation of the way to define the test cases in chapters 4, 5 and 6.

4.X.Y.Z Test Cases

4.X.Y.Z.1 TC_IUT_TestName1

General Initial Conditions	
Entity	Description of the general initial condition
Entity1	Test case - general condition 1
Entity2	Test case - general condition 2

Test Sequence #01: Short Description

Description of the aim of the test sequence N°1

Initial Conditions	
Entity	Description of the initial condition
Entity1	Test sequence N°1 - initial condition 1
Entity2	Test sequence N°1 - initial condition 2

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Entity1 → Entity2	Command or Message to send from Entity1 to Entity2	Expected result N°1.1	
1	Entity1 → Entity2	Command or Message to send from Entity1 to Entity2	1- expected result N°1.2 2- expected result N°1.3	REQ1
2	Entity2 → Entity3	Command or Message to send from Entity2 to Entity3		

Test Sequence #02

Description of the aim of the test sequence N°2

	Step	Direction	Sequence / Description	Expected result	REQ
1		Entity1 → Entity2	Command or Message to send from Entity1 to Entity2		
	2	Entity2 → Entity3	Command or Message to send from Entity2 to Entity3	1- expected result N°2.1 2- expected result N°2.2	REQ2

4.X.Y.Z.2 TC_IUT_TestName2

. . .

The test cases TC_IUT_TestName1 and TC_IUT_TestName2 are referenced in Table 5 that allows indicating the applicability of the tests.

V1.4 Page 28 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

In the test case TC_IUT_TestName1, the requirements REQ1 and REQ2 are respectively covered by the test sequences #01 and #02.

The test sequence #01 SHALL be executed if and only if these conditions are met:

- Test case general condition 1
- Test case general condition 2
- Test sequence N°1 initial condition 1
- Test sequence N°1 initial condition 2

The test sequence #02 SHALL be executed if and only if these conditions are met:

- Test case general condition 1
- Test case general condition 2

The tables defining the different initial conditions are optional.

Initial Conditions are intended to be reached dynamically using the Test Tool when possible.

No additional operation SHALL be done prior to the test sequence besides those indicated in the Initial Conditions (e.g. no other Profiles SHALL be present on the eUICC besides those defined in the Initial Conditions).

In the test sequence #01:

- the step IC1 corresponds to an additional Initial Condition
- in the step N°1, if the expected results N°1 and N°2 are validated, the requirement REQ1 (or a part of the REQ1) SHALL be considered as implemented

Note that all initial states (described in Annex G) SHALL be implemented by the entity under test whatever the test cases to execute.

In addition, following 2.2.1 sub sections present all information (e.g. Methods, Constants...) that MAY be referenced in test sequences.

After execution of each test sequence a clean-up procedure (CU) SHALL be executed to restore the IUT to the Common Initial State as defined in Annex G.

2.2.2.1 Methods and Procedures

A method is referenced as follow:

MTD NAME OF THE METHOD(PARAM1, PARAM2...)

The key word "NO_PARAM" SHALL be set in method call if the related optional parameter is not used.

All methods and their related parameters are described in Annex C.1.

A procedure is a generic sub-sequence and is referenced as follow:

PROC NAME OF THE PROCEDURE

All procedures are described in Annex C.2.

V1.4 Page 29 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

The implementation of these methods and procedures is under the responsibility of the test tool providers.

2.2.2.2 Constants and Dynamic Content

A constant (e.g. text, ASN.1 structure, hexadecimal string, icon, URI, integer, EID, AID...) is referenced as follow:

• #NAME OF THE CONSTANT

All constants are defined in Annex A.

When provided as an ASN.1 value notation, a constant SHALL be encoded in DER TLV (as specified in ITU-T X.690 [16]) by the test tool.

A dynamic content (e.g. TLV, ASN.1 structure, signature, integer, AID, one-time key pair...) is referenced as follow:

• <NAME OF THE VARIABLE>

All dynamic contents are defined in Annex B.

A dynamic content is either generated by an IUT or by a test tool provider.

2.2.2.3 Requests and Responses

An ASN.1 or a JSON request is referenced as follow:

• #NAME OF THE REQUEST

An ASN.1 or a JSON response is referenced as follows:

• #R NAME OF THE RESPONSE

Each ASN.1 or JSON request and response MAY refer to a constant or a dynamic content. All these structures are defined in Annex D.

When provided as an ASN.1 value notation, a request or a response SHALL be encoded in DER TLV (as specified in ITU-T X.690 [16]) by the test tool.

When an ASN.1 element definition contains three points (i.e. "..."), it means that fields MAY be present but SHALL not be checked by the test tool.

In the following example, several fields MAY be part of the ProfileInfoListResponse but only the profileNickname SHALL be verified.

V1.4 Page 30 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

This rule applies aslo for Constants definition.

2.2.2.4 APDUs

A C-APDU is referenced as follow:

[NAME_OF_THE_CAPDU]

All C-APDUs are defined in Annex D.4.

An R-APDU is referenced as follow:

• [R_NAME_OF_THE_RAPDU]

All R-APDUs are defined in Annex D.4.

Each APDU MAY refer to a constant or a dynamic content.

The APDU TERMINAL RESPONSE SHALL be dynamically generated by the test tool according to the related proactive command. Therefore, this particular command is not referenced with brackets in this specification. If not explicitly defined in the step, the general result SHALL be set by default to "Command performed successfully" (i.e. 0x83 01 00).

2.2.2.5 **Profiles**

In order to execute the test cases described in this document, Operational, Test and Provisioning Profiles are necessary. All these Profiles are defined in Annex E with the Profile Metadata content and the corresponding Profile Package as defined in the SIMalliance eUICC Profile Package Specification [4].

A Profile is referenced as follow:

PROFILE OPERATIONALX with x the identifier of the Operational Profile

or

• PROFILE TESTX with x the identifier of the Test Profile

or

PROFILE PROVISIONINGX with x the identifier of the Provisioning Profile

NOTE: Test Profiles and Provisioning Profiles are out of the scope of this version of test specification.

2.2.2.6 IUT Settings

For the purpose of some test cases, Device and eUICC manufacturers and Platforms (i.e. SM-DP+, SM-DS) providers need to give some information related to their products to the test tools providers (e.g. supported Java Card version).

An IUT setting is referenced as follow:

• #IUT NAME OF SETTING

V1.4 Page 31 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

All these settings are defined in Annex F.

2.2.2.7 Referenced Requirements

All requirements referenced in this document by their identifiers are present and described in Annex I. These requirements have been extracted from the specifications:

- GSMA RSP Technical Specification [2]
- GSMA RSP Architecture [3]

2.2.3 General Rules for eUICC Testing

2.2.3.1 Default Profile Downloading process

By default, when an Operational Profile needs to be downloaded on the eUICC (e.g. As mentioned in an initial condition), the following rules apply except if it is differently defined in the Test Case.

The highest priority Cl in euiccCiPKIdListForSigning SHALL be used.

In order to execute the Common Mutual Authentication procedure and the Sub-procedure Profile Download and Installation (End User Confirmation), the following requests SHALL be sent by the Test Tool:

- #GET EUICC INFO1 and #GET EUICC CHALLENGE
- #AUTH SMDP MATCH ID
 - o with the <EUICC_CI_PK_ID_TO_BE_USED> set to the Cl for signing indicated as highest priority in the #R EUICC INFO1
 - with the #CERT_S_SM_DPauth_ECDSA leading to the same Cl as the one chosen for signing
 - o with the SM-DP+ address #TEST DP ADDRESS1
- #PREP DOWNLOAD NO CC
 - with the #CERT_S_SM_DPpb_ECDSA leading to the same Cl as the one chosen for signing
- Neither ES10b.GetRAT nor ES10b.GetProfilesInfo requests SHALL be executed

During the Profile Installation, the following SCP03t TLVs SHALL be used by default:

- #S INIT SC PROF1
- #CONF ISDP EMPTY
- no TLV for "ES8+.ReplaceSessionKeys" function SHALL be used (i.e. the Profile SHALL be downloaded by using the session keys <S ENC> and <S MAC>)

2.2.3.2 Default Local Profile Management process

By default, when an Operational Profile needs to be enabled, disabled or deleted on the eUICC (e.g. As mentioned in an initial condition), the following rules apply except if it is differently defined in the Test Case.

V1.4 Page 32 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

The EnableProfileRequest and the DisableProfileRequest SHALL contain the following parameters:

- ICCID of the Profile to Enable or to Disable
- RefreshFlag set to TRUE

The eUICC SHALL send the REFRESH command in "UICC Reset" mode (i.e. the APDU[TERMINAL_PROFILE] indicating the support "UICC Reset" SHALL be used by the Test Tool).

The DeleteProfileRequest SHALL contain the following parameter:

ICCID of the Profile to Delete

2.2.3.3 ASN.1 elements verifications

Each time the eUICC returns an ASN.1 structure containing a SEQUENCE OF elements, the order of elements SHALL be checked by the Test Tool except for the particular responses:

- notificationMetadataList of ListNotificationResponse
- profileInfoListOk of ProfileInfoListResponse
- $\bullet \quad \texttt{notificationList} \ \textbf{of} \ \texttt{RetrieveNotificationsListResponse}$

When an Operational Profile class is expected to be indicated in a ProfileInfoListResponse, the Test Tool SHALL accept two different DER encodings if the eUICC supports SGP.22 V2.1 [2a]:

- either a tag 0x95 containing the integer value 2
- or an absent tag

When an Operational Profile class is expected to be indicated in a ProfileInfoListResponse, the Test Tool SHALL accept only one DER encoding if the eUICC supports SGP.22 v2.2.x [2] or SGP.22 V2.2 [2b]: a tag 0x95 containing the integer value 2.

2.2.4 General Rules for Device Testing

2.2.4.1 Default Profile Download, install and enable Process on the Device Under Test

By default, when an Operational Profile needs to be downloaded, installed (and if necessary enabled) on the (Test) eUICC resided in the Device Under Test (e.g. As mentioned in an initial condition), the following rules apply except if it is defined differently in the Test Case.

The default way to execute the Profile download SHALL be the Add Profile procedure with Activation Code #ACTIVATION_CODE_1. The way to apply the Activation Code (manual typing or QR code scanning) depends on the Device/LPAd implementation. In order to execute the Common Mutual Authentication procedure and the Sub-procedure Profile Download and Installation (End User Confirmation), the following responses SHALL be sent by the S SM-DP+:

V1.4 Page 33 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

- #INITIATE_AUTH_OK
 - o with the <EUICC_CI_PK_ID_TO_BE_USED> set to the CI for signing indicated as highest priority in euiccCiPKIdListForSigning in the #R_EUICC_INFO1
 - o with the #CERT_S_SM_DPauth_ECDSA leading to the same Cl as the one chosen for signing
 - o with the SM-DP+ address #TEST DP ADDRESS1
- #AUTH CLIENT OK
 - with the #CERT_S_SM_DPpb_ECDSA leading to the same Cl as the one chosen for signing
 - Metadata of the downloaded Profile instead of #METADATA OP PROF1
- #GET BPP OK with the content of the installed Profile (no session keys used)

All pending Notifications (sent on the best-effort basis as soon as connectivity is available as defined in section 3.5 of SGP.22 [2]) have been acknowledged by the simulated SM-DP+(s). S_SM-DP+(s) SHALL be run with suitable addresses in order to receive and acknowledge all pending Notifications (including install, enable, disable and delete). The addresses which are required depend on the server address used for recent profile downloads (typically #TEST_DP_ADDRESS1 to receive and acknowledge PIR), and the notificationAddress values in the Metadata of recently downloaded Profiles (for otherSignedNotification). Each S_SM_DP+ SHALL use the TLS certificate corresponding to its address (CERT_S_SM_DP_TLS, CERT_S_SM_DP2_TLS, etc).

If the test case requires a Profile Download to be initiated via SM-DS:

- The mechanism used to initiate this is device-specific.
- If the device is using Power-on Profile Discovery the following applies:
 - when it is supported, the value of the configuration parameter for Device Power-on Profile discovery is 'Enabled'.
 - the Device has to be powered-off and then powered-on before each test sequence.

2.2.4.2 LUI Settings and Result Verification Criteria

Some Initial Conditions require the "The protection of access to the LUI is disabled" setting. It means that no Confirmation is enforced upon entry to the LUI as defined in section 3.2 Local Profile Management of SGP.22 [2].

The way to perform Authenticated Confirmation SHALL be executed by the S_EndUser according to the description provided by the Device Vendor in #IUT_LPAd_AuthenticatedConfirmation.

Some of the Expected Results on the IUT side expect "No Error". In this case the Test Tool SHALL verify that there is no error message appears on the UI of the DUT.

V1.4 Page 34 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

The End User SHALL follow the LUI requests to successfully complete the Profile Download process. Any combined confirmation for consecutive Local Profile Management Operations SHALL be avoided by the End User. E.g.: upon installation of a new Profile, the LPA MAY propose 'add Profile' and 'enable' into one single step with a single confirmation only (e.g. "Do you want to install Profile 'ProfileName' on your Device and enable it? Yes / No / Install only") In this case the End User SHALL select the confirmation only for the single actual operation (i.e. select "Install only").

2.2.4.3 TLS Testing Recommendations

The TLS connection may be rejected either:

- by sending a TLS alert, or
- by closing of the TCP connection, though TLS handshake completed, or
- TLS handshake not completed without sending a TLS alert, or
- No further RSP communication has been initiated by LPAd on ES9+/ES11 within the #IUT_LPAd_SESSION_CLOSE_TIMEOUT

Please note that this is not an exhaustive list, and acting as guidelines for the test tools.

2.2.5 Pass Criteria

A test execution is considered as successful only if the test procedure was fully carried out successfully.

A test execution is considered as failed if the tested feature provides an unexpected behaviour.

A test execution is considered as inconclusive when the pass criteria cannot be evaluated due to issues during the setup of the initial conditions (including the ICx steps) or during the execution of steps in which no requirement is referenced.

2.2.6 Future Study

Some of the test cases or test sequences described in this Test Plan are FFS (For Future Study). This MAY mean that some clarifications are expected at the requirement level to conclude on a test method. As consequence, the corresponding test SHALL not be executed.

3 Testing Architecture

3.1 Testing Scope

All the interfaces, intended to be tested in the scope of this document, are presented hereafter:

V1.4 Page 35 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

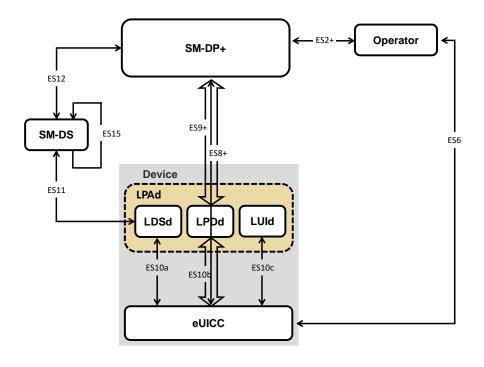




Figure 1: Scope of the Tests

Interface	Between		Description	
ES2+	Operator	SM-DP+	Used by the Operator to order Profiles for specific eUICCs as well as other administrative functions. NOTE: this interface is out of scope of this specification.	
ES6	Operator	eUICC	Used by the Operator for the management of Operator services via OTA services.	
ES8+	SM-DP+	eUICC	Provides a secure end-to-end channel between the SM-DP+ and the eUICC for the administration of the ISD-P and the associated Profile during download and installation. It provides Perfect Forward Secrecy.	
ES9+	SM-DP+	LPD	Used to provide a secure transport between the SM-DP+ and the LPA (LPD) for the delivery of the Bound Profile Package and the delivery of Remote Profile Management Commands.	
ES10a	LDSd	eUICC	Used between the LDSd and the LPA Services to handle a Profile discovery.	
ES10b	LPDd	eUICC	Used between the LPDd and the LPA services to transfer a Bound Profile Package to the eUICC. This interface plays no role in the decryption of Profile Packages.	

V1.4 Page 36 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

Interface	Between	ı	Description
ES10c	LUId	eUICC	Used between the LUId and the LPA services for Local Profile Management by the End User.
ES11	LDS	SM-DS	Used by the LDS to retrieve Event Records for the respective eUICC.
ES12	SM-DP+	SM-DS	Used by the SM-DP+ to issue or remove Event Registrations on the SM-DS.
ES15	SM-DS	SM-DS	Used in the case of deployments of cascaded SM-DSs to connect those SM-DSs.

Table 7: Interfaces Descriptions

3.2 Testing Execution

This chapter aims to describe the different testing environments and equipments to allow the test cases to be executed.

To permit the execution of the different test cases described in this Test Plan, specifics simulators SHALL be used. The simulators that have been defined are listed hereafter:

- S_Device: the Device Simulator used to send some commands to the eUICC under test using ISO/IEC 7816-4 [7] on the contact interface
- S_SM-DP+: the SM-DP+ Simulator
- S_SM-DS: the SM-DS Simulator
- S MNO: the MNO Simulator
- S LPAd: the LPAd Simulator
- S LPAe: the LPAe Simulator
- S_EndUser: the End User Simulator that acts as an End User. This simulator MAY be either a person (i.e. a Tester) or a software that simulates the End User interactions.
- S_CLIENT: the HTTPs client Simulator for the purpose of TLS testing. The S_CLIENT MAY be S_SM-DP+, S_SM-DS depending on the component under test.
- S_SERVER: the HTTPs server Simulator for the purpose of TLS testing. The S_SERVER MAY be S_SM-DP+ or S_SM-DS depending on the component under test.
- Implementation of these simulators remains under the responsibility of the test tool providers.
- The aim of all the test cases is to verify the compliance of an Actor/Component (i.e. eUICC, SM-DP+, Alternative SM-DS, Root SM-DS, LPAe, LPAd, Device).

Following notations are used:

- S_ComponentName for a simulated component
- ComponentName for the Implementation Under Test (IUT)
- Where ComponentName is indicated by CLIENT, SERVER
- Depending on the component under test, the CLIENT MAY be the SM-DP+ or the SM-DS. The Operator component is currently out of scope.

V1.4 Page 37 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

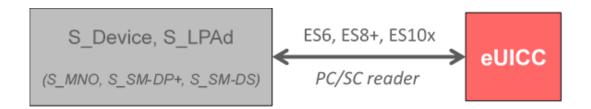
 Depending on the component under test, the SERVER MAY be the SM-DP+ or the SM-DS. The Operator component is currently out of scope.

The use of "-- optional" in any ASN.1 elements defined within this document indicate
that the test tool SHALL allow for the value either being present with that value, or
being absent.

3.2.1 eUICC - Test Environment

The following test environment is used for all eUICC test cases as defined in chapter 4.2 and 5.2 (unless it is specified differently in the specific test case). Following conditions apply:

- Removable eUICC is used
- In the scope of this Test Plan, the eUICC SHALL support Java cardTM
- EUM SHALL provide products with one of the form factors specified in ETSI TS 102 221 [5]
- EUM SHALL provide products compliant with Annex G.2 eUICC Initial States
- LPAd / MNO / SM-DP+ / SM-DS / Device Simulators SHALL be implemented by the test tools



The reference of this Test Environment is TE eUICC.

3.2.2 SM-DP+ and SM-DS - Test Environment

The following test environment is used for all SM-DP+ and SM-DS Interfaces related test cases as defined in chapter 4.3 and 4.5 (unless it is specified differently in the specific test case). Following conditions apply:

- SM-DS / SM-DP+ / LPA Simulators SHALL be implemented by the test tools
- Simulators act as a RSP server or a RSP client
- Definition of the TLS parameters/configuration is provided
- JSON (and ASN.1) input data are used (NOTE: ASN.1 format is out of scope of this specification)

3.2.2.1 Test environment for SM-DP+ under test

Test Environment reference:

• TE_P1 (SM-DP+ on ES12)

V1.4 Page 38 of 777



Test Environment reference:

• TE_P2 (SM-DP+ on ES9+)



3.2.2.2 Test environment for SM-DS under test

Test Environment reference:

• TE_S1 (SM-DS on ES11)



Test Environment reference:

• TE_S2 (SM-DS on ES12)



Test Environment reference:

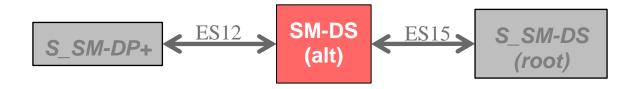
• TE_S3 (SM-DS on ES12 and ES11)



Test Environment reference:

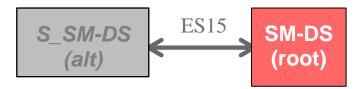
• TE_SA1 (Alternative SM-DS on ES12 and ES15)

V1.4 Page 39 of 777



Test Environment reference:

• TE_SR1 (Root SM-DS on ES15)



Test Environment reference:

TE SR2 (Root SM-DS on ES15 and ES11)



3.2.3 Device/LPAd - Test Environment

The following test environment is used for all LPAd Interfaces related test cases as defined in chapter 4.4 and 5.4 (unless it is specified differently in the specific test case). Following conditions apply:

- The Device contains an eUICC configured with Test Certificates and Test Keys
- The Test eUICC is either soldered or removable. In case the eUICC is removable, it SHALL NOT be removed during testing
- The Test eUICC is only used for LPAd testing and SHALL not be considered as an IUT
- The Test eUICC SHALL not support LPAe
- The Test eUICC SHOULD be compliant with the GSMA RSP Technical Specification
 [2]
- SM-DP+ Simulator(s) SHALL be implemented by the test tools
- SM-DS Simulator(s) SHALL be implemented by the test tools
- End User Simulator SHALL be used (S_EndUser)
- No modification of the Device HW is required

V1.4 Page 40 of 777

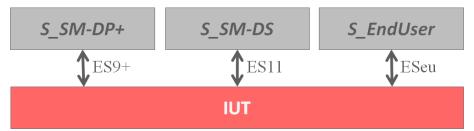
GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

 If the IUT is a Companion Device it has to be connected to a Primary Device as defined by the Device Vendor. The Device Vendor SHALL provide detailed information about which RSP functionality requires a Primary Device.

- No modification of the Device OS is required for the usage of S_EndUser
- Test Root Certificate SHALL be configured in the Device

3.2.3.1 General (Device/LPAd) Test Environment



The Test Environment consists of:

- IUT: Device, or Companion Device supporting the LPAd with a Test eUICC connected to a Primary Device
- S_SM-DP+: a simulated SM-DP+ supporting a connection used by the Device to establish ES9+, (ES8+)
- S_SM-DS: a simulated SM-DS supporting a connection used by the Device to establish ES11
- S EndUser

In case the Device supports a connection method different from Cellular Network it is expected that this connection method is used.

NOTE: Device that supports only Cellular Networks is out of scope for this specification.

3.2.3.2 Device – Test Environment

If the IUT is a Device as defined in SGP21/SGP.22 [2] it SHALL provide at least one method to establish the IP connection to the S_SM-DP+, or S_SM-DS.

When executing a test case with an IUT matching this definition, default Initial States as defined in G.1.1 apply unless it is specified differently in the specific test case.

3.2.3.3 Companion Device connected to a Primary Device – Test Environment

The Companion Device is connected to a Primary Device.

Device Vendors SHALL provide the mechanism to connect the Primary Device to the Companion Device.

User interaction and the verification of User Intents can be performed on the User Interface of the Primary Device or the companion Device.

The Companion Device MAY connect to the S_SM-DP+, or S_SM-DS directly, or MAY use a connection offered by the Primary Device.

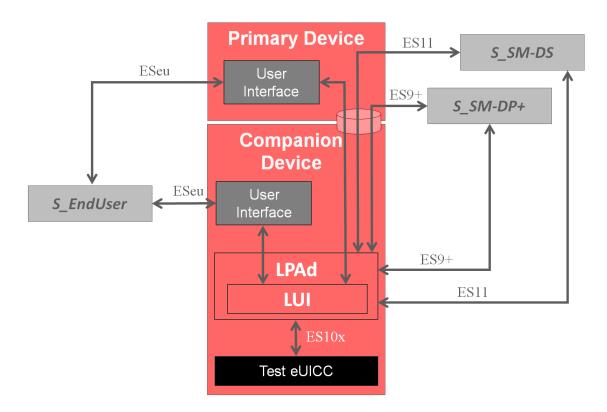
V1.4 Page 41 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

To connect to the SM-DP+ or the SM-DS the Companion Device uses a connection offered by the Primary Device.

Initial State as defined in G.1.2 applies unless otherwise stated in the test case.



3.2.4 End-to-End Testing

The aim of all the test cases related to the system behaviour sections is to verify the functional behaviour of the RSP ecosystem composed of the following Actors:

- eUICC
- SM-DP+
- Device
- LPA
- SM-DS

This test environment is defined as FFS.

4 Interface Compliance Testing

4.1 General Overview

This section focuses on the implementation of the different interfaces according to the GSMA RSP Technical Specification [2]. The aim is to verify the compliance of all interfaces within the system.

V1.4 Page 42 of 777

GSM Association
Official Document SGP.23 - SGP.23 RSP Test Specification

Non-confidential

4.2 eUICC Interfaces

4.2.1 ATR and ISD-R Selection

4.2.1.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ34_001
- RQ57_001, RQ57_003, RQ57_005
- RQD0_001

4.2.1.2 Test Cases

4.2.1.2.1 TC_eUICC_ATR_And_ISDR_Selection

Test Sequence #01 Nominal: ATR and Select ISD-R

Step	Direction	Sequence / Description	Expected result	REQ
1	S_Device → eUICC	RESET	ATR present with the first tBi (i>2) after T = 15 containing b2=1	RQ34_001
2	S_Device → eUICC	[SELECT_MF]	FCP Template present SW=0x9000	
3	S_Device → eUICC	[TERMINAL_CAPABILITY_LPAd]	SW=0x9000	
4	S_Device → eUICC	[TERMINAL_PROFILE]	Toolkit initialization THEN SW=0x9000	
5	S_LPAd → eUICC	[MANAGE_CHANNEL_OPEN]	Extract the <channel_number> from response data SW=0x9000</channel_number>	RQ57_001
6	S_LPAd → eUICC	MTD_SELECT(#ISD_R_AID)	The response data: 0x6F <l> 84 <l> #ISD_R_AID A5 <l> <proprietary_data> #R_ISDR_SELECTION SW=0x9000</proprietary_data></l></l></l>	RQ57_003 RQ57_005 RQD0_001

4.2.2 ES6 (Operator -- eUICC): UpdateMetadata

4.2.2.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

V1.4 Page 43 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

3GPP TS 23.040 - Technical realization of the Short Message Service (SMS) [22]

Requirements

- RQ24_021, RQ24_024
- RQ29_001, RQ29_021
- RQ54_001, RQ54_002, RQ54_003, RQ54_004, RQ54_005, RQ54_006, RQ54_007, RQ54_008, RQ54_009, RQ54_010, RQ54_011, RQ54_012, RQ54_013, RQ54_014, RQ54_013_1, RQ54_015, RQ54_016
- RQ57_120, RQ57_122, RQ57_123, RQ57_126

4.2.2.2 Test Cases

4.2.2.2.1 TC_eUICC_ES6.UpdateMetadata

Throughout all the ES6.UpdateMetadata test cases, SMS is used as the secure OTA channel.

General Initial Conditions		
Entity Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 with #METADATA_WITH_PPRS_AND_ICON is loaded on the eUICC	

Test Sequence #01 Nominal: Unset PPR1

The purpose of this test is to verify that the MNO can unset PPR1 from a Profile and that the eUICC can handle an Update Metadata request with only one field present.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITI	ALIZATION_SEQUENCE		
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#REMOVE_PPR1, FALSE))	SW=0x91XX	RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006 RQ54_007 RQ54_009 RQ54_010 RQ54_013_1 RQ29_021 RQ24_021 RQ54_011
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (0x9000)	RQ54_015 RQ54_011

V1.4 Page 44 of 777

3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	PROC_OPEN_LOGI	CAL_CHANNEL_AND_SELECT_ISI	DR	
5	$S_LPAd \rightarrow eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_GET_UPDATE_N1 SW=0x9000	RQ54_013_1 RQ54_009 RQ57_120 RQ57_122 RQ57_123 RQ57_126

Test Sequence #02 Nominal: Unset PPR2 and update icon

The purpose of this test is to verify that the MNO can unset PPR2 and update the icon and icon type values from a Profile.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITI	OC_EUICC_INITIALIZATION_SEQUENCE				
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#UPD_ICON_REM_PPR2, FALSE))	SW=0x91XX	RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006 RQ54_007 RQ54_009 RQ54_010 RQ54_011 RQ54_012 RQ54_013_1 RQ29_021 RQ24_021		
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (0x9000)	RQ54_015 RQ54_011		
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000			
4	PROC_OPEN_LOGI	CAL_CHANNEL_AND_SELECT_IS	DR			
5	$S_LPAd \rightarrow eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_GET_UPDATE_N2 SW=0x9000	RQ54_009 RQ54_012 RQ54_013_1 RQ57_120 RQ57_122 RQ57_123 RQ57_126		

V1.4 Page 45 of 777

Test Sequence #03 Nominal: Unset PPR1 and PPR2 and update Profile name and Service Provider name

The purpose of this test is to verify that MNO can unset PPR1 and PPR2 from a Profile and can update the Service Provider Name and Profile Name values.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#UPD_NAMES_REM_PPRS, FALSE))	SW=0x91XX	RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006 RQ54_007 RQ54_009 RQ54_010 RQ54_011 RQ54_012 RQ54_013_1 RQ29_021 RQ24_021	
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (0x9000)	RQ54_015 RQ54_011	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000		
4	PROC_OPEN_LOGI	CAL_CHANNEL_AND_SELECT_ISI	DR		
5	$S_LPAd \rightarrow eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_GET_UPDATE_N3 SW=0x9000	RQ54_009 RQ54_012 RQ54_013_1 RQ57_120 RQ57_122 RQ57_123 RQ57_126	

Test Sequence #04 Nominal: Delete PPRs, Service Provider and Profile names

The purpose of this test is to verify that the MNO can delete all PPRs, the Service Provider name and the Profile name from a Profile.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ
------	-----------	------------------------	-----------------	-----

V1.4 Page 46 of 777

IC1	PROC_EUICC_INITI	ALIZATION_SEQUENCE		
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#REMOVE_NAMES_PPRS, FALSE))	SW=0x91XX	RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006 RQ54_007 RQ54_009 RQ54_010 RQ54_011 RQ54_013 RQ54_013_1 RQ29_021 RQ24_021
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (0x9000)	RQ54_015 RQ54_011
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	PROC_OPEN_LOGI	CAL_CHANNEL_AND_SELECT_IS	DR	
5	S_LPAd \rightarrow eUICC	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_GET_UPDATE_N4 SW=0x9000	RQ54_013 RQ54_013_1 RQ54_009 RQ57_120 RQ57_122 RQ57_123 RQ57_126

Test Sequence #05 Nominal: Delete icon

The purpose of this test is to verify that the MNO can delete the icon and icon type from a Profile.

This test case is defined as FFS and not applicable for this version of test specification.

Test Sequence #06 Nominal: Delete Unset PPRs

The purpose of this test is to verify that the MNO can delete already unset PPRs using the Update Metadata request.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(SW=0x91XX			

V1.4 Page 47 of 777

	ī	"DEMOVE NAMEO DEED	ī	1
		#REMOVE_NAMES_PPRS,		
		FALSE))		
IC3	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (0x9000)	
IC4	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#UPD_NAMES_REM_PPRS, FALSE))	SW=0x91XX	RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006 RQ54_007 RQ54_009 RQ54_010 RQ54_011 RQ54_013 RQ54_015 RQ54_013_1 RQ29_021 RQ24_021
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (0x9000)	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	PROC_OPEN_LOG	ICAL_CHANNEL_AND_SELECT_IS	DR	
5	S_LPAd → eUICC	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_GET_UPDATE_N6 SW=0x9000	RQ54_013 RQ54_013_1 RQ54_009 RQ57_120 RQ57_122 RQ57_123 RQ57_126

Test Sequence #07 Error: Set a pprUpdateControl value to one

The purpose of this test is to verify that the eUICC is correctly handling a pprUpdateControl value error from the MNO request, and return the expected error code status.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INIT	IALIZATION_SEQUENCE		

V1.4 Page 48 of 777

1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#UPD_PPR_CONTROL, FALSE))	SW=0x91XX	RQ24_021 RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_010 RQ54_010 RQ54_011
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (0x6A81)	RQ54_008 RQ54_014 RQ54_015 RQ54_016 RQ54_011
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
5	$S_LPAd \rightarrow eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_METADATA_UNCHA NGED SW=0x9000	RQ54_014 RQ57_120 RQ57_122 RQ57_123 RQ57_126

Test Sequence #08 Error: Update Metadata on a Disable Profile

The purpose of this test is to verify that the eUICC is correctly rejecting an Update Metadata request from the MNO when the targeted Profile is Disabled.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#REMOVE_PPR1, FALSE))	SW=0x91XX or SW=0x9000 (i.e. envelope rejected, see Note) or any error SW (i.e. envelope rejected, see Note)	RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006 RQ54_010 RQ54_011 RQ24_024 RQ24_021
2	S_Device →eUICC	FETCH "XX"	SMS POR received SCP80 response status code equal to 0x06 (Unidentified security error) or 0x09 (TAR unknown)	RQ54_011 RQ54_014
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	

V1.4 Page 49 of 777

4	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
5	$S_LPAd \to eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_METADATA_UNCHAN GED SW=0x9000	RQ54_014 RQ57_120 RQ57_122 RQ57_123 RQ57_126	

NOTE: Depending on the implementation, the eUICC MAY decide to not send back a POR (i.e. SW=0x9000 on the ENVELOPE command). Therefore, the steps 2 and 3 SHALL only be executed in case SW=0x91XX.

Test Sequence #09 Error: Empty request

The purpose of this test is to verify that the eUICC is correctly rejecting an Update Metadata request from the MNO when no field is present.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Ste p	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITI	ALIZATION_SEQUENCE		
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#UPD_NO_METADATA, FALSE))	SW=0x91XX	RQ24_021 RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_010 RQ54_010 RQ54_011
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (<any_sw_in_error>)</any_sw_in_error>	RQ54_011 RQ54_014 RQ54_015
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	PROC_OPEN_LOGI	DR		
5	$S_LPAd \to eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_METADATA_UNCHA NGED SW=0x9000	RQ57_120 RQ57_122 RQ57_123 RQ57_126 RQ54_014

Test Sequence #10 Error: Update Icon without Icon Type field

The purpose of this test is to verify that the eUICC is correctly rejecting an Update Metadata request from the MNO when the icon field is present but not the icon type field.

V1.4 Page 50 of 777

Non-confidential

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ			
IC1	PROC_EUICC_INIT	PROC_EUICC_INITIALIZATION_SEQUENCE					
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#UPD_ICON_NO_TYPE, FALSE))	SW=0x91XX	RQ24_021 RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006 RQ54_010 RQ54_011			
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (<any_sw_in_error>)</any_sw_in_error>	RQ54_011 RQ54_014 RQ54_015			
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000				
4	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR						
5	$S_LPAd \to eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_METADATA_UNCHA NGED SW=0x9000	RQ54_014 RQ57_120 RQ57_122 RQ57_123 RQ57_126			

Test Sequence #11 Error: Update Icon Type without Icon field

The purpose of this test is to verify that the eUICC is correctly rejecting an Update Metadata request from the MNO when the Icon Type field is present but not the Icon field.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
1	S_Device → eUICC	MTD_SEND_SMS_PP([INSTALL_PERSO_RES_ISDP]; MTD_STORE_DATA_SCRIPT(#UPD_ICON_TYPE_ONLY,	SW=0x91XX	RQ24_021 RQ54_001 RQ54_002 RQ54_003 RQ54_004 RQ54_005 RQ54_006	

V1.4 Page 51 of 777

		FALSE))		RQ54_010 RQ54_011
2	S_Device →eUICC	FETCH "XX"	MTD_CHECK_SMS_POR (<any_sw_in_error>)</any_sw_in_error>	RQ54_011 RQ54_014 RQ54_015
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	PROC_OPEN_LOGI	CAL_CHANNEL_AND_SELECT_ISI	DR	
5	$S_LPAd \rightarrow eUICC$	MTD_STORE_DATA(#GET_NEW_METADATA)	#R_METADATA_UNCHA NGED SW=0x9000	RQ54_014 RQ57_120 RQ57_122 RQ57_123 RQ57_126

4.2.3 ES8+ (SM-DP+ -- eUICC): InitialiseSecureChannel

4.2.3.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ25_024, RQ25_025, RQ25_026
- RQ31_162, RQ31_163
- RQ35_003_1
- RQ55_011, RQ55_012, RQ55_013, RQ55_014, RQ55_015, RQ55_019, RQ55_023
- RQ57_041_1, RQ57_013, RQ57_016

4.2.3.2 Test Cases

4.2.3.2.1 TC_eUICC_ES8+.InitialiseSecureChannel

General Initial Conditions			
Entity	Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC		
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.		
	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+		
eUICC	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 		
	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+		
	#PREP_DOWNLOAD_NO_CC has been sent to the eUICC		

V1.4 Page 52 of 777

Test Sequence #01 Error: Invalid Remote Operation

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>				
IC2	<pre><bpp> = MTD_GENERATE_BPP(#INIT_SC_INVALID_OP_ID, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>					
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>					
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands except the last one SW=0x9000 with the response data #R_PIR_INVALID_OP_ID for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ31_162 RQ31_163 RQ55_012 RQ55_015 RQ55_023 RQ25_024 RQ25_025 RQ25_026 RQ35_003_1		

Test Sequence #02 Error: Invalid SM-DP+ Signature

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	Generate the	<otpk_s_sm_dp+_ecka> and <</otpk_s_sm_dp+_ecka>	COT_SK_S_SM_DP+_ECKA>		
IC2	<pre><bpp> = MTD_GENERATE_BPP(#INIT_SC_INVALID_SIGN, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				
IC3	Execute the st	ep IC3 of the Test Sequence #01 c	lefined in this section		
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_INVALID_SIGN for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ31_162 RQ31_163 RQ55_011 RQ55_015 RQ25_024 RQ25_025 RQ25_026 RQ35_003_1	

V1.4 Page 53 of 777

Test Sequence #03 Error: Invalid Transaction Identifier

Step	Directio n	Sequence / Description	Expected result	REQ	
IC1	Generate the	e <otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>		
IC2	<pre><bpp> = MTD_GENERATE_BPP(#INIT_SC_INVALID_TRANS_ID, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				
IC3	Execute the	step IC3 of the Test Sequence #01	defined in this section		
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands except the last one SW=0x9000 with the response data #R_PIR_INVALID_TRANS_ID for the last STORE DATA command The transactionId returned in the response SHALL not be checked (any value SHALL be accepted) The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ31_162 RQ31_163 RQ55_013 RQ55_015 RQ25_024 RQ25_025 RQ25_026 RQ35_003_1	

Test Sequence #04 Error: Invalid CRT Values

Step	Directio n	Sequence / Description	Expected result	REQ	
IC1	Generate ti	ne <otpk_s_sm_dp+_ecka> ar</otpk_s_sm_dp+_ecka>	nd <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>		
IC2	<pre><bpp> = MTD_GENERATE_BPP(#INIT_SC_INVALID_CRT, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				
IC3	Execute the	e step IC3 of the Test Sequence #0	01 defined in this section		
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for the intermediate STORE DATA commands (if any) SW=0x9000 with the response data #R_PIR_INVALID_CRT for the last STORE DATA command	RQ31_162 RQ31_163 RQ55_014 RQ55_015 RQ55_019 RQ25_024 RQ25_025 RQ25_026 RQ35_003_1	

V1.4 Page 54 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

	The euiccSignPIR SHALL be verified	
	with the #PK_EUICC_ECDSA	

Test Sequence #05 Error: InitialiseSecureChannel request while Secure Channel Session is ongoing

The purpose of this test is to ensure that the eUICC rejects an InitialiseSecureChannel request if a secure channel session is already ongoing.

Ste p	Directio n	Sequence / Description	Expected result	REQ	
IC1	Generate the	e <otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>		
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				
IC3	Execute the	step IC3 of the Test Sequence #01	defined in this section		
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands		
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands		
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x6A88 or 0x6985 or SW=0x9000 with a ProfileInstallationResult containing an ErrorResult	RQ55_010 RQ57_041_1 RQ57_013 RQ57_016	

4.2.4 ES8+ (SM-DP+ -- eUICC): ConfigureISDP

4.2.4.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_010
- RQ25_023, RQ25_024, RQ25_025, RQ25_026
- RQ31_165
- RQ35_003_1
- RQ55_025, RQ55_026, RQ55_027, RQ55_028

V1.4 Page 55 of 777

4.2.4.2 Test Cases

4.2.4.2.1 TC_eUICC_ES8+.ConfigureISDP

General Initial Conditions				
Entity	Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC			
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.			
	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+			
eUICC	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 			
	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+			
	#PREP_DOWNLOAD_NO_CC has been sent to the eUICC			

Test Sequence #01 Nominal: Empty Proprietary Data

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>				
IC2	#S_INIT_S #CONF_IS #METADAT NO_PARAI	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_EMPTY, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>					
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands			
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	RQ31_165 RQ55_028 RQ24_010		
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands			
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except the last one	RQ25_023 RQ25_024		

V1.4 Page 56 of 777

			SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command	
			The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA.	
4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_CONF_OP_PROF1)	resp ProfileInfoListResponse ::= profileInfoListOk :{ { isdpAid <isd_p_aid> dpProprietaryData SHALL not be present } } SW=0x9000</isd_p_aid>	RQ55_025 RQ24_010

Test Sequence #02 Nominal: Proprietary Data with the maximum length authorized (i.e. 128 bytes)

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>				
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_MAX_LENGTH, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>					
IC3	Execute the s	step IC3 of the Test Sequence #01	defined in this section			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands			
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	RQ31_165 RQ55_028 RQ24_010		
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands			
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA.	RQ25_023 RQ25_024		

V1.4 Page 57 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

S_LPAd —	$S_LPAd \to$	MTD_STORE_DATA(#R_CONF_OP_PROF1	RQ55_027		
	4	eUICC	#GET_CONF_OP_PROF1)	SW=0x9000	RQ24_010	

Test Sequence #03 Error: Proprietary Data with the maximum length exceeded (i.e. 129 bytes)

Step	Directio n	Sequence / Description	Expected result	REQ
IC1	Generate the	e <otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	I <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_SIZE_EXCEEDED, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>			
IC3	Execute the	step IC3 of the Test Sequence #01	defined in this section	
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands except the last one SW=0x9000 with the response data #R_PIR_INVALID_DATA for the last STORE DATA command	RQ55_028 RQ31_165 RQ55_026 RQ25_025 RQ25_026 RQ35_003 _1

4.2.5 ES8+ (SM-DP+ -- eUICC): StoreMetadata

4.2.5.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_028
- RQ25_017, RQ25_023, RQ25_024, RQ25_025, RQ25_026
- RQ29_001, RQ29_002
- RQ31_166, RQ31_167
- RQ32_071,
- RQ55_029, RQ55_030, RQ55_031, RQ55_032, RQ55_033, RQ55_034, RQ55_035, RQ55_036, RQ55_037

• RQ57_040

V1.4 Page 58 of 777

4.2.5.2 Test Cases

4.2.5.2.1 TC_eUICC_ES8+.StoreMetadata

General Initial Conditions				
Entity	Description of the general initial condition			
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.			
	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+			
eUICC	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 			
	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ #PREP_DOWNLOAD_NO_CC has been sent to the eUICC			

Test Sequence #01 Nominal: All Metadata fields present (PNG icon used and PPR1 set)

The purpose of this test is to download the PROFILE_OPERATIONAL1 by setting all Metadata fields. In this sequence, a PNG icon is used and PPR1 is set.

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Operational Profile is present on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and <</otpk_s_sm_dp+_ecka>	OT_SK_S_SM_DP+_ECKA>	
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #FULL_METADATA, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>			
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	

V1.4 Page 59 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ31_166 RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ29_001
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands expect the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024
3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_METADATA_OP_PROF1)	#R_GET_METADATA_OP_PROF1 SW=0x9000	RQ32_071 RQ29_001 RQ29_002

Test Sequence #02 Nominal: With JPG icon

The purpose of this case is to verify the ability to download JPG icon. The icon size does not allow for the command to fit into one data sequence.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_WITH_JPG, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>			
IC3	Execute the s	tep IC3 of the Test Sequence #01	defined in this section	
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands	

V1.4 Page 60 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ31_166 RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ29_001
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { iccid #ICCID_OP_PROF1, iconType jpg, icon #ICON_JPG, } } SW=0x9000	RQ32_071

Test Sequence #03 Nominal: Without providing Profile Class

The purpose of this test is to download the PROFILE_OPERATIONAL1 by not indicating the Profile Class in the Metadata. In such a case, the default Profile Class 'Operational' SHALL be set by the eUICC.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_NO_CLASS, NO_PARAM,</bpp></pre>			

V1.4 Page 61 of 777

	#UPP_OP_	PROF1)		
IC3	Execute the step IC3 of the Test Sequence #01 defined in this section			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ31_166 RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ29_001
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { iccid #ICCID_OP_PROF1, profileClass operational } } SW=0x9000	RQ32_071 RQ29_001 RQ29_002

Test Sequence #04 Nominal: With PPR2 set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and <ot< td=""><td>_SK_S_SM_DP+_ECKA></td><th></th></ot<></otpk_s_sm_dp+_ecka>	_SK_S_SM_DP+_ECKA>	
IC2		<bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1,</bpp>		

V1.4 Page 62 of 777

Non-confidential

	#CONF_IS	DP_PROF1,		
		#METADATA_WITH_PPR2,		
	NO_PARAM, #UPP_OP_PROF1)			
100		•	11. 41.	
IC3	Execute the s	step IC3 of the Test Sequence #01 defir	1	Ι
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ31_166 RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ29_001
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024
3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PPR_OP_PROF1)	resp ProfileInfoListResponse ::= profileInfoListOk :{ { iccid #ICCID_OP_PROF1, profilePolicyRules {ppr2} } } SW=0x9000	RQ32_071 RQ29_001 RQ29_002

Test Sequence #05 Nominal: With PPR1 and PPR2 set

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Operational Profile is present on the eUICC

V1.4 Page 63 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>		
IC2	#S_INIT_S	DP_PROF1, FA_WITH_PPR1_PPR2, M,		
IC3	Execute the s	step IC3 of the Test Sequence #01	defined in this section	
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ31_166 RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ29_001
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024
3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PPR_OP_PROF1)	resp ProfileInfoListResponse ::= profileInfoListOk :{ { iccid #ICCID_OP_PROF1, profilePolicyRules {ppr1,ppr2} } } SW=0x9000	RQ32_071 RQ29_001 RQ29_002

Test Sequence #06 Nominal: With several Notification events configured

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

V1.4 Page 64 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the <	COTPK_S_SM_DP+_ECKA> and <ot_< td=""><td>SK_S_SM_DP+_ECKA></td><td></td></ot_<>	SK_S_SM_DP+_ECKA>	
IC2	#S_INIT_SC #CONF_ISD #METADATA NO_PARAM	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_WITH_NOTIFS, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>		
IC3	Execute the st	ep IC3 of the Test Sequence #01 define	ed in this section	
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ31_166 RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024
3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_NOTIF_CONF_OP_PROF1)	#R_GET_PROF_NOTIF_CONF SW=0x9000	RQ32_071

Test Sequence #07 Error: ICCID already present in the eUICC

Initial Conditions	
Entity	Description of the initial condition
eUICC	General Initial Conditions do not apply
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC

V1.4 Page 65 of 777

eUICC	The PROFILE_OPERATIONAL1 is Disabled	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R. Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+ • #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC • the same GSMA CI has been chosen for signing and for verification Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ • #PREP_DOWNLOAD_NO_CC has been sent to the eUICC			eUICC and
IC2	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC3	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>			
IC4	Execute the s	step IC3 of the Test Sequence #01	defined in this section	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_ICCID_ALREADY_EXIST for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ25_017 RQ31_166 RQ55_030 RQ55_032 RQ55_032 RQ25_024 RQ25_025 RQ25_026

Test Sequence #08 Error: Profile Policy Rule is set but Profile Owner is not

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

V1.4 Page 66 of 777

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	I <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>			
IC2	#S_INIT_S #CONF_IS #METADA ⁻ NO_PARAI	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_PPR_NO_OWNER, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				
IC3	Execute the s	step IC3 of the Test Sequence #01	defined in this section			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands			
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands			
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_METADATA_INVALID (See Note) for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ31_166 RQ55_030 RQ55_032 RQ25_024 RQ25_025 RQ25_026 RQ25_026		
Note: T	The errorReason "pprNotAllowed" or "installFailedDueToUnknownError" MAY be also returned by the					

Note: The errorReason "pprNotAllowed" or "installFailedDueToUnknownError" MAY be also returned by the eUICC

Test Sequence #09 Error: Profile Owner is set with a wildcard ('E') digits

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>			
IC2	#S_INIT_SO #CONF_ISO #METADAT NO_PARAN	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka> <bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_WILDCARD, NO_PARAM, #UPP_OP_PROF1)</bpp></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>		

V1.4 Page 67 of 777

IC3	Execute the	Execute the step IC3 of the Test Sequence #01 defined in this section		
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_METADATA_INVALID (See Note) for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ31_166 RQ55_030 RQ55_032 RQ25_024 RQ25_025 RQ25_026 RQ25_026
Note: T	Note: The errorReason "pprNotAllowed" MAY be also returned by the eUICC			

Test Sequence #10 Error: Icon Type is set but icon is not

The purpose of this test is to check ASN.1 conditional requirement for icon presence. If icon type is present then icon SHALL also be present.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC2	<bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_WITHOUT_ICON, NO_PARAM, #UPP_OP_PROF1)</bpp>			
IC3	Execute the step IC3 of the Test Sequence #01 defined in this section			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	

V1.4 Page 68 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_METADATA_INVALID for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ31_167 RQ55_029 RQ55_031 RQ55_033 RQ55_035 RQ24_028 RQ57_040 RQ31_166 RQ55_030 RQ55_032 RQ25_024 RQ25_025 RQ25_026 RQ25_017
---	-------------------	--	---	--

4.2.6 ES8+ (SM-DP+ -- eUICC): ReplaceSessionKeys

4.2.6.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ25_024, RQ25_025, RQ25_026
- RQ26_021, RQ26_022
- RQ31_168
- RQ55_038, RQ55_041

4.2.6.2 Test Cases

4.2.6.2.1 TC_eUICC_ES8+.ReplaceSessionKeys

General Initial Condit	General Initial Conditions	
Entity	Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC	
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.	
	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+	
eUICC	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification and for verification 	
	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+	
	 #PREP_DOWNLOAD_NO_CC has been sent to the eUICC 	

V1.4 Page 69 of 777

Test Sequence #01 Error: Incorrect PPK size

The purpose of this test is to verify that the eUICC checks that all PPK sizes are the same as session keys.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>			
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, #REPLACE_S_KEYS_REQ_INV_SIZE, #UPP_OP_PROF1)</bpp></pre>				
	MTD_GENERATE_BPP overriding: For this test sequence, session keys SHALL be used for UPP SCP03t protection. Therefore: Encrypt all <upp_seg> with <s_enc> Calculate and add a MAC to all tags 0x86 of sequenceOf86 by using <s_mac></s_mac></s_enc></upp_seg>				
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a2> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a2></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>				
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands		
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands		
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands		
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a2>)</bpp_seg_a2>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_PPK_INV for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ55_038 RQ55_041 RQ31_168 RQ26_021 RQ26_022 RQ25_024 RQ25_025 RQ25_026	

V1.4 Page 70 of 777

4.2.7 ES8+ (SM-DP+ -- eUICC): LoadProfileElements

4.2.7.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ25_023, RQ25_024, RQ25_025, RQ25_026
- RQ31_173
- RQ32_071
- RQ55_045, RQ55_045_2, RQ55_045_3, RQ55_047, RQ55_048
- RQ57_071, RQ57_074

4.2.7.2 Test Cases

4.2.7.2.1 TC_eUICC_ES8+.LoadProfileElements

General Initial Conditions			
Entity	Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC		
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.		
	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+		
eUICC	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 		
	Sub-procedure Profile Download and Installation – End User Confirmation has beer successfully executed between the eUICC and the S_SM-DP+		
	 #PREP_DOWNLOAD_NO_CC has been sent to the eUICC 		

Test Sequence #01 Error: EF_{ICCID} different from the ICCID provided in the Profile Metadata

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL2 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>			
IC2	<bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1,</bpp>			

V1.4 Page 71 of 777

	#METADA	TA_ICCID_MISMATCH,		
	NO_PARAM,			
	#UPP_OP_PROF1)			
	<u>'</u>			
	Split the <bpp> into several segments arrays named:</bpp>			
IC3	 <bpp_seg_init></bpp_seg_init> <bpp_seg_a0></bpp_seg_a0> <bpp_seg_a1></bpp_seg_a1> <bpp_seg_a3></bpp_seg_a3> 			
10.4	S LPAd →	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for	
IC4	eŪICC	<bpp_seg_init>)</bpp_seg_init>	all STORE DATA commands	
	S LPAd \rightarrow	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for	
IC5	eUICC	<bpp_seg_a0>)</bpp_seg_a0>	all STORE DATA commands	
	S LPAd →	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for	
IC6	eUICC	<pre><bpp_seg_a1>)</bpp_seg_a1></pre>	all STORE DATA commands	
			SW=0x9000 with the response data	RQ25_023
			#R_PIR_DATA_MISMATCH	RQ25_024
1	$S_LPAd \rightarrow$	MTD_STORE_DATA_SCRIPT(for one of the STORE DATA	RQ55_045 RQ55_048
'	eUICC	<bpp_seg_a3>)</bpp_seg_a3>	commands	RQ25_025
			The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_026
			With the #1 N_LOIGO_LODGA	RQ31_173
		MTD_STORE_DATA(resp ProfileInfoListResponse ::=	
2	S_LPAd → eUICC	MTD_GET_PROFILE_INFO(profileInfoListOk :{}	RQ32_071
	eoicc	#ICCID_OP_PROF1,	SW=0x9000	RQ55_048
		NO_PARAM))		
		MTD_STORE_DATA(resp ProfileInfoListResponse ::=	
3	S_LPAd →	MTD_GET_PROFILE_INFO(profileInfoListOk :{}	RQ32_071
	eUICC	#ICCID_OP_PROF2,	SW=0x9000	RQ55_048
		NO_PARAM))		

Test Sequence #02 Error: MCC / MNC of EF_{IMSI} different from MCC / MNC of Profile Owner present in Metadata

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>			
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_MCCMNC_MISMATCH, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>			
IC3	Execute the step IC3 of the Test Sequence #01 defined in this section			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	

V1.4 Page 72 of 777

IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 with the response data #R_PIR_DATA_MISMATCH for one of the STORE DATA commands The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024 RQ55_043 RQ55_047 RQ55_048 RQ25_025 RQ25_026 RQ31_173
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{} SW=0x9000	RQ32_071 RQ55_043 RQ55_048

Test Sequence #03 Error: Session MAC chaining used instead of new Initial MAC chaining

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>		
IC2	<pre><bpp> = MTD_GENERATE_BPP (#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, #REPLACE_S_KEYS_REQ, #UPP_OP_PROF1) MTD_GENERATE_BPP overriding: For this test sequence, <s_mac_chain> SHALL be used instead of <ppk_init_mac> for UPP SCP03t protection.</ppk_init_mac></s_mac_chain></bpp></pre>				
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a2> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a2></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>				
IC4	S_LPAd → MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands				
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands		
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands		

V1.4 Page 73 of 777

Non-confidential

IC7	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a2>)</bpp_seg_a2>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 with the response data #R_PIR_SECU_INVALID for one of the STORE DATA commands The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ55_048 RQ31_173
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{} SW=0x9000	RQ32_071 RQ55_048

Test Sequence #04 Error: S-MAC used instead of PPK-MAC

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>				
IC2	<pre><bpp> = MTD_GENERATE_BPP (#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, #REPLACE_S_KEYS_REQ, #UPP_OP_PROF1)</bpp></pre> MTD_GENERATE_BPP overriding:					
	For this test s protection.	sequence <s_mac> SHALL be us</s_mac>	ed instead of <ppk_mac> for UPP SCP0</ppk_mac>	3t		
IC3	Execute the s	step IC3 of the Test Sequence #03	defined in this section			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands			
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands			
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands			
IC7	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands			
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 with the response data #R_PIR_SECU_INVALID for one of the STORE DATA commands The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ55_048 RQ31_173		
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(resp ProfileInfoListResponse ::= profileInfoListOk :{}	RQ32_071 RQ55_048		

V1.4 Page 74 of 777

	#ICCID_OP_PROF1,	SW=0x9000	
	NO_PARAM))		

Test Sequence #05 Error: S-ENC used instead of PPK-ENC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>			
IC2	#S_INIT_S #CONF_IS #METADAT	DP_PROF1, FA_OP_PROF1, E_S_KEYS_REQ,			
		RATE_BPP overriding: sequence <s_enc> SHALL be use</s_enc>	ed instead of <ppk_enc> for UPP SCP0</ppk_enc>	3t	
IC3	Execute the s	step IC3 of the Test Sequence #03	defined in this section		
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands		
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands		
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands		
IC7	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a2>)</bpp_seg_a2>	SW=0x9000 without response data for all STORE DATA commands		
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 with the response data #R_PIR_SECU_INVALID for one of the STORE DATA commands The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ55_048 RQ31_173	
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{} SW=0x9000	RQ32_071 RQ55_048	

Test Sequence #06 Error: Profile Downloading stopped by a Reset

Initial Conditions	
Entity	Description of the initial condition
eUICC	No pending Notification is present on the eUICC

V1.4 Page 75 of 777

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>				
IC2	#S_INIT_S #CONF_IS #METADA ⁻ NO_PARAI	<pre><bpp> = MTD_GENERATE_BPP (#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				
IC3	Execute the s	step IC3 of the Test Sequence #01	defined in this section			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands			
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands			
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands			
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except the last one. Step 2 SHALL be triggered before sending the last STORE DATA	RQ25_023		
2	PROC_EUICC_INITIALIZATION_SEQUENCE					
3	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR					
4	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{} SW=0x9000	RQ32_071 RQ55_048		

Test Sequence #07 Nominal: ICCID in the 'ProfileHeader' PE is ignored by the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC2	#S_INIT_S(#CONF_ISI #METADAT NO_PARAN #UPP_OP_	DP_PROF1, TA_OP_PROF1 M, PROF1) ROF1 overriding:	to #ICCID_OP_PROF2 in the <i>ProfileHe</i> ad	<i>ler</i> element
IC3		P> into several segments arrays n EG_INIT>	amed:	

V1.4 Page 76 of 777

	 <bpp_seg_a0></bpp_seg_a0> <bpp_seg_a1></bpp_seg_a1> <bpp_seg_a3></bpp_seg_a3>			
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands	
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA. <isd_p_aid> SHALL be in the range as defined SGP.02 [1].</isd_p_aid>	RQ25_023 RQ25_024 RQ55_045 RQ55_048 RQ25_025 RQ25_026 RQ55_044
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { iccid #ICCID_OP_PROF1, isdpAid <isd_p_aid>, profileState disabled, } } SW=0x9000</isd_p_aid>	RQ32_071 RQ55_048

Test Sequence #08 Nominal: With gid1 and gid2 set

The purpose of this test is to verify that an Operational Profile configured with gid1 and gid2 can be downloaded on the eUICC.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL9 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>				
IC2	<bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1,</bpp>				

V1.4 Page 77 of 777

Non-confidential

	#CONF_ISDP_PROF1, #METADATA_OP_PROF9, NO_PARAM, #UPP_OP_PROF9)			
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>			
IC4	S_LPAd → eUICC	Ad → MTD_STORE_DATA_SCRIP SW=0x9000 without response data		
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIP T(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIP T(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIP T(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK_PROF9 for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024 RQ55_045_ 2
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_OWNERS)	resp ProfileInfoListResponse ::= profileInfoListOk :{ { profileOwner { mccMnc #MCC_MNC9, gid1 #GID1, gid2 #GID2 } } } SW=0x9000	RQ32_071

Test Sequence #09 Error: gid1 and gid2 provided in the Profile Metadata but not in the Profile Package

The purpose of this test is to verify that if gid1 and gid2 are provided in the Profile Metadata but ef-gid1 and ef-gid2 are not present and the related services (17 and 18) in ef-ust are not available, the eUICC returns an error during the LoadProfileElements process.

V1.4 Page 78 of 777

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC

Ste p	Directio n	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC2	#S_INIT_S #CONF_IS #METADA NO_PARAI	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP1_GID1GID2_PRESENT, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>		
IC3	<bpp_s< li=""><bpp_s< li=""></bpp_s<></bpp_s<>	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>		
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 with the response data #R_PIR_DATA_MISMATCH for one of the STORE DATA commands The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024 RQ55_045 RQ55_048 RQ25_025 RQ25_026 RQ55_045_ 2
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{} SW=0x9000	RQ32_071 RQ55_048

Test Sequence #10 Error: gid1 and gid2 not provided in the Profile Metadata but present in Profile Package

The purpose of this test is to verify that if gid1 and gid2 are not provided in the Profile Metadata but ef-gid1 and ef-gid2 are present and the related services (17 and 18) in ef-ust are available, the eUICC returns an error during the LoadProfileElements process.

V1.4 Page 79 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL9 is not loaded on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>			
IC2	#S_INIT_S #CONF_IS #METADAT NO_PARAI	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP9_GID1GID2_MISSING, NO_PARAM, #UPP_OP_PROF9)</bpp></pre>		
IC3	<bpp_s< li=""><bpp_s< li=""><bpp_s< li=""></bpp_s<></bpp_s<></bpp_s<>	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>		
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 with the response data #R_PIR_DATA_MISMATCH for one of the STORE DATA commands The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA	RQ25_023 RQ25_024 RQ55_045 RQ55_048 RQ25_025 RQ25_026 RQ55_045_3
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF9, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{} SW=0x9000	RQ32_071 RQ55_048

4.2.8 ES10a (LPA -- eUICC): GetEuiccConfiguredAddresses

4.2.8.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

• RQ31_066

V1.4 Page 80 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

- RQ33_021_1
- RQ57_017, RQ57_018, RQ57_019

4.2.8.2 Test Cases

4.2.8.2.1 TC_eUICC_ES10a.GetEuiccConfiguredAddresses

Test Sequence #01 Nominal: Only Root SM-DS Address

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Default SM-DP+ address has been set on the ISD-R

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADDRESS ES)	#R_ES10a_GECA_DS SW = 0x9000	RQ57_017 RQ57_018 RQ57_019 RQ33_021 _1

Test Sequence #02 Nominal: Root SM-DS and Default SM-DP+ Addresses

Initial Conditions	
Entity	Description of the initial condition
eUICC	The ISD-R is provisioned with the Default SM-DP+ Address #TEST_DP_ADDRESS1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_IN	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADD RESSES)	#R_ES10a_GECA_DS_DP_1 SW = 0x9000	RQ57_017 RQ57_018 RQ57_019 RQ31_066 RQ33_021_1

4.2.9 ES10a (LPA -- eUICC): SetDefaultDpAddress

4.2.9.1 Conformance Requirements

References

V1.4 Page 81 of 777

GSMA RSP Technical Specification [2]

Requirements

- RQ33_021_4, RQ33_021_5
- RQ57_020, RQ57_021, RQ57_022, RQ57_023, RQ57_024

4.2.9.2 Test Cases

4.2.9.2.1 TC_eUICC_ES10a.SetDefaultDpAddress

Test Sequence #01 Nominal: Set SM-DP+ Address with Address Empty in eUICC

Initial Conditions	
Entity	Description of the initial condition
eUICC	No value is assigned to the Default SM-DP+ Address field.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SELECT_ISDF	₹	
1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_EUICC_CONFIGURED_ADDRES S_1)	#R_ES10a_SD_DP_A_OK SW = 0x9000	RQ57_020 RQ57_021 RQ57_023 RQ57_024 RQ33_021_ 4
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADDRES SES)	#R_ES10a_GECA_DS_DP _1 SW = 0x9000	RQ57_020 RQ57_021 RQ57_023 RQ57_024 RQ33_021_ 5

Test Sequence #02 Nominal: Set SM-DP+ Address with SM-DP+ Address already in eUICC

Initial Conditions	
Entity	Description of the initial condition
eUICC	The SM-DP+ address #TEST_DP_ADDRESS1 is provisioned

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_ISDF	र	

V1.4 Page 82 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_EUICC_CONFIGURED_ADDRES S_2)	#R_ES10a_SD_DP_A_OK SW = 0x9000	RQ57_020 RQ57_021 RQ57_023 RQ57_024 RQ33_021 _4
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADDRES SES)	#R_ES10a_GECA_DS_DP _2 SW = 0x9000	RQ57_020 RQ57_021 RQ57_023 RQ57_024 RQ33_021 _5

Test Sequence #03 Nominal: Set Empty SM-DP+ Address with SM-DP+ Address already in eUICC

Initial Conditions	
Entity	Description of the initial condition
eUICC	The SM-DP+ address #TEST_DP_ADDRESS1 is provisioned

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_ISDF	₹	
1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_EUICC_CONFIGURED_ADDRES S_EMPTY)	#R_ES10a_SD_DP_A_OK SW = 0x9000	RQ57_022 RQ57_023 RQ57_024 RQ33_021 _4
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADDRES SES)	#R_ES10a_GECA_DS SW = 0x9000	RQ57_022 RQ57_023 RQ57_024 RQ33_021 _5

Test Sequence #04 Nominal: Set Empty SM-DP+ Address with Empty SM-DP+ Address in eUICC

Initial Conditions	
Entity	Description of the initial condition
eUICC	No value is assigned to the Default SM-DP+ Address field.

Step	tep Direction Sequence / Description		Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SELECT_ISDR		

V1.4 Page 83 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_EUICC_CONFIGURED_ADDRESS _EMPTY)	#R_ES10a_SD_DP_A_ OK SW = 0x9000	RQ57_022 RQ57_023 RQ57_024 RQ33_021 _4
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADDRESS ES)	#R_ES10a_GECA_DS SW = 0x9000	RQ57_022 RQ57_023 RQ57_024 RQ33_021 _5

4.2.10 ES10b (LPA -- eUICC): PrepareDownload

4.2.10.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26_011, RQ26_029, RQ26_030, RQ26_034, RQ26_035
- RQ31_062, RQ31_130, RQ31_131, RQ31_132, RQ31_133, RQ31_134, RQ31_135,
 RQ31_136, RQ31_137, RQ31_138, RQ31_139, RQ31_140, RQ31_141
- RQ45_006, RQ45_026_1, RQ45_026, RQ45_028, RQ45_030
- RQ57_025, RQ57_026, RQ57_027, RQ57_028, RQ57_029, RQ57_030, RQ57_031,
 RQ57_033, RQ57_034, RQ57_035, RQ57_036, RQ57_037, RQ57_038, RQ57_039

4.2.10.2 Test Cases

4.2.10.2.1TC_eUICC_ES10b.PrepareDownloadNIST

General Initial Condit	General Initial Conditions			
Entity	Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC			
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.			
eUICC	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+			
eoicc	#GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC			
	the same GSMA CI based on NIST P-256 curve has been chosen for signing and for verification			

Test Sequence #01 Nominal: Without Confirmation Code

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_NO_CC)	#R_PREP_DOWNLOAD_NO_CC SW=0x9000	RQ31_130 RQ31_131 RQ31_132 RQ31_133

V1.4 Page 84 of 777

		The <euicc_signature2> SHALL</euicc_signature2>	RQ31_134
		be verified with the	RQ31_135
		#PK_EUICC_ECDSA.	RQ31_139
		Verify that the	RQ31_140
		<s_transaction_id> present in</s_transaction_id>	RQ31_141
	the euiccSigned2 is the same as in	RQ57_025	
		#PREP_DOWNLOAD_NO_CC.	RQ57_026
		RQ57_027	
			RQ57_028
			RQ57_029
			RQ57_030
			RQ57_034
			RQ57_035
			RQ57_036
			RQ57_037
			RQ57_038
			RQ57_039
			RQ26_029
			RQ26_030
			RQ26_011
			RQ26_034
			RQ26_035
			RQ31_062

Test Sequence #02 Nominal: With Confirmation Code

Step	Direction	Sequence / Description	Expected result	REQ
IC1	<s_hashed <s_transa< td=""><td>D_CC> = MTD_GENERATE_HASHEI CTION_ID>)</td><td>D_CC(#CONFIRMATION_CODE1,</td><td></td></s_transa<></s_hashed 	D_CC> = MTD_GENERATE_HASHEI CTION_ID>)	D_CC(#CONFIRMATION_CODE1,	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_WITH_CC)	#R_PREP_DOWNLOAD_WITH_CC SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC.</s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_036 RQ57_035 RQ57_036 RQ57_037 RQ57_036 RQ57_037 RQ57_038 RQ57_037 RQ57_038 RQ57_039 RQ26_029 RQ26_029 RQ26_030 RQ26_011 RQ26_031 RQ26_035 RQ31_062

V1.4 Page 85 of 777

Test Sequence #03 Nominal: With an unknown otPK.EUICC.ECKA

The purpose of this test is to verify that the eUICC does not use the one-time key pair given by the SM-DP+ when its value does not correspond to a stored one-time key pair. In this case, the eUICC SHALL generate a new set of key.

Step	Direction	Sequence / Description	Expected result	REQ			
IC1	<s_hashed_cc> = MTD_GENERATE_HASHED_CC(#CONFIRMATION_CODE1, <s_transaction_id>)</s_transaction_id></s_hashed_cc>						
IC2	S_SM-DP+ g	enerates a random <otpk_euicc_e< td=""><td>CKA></td><td></td></otpk_euicc_e<>	CKA>				
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_RETRY_CC)	#R_PREP_DOWNLOAD_WITH_CC SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_CC. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_CC. Verify that the <otpk_euicc_ecka> present in the euiccSigned2 is not the same as in #PREP_DOWNLOAD_RETRY_CC.</otpk_euicc_ecka></s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ31_138 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_036 RQ57_035 RQ57_035 RQ57_035 RQ57_036 RQ57_037 RQ57_038 RQ57_037 RQ57_038 RQ57_039 RQ57_030			

4.2.10.2.2TC_eUICC_ES10b.PrepareDownloadBRP

General Initial Conditions				
Entity	Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC			
eUICC	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R. Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+ • #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC • the same GSMA CI based on BrainpoolP256r1 curve has been chosen for signing and for verification			

V1.4 Page 86 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #01 Nominal: Without Confirmation Code

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.2.10.2.1 – TC_eUICC_ES10b.PrepareDownloadNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #02 Nominal: With Confirmation Code

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.2.10.2.1 – TC_eUICC_ES10b.PrepareDownloadNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #03 Nominal: With an unknown otPK.EUICC.ECKA

This test sequence SHALL be the same as the Test Sequence #03 defined in section 4.2.10.2.1 – TC_eUICC_ES10b.PrepareDownloadNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.2.10.2.3TC_eUICC_ES10b.PrepareDownloadFRP

This test case is defined as FFS and not applicable for this version of test specification.

4.2.10.2.4TC_eUICC_ES10b.PrepareDownloadErrorCases

General Initial Conditions				
Entity	Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC			
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.			
eUICC	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+			
	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 			

Test Sequence #01 Error: No Hashed Confirmation Code but with Confirmation Code Required Flag set to TRUE

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	<pre><s_hashed_cc> = MTD_GENERATE_HASHED_CC(#CONFIRMATION_CODE1, <s_transaction_id>)</s_transaction_id></s_hashed_cc></pre>				
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_INVALID_CC)	SW different from 0x9000 without response data or SW=0x9000 with a response data containing a downloadResponseError	RQ31_130 RQ31_135 RQ31_136 RQ57_031 RQ57_036 RQ57_037	

V1.4 Page 87 of 777

		RQ57_038
		RQ31_136

Test Sequence #02 Error: With incorrect CERT.DPpb.ECDSA (i.e. invalid signature)

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_INV_CERT)	#R_PREP_DOWNLOAD_INV_CERT SW=0x9000 Verify that the <s_transaction_id> present in the response is the same as in #PREP_DOWNLOAD_INV_CERT.</s_transaction_id>	RQ31_130 RQ31_131 RQ31_136 RQ57_027 RQ57_030 RQ57_031 RQ57_036 RQ57_037 RQ57_038 RQ31_136 RQ45_006 RQ45_026_1 RQ45_026 RQ45_026

Test Sequence #03 Error: CERT.DPpb.ECDSA and CERT.DPauth.ECDSA not belonging to the same entity

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_CERT_SMDP2)	#R_PREP_DOWNLOAD_INV _CERT SW=0x9000 Verify that the <s_transaction_id> present in the response is the same as in #PREP_DOWNLOAD_CERT _SMDP2.</s_transaction_id>	RQ31_130 RQ31_132 RQ31_136 RQ57_029 RQ57_031 RQ57_036 RQ57_037 RQ57_038 RQ31_136 RQ45_006 RQ45_026 _1 RQ45_026 RQ45_028

Test Sequence #04 Error: With invalid SM-DP+ signature

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_INV_SIGN)	#R_PREP_DOWNLOAD_INV_SIGN SW=0x9000 Verify that the <s_transaction_id> present in the response is the same as in #PREP_DOWNLOAD_INV_SIGN.</s_transaction_id>	RQ31_130 RQ31_133 RQ31_136 RQ57_028 RQ57_031 RQ57_036 RQ57_038 RQ31_136 RQ45_006 RQ45_026_1

V1.4 Page 88 of 777

	RQ45_026
	RQ45_028

Test Sequence #05 Error: With invalid Transaction ID

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_INV_TRANS_I D)	#R_PREP_DOWN_INV_TRA NS_ID SW=0x9000 The transactionId returned in the response SHALL not be checked (any value SHALL be accepted)	RQ31_130 RQ31_134 RQ31_136 RQ57_025 RQ57_031 RQ57_036 RQ57_037 RQ57_038 RQ31_136

Test Sequence #06 Error: SM-DP+ has not been previously authenticated

Initial Conditions	
Entity Description of the initial condition	
eUICC	No Common Mutual Authentication procedure has been executed between the eUICC and the S_SM-DP+
	(this condition overrides the last general initial condition defined in this test case)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELEC	Γ_ISDR	
IC3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the highest priority CI from <euicc_ci_pk_id_list_fo r_verification=""> and choose #CERT_S_SM_DPpb_ECDS A according to this CI curve.</euicc_ci_pk_id_list_fo>	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_NO_AUTH)	#R_PREP_DOWN_NO_SES SION SW=0x9000 The transactionId returned in the response SHALL not be checked (any value SHALL be accepted)	RQ31_130 RQ31_136 RQ57_031 RQ57_026 RQ57_036 RQ57_037 RQ57_038

V1.4 Page 89 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #07 Error: Unsupported curve

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWN_INV_CURVE)	#R_PREP_DOWN_INV_CURVE SW=0x9000 Verify that the <s_transaction_id> present in the response is the same as in #PREP_DOWN_INV_CURVE.</s_transaction_id>	RQ31_130 RQ31_134 RQ31_136 RQ57_025 RQ57_031 RQ57_036 RQ57_037 RQ57_038 RQ31_136 RQ45_006 RQ45_026 _1 RQ45_026 RQ45_028

Test Sequence #08 Error: Invalid Certificate Role OID

The purpose of this sequence is to make sure that the eUICC refuses any SM-DP+ Certificate for Profile Package Binding that does not indicate "id-rspRole-dp-pb" in its extension for Certificate Policies.

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#PREP_DOWNLOAD_INV_OI D)	#R_PREP_DOWNLOAD_INV_CERT SW=0x9000 Verify that the <s_transaction_id> present in the response is the same as in #PREP_DOWNLOAD_INV_OID.</s_transaction_id>	RQ31_130 RQ31_131 RQ31_136 RQ57_027 RQ57_030 RQ57_031 RQ57_036 RQ57_037 RQ57_038 RQ31_136 RQ45_006 RQ45_026 _1 RQ45_026 RQ45_028 RQ45_028 RQ45_030

4.2.11 ES10b (LPA -- eUICC): LoadBoundProfilePackage

4.2.11.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_010, RQ24_028
- RQ25_003, RQ25_007, RQ25_016, RQ25_018, RQ25_019, RQ25_023, RQ25_024
- RQ26_011, RQ26_012, RQ26_013, RQ26_016, RQ26_018, RQ26_019, RQ26_020,

V1.4 Page 90 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

- RQ26_021, RQ26_022, RQ26_029, RQ26_034, RQ26_035, RQ26_036
- RQ31_161, RQ31_162, RQ31_163, RQ31_164, RQ31_165, RQ31_166, RQ31_168, RQ31_169, RQ31_170, RQ31_171, RQ31_185, RQ31_186_1, RQ31_188_1
- RQ32_070
- RQ35_003_1
- RQ44 003
- RQ55_001, RQ55_002, RQ55_003, RQ55_006, RQ55_007, RQ55_008, RQ55_016, RQ55_017, RQ55_018, RQ55_020, RQ55_021, RQ55_022, RQ55_024, RQ55_025, RQ55_028, RQ55_033, RQ55_036, RQ55_037, RQ55_039, RQ55_040, RQ55_041
- RQ57_010, RQ57_011, RQ57_012, RQ57_013, RQ57_014, RQ57_016, RQ57_040, RQ57_042, RQ57_043, RQ57_044, RQ57_045
- RQD0_001
- RQG0_001, RQG0_002, RQG0_003, RQG0_004, RQG0_005, RQG0_006

4.2.11.2 Test Cases

4.2.11.2.1TC_eUICC_ES10b.LoadBoundProfilePackageNIST

General Initial Condition	s
Entity	Description of the general initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.
	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+
eUICC	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI based on NIST P-256 curve has been chosen for signing and for verification
	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+
	#PREP_DOWNLOAD_NO_CC has been sent to the eUICC

Test Sequence #01 Nominal: By using S-ENC and S-MAC

The purpose of this test is to download the PROFILE_OPERATIONAL1 by using only the session S-ENC and S-MAC keys resulting from key agreement.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>			
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>				

V1.4 Page 91 of 777

Split the <BPP> into several segments arrays named:

- <BPP_SEG_INIT>
- <BPP_SEG_A0>
- <BPP_SEG_A1>
- <BPP_SEG_A3>

NOTE: In this test sequence, the data resulting of this operation SHALL be composed of the following TLV arrays:

IC3

- <BPP_SEG_INIT> contains the tag and length fields of the BoundProfilePackage TLV plus the #S_INIT_SC_PROF1 command
- <BPP_SEG_A0> contains the tag and length fields of the firstSequenceOf87 TLV plus the first 0x87 TLV containing #CONF_ISDP_PROF1 command
- <BPP_SEG_A1> contains the tag and length fields of the sequenceOf88 TLV and each of the '88' TLVs containing #METADATA_OP_PROF1 command
- <BPP_SEG_A3> contains the tag and length fields of the sequenceOf86 TLV and each of the
 '86' TLVs containing #UPP_OP_PROF1 protected with <S_ENC> and <S_MAC>

	86 1	LVS containing #UPP_UP_PRUF	1 protected with <s_enc> and <s_mac< th=""><th><u> </u></th></s_mac<></s_enc>	<u> </u>
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014 RQ26_029 RQ31_162 RQ31_163 RQ31_164 RQ55_003 RQ55_016 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_010 RQ55_017 RQ55_018 RQ55_010 RQ55_017 RQ55_018 RQ55_010 RQ55_010 RQ55_010 RQ55_010 RQ55_010 RQ55_010 RQ55_010 RQ55_010 RQ55_010 RQ55_020 RQ55_021
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014

V1.4 Page 92 of 777

				RQ26_029 RQ31_165 RQ55_028 RQ26_012 RQ26_013 RQ26_016 RQ26_019 RQ26_036 RQ31_161 RQG0_001 RQG0_002 RQG0_003 RQG0_003 RQG0_004 RQG0_005 RQG0_006
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014 RQ26_029 RQ31_166 RQ55_033 RQ55_036 RQ55_037 RQ24_028 RQ26_012 RQ26_013 RQ26_018 RQ26_018 RQ26_018 RQ26_019 RQ26_019 RQ26_019 RQ26_036 RQ31_161 RQG0_005 RQG0_006
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA. <isd_p_aid> SHALL be in the range as defined SGP.02 [1].</isd_p_aid>	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014 RQ26_029 RQ31_170 RQ31_171 RQ57_045

V1.4 Page 93 of 777

				RQ55_008 RQ25_003 RQ25_007 RQ25_018 RQ25_019 RQ25_023 RQ25_024 RQ55_025 RQ25_016 RQ26_012 RQ26_013 RQ26_016 RQ26_018 RQ26_019 RQ26_034 RQ26_035 RQ26_036 RQ31_161 RQ35_003_ 1 RQ44_003 RQD0_001 RQG0_005 RQG0_006
5	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { iccid #ICCID_OP_PROF1, isdpAid <isd_p_aid>, profileState disabled, } } SW=0x9000</isd_p_aid>	RQ32_070 RQ55_025 RQ24_010 RQ26_020 RQ31_161 RQD0_001

Test Sequence #02 Nominal: By using PPK-ENC and PPK-MAC

The purpose of this test is to download the PROFILE_OPERATIONAL1 by using a new set of random session keys: PPK-ENC, PPK-MAC and Initial MAC chaining value.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Generate the	<otpk_s_sm_dp+_ecka> and</otpk_s_sm_dp+_ecka>	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>	
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, #REPLACE_S_KEYS_REQ, #UPP_OP_PROF1)</bpp></pre>			
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>			

V1.4 Page 94 of 777

- <BPP_SEG_A2>
- <BPP_SEG_A3>

NOTE: In this test sequence, the data resulting of this operation SHALL be composed of the following TLV arrays:

- <BPP_SEG_INIT> contains the tag and length fields of the BoundProfilePackage TLV plus the #S_INIT_SC_PROF1 command
- <BPP_SEG_A0> contains the tag and length fields of the firstSequenceOf87 TLV plus the first 0x87 TLV containing #CONF_ISDP_PROF1 command
- <BPP_SEG_A1> contains the tag and length fields of the sequenceOf88 TLV and each of the '88' TLVs containing #METADATA_OP_PROF1 command
- <BPP_SEG_A2> contains the tag and length fields of the secondSequenceOf87 TLV plus the first '87' TLV, containing the #REPLACE S_KEYS_REQ command
- <BPP_SEG_A3> contains the tag and length fields of the sequenceOf86 TLV and each of the
 '86' TLVs containing #UPP_OP_PROF1 protected with PPK-ENC and PPK-MAC

	.86	TLVs containing #UPP_OP_PROF	1 protected with PPK-ENC and PPK-MA	AC .
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014 RQ26_029 RQ31_162 RQ31_163 RQ31_164 RQ55_003 RQ55_016 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_010 RQ55_011 RQ55_010 RQ55_011 RQ55_021 RQ56_011 RQ26_013 RQ26_016 RQ26_034 RQ26_035 RQ31_161
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014 RQ57_014

V1.4 Page 95 of 777

	Ī	1		
				RQ31_165 RQ55_028 RQ26_012 RQ26_013 RQ26_016 RQ26_018 RQ26_019 RQ26_020 RQ26_036 RQ31_161 RQ26_013 RQ26_016 RQ26_034 RQ26_035 RQ31_161 RQ60_001 RQG0_001 RQG0_001 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005 RQG0_006
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014 RQ26_029 RQ31_166 RQ55_033 RQ55_036 RQ55_037 RQ26_012 RQ26_013 RQ26_018 RQ26_018 RQ26_019 RQ26_019 RQ26_019 RQ26_036 RQ31_161 RQG0_005 RQG0_006
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a2>)</bpp_seg_a2>	SW=0x9000 without response data for all STORE DATA commands	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_011 RQ57_012 RQ57_014

V1.4 Page 96 of 777

				RQ26_029 RQ31_168 RQ31_169 RQ55_039 RQ55_040 RQ55_041 RQ26_021 RQ26_012 RQ26_012 RQ26_018 RQ26_016 RQ26_018 RQ26_019 RQ26_036 RQ31_161 RQG0_005 RQG0_006
5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command The euiccSignPIR SHALL be verified with the #PK_EUICC_ECDSA. <isd_p_aid> SHALL be in the range as defined SGP.02 [1].</isd_p_aid>	RQ57_040 RQ57_042 RQ57_043 RQ57_044 RQ55_001 RQ55_002 RQ55_006 RQ55_007 RQ57_010 RQ57_011 RQ57_012 RQ57_014 RQ26_029 RQ31_170 RQ31_171 RQ57_045 RQ55_008 RQ25_003 RQ25_007 RQ25_018 RQ25_019 RQ25_019 RQ25_019 RQ25_019 RQ25_019 RQ25_023 RQ25_016 RQ26_012 RQ26_013 RQ26_012 RQ26_013 RQ26_035 RQ31_161 RQ35_003_1 RQ44_003 RQD0_001 RQG0_005 RQG0_006
6	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { iccid #ICCID_OP_PROF1, isdpAid <isd_p_aid>,</isd_p_aid>	RQ55_025 RQ32_070 RQ24_010 RQ26_020 RQ31_161 RQD0_001

V1.4 Page 97 of 777

		profileState disabled,	l
			l
		}	l
		}	l
		SW=0x9000	l

4.2.11.2.2TC_eUICC_ES10b.LoadBoundProfilePackageBRP

General Initial Condition	General Initial Conditions	
Entity	Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC	
eUICC	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R. Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+ • #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC • the same GSMA CI based on BrainpoolP256r1 curve has been chosen for signing and for verification Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ • #PREP_DOWNLOAD_NO_CC has been sent to the eUICC	

Test Sequence #01 Nominal: By using S-ENC and S-MAC

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.2.11.2.1 – TC_eUICC_ES10b.LoadBoundProfilePackageNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #02 Nominal: By using PPK-ENC and PPK-MAC

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.2.11.2.1 – TC_eUICC_ES10b. LoadBoundProfilePackageNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.2.11.2.3TC_eUICC_ES10b.LoadBoundProfilePackageFRP

This test case is defined as FFS and not applicable for this version of test specification.

4.2.11.2.4TC_eUICC_ES10b.LoadBoundProfilePackage_ErrorCases

General Initial Conditions			
Entity Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC		
eUICC	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.		
	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+		

V1.4 Page 98 of 777

#GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC
 the same GSMA CI has been chosen for signing and for verification
Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+
 #PREP_DOWNLOAD_NO_CC has been sent to the eUICC

Test Sequence #01 Error: Unrecognized leading tag in BPP

The purpose of this test is to ensure that the eUICC rejects any BPP segment with an unrecognized leading tag during Profile download. In such case, the eUICC SHALL return a SW of 0x6A88 and SHALL not discard the download session state.

Step	Direction	Sequence / Description	Expected result	REQ			
IC1	Generate the	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>					
IC2	#S_INIT_S #CONF_IS #METADA NO_PARA	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>					
IC3	 <bpp_s< li=""> <bpp_s< li=""></bpp_s<></bpp_s<>	PP> into several segments arrays na SEG_INIT> SEG_A0> SEG_A1> SEG_A3>	med:				
IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands				
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands	RQ31_186_1			
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#UNKNOWN_BPP_SEGMENT)	SW=0x6A88	RQ31_186_1 RQ57_013 RQ57_016			
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands	RQ31_186_1			
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a3>)</bpp_seg_a3>	SW=0x9000 without response data for all STORE DATA commands except for the last one SW=0x9000 with the response data #R_PIR_OK for the last STORE DATA command	RQ31_186_1			
4	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1,	resp ProfileInfoListResponse ::= profileInfoListOk :{				

V1.4 Page 99 of 777

	NO_PARAM))	{	
		iccid #ICCID_OP_PROF1, isdpAid <isd_p_aid>, profileState disabled,</isd_p_aid>	
		promestate disabled, 	
		}	
		}	
		SW=0x9000	

Test Sequence #02 Error: GetEUICCChallenge during BPP loading

The purpose of this test is to ensure that the eUICC accepts an ES10b.GetEUICCChallenge request indicating the start of a new RSP session while a BPP is loaded.

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Notification is stored in the eUICC's Pending Notifications List

Step	Direction	Sequence / Description	Expected result	REQ			
IC1	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>						
IC2	#S_INIT_SC #CONF_ISD #METADAT/ NO_PARAM	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>					
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>						
IC4	S_LPAd → eUICC						
IC5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands				
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 without response data for all STORE DATA commands				
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW=0x9000	RQ31_188_1			

V1.4 Page 100 of 777

Non-confidential

2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (<bpp_seg_a3>)</bpp_seg_a3>	SW=0x6A88 or 0x6985	RQ31_185 RQ57_013 RQ57_016
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{} SW=0x9000	RQ31_185
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ31_185

4.2.12 ES10b (LPA -- eUICC): GetEUICCChallenge

4.2.12.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_029, RQ31_030, RQ31_031
- RQ57_048, RQ57_049, RQ57_050

4.2.12.2 Test Cases

4.2.12.2.1TC_eUICC_ES10b.GetEUICCChallenge

Test Sequence #01 Nominal

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIA	ALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGIC	CAL_CHANNEL_AND_SELECT_	ISDR	
1	$S_LPAd \rightarrow eUICC$	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000	RQ31_029 RQ31_030 RQ31_031 RQ57_049 RQ57_050
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 <euicc_challenge> received in this step is different to the <euicc_challenge> in Step 1</euicc_challenge></euicc_challenge>	RQ57_048

4.2.13 ES10b (LPA -- eUICC): GetEUICCInfo

4.2.13.1 Conformance Requirements

References

V1.4 Page 101 of 777

GSMA RSP Technical Specification [2]

Requirements

- RQ31_027, RQ31_028, RQ31_053, RQ31_060
- RQ43_001, RQ43_002, RQ43_003, RQ43_004, RQ43_005, RQ43_006, RQ43_007, RQ43_008, RQ43_009, RQ43_010, RQ43_011, RQ43_012, RQ43_013
- RQ57_051, RQ57_052, RQ57_053, RQ57_054, RQ57_057_1, RQ57_058,
 RQ57_059, RQ57_060, RQ57_062, RQ57_061, RQ57_063, RQ57_064, RQ57_066

4.2.13.2 Test Cases

4.2.13.2.1TC_eUICC_ES10b.GetEUICCInfo1

Test Sequence #01 Nominal

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR					
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	RQ31_027, RQ31_028, RQ57_051, RQ57_052, RQ57_054		

Test Sequence #02 Nominal: GetEUICCInfo call after GetEUICCChallenge

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_I	NITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LO	OGICAL_CHANNEL_AND_SELEC	T_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	RQ31_027 RQ31_028 RQ57_051 RQ57_052 RQ57_054

Test Sequence #03 Nominal: GetEUICCInfo1 call after AuthenticateServer

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				

V1.4 Page 102 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_veri fication=""> from response data and verify if they contain at least one same GSMA CI Key ID</euicc_ci_pk_id_list_for_veri></euicc_ci_pk_id_list_for_sig>		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDP)	#R_AUTHENTICATE_SMDP SW = 0x9000		
5	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	RQ57_051	

4.2.13.2.2TC_eUICC_ES10b.GetEUICCInfo2_RSP_V2.1

Test Sequence #01 Nominal – RSP Version 2.1

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR					
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO2)	#R_EUICC_INFO2 Verify if: <ext_card_resource> contains a "number of installed application" value field set to '00' #IUT_TS102241_VERSION is equal to 0x090000 or higher #IUT_GLOBALPLATFORM_VERS ION is equal to 0x020300 or higher #RSP_SVN_H is equal to 0x020100 #IUT_SIMA_VERSION is equal to 0x020000 or to 0x020100 <euicc_rsp_capability> contains</euicc_rsp_capability></ext_card_resource>	RQ43_001 RQ43_002 RQ43_003 RQ43_004 RQ43_005 RQ43_006 RQ43_007 RQ43_008 RQ43_010 RQ43_011 RQ43_011 RQ43_012 RQ43_013 RQ57_057 _1 RQ57_060 RQ57_061 RQ57_063		

V1.4 Page 103 of 777

	0	crlSupport set to '0' if	RQ57_064
		O_E_CRL is not supported	RQ57_066
		(otherwise, it SHALL be set	
		to '1')	
	0	testProfileSupport set to '0' if	
		O_E_TEST_PROF is not	
		supported	
		(otherwise, it SHALL be set	
		to '1')	
	0	rpmSupport set to '0'	
	0	additionalProfile set to '1'	
	• #IUT	_UICC_CAPABILITY contains	
	0	javacard and akaMilenage	
		set to '1'	
	0	Either akaTuak128 or	
		akaTuak256 set to '1'	
	SW = 0x9	0000	

$4.2.13.2.3\ \mathsf{TC_eUICC_ES10b.GetEUICCInfo2_RSP_V2.2.x}$

Test Sequence #01 Nominal – RSP Version 2.2

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO2)	#R_EUICC_INFO2 Verify if: • <ext_card_resource> contains a "number of installed application" value field set to '00' • #IUT_TS102241_VERSION is equal to 0x090000 or higher • #IUT_GLOBALPLATFORM_VERSI ON is equal to 0x020300 or higher • #RSP_SVN_H is equal to 0x0202ab 'ab' representing the 'x' in version 2.2.x • #IUT_SIMA_VERSION is equal to 0x020100 • <euicc_rsp_capability> contains • crlSupport set to '0' if O_E_CRL is not supported (otherwise, it SHALL be set to '1') • testProfileSupport set to '0' if O_E_TEST_PROF is not supported (otherwise, it SHALL be set to '1') • rpmSupport set to '0' • additionalProfile set to '1'</euicc_rsp_capability></ext_card_resource>	RQ43_001 RQ43_002 RQ43_003 RQ43_004 RQ43_005 RQ43_006 RQ43_007 RQ43_010 RQ43_011 RQ43_012 RQ43_013 RQ57_057 _1 RQ57_060 RQ57_061 RQ57_061 RQ57_064 RQ57_066	

V1.4 Page 104 of 777

	• #	IUT_I	JICC_CAPABILITY contains	
		0	avacard and akaMilenage	
			set to '1'	
		0	Either akaTuak128 or	
			akaTuak256 set to '1'	
	SW = 0	0x90	00	

4.2.13.2.4TC_eUICC_ES10b.GetEUICCInfo2

Test Sequence #01 Nominal: GetEUICCInfo2 call after AuthenticateServer

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR					
IC3	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ve rification=""> from response data and verify if they contain at least one same GSMA CI Key ID</euicc_ci_pk_id_list_for_ve></euicc_ci_pk_id_list_for_sig>			
IC4	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>			
IC5	 <s_tran:< li=""> <euicc_0< li=""> <s_smdp< li=""> <s_smdp< li=""> Set the <e< li=""> <euicc_0< li=""> </euicc_0<></e<></s_smdp<></s_smdp<></euicc_0<></s_tran:<>	Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used>				
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTHENTICATE_SMDP)	T(#R_AUTHENTICATE_SMDP SW = 0x9000			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO2)	#R_EUICC_INFO2 same EUICCInfo2 data object as in Step IC6 SW = 0x9000	RQ57_051 RQ57_053 RQ57_054 RQ57_058 RQ57_059 RQ57_062 RQ31_053 RQ31_060 RQ43_001 RQ43_002		

V1.4 Page 105 of 777

4.2.14 ES10b (LPA -- eUICC): ListNotification

4.2.14.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ25_020
- RQ31_172
- RQ35 016
- RQ57_068, RQ57_068_1, RQ57_068_2, RQ57_068_3, RQ57_068_4, RQ57_069, RQ57_070

4.2.14.2 Test Cases

Throughout all the ListNotification test cases the maximum number of Notifications simultaneously tested has been set as to two as there is not minimum defined in SGP.21 [3] or SGP.22 [2] for the number of Notifications that can be stored by the eUICC.

4.2.14.2.1TC_eUICC_ES10b.ListNotification

General Initial Conditions			
Entity	Description of the general initial condition		
eUICC	No Operational Profile is installed on the eUICC		
eUICC	No Notifications are stored in the eUICC's Pending Notifications List		

Test Sequence #01 Nominal: Install Notification

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SEL	LECT_ISDR			
IC3	Install PROFI	LE_OPERATIONAL1. Do not remo	ve both the Notifications.			
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_IN1_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020 RQ31_172		
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_IN1_IN1_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070 RQ25_020		

V1.4 Page 106 of 777

3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_IN1_IN1_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENAB LE)	#R_LIST_NOTIF_IN1_IN1_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELE TE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENA BLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENAB LE_DISABLE)	#R_LIST_NOTIF_IN1_IN1_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020

V1.4 Page 107 of 777

Test Sequence #02 Nominal: Enable Notification

Step	Direction	Sequence / Description	Expected result	REQ			
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE						
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR						
IC3	Install PROFILE_OPERATIONAL1. Remove both the Notifications.						
IC4	Enable PROFI	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.					
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070 RQ31_172			
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070			
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ER ROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069			
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069			
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070			
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069			
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069			
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENA BLE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070			

V1.4 Page 108 of 777

9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DEL ETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENA BLE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENA BLE_DISABLE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070

Test Sequence #03 Nominal: Disable Notification

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
IC3	Install PROFIL	E_OPERATIONAL1. Remove both the	ne Notifications.			
IC4	Enable PROFI	LE_OPERATIONAL1. Remove the N	lotification.			
IC5	Disable PROF	ILE_OPERATIONAL1. Do not remov	e the Notification.			
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070 RQ31_172		
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070		
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069		
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069		
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1		

V1.4 Page 109 of 777

				RQ57_068_4 RQ57_069
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELET E)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENABL E)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E_DISABLE)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070

Test Sequence #04 Nominal: Delete Notification

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR		
IC3	Install PROFILE_OPERATIONAL1. Remove both the Notifications.				
IC4	Enable PROFILE_OPERATIONAL1. Remove the Notification.				
IC5	Disable PROFILE_OPERATIONAL1. Remove the Notification.				
IC6	Delete PROFILE_OPERATIONAL1. Do not remove the Notification.				
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070 RQ31_172	

V1.4 Page 110 of 777

2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELET E)	#R_LIST_NOTIF_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENABL E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE_DISABL E_DELETE)	#R_LIST_NOTIF_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070

V1.4 Page 111 of 777

Test Sequence #05 Nominal: Two Install Notifications (PIR) with different Notification Address

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR		
IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.				
IC4	Install PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_NO_INSTALL. The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions: • #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than #CERT_S_SM_DPauth_ECDSA • #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1 • #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA Do not remove the Notification.				
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR_IN2_ PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020 RQ31_172	
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_IN1_PIR_IN2_ PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070 RQ25_020	
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069	
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_IN1_PIR_IN2_ PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020	
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069	

V1.4 Page 112 of 777

6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E)	#R_LIST_NOTIF_IN1_PIR_IN2_ PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELET E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENABL E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E_DISABLE)	#R_LIST_NOTIF_IN1_PIR_IN2_ PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020

Test Sequence #06 Nominal: Install Notification (PIR) and Enable Notification

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC	C_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR		
IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.				
IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.				
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020 RQ31_172	

V1.4 Page 113 of 777

2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_IN1_PIR_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070 RQ25_020
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_IN1_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E)	#R_LIST_NOTIF_IN1_PIR_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELET E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENABL E)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070

V1.4 Page 114 of 777

11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E_DISABLE)	#R_LIST_NOTIF_IN1_PIR_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020
----	-------------------	--	--	--

Test Sequence #07 Nominal: Disable and Delete Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	Install PROFIL	E_OPERATIONAL1. Remove both the	ne notifications.	
IC4	Enable PROFI	LE_OPERATIONAL1. Remove the n	otification	
IC5	Disable PROF	ILE_OPERATIONAL1. Do not remov	e the notification	
IC6	Delete PROFII	LE_OPERATIONAL1. Do not remove	the Notification	
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070 RQ31_172
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_DI1_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070

V1.4 Page 115 of 777

7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELET E)	#R_LIST_NOTIF_DI1_DE1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENABL E)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E_DISABLE)	#R_LIST_NOTIF_DI1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070

Test Sequence #08 Nominal: Install (OtherSignedNotification) and Enable Notification

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELI	ECT_ISDR		
IC3	Install PROFIL OtherSignedNo	_	PIR notification, but do not remove the	ne	
IC4	Enable PROFI	LE_OPERATIONAL1. Do not remo	ve the Notification.		
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070 RQ31_172	
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_IN1_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070	
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069	

V1.4 Page 116 of 777

4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_IN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENAB LE)	#R_LIST_NOTIF_IN1_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELE TE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENAB LE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENAB LE_DISABLE)	#R_LIST_NOTIF_IN1_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070

Test Sequence #09 Nominal: Enable and Install (PIR) Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR	
IC3	Install PROFILE_OPERATIONAL1. Remove both notifications.			
IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.			
IC5	Install PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_NO_INSTALL.			

V1.4 Page 117 of 777

The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions:

- #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than #CERT_S_SM_DPauth_ECDSA
- #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1
- #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA

Do not remove the Notification.

	Do not remove the rectinisation.				
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1_IN2_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020 RQ31_172	
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_EN1_IN2_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_3 RQ57_069 RQ57_070 RQ25_020	
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069	
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_IN2_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020	
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070	
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069	
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069	

V1.4 Page 118 of 777

8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E)	#R_LIST_NOTIF_EN1_IN2_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELET E)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENABL E)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_069 RQ57_070
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENABL E_DISABLE)	#R_LIST_NOTIF_EN1_IN2_PIR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_2 RQ57_069 RQ57_070 RQ25_020

Test Sequence #10 Nominal: No Notifications available

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELE	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_OMITTED)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_3 RQ57_068_4 RQ57_069
3	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_NONE)	#R_LIST_NOTIF_NONE SW = 0x9000 OR #R_LIST_NOTIF_UNDEFINED_ ERROR SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1

V1.4 Page 119 of 777

				RQ57_068_4 RQ57_069
5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ENABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DELETE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENAB LE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_DELE TE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_DISABLE_ENAB LE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069
11	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_INSTALL_ENAB LE_DISABLE)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ35_016 RQ57_068 RQ57_068_1 RQ57_068_4 RQ57_069

4.2.15 ES10b (LPA -- eUICC): RetrieveNotificationsList

4.2.15.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ25_020, RQ25_021
- RQ26_034, RQ26_035
- RQ31_174
- RQ35_001_1, RQ35_001_2, RQ35_003_1
- RQ57_071, RQ57_071_1, Q57_071_2, RQ57_071_3, RQ57_071_4

V1.4 Page 120 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

 RQ57_072, RQ57_072_1, RQ57_072_2, RQ57_073, RQ57_074, RQ57_075, RQ57_076

4.2.15.2 Test Cases

Throughout all the RetrieveNotificationsList test cases the maximum number of Notifications simultaneously tested has been set to two as there is no minimum defined in SGP.21 [3] or SGP.22 [2] for the number of Notifications that can be stored by the eUICC.

In some test sequences defined below, it is expected to retrieve especially either a ProfileInstallationResult or an OtherSignedNotification for installation. When both are present in the eUICC, the only way to distinguish these two notifications is to compare their sequence numbers in the ListNotificationResponse. The sequence number related to the ProfileInstallationResult SHALL be lower than the one linked to the OtherSignedNotification.

This assumption is based on the requirement defined in section 5.5.5 of SGP.22 [2] stating that the eUICC SHALL first generate the Profile Installation Result and then as many Notifications as configured in its metadata in the format of OtherSignedNotification.

4.2.15.2.1TC_eUICC_ES10b.RetrieveNotificationsList

General Initial Conditions		
Entity Description of the general initial condition		
eUICC	No Operational Profile is installed on the eUICC	
eUICC No Notifications are stored in the eUICC's Pending Notifications List		

Test Sequence #01 Nominal: Retrieve by Sequence Number for Install Notification

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUIC	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR		
IC3	Install PROF	ILE_OPERATIONAL1. Do not rem	ove both the notifications.		
IC4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_IN1_PIR SW = 0x9000		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_in 1="">))</notif_seq_no_in>	#R_RETRIEVE_NOTIF_IN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	

V1.4 Page 121 of 777

				RQ35_001_2 RQ35_003_1
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_in 1_pir="">))</notif_seq_no_in>	#R_RETRIEVE_NOTIF_IN1_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1 RQ35_001_1 RQ35_001_2 RQ35_003_1

Test Sequence #02 Nominal: Retrieve by Sequence Number for Enable Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
IC3	Install PROF	ILE_OPERATIONAL1. Remove bo	oth the notifications.	
IC4	Enable PRO	FILE_OPERATIONAL1. Do not rer	move the Notification.	
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1 SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_e n1="">))</notif_seq_no_e>	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_2 RQ35_003_1

Test Sequence #03 Nominal: Retrieve by Sequence Number for Disable Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	Install PROFILE_OPERATIONAL1. Remove both the notifications.			
IC4	Enable PROFILE_OPERATIONAL1. Remove the Notification.			

V1.4 Page 122 of 777

IC5	Disable PROFILE_OPERATIONAL1. Do not remove the Notification.			
IC6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1 SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_di 1="">))</notif_seq_no_di>	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_2 RQ35_003_1

Test Sequence #04 Nominal: Retrieve by Sequence Number for Delete Notification

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUIC	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR			
IC3	Install PROF	ILE_OPERATIONAL1. Remove bo	oth the notifications.			
IC4	Enable PROF	FILE_OPERATIONAL1. Remove t	he Notification.			
IC5	Disable PRO	FILE_OPERATIONAL1. Remove t	the Notification.			
IC6	Delete PROF	ILE_OPERATIONAL1. Do not ren	nove the Notification.			
IC7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DE1 SW = 0x9000			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_d e1="">))</notif_seq_no_d>	#R_RETRIEVE_NOTIF_DE1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_2 RQ35_003_1		

Test Sequence #05 Nominal: Retrieve by Sequence Number for Two Install (PIR) Notifications with different Notification Addresses

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 123 of 777

Non-confidential

IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.				
IC4	Install PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_NO_INSTALL. The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions: • #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than #CERT_S_SM_DPauth_ECDSA • #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1 • #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA Do not remove the Notification.				
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR_IN2_ PIR SW = 0x9000		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_in 1_pir="">))</notif_seq_no_in>	#R_RETRIEVE_NOTIF_IN1_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_in 2_pir="">))</notif_seq_no_in>	#R_RETRIEVE_NOTIF_IN2_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	

Test Sequence #06 Nominal: Retrieve by Sequence Number for Install (PIR) and **Enable Notifications**

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.				

V1.4 Page 124 of 777

IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.				
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR_EN1 SW = 0x9000		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_in 1_pir="">))</notif_seq_no_in>	#R_RETRIEVE_NOTIF_IN1_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_e n1="">))</notif_seq_no_e>	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035	

Test Sequence #07 Nominal: Retrieve by Sequence Number for Disable and Delete Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
IC3	Install PROF	ILE_OPERATIONAL1. Remove bo	oth the notifications.	
IC4	Enable PROF	FILE_OPERATIONAL1. Remove t	he notification	
IC5	Disable PRO	FILE_OPERATIONAL1. Do not re	move the notification	
IC6	Delete PROFILE_OPERATIONAL1. Do not remove the Notification			
IC7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1_DE1 SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_di 1="">))</notif_seq_no_di>	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076

V1.4 Page 125 of 777

				RQ26_034 RQ26_035
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_d e1="">))</notif_seq_no_d>	#R_RETRIEVE_NOTIF_DE1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035

Test Sequence #08 Nominal: Retrieve by Sequence Number for Install (OtherSignedNotification) and Enable Notifications

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR			
IC3	Install PROFIL OtherSignedN	_	PIR notification, but do not remove the	ne		
IC4	Enable PROFI	LE_OPERATIONAL1. Do not rem	ove the Notification.			
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_EN1 SW = 0x9000			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_in 1="">))</notif_seq_no_in>	#R_RETRIEVE_NOTIF_IN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_1		
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SE Q_NUM(<notif_seq_no_e n1="">))</notif_seq_no_e>	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035		

V1.4 Page 126 of 777

Test Sequence #09 Nominal: Retrieve by Sequence Number for Enable and Install (PIR) notifications

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR		
IC3	Install PROFILE_OPERATIONAL1. Remove both notifications.				
IC4	Enable PROF	ILE_OPERATIONAL1. Do not remo	ove the Notification.		
IC5	The default Pr following exce • #CERT_S #CERT_S • #TEST_D • #CERT_S	#CERT_S_SM_DPauth_ECDSA • #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1 • #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA			
IC6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1_IN2_PIR SW = 0x9000		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SEQ _NUM(<notif_seq_no_in2_ pir="">))</notif_seq_no_in2_>	#R_RETRIEVE_NOTIF_IN2_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SEQ _NUM(<notif_seq_no_en1>))</notif_seq_no_en1>	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035	

Test Sequence #10 Nominal: Retrieve Sequence Numbers that are not present

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 127 of 777

IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.			
IC4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SEQ _NUM(<notif_seq_no_in1_ pir="">))</notif_seq_no_in1_>	#R_RETRIEVE_NOTIF_IN1_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ26_034 RQ26_035
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_RETRIEVE_NOTIF_SEQ _NUM(<notif_seq_no_in1_ pir=""> +1))</notif_seq_no_in1_>	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074

Test Sequence #11 Nominal: Retrieve by Notification Type for Install Notifications

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_	INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
IC3	Install PROFILE	_OPERATIONAL1. Do not remove	e both the notifications.		
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_IN1_IN1 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTED)	#R_RETRIEVE_NOTIF_IN1_IN1 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_3 RQ57_071_4 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076	

V1.4 Page 128 of 777

			Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_IN1_IN1 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_IN1_IN1 _PIR SW = 0x9000 • Verify the euiccNotificationSignature	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_1

V1.4 Page 129 of 777

			<tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_IN1_IN1 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_071_3 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1

Test Sequence #12 Nominal: Retrieve by Notification Type for Enable Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
IC3	Install PROFILE_OPERATIONAL1. Remove both the notifications.			
IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.			
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074

V1.4 Page 130 of 777

				RQ57_075 RQ57_076 RQ26_034 RQ26_035
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTED)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_4 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074

V1.4 Page 131 of 777

8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035

Test Sequence #13 Nominal: Retrieve by Notification Type for Disable Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
IC3	Install PROFI	Install PROFILE_OPERATIONAL1. Remove both the notifications.		
IC4	Enable PROFILE_OPERATIONAL1. Remove the Notification.			
IC5	Disable PRO	FILE_OPERATIONAL1. Do not re	move the Notification.	
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074

V1.4 Page 132 of 777

				,
				RQ57_075 RQ57_076 RQ26_034 RQ26_035
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTE D)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_4 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074

V1.4 Page 133 of 777

8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_DELETE)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_ENABLE)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035

Test Sequence #14 Nominal: Retrieve by Notification Type for Delete Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	Install PROFILE_OPERATIONAL1. Remove both the notifications.			
IC4	Enable PROFILE_OPERATIONAL1. Remove the Notification.			
IC5	Disable PROFILE_OPERATIONAL1. Remove the Notification.			
IC6	Delete PROFI	LE_OPERATIONAL1. Do not remo	ove the Notification.	

V1.4 Page 134 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_DE1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTED)	#R_RETRIEVE_NOTIF_DE1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_4 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_DE1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074

V1.4 Page 135 of 777

				RQ57_075 RQ57_076 RQ26_034 RQ26_035
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _DELETE)	#R_RETRIEVE_NOTIF_DE1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074

Test Sequence #15 Nominal: Retrieve by Notification Type for Two Install (PIR) Notifications with different Notification Addresses

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR		
IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.				
IC4	Install PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_NO_INSTALL. The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions: • #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than				
	#CERT_S_SM_DPauth_ECDSA • #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1				

V1.4 Page 136 of 777

	#CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA			
	Do not remove	the Notification.		
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_IN1_PIR _IN2_PIR SW = 0x9000 • Verify both the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTE D)	#R_RETRIEVE_NOTIF_IN1_PIR _IN2_PIR SW = 0x9000 • Verify both the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_072_4 RQ57_073_1 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_IN1_PIR _IN2_PIR SW = 0x9000 • Verify both the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1

V1.4 Page 137 of 777

				RQ57_073 RQ57_074
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_IN1_PIR _IN2_PIR SW = 0x9000 • Verify both the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABLE _ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_IN1_PIR _IN2_PIR SW = 0x9000 • Verify both the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1

Test Sequence #16 Nominal: Retrieve by Notification Type for Install (PIR) and Enable Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.			

V1.4 Page 138 of 777

IC4	Enable PROI	FILE_OPERATIONAL1. Do not rer	move the Notification.	
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_IN1_PIR _EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTE D)	#R_RETRIEVE_NOTIF_IN1_PIR _EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_IN1_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076

V1.4 Page 139 of 777

				RQ26_034 RQ26_035
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_IN1_PIR _EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_IN1_PIR _EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1

V1.4 Page 140 of 777

Test Sequence #17 Nominal: Retrieve by Notification Type for Disable and Delete Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
IC3	Install PROFI	LE_OPERATIONAL1. Remove bo	oth the notifications.	
IC4	Enable PROF	FILE_OPERATIONAL1. Remove to	he notification	
IC5	Disable PROFILE_OPERATIONAL1. Do not remove the notification			
IC6	Delete PROF	ILE_OPERATIONAL1. Do not rem	nove the Notification	
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_DI1_DE1 SW = 0x9000 • Verify both the euiccNotificationSignatures <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTE D)	#R_RETRIEVE_NOTIF_DI1_DE1 SW = 0x9000 • Verify both the euiccNotificationSignatures <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_4 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_074
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075

V1.4 Page 141 of 777

				RQ57_076 RQ26_034 RQ26_035
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_DE1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_DELETE)	#R_RETRIEVE_NOTIF_DI1_DE1 SW = 0x9000 • Verify both the euiccNotificationSignatures <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_ENABLE)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_DI1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035

Test Sequence #18 Nominal: Retrieve by Notification Type for Install (OtherSignedNotification) and Enable Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			

V1.4 Page 142 of 777

IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	Install PROFILE_OPERATIONAL1. Remove the PIR notification, but do not remove the OtherSignedNotification.			
IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.			
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_IN1_EN1 SW = 0x9000 • Verify both the euiccNotificationSignatures <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_1
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTE D)	#R_RETRIEVE_NOTIF_IN1_EN1 SW = 0x9000 • Verify both the euiccNotificationSignatures <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_1
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_IN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_1
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1

V1.4 Page 143 of 777

				RQ57_073 RQ57_074
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_IN1_EN1 SW = 0x9000 • Verify both the euiccNotificationSignatures <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_1
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_IN1_EN1 SW = 0x9000 • Verify both the euiccNotificationSignatures <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035 RQ35_001_1

Test Sequence #19 Nominal: Retrieve by Notification Type for Enable and Install (PIR) notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	Install PROFILE_OPERATIONAL1. Remove both notifications.			

V1.4 Page 144 of 777

IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.				
IC5	Install PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_NO_INSTALL. The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions: • #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than #CERT_S_SM_DPauth_ECDSA • #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1 • #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA Do not remove the Notification.				
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_EN1_IN2 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTE D)	#R_RETRIEVE_NOTIF_EN1_IN2 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_072_4 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1	
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074	
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_IN2_PIR SW = 0x9000 • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ25_020 RQ25_021	

V1.4 Page 145 of 777

				RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_EN1_IN2 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_ENABLE)	#R_RETRIEVE_NOTIF_EN1 SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ26_034 RQ26_035

V1.4 Page 146 of 777

11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_EN1_IN2 _PIR SW = 0x9000 • Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir></tbs_euicc_notif_sig>	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_072_3 RQ57_073_1 RQ57_074 RQ57_075 RQ57_076 RQ25_020 RQ25_021 RQ26_034 RQ26_035 RQ31_174 RQ35_001_1
----	----------------	--	--	--

Test Sequence #20 Nominal: Retrieve by Notification Type for No Notifications available

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUIC	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ALL)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074		
2	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_OMITTE D)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_072_4 RQ57_073 RQ57_074		
3	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_NONE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074		
4	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074		
5	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074		
6	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074		

V1.4 Page 147 of 777

7	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
8	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
9	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_DELETE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
10	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_DISABL E_ENABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074
11	S_LPAd → eUICC	MTD_STORE_DATA(#RETRIEVE_NOTIF_INSTALL _ENABLE_DISABLE)	#R_RETRIEVE_NOTIF_NONE SW = 0x9000	RQ57_071 RQ57_072 RQ57_072_1 RQ57_073 RQ57_074

4.2.16 ES10b (LPA -- eUICC): RemoveNotificationFromList

4.2.16.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ25_020
- RQ31_182
- RQ35 021
- RQ57_077, RQ57_078, RQ57_079

4.2.16.2 Test Cases

Throughout all the RemoveNotificationFromList test cases the maximum number of Notifications simultaneously tested has been set as to two as there is no minimum defined in SGP.21 [3] or SGP.22 [2] for the number of Notifications that can be stored by the eUICC.

The rule specified in section 4.2.15.2 explaining the way to distinguish a ProfileInstallationResult from an OtherSignedNotification for installation also applies for the test cases defined below.

V1.4 Page 148 of 777

${\bf 4.2.16.2.1TC_eUICC_ES10b.} Remove Notification From List$

General Initial Conditions		
Entity	Description of the general initial condition	
eUICC	No Operational Profile is installed on the eUICC	
eUICC	No Notifications are stored in the eUICC's Pending Notifications List	

Test Sequence #01 Nominal: Install Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELE	CT_ISDR	
IC3	Install PROFIL	E_OPERATIONAL1. Do not remove	e both the notifications.	
IC4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_IN1_PIR SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1>))</notif_seq_no_in1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR SW = 0x9000	
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir>))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079 RQ31_182
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ25_020 RQ31_182

Test Sequence #02 Nominal: Enable Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SELECT_ISE	DR	
IC3	Install PROFILE_OPERATIONAL1. Remove both the notifications.			
IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.			
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1 SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_en1>))</notif_seq_no_en1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079

V1.4 Page 149 of 777

2 S_LPAd → MTD_STORE_DATA(#R_LIST_NOTIF_NONE SW = 0x9000	
---	--

Test Sequence #03 Nominal: Disable Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELI	ECT_ISDR	
IC3	Install PROFIL	LE_OPERATIONAL1. Remove both	the notifications.	
IC4	Enable PROF	ILE_OPERATIONAL1. Remove the	Notification.	
IC5	Disable PROFILE_OPERATIONAL1. Do not remove the Notification.			
IC6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1 SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_di1>))</notif_seq_no_di1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	

Test Sequence #04 Nominal: Delete Notification

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
IC3	Install PROFII	LE_OPERATIONAL1. Remove both	the notifications.	
IC4	Enable PROF	ILE_OPERATIONAL1. Remove the	Notification.	
IC5	Disable PROF	FILE_OPERATIONAL1. Remove the	e Notification.	
IC6	Delete PROFI	LE_OPERATIONAL1. Do not remo	ve the Notification.	
IC7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DE1 SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_de1>))</notif_seq_no_de1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	

V1.4 Page 150 of 777

Test Sequence #05 Nominal: Two Install (PIR) Notifications with different Notification Addresses

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELE	CT_ISDR			
IC3		LE_OPERATIONAL1 with #METADA e the Notification.	TA_OP_PROF1_NO_INSTALL.			
IC4	Install PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_NO_INSTALL. The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions: • #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than #CERT_S_SM_DPauth_ECDSA • #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1 • #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA Do not remove the Notification.					
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR_IN2_PIR SW = 0x9000			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir>))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079 RQ31_182		
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN2_PIR SW = 0x9000	RQ25_020 RQ31_182		
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in2_pir>))</notif_seq_no_in2_pir>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079 RQ31_182		
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	RQ25_020 RQ31_182		

Test Sequence #06 Nominal: Install (PIR) and Enable Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	Install PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_NO_INSTALL. Do not remove the Notification.			
IC4	Enable PROFILE_OPERATIONAL1. Do not remove the Notification.			
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR_EN1 SW = 0x9000	

V1.4 Page 151 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir>))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079 RQ31_182
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ25_020 RQ31_182
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_en1>))</notif_seq_no_en1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	

Test Sequence #07 Nominal: Disable and Delete Notifications

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	ISDR		
IC3	Install PROFII	LE_OPERATIONAL1. Remove both the	Notifications.		
IC4	Enable PROF	ILE_OPERATIONAL1. Remove the Noti	fication		
IC5	Disable PROF	FILE_OPERATIONAL1. Do not remove the	he Notification		
IC6	Delete PROFI	LE_OPERATIONAL1. Do not remove th	e Notification		
IC7	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1_DE1 SW = 0x9000		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_di1>))</notif_seq_no_di1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079	
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DE1 SW = 0x9000		
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_de1>))</notif_seq_no_de1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079	
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000		

Test Sequence #08 Nominal: Install (OtherSignedNotification) and Enable Notifications

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 152 of 777

IC3	Install PROFILE_OPERATIONAL1. Remove the PIR notification, but do not remove the OtherSignedNotification.			
IC4	Enable PROF	ILE_OPERATIONAL1. Do not remo	ove the Notification.	
IC5	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_EN1 SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1>))</notif_seq_no_in1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1 SW = 0x9000	
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_en1>))</notif_seq_no_en1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	

Test Sequence #09 Nominal: Enable and Install (PIR) notifications

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	ISDR			
IC3	Install PROFII	LE_OPERATIONAL1. Remove both noti	fications.			
IC4	Enable PROF	ILE_OPERATIONAL1. Do not remove the	ne Notification.			
IC5	Install PROFILE_OPERATIONAL2 with METADATA_OP_PROF2_NO_INSTALL. The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions: • #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than #CERT_S_SM_DPauth_ECDSA • #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1 • #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA Do not remove the Notification.					
IC6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1_IN2_PIR SW = 0x9000			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in2_pir>))</notif_seq_no_in2_pir>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079 RQ31_182		
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1 SW = 0x9000	RQ25_020 RQ31_182		

V1.4 Page 153 of 777

3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_en1>))</notif_seq_no_en1>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	

Test Sequence #10 Nominal: Removing Sequence Numbers that are not present

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	L C_INITIALIZATION_SEQUENCE	•	
IC2	PROC_OPEN		ISDR	
IC3	Install PROFII Notification.	LE_OPERATIONAL1 with #METADATA	_OP_PROF1_NO_INSTALL. Do not	remove the
IC4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR SW = 0x9000	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir> - 1))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_NOTHING _TO_DELETE SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
2	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR SW = 0x9000	
3	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir> + 1))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_NOTHING _TO_DELETE SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN1_PIR SW = 0x9000	
5	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir>))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_OK SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	
7	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir>))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_NOTHING _TO_DELETE SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
8	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	
9	S_LPAd → eUICC	MTD_STORE_DATA(MTD_REMOVE_NOTIF(<notif_seq_no_in1_pir> + 1))</notif_seq_no_in1_pir>	#R_REMOVE_NOTIF_NOTHING _TO_DELETE SW = 0x9000	RQ35_021 RQ57_077 RQ57_078 RQ57_079
10	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_NONE SW = 0x9000	

V1.4 Page 154 of 777

4.2.17 ES10b (LPA -- eUICC): LoadCRL

This section is defined as FFS.

4.2.18 ES10b (LPA -- eUICC): AuthenticateServer

4.2.18.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24 008
- RQ26_005, RQ26_006, RQ26_007, RQ26_008, RQ26_010, RQ26_012, RQ26_013, RQ26_029, RQ26_033, RQ26_034, RQ26_035
- RQ31_025, RQ31_046, RQ31_047, RQ31_048, RQ31_049, RQ31_050, RQ31_051, RQ31_052, RQ31_053, RQ31_054, RQ31_055, RQ31_076, RQ31_077, RQ31_078, RQ31_079
- RQ36_017
- RQ42_001
- RQ43_001, RQ43_002
- RQ45_002, RQ45_006, RQ45_026, RQ45_026_1, RQ45_028, RQ45_030, RQ45_032
- RQ55_004, RQ55_005
- RQ57_093, RQ57_094, RQ57_095, RQ57_096, RQ57_097, RQ57_098, RQ57_099, RQ57_100, RQ57_101, RQ57_102, RQ57_103, RQ57_104, RQ57_105, RQ57_106, RQ57_107, RQ57_108

4.2.18.2 Test Cases

4.2.18.2.1TC_eUICC_ES10b.AuthenticateServer_SM-DP+_NIST

Test Sequence #01 Nominal: Without MatchingID in CtxParams1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on NIST P-256 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>	

V1.4 Page 155 of 777

Non-confidential

2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID based on NIST P-256 curve - Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDP)	#R_AUTHENTICATE_SMDP SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euiccSigned1 is the same as in #AUTHENTICATE_SMDP. • Verify that the <s_smdp_challenge> present in the euiccSigned1 is the same as in #AUTHENTICATE_SMDP</s_smdp_challenge></s_transaction_id></euicc_signature1>	RQ26_029 RQ26_005 RQ26_006 RQ26_007 RQ26_008 RQ26_034 RQ26_035 RQ31_025 RQ31_046 RQ31_047 RQ31_049 RQ31_050 RQ31_051 RQ31_051 RQ31_055 RQ31_055 RQ31_056 RQ31_076 RQ31_076 RQ31_079 RQ42_001 RQ43_001 RQ43_001 RQ43_002 RQ45_002 RQ55_004 RQ55_005 RQ57_096 RQ57_096 RQ57_097 RQ57_098 RQ57_099 RQ57_101 RQ57_101 RQ57_102 RQ57_103 RQ57_104 RQ57_105 RQ57_106 RQ57_106 RQ57_106 RQ57_107 RQ57_106 RQ57_107 RQ57_107	

Test Sequence #02 Nominal: With MatchingID in CtxParams1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 156 of 777

	Ī		Т	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on NIST P-256 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	
3	 <s_trai< li=""> <euicc_< li=""> <s_smd< li=""> <s_smd< li=""> Set the </s_smd<></s_smd<></euicc_<></s_trai<>	NSACTION_ID> _CHALLENGE> P_CHALLENGE> P_SIGNATURE1> EUICC_CI_PK_ID_TO_BE_USED	escribed in the InitiateAuthentication fund > to the CI Key ID based on NIST P-256 A leading to the same Root CI certificate	
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTH_SMDP_MATCH_ID)	#R_AUTH_SMDP_MATCH_ID SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euiccSigned1 is the same as in #AUTH_SMDP_MATCH_ID • Verify that the <s_smdp_challenge> present in the euiccSigned1 is the same as in #AUTH_SMDP_MATCH_ID</s_smdp_challenge></s_transaction_id></euicc_signature1>	RQ26_029 RQ26_005 RQ26_006 RQ26_007 RQ26_008 RQ26_034 RQ26_035 RQ31_025 RQ31_046 RQ31_047 RQ31_049 RQ31_050 RQ31_051 RQ31_051 RQ31_055 RQ31_055 RQ31_055 RQ31_076 RQ31_077 RQ42_001 RQ43_001 RQ43_001 RQ43_001 RQ43_002 RQ45_002 RQ55_004 RQ55_005 RQ57_096 RQ57_096 RQ57_097 RQ57_098 RQ57_101 RQ57_102 RQ57_101 RQ57_102 RQ57_104 RQ57_105 RQ57_105 RQ57_106

V1.4 Page 157 of 777

	RQ57_107
	RQ57_108

Test Sequence #03 Nominal: With IMEI in Device Capabilities

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SEL	LECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on NIST P-256 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID based on NIST P-256 curve - Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>			
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTH_SMDP_IMEI)	#R_AUTH_SMDP_IMEI SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euiccSigned1 is the same as in #AUTH_SMDP_IMEI • Verify that the <s_smdp_challenge> present in the euiccSigned1 is the same as in #AUTH_SMDP_IMEI</s_smdp_challenge></s_transaction_id></euicc_signature1>	RQ26_029 RQ26_005 RQ26_006 RQ26_007 RQ26_008 RQ26_034 RQ26_035 RQ31_025 RQ31_046 RQ31_047 RQ31_049 RQ31_050 RQ31_051 RQ31_051 RQ31_053 RQ31_054 RQ31_055 RQ31_055 RQ31_056 RQ31_056 RQ31_056 RQ31_055 RQ31_076 RQ42_001 RQ43_001 RQ43_001 RQ43_002 RQ45_002 RQ55_004 RQ55_005 RQ57_094

V1.4 Page 158 of 777

		RQ57_095
		RQ57_096
		RQ57_097
		RQ57_098
		RQ57_099
		RQ57_101
		RQ57_102
		RQ57_103
		RQ57_104
		RQ57_105
		RQ57_106
		RQ57_107
		RQ57_108

4.2.18.2.2TC_eUICC_ES10b.AuthenticateServer_SM-DP+_BRP

Test Sequence #01 Nominal: Without MatchingID in CtxParams1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on BrainpoolP256r1 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID based on BrainpoolP256r1 curve - Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>			
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDP)	#R_AUTHENTICATE_SMDP SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euiccSigned1 is the same as in #AUTHENTICATE_SMDP. • Verify that the</s_transaction_id></euicc_signature1>	RQ26_029 RQ26_005 RQ26_006 RQ26_007 RQ26_008 RQ26_034 RQ26_035 RQ31_025 RQ31_046 RQ31_047 RQ31_048

V1.4 Page 159 of 777

	<s_smdp_challenge> present in</s_smdp_challenge>	RQ31_049
	the euiccSigned1 is the same as in	RQ31_050
	#AUTHENTICATE_SMDP	RQ31_051
		RQ31_053
		RQ31_054
		RQ31_055
		RQ31_076
		RQ31_079
		RQ42_001
		RQ43_001
		RQ43_002
		RQ45_002
		RQ55_004
		RQ55_005
		RQ57_094
		RQ57_095
		RQ57_096
		RQ57_097
		RQ57_098
		RQ57_099
		RQ57_101
		RQ57_102
		RQ57_103
		RQ57_104
		RQ57_105
		RQ57_106
		RQ57_107
		RQ57_108

Test Sequence #02 Nominal: With MatchingID in CtxParams1

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on BrainpoolP256r1 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function:				

V1.4 Page 160 of 777

				RQ26_029
				RQ26_005
				RQ26_006
				RQ26_007
				RQ26_008
				RQ26_034
				RQ26_035
				RQ31_025
				RQ31_046
				RQ31_047
				RQ31_048
				RQ31_049
			#R_AUTH_SMDP_MATCH_ID	RQ31_050
			SW = 0x9000	RQ31_051
			300 - 003000	RQ31_053
				RQ31_054
			 Verify the <euicc_signature1></euicc_signature1> 	RQ31_055 RQ31_076
			using the #PK_EUICC_ECDSA	RQ31_076 RQ31_079
4	$S_LPAd \rightarrow$	MTD_STORE_DATA_SCRIPT(Verify that the	RQ42_001
7	eUICC	#AUTH_SMDP_MATCH_ID)	<s_transaction_id> present in</s_transaction_id>	RQ42_001
			the euiccSigned1 is the same as in	RQ43_002
			#AUTH_SMDP_MATCH_ID	RQ45_002
			Verify that the	RQ55_004
			<s_smdp_challenge> present in</s_smdp_challenge>	RQ55_005
			the euiccSigned1 is the same as in	RQ57_094
			#AUTH_SMDP_MATCH_ID	RQ57_095
				RQ57_096
				RQ57_097
				RQ57_098
				RQ57_099
				RQ57_101
				RQ57_102
				RQ57_103
				RQ57_104
				RQ57_105
				RQ57_106
				RQ57_107
				RQ57_108

Test Sequence #03 Nominal: With IMEI in Device Capabilities

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on BrainpoolP256r1 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>	

V1.4 Page 161 of 777

3	 <s_t< li=""> <eui< li=""> <s_s< li=""> <s_s< li=""> set the curve </s_s<></s_s<></eui<></s_t<>	RANSACTION_ID> CC_CHALLENGE> MDP_CHALLENGE> MDP_SIGNATURE1> ne <euicc_ci_pk_id_to_be_us< th=""><th>#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge> escribed in the InitiateAuthentication function SED> to the CI Key ID based on Brainpoon</euicc_challenge></th><th>oIP256r1</th></euicc_ci_pk_id_to_be_us<>	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge> escribed in the InitiateAuthentication function SED> to the CI Key ID based on Brainpoon</euicc_challenge>	oIP256r1
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTH_SMDP_IMEI)	#R_AUTH_SMDP_IMEI SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euicsigned1 is the same as in #AUTH_SMDP_IMEI • Verify that the <s_smdp_challenge> present in the euicsigned1 is the same as in #AUTH_SMDP_IMEI</s_smdp_challenge></s_transaction_id></euicc_signature1>	RQ26_029 RQ26_005 RQ26_006 RQ26_007 RQ26_008 RQ26_034 RQ26_035 RQ31_025 RQ31_046 RQ31_047 RQ31_048 RQ31_050 RQ31_051 RQ31_051 RQ31_055 RQ31_055 RQ31_055 RQ31_056 RQ31_076 RQ31_079 RQ42_001 RQ43_001 RQ43_002 RQ45_002 RQ55_004 RQ55_005 RQ57_096 RQ57_096 RQ57_097 RQ57_098 RQ57_099 RQ57_101 RQ57_102 RQ57_101 RQ57_102 RQ57_103 RQ57_104 RQ57_105 RQ57_106 RQ57_106 RQ57_106 RQ57_107 RQ57_106 RQ57_107 RQ57_106 RQ57_107

4.2.18.2.3TC_eUICC_ES10b.AuthenticateServer_SM-DP+_FRP

This test case is defined as FFS and not applicable for this version of test specification.

V1.4 Page 162 of 777

4.2.18.2.4TC_eUICC_ES10b.AuthenticateServer_SM-DP+_ErrorCases

Test Sequence #01 Error: With Incorrect SM-DPauth certificate (i.e. invalid signature)

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR					
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000			
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>			
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DPauth_INV_SIGN leading to the same Root CI certificate apart from the signature</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>					
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTH_SMDP_INV_CERT)	#R_AUTH_SERVER_INV_CERT SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTH_SMDP_INV_CERT.</s_transaction_id>	RQ26_005 RQ26_006 RQ31_052 RQ45_006 RQ45_026_1 RQ45_026 RQ45_028 RQ55_005 RQ57_100 RQ57_100 RQ57_100 RQ57_100 RQ57_100 RQ57_105 RQ57_107		

Test Sequence #02 Error: With Invalid SM-DP+ Signature

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function:			

V1.4 Page 163 of 777

	 <s_transaction_id></s_transaction_id> <euicc_challenge></euicc_challenge> <s_smdp_challenge></s_smdp_challenge> <s_smdp_signature1> NOT computed with the #SK_S_SM_DPauth_ECDSA but SHALL have the same length as for a valid signature</s_smdp_signature1> Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used> Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate 				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDP)	#R_AUTH_SERVER_INV_SIGN SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTHENTICATE_SMDP</s_transaction_id>	RQ31_052 RQ45_006 RQ45_026_1 RQ45_026 RQ45_028 RQ55_005 RQ57_100 RQ57_100 RQ57_107 RQ57_107 RQ57_107	

Test Sequence #03 Error: Unsupported Curve

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000			
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>			
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smdp_challenge> - <random_sm_dp+_sign> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - #CERT_S_SM_DPauth_INV_CURVE</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></random_sm_dp+_sign></s_smdp_challenge></euicc_challenge></s_transaction_id>					
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTH_SMDP_INV_CURV)	#R_AUTH_SERVER_INV_CURV SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTH_SMDP_INV_CURV.</s_transaction_id>	RQ26_005 RQ26_006 RQ31_049 RQ31_052 RQ45_006 RQ45_026_1 RQ45_026 RQ45_028 RQ55_005 RQ57_097 RQ57_100		

V1.4 Page 164 of 777

		RQ57_105	
		RQ57_107	
		RQ26_010	

Test Sequence #04 Error: eUICC Challenge Mismatch

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - #S_EUICC_CHALLENGE considered as different from <euicc_challenge> - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTH_SMDP_INV_CHALLE NGE)	#R_AUTH_SERVER_INV_CHALLEN GE SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTH_SMDP_INV_CHALLENGE.</s_transaction_id>	RQ26_005 RQ26_006 RQ31_050 RQ31_052 RQ57_098 RQ57_100 RQ57_105 RQ57_107 RQ26_010	

Test Sequence #05 Error: Unknown CI PK

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	.ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: • <s_transaction_id> • <euicc_challenge> • <s_smdp_challenge></s_smdp_challenge></euicc_challenge></s_transaction_id>			

V1.4 Page 165 of 777

	 <s_smdp_signature1></s_smdp_signature1> Set the <euicc_ci_pk_id_to_be_used> to a CI Key ID not present in the <euicc_ci_pk_id_list_for_signing> (a random SubjectKeyIdentifier can be used)</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used> Choose the #CERT_S_SM_DPauth_ECDSA leading to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_verification></euicc_ci_pk_id_list_for_verification> 				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDP)	#R_AUTH_SERVER_INV_CI SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTHENTICATE_SMDP.</s_transaction_id>	RQ26_005 RQ26_006 RQ26_033 RQ31_048 RQ31_051 RQ31_052 RQ45_006 RQ45_026_1 RQ45_026 RQ45_028 RQ57_099 RQ57_100 RQ57_105 RQ57_107 RQ26_010	

Test Sequence #06 Error: Invalid Certificate Role OID

The purpose of this sequence is to make sure that the eUICC refuses any SM-DP+ Certificate for authentication that does not indicate "id-rspRole-dp-auth" in its extension for Certificate Policies.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DPpb_ECDSA (instead of #CERT_S_SM_DPauth_ECDSA) leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTH_SMDP_INV_OID)	#R_AUTH_SERVER_INV_OID SW = 0x9000 OR #R_AUTH_SERVER_INV_CERT SW = 0x9000	RQ26_005 RQ26_006 RQ31_052 RQ45_006 RQ45_026_1 RQ45_026 RQ45_028	

V1.4 Page 166 of 777

		RQ45_030
	 Verify that the 	RQ57_096
	<s_transaction_id> present in</s_transaction_id>	RQ57_100
	the AuthenticateResponseError is the	RQ57_105
	same as in #AUTH_SMDP_INV_OID.	RQ57_107
		RQ26_010

Test Sequence #07 Error: No RSP session on-going

Initial Conditions	
Entity	Description of the initial state
eUICC	No RSP session is on-going (i.e. no ES10b.getEUICCChallenge has been sent to the eUICC)

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000		
2	The following inputs are required for Step 3 as described in the InitiateAuthentication function: - <s_transaction_id> - #S_EUICC_CHALLENGE - <s_smdp_challenge> - <s_smdp_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></s_transaction_id>				
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTH_SMDP_INV_CHALLE NGE)	#R_AUTH_SERVER_NO_SESSION SW = 0x9000 The transactionId returned in the response SHALL not be checked (any value SHALL be accepted)	RQ26_005 RQ26_006 RQ31_052 RQ57_094 RQ57_100 RQ57_105 RQ57_107	

4.2.18.2.5TC_eUICC_ES10b.AuthenticateServer_SM-DS_BRP

Test Sequence #01 Nominal: With EventID in CtxParams1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig< td=""><td></td></euicc_ci_pk_id_list_for_sig<>	

V1.4 Page 167 of 777

Non-confidential

			NING> and <euicc_ci_pk_id_list_for_ver IFICATION> from response data and verify if they contain at least one same GSMA CI Key ID based on BrainpoolP256r1 curve</euicc_ci_pk_id_list_for_ver 	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	
3	 <s_trai< li=""> <euicc_< li=""> <s_smd< li=""> <s_smd< li=""> Set the </s_smd<></s_smd<></euicc_<></s_trai<>	NSACTION_ID> _CHALLENGE> S_CHALLENGE> S_SIGNATURE1> EUICC_CI_PK_ID_TO_BE_USED	escribed in the InitiateAuthentication full secribed in the InitiateAuthentication full secretary is to the CI Key ID based on Brainpool A leading to the same Root CI certifica	P256r1 curve
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTHENTICATE_SMDS)	#R_AUTHENTICATE_SMDS SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euicsigned1 is the same as in #AUTHENTICATE_SMDS. • Verify that the <s_smds_challenge> present in the euicsigned1 is the same as in #AUTHENTICATE_SMDS</s_smds_challenge></s_transaction_id></euicc_signature1>	RQ24_008 RQ26_005 RQ26_006 RQ26_008 RQ26_012 RQ26_013 RQ26_029 RQ26_034 RQ31_025 RQ31_078 RQ43_002 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ57_094 RQ57_095 RQ57_096 RQ57_097 RQ57_098 RQ57_101 RQ57_102 RQ57_103 RQ57_104 RQ57_105 RQ57_106 RQ57_107 RQ57_106 RQ57_107 RQ57_108 RQ31_046 RQ31_047 RQ31_048 RQ31_049 RQ31_050 RQ31_051 RQ31_051 RQ31_053 RQ31_055 RQ26_029

V1.4 Page 168 of 777

Test Sequence #02 Nominal: With IMEI and EventID in Device Capabilities

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on BrainpoolP256r1 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	 <s_trai< li=""> <euicc_< li=""> <s_smd< li=""> <s_smd< li=""> Set the </s_smd<></s_smd<></euicc_<></s_trai<>	 <euicc_challenge></euicc_challenge> <s_smds_challenge></s_smds_challenge> <s_smds_signature1></s_smds_signature1> Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID based on BrainpoolP256r1 curve</euicc_ci_pk_id_to_be_used> 			
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTH_SMDS_IMEI)	#R_AUTH_SMDS_IMEI SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euiccSigned1 is the same as in #AUTH_SMDS_IMEI • Verify that the <s_smds_challenge> present in the euiccSigned1 is the same as in #AUTH_SMDS_IMEI</s_smds_challenge></s_transaction_id></euicc_signature1>	RQ24_008 RQ26_005 RQ26_006 RQ26_008 RQ26_012 RQ26_013 RQ26_029 RQ26_034 RQ31_025 RQ31_078 RQ43_002 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ57_094 RQ57_095 RQ57_096 RQ57_097 RQ57_098 RQ57_101 RQ57_102 RQ57_101 RQ57_102 RQ57_103 RQ57_104 RQ57_105 RQ57_106 RQ57_106 RQ57_107 RQ57_107 RQ57_108 RQ57_108 RQ57_108 RQ57_108 RQ57_108 RQ57_108	

V1.4 Page 169 of 777

		RQ31_047
		RQ31_048
		RQ31_049
		RQ31_050
		RQ31_051
		RQ31_053
		RQ31_054
		RQ31_055
		RQ26_029

4.2.18.2.6TC_eUICC_ES10b.AuthenticateServer_SM-DS_NIST

Test Sequence #01 Nominal: With EventID in CtxParams1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SE	LECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ve rification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on NIST P-256 curve</euicc_ci_pk_id_list_for_ve></euicc_ci_pk_id_list_for_sig>	RQ36_017
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	RQ36_017
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smds_challenge> - <s_smds_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID based on NIST P-256 curve - Choose the #CERT_S_SM_DSauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></euicc_challenge></s_transaction_id>			
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDS)	#R_AUTHENTICATE_SMDS SW = 0x9000 • Verify the <euicc_signature1> using the #PK_EUICC_ECDSA • Verify that the <s_transaction_id> present in the euiccSigned1 is the same as in #AUTHENTICATE_SMDS. • Verify that the <s_smds_challenge> present in the euiccSigned1 is the same as in #AUTHENTICATE_SMDS</s_smds_challenge></s_transaction_id></euicc_signature1>	RQ24_008 RQ26_005 RQ26_006 RQ26_008 RQ26_012 RQ26_013 RQ26_029 RQ26_034 RQ31_025 RQ31_078 RQ43_002 RQ45_006 RQ45_026 LQ45_026

V1.4 Page 170 of 777

		RQ57_094
		RQ57_095
		RQ57_096
		RQ57_097
		RQ57_098
		RQ57_099
		RQ57_101
		RQ57_102
		RQ57_103
		RQ57_104
		RQ57_105
		RQ57_106
		RQ57_107
		RQ57_108
		RQ31_046
		RQ31_047
		RQ31_048
		RQ31_049
		RQ31_050
		RQ31_051
		RQ31_053
		RQ31_054
		RQ31_055
		RQ26_029
		RQ36_017

Test Sequence #02 Nominal: With IMEI and EventID in Device Capabilities

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ver ification=""> from response data and verify if they contain at least one same GSMA CI Key ID based on NIST P-256 curve</euicc_ci_pk_id_list_for_ver></euicc_ci_pk_id_list_for_sig>	RQ36_017		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	RQ36_017		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smds_challenge> - <s_smds_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID based on NIST P-256 curve - Choose the #CERT_S_SM_DSauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></euicc_challenge></s_transaction_id>					
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#R_AUTH_SMDS_IMEI	RQ24_008 RQ26_005		

V1.4 Page 171 of 777

	#AUTH_SMDS_IMEI)	SW = 0x9000	RQ26_006
			RQ26_008
			RQ26_012
		Verify the <euicc_signature1></euicc_signature1>	RQ26_013
		using the #PK_EUICC_ECDSA	RQ26_029
		 Verify that the 	RQ26_034
		<s_transaction_id> present in</s_transaction_id>	RQ31_025
		the euiccSigned1 is the same as in	RQ31_078
		#AUTH_SMDS_IMEI	RQ43_002
		Verify that the	RQ45_006
		<s_smds_challenge> present in</s_smds_challenge>	RQ45_026
		the euiccSigned1 is the same as in	RQ45_026_1
		#AUTH_SMDS_IMEI	RQ57_094
			RQ57_095
			RQ57_096
			RQ57_097
			RQ57_098
			RQ57_099
			RQ57_101
			RQ57_102
			RQ57_103
			RQ57_104
			RQ57_105
			RQ57_106
			RQ57_107
			RQ57_108
			RQ31_046
			RQ31_047
			RQ31_048
			RQ31_049 RQ31_050
			RQ31_050 RQ31_051
			RQ31_051
			RQ31_053
			RQ31_055
			RQ26_029
			RQ36_017
			1.000_017

4.2.18.2.7TC_eUICC_ES10b.AuthenticateServer_SM-DS_FRP

This test case is defined as FFS and not applicable for this version of test specification.

4.2.18.2.8TC_eUICC_ES10b.AuthenticateServer_SM-DS_ErrorCases

Test Sequence #01 Error: With Incorrect SM-DSauth certificate (i.e. invalid signature)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>	

V1.4 Page 172 of 777

3	 <s_tran< li=""> <euicc_< li=""> <s_smd< li=""> <s_smd< li=""> Set the < <euicc_< li=""> </euicc_<></s_smd<></s_smd<></euicc_<></s_tran<>	following inputs are required for Step 4 as described in the InitiateAuthentication function: <s_transaction_id> <euicc_challenge> <s_smds_challenge> <s_smds_signature1> Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> Choose the #CERT_S_SM_DSauth_INV_SIGN leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></euicc_challenge></s_transaction_id>		
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTH_SMDS_INV_CERT)	#R_AUTH_SERVER_INV_CERT SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTH_SMDS_INV_CERT.</s_transaction_id>	RQ45_028 RQ57_100 RQ31_052 RQ57_095 RQ57_105 RQ57_107 RQ26_010

Test Sequence #02 Error: With Invalid SM-DS Signature

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smds_challenge> - <s_smds_signature1> NOT computed with the #SK_S_SM_DSauth_ECDSA but SHALL have the same length as for a valid signature - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DSauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></euicc_challenge></s_transaction_id>				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDS)	#R_AUTH_SERVER_INV_SIGN SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTHENTICATE_SMDS</s_transaction_id>	RQ57_100 RQ31_052 RQ57_097 RQ57_105 RQ57_107 RQ31_049 RQ26_010	

V1.4 Page 173 of 777

Test Sequence #03 Error: Unsupported Curve

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_	ROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	C_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smds_challenge> - <random_sm_ds_sign> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - #CERT_S_SM_DSauth_INV_CURVE</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></random_sm_ds_sign></s_smds_challenge></euicc_challenge></s_transaction_id>				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTH_SMDS_INV_CURV)	#R_AUTH_SERVER_INV_CURV SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTH_SMDS_INV_CURV.</s_transaction_id>	RQ57_100 RQ31_052 RQ57_105 RQ57_107 RQ26_010	

Test Sequence #04 Error: eUICC Challenge Mismatch

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000	
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - #S_EUICC_CHALLENGE considered as different from <euicc_challenge> - <s_smds_challenge> - <s_smds_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DSauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></euicc_challenge></s_transaction_id>		rom the	

V1.4 Page 174 of 777

			#R_AUTH_SERVER_INV_CH ALLENGE	
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTH_SMDS_INV_CHALLENGE)	• Verify that the <s_transaction_id> present in the AuthenticateResponseEr ror is the same as in #AUTH_SMDS_INV_CHALLE NGE.</s_transaction_id>	RQ57_100 RQ31_052 RQ57_098 RQ57_105 RQ57_107 RQ31_050 RQ26_010

Test Sequence #05 Error: Unknown CI PK

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	LECT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000		
2	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000 Extract the <euicc_challenge></euicc_challenge>		
3	The following inputs are required for Step 4 as described in the InitiateAuthentication function: - <s_transaction_id> - <euicc_challenge> - <s_smds_challenge> - <s_smds_signature1> - Set the <euicc_ci_pk_id_to_be_used> to a CI Key ID not present in the <euicc_ci_pk_id_list_for_signing> (a random SubjectKeyIdentifier can be used) - Choose the #CERT_S_SM_DSauth_ECDSA leading to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_verification></euicc_ci_pk_id_list_for_verification></euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></euicc_challenge></s_transaction_id>				
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#AUTHENTICATE_SMDS)	#R_AUTH_SERVER_INV_CI SW = 0x9000 • Verify that the <s_transaction_id> present in the AuthenticateResponseError is the same as in #AUTHENTICATE_SMDS.</s_transaction_id>	RQ26_029 RQ45_028 RQ57_100 RQ31_052 RQ57_099 RQ57_105 RQ57_107 RQ31_051 RQ31_048 RQ26_010	

Test Sequence #06 Error: No RSP session on-going

Initial Conditions	
Entity	Description of the initial state
eUICC	No RSP session is on-going (i.e. no ES10b.getEUICCChallenge has been sent to the eUICC)

V1.4 Page 175 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000	
2	The following inputs are required for Step 3 as described in the InitiateAuthentication function: - <s_transaction_id> - #S_EUICC_CHALLENGE - <s_smds_challenge> - <s_smds_signature1> - Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> - Choose the #CERT_S_SM_DSauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></s_transaction_id>			
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTH_SMDS_INV_CHALLENGE)	#R_AUTH_SERVER_NO_SE SSION SW = 0x9000 The transactionId returned in the response SHALL not be checked (any value SHALL be accepted)	RQ57_100 RQ31_052 RQ57_094 RQ57_105 RQ57_107

4.2.19 ES10b (LPA -- eUICC): CancelSession

4.2.19.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26_034, RQ26_035
- RQ31_099, RQ31_101, RQ31_114, RQ31_115, RQ31_116, RQ31_117, RQ31_160, RQ31_162_1, RQ31_188_1
- RQ57_041_1, RQ57_109, RQ57_110, RQ57_111, RQ57_113, RQ57_114, RQ57_115, RQ57_116

4.2.19.2 Test Cases

4.2.19.2.1TC_eUICC_ES10b.CancelSessionNIST

General Initial Conditions			
Entity Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC		
eUICC	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.		

V1.4 Page 176 of 777

Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+ (i.e. the response has been sent by the eUICC for ES10b.AuthenticateServer)

• #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC

• the same GSMA CI based on NIST P-256 curve has been chosen for signing and for verification

Test Sequence #01 Nominal: End User Rejection

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_REJECT)	#R_CANCEL_SESSION_REJ SW = 0x9000 The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_REJECT</s_transaction_id></euicc_cs_signature>	RQ31_114 RQ31_115 RQ31_116 RQ31_117 RQ57_110 RQ57_111 RQ57_114 RQ57_115 RQ57_116 RQ26_034 RQ26_035 RQ31_160
2	PROC_VERIFY_SESSION_IS_CANCELLED			RQ57_113

Test Sequence #02 Nominal: End User Postponed

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_POSTPON ED)	#R_CANCEL_SESSION_POSTPONED SW = 0x9000 The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_POSTPONED</s_transaction_id></euicc_cs_signature>	RQ31_114 RQ31_115 RQ31_116 RQ31_117 RQ57_110 RQ57_111 RQ57_114 RQ57_115 RQ57_116 RQ26_034 RQ26_035 RQ31_160
2	PROC_VERIFY_SESSION_IS_CANCELLED			RQ57_113

Test Sequence #03 Nominal: Timeout

The RSP session is delayed because the End User does not confirm the download of the Profile within the timeout interval defined by the LPAd.

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#R_CANCEL_SESSION_TIMEOUT SW = 0x9000	RQ31_114 RQ31_115 RQ31_116 RQ31_117

V1.4 Page 177 of 777

		#CANCEL_SESSION_TIMEO UT)	The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_TIMEOUT</s_transaction_id></euicc_cs_signature>	RQ57_110 RQ57_111 RQ57_114 RQ57_115 RQ57_116 RQ26_034 RQ26_035
2	PROC_VERIF	Y_SESSION_IS_CANCELLED		RQ57_113

Test Sequence #04 Nominal: PPR not allowed

The RSP session is terminated because the LPAd detected that PPR(s) set in the Profile Metadata is/are not allowed.

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_PPR)	#R_CANCEL_SESSION_PPR SW = 0x9000 The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_PPR</s_transaction_id></euicc_cs_signature>	RQ31_114 RQ31_115 RQ31_116 RQ31_117 RQ57_110 RQ57_111 RQ57_114 RQ57_115 RQ57_116 RQ26_034 RQ26_035 RQ31_099 RQ31_101
2	PROC_VERIFY_SESSION_IS_CANCELLED			RQ57_113

Test Sequence #05 Nominal: Metadata Mismatch

The RSP session is terminated because the LPAd detected that the Profile Metadata in the response to "ES9+.AuthenticateClient" does not match the Profile Metadata in the Bound Profile Package.

Initial Conditions	
Entity	Description of the initial condition
eUICC	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ (i.e. the response has been sent by the eUICC for ES10b.PrepareDownload)
	 #PREP_DOWNLOAD_NO_CC has been sent to the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_METADA TA)	#R_CANCEL_SESSION_METADAT A SW = 0x9000	RQ31_114 RQ31_115 RQ31_116 RQ31_117 RQ57_110 RQ57_111

V1.4 Page 178 of 777

			The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_METADATA</s_transaction_id></euicc_cs_signature>	RQ57_114 RQ57_115 RQ57_116 RQ26_034 RQ26_035
2	Generate the	:OTPK_S_SM_DP+_ECKA> and <	OT_SK_S_SM_DP+_ECKA>	
3	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>			
4	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>			
5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x6985 or 0x6A88	RQ57_113 RQ57_041_1
6	PROC_VERIFY_SESSION_IS_CANCELLED RQ57_113			

Test Sequence #06 Nominal: BPP Parsing Error

The RSP session is terminated because the LPAd has encountered an error while parsing the Bound Profile Package received from the SM-DP+.

Initial Conditions		
Entity	Description of the initial condition	
eUICC	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ (i.e. the response has been sent by the eUICC for ES10b.PrepareDownload)	
	#PREP_DOWNLOAD_NO_CC has been sent to the eUICC	

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_LOAD_B PP)	#R_CANCEL_SESSION_LOAD_B PP SW = 0x9000 The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_LOAD_BPP</s_transaction_id></euicc_cs_signature>	RQ31_114 RQ31_115 RQ31_116 RQ31_117 RQ57_110 RQ57_111 RQ57_114 RQ57_115 RQ57_116 RQ26_034 RQ26_035

V1.4 Page 179 of 777

				RQ31_162 _1		
2	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>					
3	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>					
4	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>					
5	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x6985 or 0x6A88	RQ57_113		
6	PROC_VERIFY_SESSION_IS_CANCELLED			RQ57_113		

Test Sequence #07 Nominal: Load BPP Execution Error

The RSP session is terminated because the LPAd has encountered an error while installing the Bound Profile Package received from the SM-DP+.

Initial Conditions	
Entity Description of the initial condition	
eUICC	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ (i.e. the response has been sent by the eUICC for ES10b.PrepareDownload)
	#PREP_DOWNLOAD_NO_CC has been sent to the eUICC

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	Generate the <otpk_s_sm_dp+_ecka> and <ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka></otpk_s_sm_dp+_ecka>					
IC2	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_PROF1, #METADATA_OP_PROF1, NO_PARAM, #UPP_OP_PROF1)</bpp></pre>					
IC3	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>					

V1.4 Page 180 of 777

IC4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands	
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_LOAD_BPP)	#R_CANCEL_SESSION_LOAD_BPP SW = 0x9000 The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_LOAD_BP P</s_transaction_id></euicc_cs_signature>	RQ31_114 RQ31_115 RQ31_116 RQ31_117 RQ57_110 RQ57_111 RQ57_114 RQ57_115 RQ57_116 RQ31_188_1 RQ26_034 RQ26_035 RQ31_162_1
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0)< td=""><td>SW=0x6985 or 0x6A88</td><td>RQ57_113</td></bpp_seg_a0)<>	SW=0x6985 or 0x6A88	RQ57_113
3	3 PROC_VERIFY_SESSION_IS_CANCELLED			RQ57_113

Test Sequence #08 Nominal: Undefined Reason

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_UNDEF)	#R_CANCEL_SESSION_UNDEF SW = 0x9000 The <euicc_cs_signature> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the response is the same as in #CANCEL_SESSION_UNDEF</s_transaction_id></euicc_cs_signature>	RQ31_114 RQ31_115 RQ31_116 RQ31_117 RQ57_110 RQ57_111 RQ57_114 RQ57_115 RQ57_116 RQ26_034 RQ26_035
2	PROC_VERIF	FY_SESSION_IS_CANCELLED		RQ57_113

4.2.19.2.2TC_eUICC_ES10b.CancelSessionBRP

In these test sequences, once the RSP session has been cancelled, verifications are performed in order to check that it is neither possible to execute the Download Confirmation procedure nor to execute the Common Mutual Authentication procedure by referring to the cancelled TransactionID.

General Initial Conditions			
Description of the general initial condition			
The PROFILE_OPERATIONAL1 is not loaded on the eUICC			
The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R. Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+			

V1.4 Page 181 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

	•	#GET_EUICC_INFO1,	#GET_EUICC_CHALLENGE	and
		#AUTHENTICATE_SMDP	have been sent to the eUICC	
•	•	the same GSMA CI based chosen for signing and for v	d on BrainpoolP256r1 curve has verification	been

Test Sequence #01 Nominal: End User Rejection

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #02 Nominal: End User Postponed

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #03 Nominal: Timeout

This test sequence SHALL be the same as the Test Sequence #03 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #04 Nominal: PPR not allowed

This test sequence SHALL be the same as the Test Sequence #04 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #05 Nominal: Metadata Mismatch

Initial Conditions	
Entity	Description of the initial state
eUICC	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ #PREP_DOWNLOAD_NO_CC has been sent to the eUICC

This test sequence SHALL be the same as the Test Sequence #05 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #06 Nominal: BPP Parsing Error

Initial Conditions	
Entity	Description of the initial state
eUICC	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ #PREP_DOWNLOAD_NO_CC has been sent to the eUICC

V1.4 Page 182 of 777

This test sequence SHALL be the same as the Test Sequence #06 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #07 Nominal: Load BPP Execution Error

Initial Conditions	
Entity Description of the initial state	
eUICC	Sub-procedure Profile Download and Installation – End User Confirmation has been successfully executed between the eUICC and the S_SM-DP+ #PREP_DOWNLOAD_NO_CC has been sent to the eUICC

This test sequence SHALL be the same as the Test Sequence #07 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #08 Nominal: Undefined Reason

This test sequence SHALL be the same as the Test Sequence #08 defined in section 4.2.19.2.1 – TC_eUICC_ES10b.CancelSessionNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.2.19.2.3TC_eUICC_ES10b.CancelSessionFRP

This test case is defined as FFS and not applicable for this version of test specification.

4.2.19.2.4TC_eUICC_ES10b.CancelSession_ErrorCase

Test Sequence #01 Error: No on-going RSP session

On receiving a CancelSession request whereas there is no on-going RSP session, the eUICC SHALL return an error code.

Initial Conditions	
Entity	Description of the initial condition
eUICC	No RSP session is on-going (i.e. no Common Mutual Authentication procedure has been executed)

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				

V1.4 Page 183 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

	0.154.1	MTD_STORE_DATA(#R_CANCEL_SESSION_INV_T	RQ57_109
1	S_LPAd → eUICC	#CANCEL_SESSION_INV_TRANS	RANS_ID	RQ57_114
	60100	_ID)	SW = 0x9000	RQ57_115

Test Sequence #02 Error: Invalid Transaction ID

On receiving a CancelSession request with a TransactionID different from the on-going one, the eUICC SHALL not discard the current RSP session and return an error code.

Initial Conditions		
Entity	Description of the initial condition	
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.	
eUICC	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 	

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_INV_TRANS_I D)	#R_CANCEL_SESSION_INV_T RANS_ID SW = 0x9000	RQ57_109 RQ57_114 RQ57_115
2	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_NO_CC)	#R_PREP_DOWNLOAD_NO_C C SW=0x9000	

4.2.20 ES10c (LPA -- eUICC): GetProfilesInfo

4.2.20.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_029
- RQ32_057
- RQ31_183
- RQ57_117, RQ57_118, RQ57_119, RQ57_120, RQ57_121, RQ57_122, RQ57_123, RQ57_124, RQ57_125, RQ57_126

4.2.20.2 Test Cases

4.2.20.2.1TC_eUICC_ES10c.GetProfilesInfo

V1.4 Page 184 of 777

General Initial Conditions			
Entity	Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC		
eUICC	The PROFILE_OPERATIONAL2 has been installed on the eUICC		
eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC		
eUICC	The PROFILE_OPERATIONAL1 is Enabled		
eUICC	The Nickname of PROFILE_OPERATIONAL1 and PROFILE_OPERATIONAL2 is empty		
eUICC	The Nickname of the PROFILE_OPERATIONAL3 is equal to #NICKNAME3		

Test Sequence #01 Nominal: Get All Profiles

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT	LISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1, #PROFILE_INFO2, #PROFILE_INFO3 } SW = 0x9000	RQ32_057 RQ57_117 RQ57_118 RQ57_119 RQ57_123 RQ24_029 RQ31_183

Test Sequence #02 Nominal: Get Profile by ICCID

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW = 0x9000	RQ57_117 RQ57_119 RQ57_121 RQ57_123	

Test Sequence #03 Nominal: Get Profile by AID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

V1.4 Page 185 of 777

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW = 0x9000	RQ57_117 RQ57_119 RQ57_121 RQ57_123	

Test Sequence #04 Nominal: Get All Operational Profiles

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_ISE	DR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_PROFCLASS)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1, #PROFILE_INFO2, #PROFILE_INFO3 } SW = 0x9000	RQ57_119 RQ57_120 RQ57_122 RQ57_123

Test Sequence #05 Nominal: Get Profile ICCID list

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUIC	C_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLI ST_ICCID)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLIST_ ICCID } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123		

V1.4 Page 186 of 777

Test Sequence #06 Nominal: Get Profile AID list

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLI ST_ISDPAID)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLIST_IS DPAID } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123	

Test Sequence #07 Nominal: Get Profile Nickname list

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIS T_PROFILE_NICKNAME)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_TAGLIST_PR OFILE_NICKNAME } SW = 0x9000	RQ57_119 RQ57_120 RQ57_122 RQ57_123	

Test Sequence #08 Nominal: Get Profile SP Name list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	CC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SELECT_	ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST_S P_NAME)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLIST_S P_NAME } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123

V1.4 Page 187 of 777

Test Sequence #09 Nominal: Get Profile Name list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_ISI	DR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST_P ROFILE_NAME)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_TAGLI ST_PROFILE_NAME } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123

Test Sequence #10 Nominal: Get Profile Icon list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_ISI	OR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST_ICO N)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_TAGLI ST_ICON } SW = 0x9000	RQ57_120, RQ57_122, RQ57_123

Test Sequence #11 Nominal: Get Profile Owner list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_ISI	OR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST_P ROFILE_OWNER)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLI ST_PROFILE_OWNER } SW = 0x9000	RQ57_120, RQ57_122, RQ57_123, RQ57_125

V1.4 Page 188 of 777

Test Sequence #12 Nominal: Get Profile SM-DP+ proprietary data list

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC with dpProprietaryData #SMDP_PROP_DATA1 (i.e. #CONF_ISDP_PROF1 is used during the Profile downloading)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST_ SMDP_PROP_DATA)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_TAGLIS T_SMDP_PROP_DATA } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123

Test Sequence #13 Nominal: Get Profile ICCID and State list

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR					
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST1)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_TAGLIS T1 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123		

Test Sequence #14 Nominal: Get Profile Nickname and State list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST 2)	response ProfileInfoListResponse::= profileInfoListOk : {	RQ57_119 RQ57_120 RQ57_122 RQ57_123

V1.4 Page 189 of 777

#PROFILES_INFO_TAGLIS
T2
}
SW = 0x9000

Test Sequence #15 Nominal: Get Profile Icon and Icon Type list

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	OC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST 3)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_TAGLIS T3 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123		

Test Sequence #16 Nominal: Get Profile Icon and State list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_TAGLIST 4)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLIS T4 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123

Test Sequence #17 Nominal: Get Operational Profile ICCID and State list

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SELECT	_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_OPTAGL IST1)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_TAGLIS T1 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123		

V1.4 Page 190 of 777

Test Sequence #18 Nominal: Get Operational Profile Nickname and State list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_OPTAGL IST2)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLIST2 } SW = 0x9000	RQ57_119 RQ57_120 RQ57_122 RQ57_123

Test Sequence #19 Nominal: Get Operational Profile Icon and Icon type list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_OPTAGL IST3)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLIST3 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123

Test Sequence #20 Nominal: Get Operational Profile Icon and State list

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_OPTAGL IST4)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_TAGLIST4 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123

Test Sequence #21 Nominal: Get Profile State of the defined Profile

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 191 of 777

			response ProfileInfoListResponse::=	
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ICCID_T AGLIST1)	profileInfoListOk : { #PROFILES_INFO_ICCID_TAG LIST1	RQ57_120 RQ57_122 RQ57_123
			}	
			SW = 0x9000	

Test Sequence #22 Nominal: Get Profile Icon Type of the defined Profile

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT	_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ICCID_T AGLIST2)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_ICCID_TAG LIST2 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123	

Test Sequence #23 Nominal: Get Profile Class of the defined Profile

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ICCI D_TAGLIST3)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILES_INFO_ICCID_TAG LIST3 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123	

Test Sequence #24 Nominal: Get Notification Configuration of the defined Profile

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ICCID_ TAGLIST4)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_ICCID_TAGLI ST4	RQ57_120 RQ57_122 RQ57_123	

V1.4 Page 192 of 777

Non-confidential

	}	
	SW = 0x9000	

Test Sequence #25 Nominal: Get Profile Policy Rules of the defined Profile

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ICCID_ TAGLIST5)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILES_INFO_ICCID_TAGLI ST5 } SW = 0x9000	RQ57_120 RQ57_122 RQ57_123 RQ57_126	

Test Sequence #26 Nominal: Get empty Profile list. No Profile installed

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Profile is loaded on the eUICC (this condition overrides the general initial condition defined in this test case)

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { } SW = 0x9000	RQ57_124	

4.2.21 ES10c (LPA -- eUICC): EnableProfile

4.2.21.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_010
- RQ29_002, RQ29_022
- RQ32_011, RQ32_012, RQ32_016_1, RQ32_016_2, RQ32_016_3, RQ32_017, RQ32_017_1, RQ32_017_2, RQ32_018_1

V1.4 Page 193 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

- RQ34_015
- RQ57_127, RQ57_127_1, RQ57_127_2, RQ57_128, RQ57_129, RQ57_130, RQ57_132, RQ57_132_1, RQ57_133_1, RQ57_133_3, RQ57_134, RQ57_135_1, RQ57_135_2, RQ57_135_4, RQ57_136, RQ57_137, RQ57_138, RQ57_139, RQ57_140, RQ57_140_1

4.2.21.2 Test Cases

4.2.21.2.1TC_eUICC_ES10c.EnableProfile_Case3

General Initial Conditions			
Entity Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC		

Test Sequence #01 Nominal: Enable Profile by ISD-P AID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUIC	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_IS	DR		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	No response data is returned SW=0x91XX	RQ24_010 RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_132 RQ57_133_3 RQ57_138	
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_016_3 RQ32_017 RQ57_134 RQ57_135_1	
3	Repeat IC1 a	nd IC2			
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	RQ24_010 RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129	

V1.4 Page 194 of 777

				RQ57_133_3 RQ57_138
5	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
6	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

Test Sequence #02 Nominal: Enable Profile by ICCID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_ISDR	2		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	No response data is returned SW=0x91XX	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_138	
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_016_3 RQ32_017 RQ57_134 RQ57_135_1	
3	Repeat IC1 ar	nd IC2			
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_138	
5	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000		
6	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015	

V1.4 Page 195 of 777

Test Sequence #03 Nominal: Enable Profile by ISD-P AID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileStateChanged			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_IS	DR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	No response data is returned SW=0x91XX	RQ24_010 RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_138
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State change")	RQ32_016_3 RQ32_017 RQ57_134 RQ57_135_1
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	Execute IC1 fr	om step 2 to step 4		
5	Repeat IC2			
6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ24_010 RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_138
7	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
8	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

V1.4 Page 196 of 777

Test Sequence #04 Nominal: Enable Profile by ICCID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileStateChanged		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_	ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	No response data is returned SW=0x91XX	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_138
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State change")	RQ32_016_3 RQ32_017 RQ57_134 RQ57_135_1
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	Execute IC1	from step 2 to step 4		
5	Repeat IC2			
6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_138
7	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
8	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

Test Sequence #05 Nominal: Enable Profile by ISD-P AID and "refreshFlag" not set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

V1.4 Page 197 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SELECT_IS	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, FALSE))</isd_p_aid1>	No response data is returned SW=0x9000	RQ24_010 RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_132 RQ57_132_1 RQ57_138 RQ57_132_1
2	S_Device → eUICC	[TERMINAL_PROFILE]	Toolkit initialization THEN SW=0x9000	RQ32_018_1 RQ57_135_4
3	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_132_1 RQ57_138 RQ57_138_1 RQ57_132_1 RQ24_010
4	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
5	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

Test Sequence #06 Nominal: Enable Profile by ICCID and "refreshFlag" not set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, FALSE))	No response data is returned SW=0x9000	RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_132_1 RQ57_132_1 RQ57_138 RQ57_132_1	

V1.4 Page 198 of 777

2	S_Device → eUICC	[TERMINAL_PROFILE]	Toolkit initialization THEN SW=0x9000	RQ32_018_1 RQ57_135_4
3	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_132_1 RQ57_138 RQ57_132_1
4	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
5	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

${\bf 4.2.21.2.2TC_eUICC_ES10c.} Enable Profile_Error Cases_Case {\bf 3}$

General Initial Conditions		
Entity	Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	

Test Sequence #01 Error: Enable Profile by an unknown ISD-P AID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>
eUICC	The Operational Profile identified by the ISD-P AID <isd_p_aidx> is not loaded</isd_p_aidx>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT	LISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aidx>, TRUE))</isd_p_aidx>	SW=0x6A82	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_139
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM,	response ProfileInfoListResponse::= profileInfoListOk : {	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128

V1.4 Page 199 of 777

	<isd_p_aid1>))</isd_p_aid1>	#PROFILE_INFO1_DISABLE	RQ57_129
		D	RQ57_130
		1	RQ57_135_2
		'	RQ57_138
		SW=0x9000	RQ57_139

Test Sequence #02 Error: Enable Profile by an unknown ICCID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The Operational Profile identified by the ICCID #ICCID_OP_PROFX is not loaded

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SELECT_IS	DR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(#ICCID_OP_PROFX, NO_PARAM, TRUE))	SW=0x6A82	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_139
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLE D } SW=0x9000	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_139

Test Sequence #03 Error: Enable Profile (by ISD-P AID) is not possible when this Operational Profile is in Enabled state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		

V1.4 Page 200 of 777

IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	SW=0x6985	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_140
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_140

Test Sequence #04 Error: Enable Profile (by ICCID) is not possible when this Operational Profile is in Enabled state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	SW=0x6985	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_140
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_012 RQ32_016_1 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_140

V1.4 Page 201 of 777

Test Sequence #05 Error: Enable Profile (by ISD-P AID) not possible when an Operational Profile with a PPR1 is loaded

The purpose of this test is to ensure that it is NOT possible to enable an Operational Profile when there is another Operational Profile Enabled with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Profile is installed on the eUICC
	(this condition overrides the general initial condition defined in this test case)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT	_ISDR	
IC3		Install PROFILE_OPERATIONAL4 NOTE: The PROFILE_OPERATIONAL4 corresponds to <isd_p_aid4></isd_p_aid4>		
IC4		Install PROFILE_OPERATIONAL1 NOTE: The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>		
IC5	Enable PROFI	LE_OPERATIONAL4		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	SW=0x6985	RQ29_002 RQ29_022 RQ32_011 RQ32_012 RQ32_014 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_138
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED #PROFILE_INFO4_ENABLED } SW=0x9000	RQ29_002 RQ32_011 RQ32_012 RQ32_014 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_140

V1.4 Page 202 of 777

Test Sequence #06 Error: Enable Profile (by ICCID) not possible with an Operational Profile with PPR1 is loaded

The purpose of this test is to ensure that it is NOT possible to enable an Operational Profile when there is another Operational Profile Enabled with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Profile is installed on the eUICC
60100	(this condition overrides the general initial condition defined in this test case)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SELECT_	ISDR	
IC3	Install PROF	TILE_OPERATIONAL4		
IC4	Install PROF	ILE_OPERATIONAL1		
IC5	Enable PRO	FILE_OPERATIONAL4		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	SW=0x6985	RQ29_002 RQ29_022 RQ32_011 RQ32_012 RQ32_014 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_140
2	S_LPAd →eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED #PROFILE_INFO4_ENABLED } SW=0x9000	RQ29_002 RQ32_011 RQ32_012 RQ32_014 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_135_2 RQ57_138 RQ57_138

V1.4 Page 203 of 777

Test Sequence #07 Error: Enable Profile by ISD-P AID without refreshFlag while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 corresponds to <isd_p_aid2></isd_p_aid2>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR	
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	
IC4	Do not send F	FETCH command		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid2>, FALSE))</isd_p_aid2>	SW=0x9300	RQ57_127_1 RQ57_140_1
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1, #PROFILE_INFO2 } SW=0x9000	

Test Sequence #08 Error: Enable Profile by ICCID with refreshFLag set while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 has been installed on the eUICC

V1.4 Page 204 of 777

eUICC	The PROFILE_OPERATIONAL2 is Disabled on the eUICC
-------	---

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR	
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	
IC4	Do not send F	FETCH command		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_ENABLE_PROFILE(#ICCID_OP_PROF2, NO_PARAM, TRUE))	SW=0x9300	RQ57_133_1 RQ57_140_1
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1, #PROFILE_INFO2 } SW=0x9000	

4.2.21.2.3TC_eUICC_ES10c.EnableProfile_Case4

General Initial Conditions		
Entity Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	

Test Sequence #01 Nominal: Enable Profile by ISD-P AID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

V1.4 Page 205 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SELECT_	ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	#R_ENABLE_PROFILE_ OK SW=0x91XX	RQ24_010 RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_136 RQ57_137
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_016_3 RQ32_017 RQ57_134
3	Repeat IC1 a	nd IC2		
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse:: = profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ24_010 RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_136 RQ57_137
5	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
6	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

Test Sequence #02 Nominal: Enable Profile by ICCID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM,	#R_ENABLE_PROFILE_OK SW=0x91XX	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3

V1.4 Page 206 of 777

		TRUE))		RQ57_136 RQ57_137
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_016_3 RQ32_017 RQ57_134
3	Repeat IC1 and	d IC2		
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_136 RQ57_137
5	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
6	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

Test Sequence #03 Nominal: Enable Profile by ISD-P AID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE_eUICC	CProfileStateChanged	
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SELECT_	ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	#R_ENABLE_PROFILE_O K SW=0x91XX	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_136 RQ57_137
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State change")	RQ32_016_3 RQ32_017 RQ57_134
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	Execute IC1 from step 2 to step 4			

V1.4 Page 207 of 777

5	Repeat IC2			
6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_136 RQ57_137
7	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
8	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

Test Sequence #04 Nominal: Enable Profile by ICCID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileStateChanged				
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SELEC	T_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	#R_ENABLE_PROFILE_OK SW=0x91XX	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3 RQ57_136 RQ57_137	
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State change")	RQ32_016_3 RQ32_017 RQ57_134	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000		
4	Execute IC1 from	om step 2 to step 4			
5	Repeat IC2				
6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_016_1 RQ32_016_2 RQ57_128 RQ57_129 RQ57_133_3	

V1.4 Page 208 of 777

				RQ57_136 RQ57_137
7	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
8	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

Test Sequence #05 Nominal: Enable Profile by ISD-P AID and "refreshFlag" not set

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, FALSE))</isd_p_aid1>	#R_ENABLE_PROFILE_O K SW=0x9000	RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_136 RQ57_137 RQ57_137
2	S_Device → eUICC	[TERMINAL_PROFILE]	Toolkit initialization THEN SW=0x9000	RQ32_018_1 RQ57_135_4
3	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_136 RQ57_137 RQ57_137
4	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000	
5	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015

V1.4 Page 209 of 777

Test Sequence #06 Nominal: Enable Profile by ICCID and "refreshFlag" not set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC	UICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	_LOGICAL_CHANNEL_AND_SELECT_I	SDR		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, FALSE))	#R_ENABLE_PROFILE_ OK SW=0x9000	RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_136 RQ57_137 RQ57_137	
2	S_Device → eUICC	[TERMINAL_PROFILE]	Toolkit initialization THEN SW=0x9000	RQ32_018_1 RQ57_135_4	
3	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_017_1 RQ32_017_2 RQ57_128 RQ57_129 RQ57_132 RQ57_136 RQ57_137 RQ57_137	
4	S_Device → eUICC	[SELECT_ICCID]	SW=0x9000		
5	S_Device → eUICC	[READ_BINARY] with <l>=0x0A</l>	#ICCID_OP_PROF1 SW=0x9000	RQ34_015	

4.2.21.2.4TC_eUICC_ES10c.EnableProfile_ErrorCases_Case4

General Initial Conditions	
Entity Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC

Test Sequence #01 Error: Enable Profile by an unknown ISD-P AID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

V1.4 Page 210 of 777

eUICC The Operational Profile identified by the ISD-P AID <isd_p_aidx> is not lo</isd_p_aidx>	aded
---	------

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aidx>, TRUE))</isd_p_aidx>	#R_ENABLE_PROFILE_ICCID_ISD P_NOTFOUND SW=0x9000	RQ32_011 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_136 RQ57_137
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000	RQ32_011 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_136 RQ57_137

Test Sequence #02 Error: Enable Profile by an unknown ICCID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The Operational Profile identified by the ICCID #ICCID_OP_PROFX is not loaded

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(#ICCID_OP_PROFX, NO_PARAM, TRUE))	#R_ENABLE_PROFILE_ICCID_ISDP _NOTFOUND SW=0x9000	RQ32_011 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_136 RQ57_137
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000	RQ32_011 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_130 RQ57_136 RQ57_137

V1.4 Page 211 of 777

Test Sequence #03 Error: Enable Profile (by ISD-P AID) is not possible when this Operational Profile is in Enable state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SE	LECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	#R_ENABLE_PROFILE_NOT_DISAB LE_STATE SW=0x9000	RQ32_011 RQ32_012 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_136 RQ57_137
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_012 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_136 RQ57_137

Test Sequence #04 Error: Enable Profile (by ICCID) is not possible when this Operational Profile is in Enabled state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	JICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	#R_ENABLE_PROFILE_NOT_ DISABLE_STATE SW=0x9000	RQ32_011 RQ32_012 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_136 RQ57_137

V1.4 Page 212 of 777

2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_011 RQ32_012 RQ32_016_1 RQ57_127 RQ57_128 RQ57_129 RQ57_136 RQ57_137
---	------------------	--	--	--

Test Sequence #05 Error: Enable Profile (by ISD-P AID) not possible when an Operational Profile with PPR1 is loaded

The purpose of this test is to ensure that it is NOT possible to enable an Operational Profile when there is another Operational Profile Enabled with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Profile is installed on the eUICC (this condition overrides the general initial condition defined in this test case)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT	_ISDR	
IC3		Install PROFILE_OPERATIONAL4 NOTE: The PROFILE_OPERATIONAL4 corresponds to <isd_p_aid4></isd_p_aid4>		
IC4		Install PROFILE_OPERATIONAL1 NOTE: The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>		
IC5	Enable PROFILE_OPERATIONAL4			
1	S_LPAd → eUICC	MTD_STORE_DATA (MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	#R_ENABLE_PROFILE_DISA LLOWEDbyPOLICY SW=0x9000	RQ57_127 RQ57_128 RQ57_129 RQ57_136 RQ57_147
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED #PROFILE_INFO4_ENABLED } SW=0x9000	RQ57_127 RQ57_128 RQ57_129

V1.4 Page 213 of 777

Test Sequence #06 Error: Enable Profile (by ICCID) not possible when an Operational Profile with PPR1 is loaded

The purpose of this test is to ensure that it is NOT possible to enable an Operational Profile when there is another Operational Profile Enabled with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	No Profile is installed on the eUICC (this condition overrides the general initial condition defined in this test case)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	ISDR	
IC3	Install PROFIL	LE_OPERATIONAL4		
IC4	Install PROFIL	LE_OPERATIONAL1		
IC5	Enable PROF	Enable PROFILE_OPERATIONAL4		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	#R_ENABLE_PROFILE_DISA LLOWEDbyPOLICY SW=0x9000	RQ57_127 RQ57_128 RQ57_129 RQ57_136 RQ57_147
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED #PROFILE_INFO4_ENABLED } SW=0x9000	RQ57_127 RQ57_128 RQ57_129

Test Sequence #07 Error: Enable Profile by ISD-P AID without refreshFlag while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 corresponds to <isd_p_aid2></isd_p_aid2>

V1.4 Page 214 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR	
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	
IC4	Do not send F	FETCH command		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(NO_PARAM, <isd_p_aid2>, FALSE))</isd_p_aid2>	resp EnableProfileResponse ::= { enableResult catBusy } SW=0x9000 or 0x91XX	RQ57_127_1
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1, #PROFILE_INFO2 } SW=0x9000	

Test Sequence #08 Error: Enable Profile by ICCID with refreshFlag set while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	

V1.4 Page 215 of 777

IC4	Do not send FETCH command			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_ENABLE_PROFILE(#ICCID_OP_PROF2, NO_PARAM, TRUE))	resp EnableProfileResponse ::= { enableResult catBusy } SW=0x9000 or 0x91XX	RQ57_133_1
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1, #PROFILE_INFO2 } SW=0x9000	

4.2.22 ES10c (LPA -- eUICC): DisableProfile

4.2.22.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_025
- RQ29 002, RQ29 022
- RQ32_031, RQ32_032, RQ32_033, RQ32_034, RQ32_038, RQ32_037_1, RQ32_039, RQ32_039_1, RQ32_041_1, RQ32_041_2
- RQ57_141, RQ57_142, RQ57_142_1, RQ57_142_2, RQ57_142_3, RQ57_142_4, RQ57_142_6, RQ57_142_9, RQ57_142_10, RQ57_142_12, RQ57_142_13, RQ57_142_14, RQ57_149, RQ57_150, RQ57_151, RQ57_152, RQ57_153, RQ57_153_1

4.2.22.2 Test Cases

4.2.22.2.1TC_eUICC_ES10c.DisableProfile_Case3

General Initial Conditions		
Entity	Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	

V1.4 Page 216 of 777

Test Sequence #01 Nominal: Disable Profile by ISD-P AID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SELECT_IS	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	No response data is returned SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151 RQ24_010
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14
3	Repeat IC1 and	d IC2		
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABL ED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151 RQ24_010
5	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025

Test Sequence #02 Nominal: Disable Profile by ICCID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

V1.4 Page 217 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	No response data is returned SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14
3	Repeat IC1 an	d IC2		
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151
5	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025

Test Sequence #03 Nominal: Disable Profile by ISD-P AID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

St	tep	Direction	Sequence / Description	Expected result	REQ
IC	1	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileStateChanged			
IC:	2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 218 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	No response data is returned SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151 RQ24_010
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State changed")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	Execute IC1 fr	om step 2 to step 4		
5	Repeat IC2			
6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABL ED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151 RQ24_010
7	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025

Test Sequence #04 Nominal: Disable Profile by ICCID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileStateChanged			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	No response data is returned SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151

V1.4 Page 219 of 777

2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State changed")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	Execute IC1 from step 2 to step 4			
5	Repeat IC2			
6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABL ED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_151
7	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025

Test Sequence #05 Nominal: Disable Profile by ISD-P AID and "refreshFlag" no set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, FALSE))</isd_p_aid1>	No response data is returned SW=0x9000	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1 RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_151 RQ29_002 RQ29_022
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM,	response ProfileInfoListResponse::= profileInfoListOk : {	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1

V1.4 Page 220 of 777

		<isd_p_aid1>))</isd_p_aid1>	#PROFILE_INFO1_DISAB LED } SW=0x9000	RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_151
3	S_Device → eUICC	[SELECT_ICCID]	SW=0x6A82	RQ24_025

Test Sequence #06 Nominal: Disable Profile by ICCID and "refreshFlag" no set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, FALSE))	No response data is returned SW=0x9000	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1 RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_151 RQ29_002 RQ29_022
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISAB LED } SW=0x9000	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1 RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_151
3	S_Device → eUICC	[SELECT_ICCID]	SW=0x6A82	RQ24_025

V1.4 Page 221 of 777

4.2.22.2.2TC_eUICC_ES10c.DisableProfile_ErrorCases_Case3

General Initial Conditions		
Entity	Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	

Test Sequence #01 Error: Disable Profile by an unknown ISD-P AID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>
eUICC	The Operational Profile identified by the ISD-P AID <isd_p_aidx> is not loaded</isd_p_aidx>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aidx>, TRUE))</isd_p_aidx>	SW=0x6A82	RQ32_031 RQ32_033 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_151 RQ57_152
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_031 RQ32_033 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_151 RQ57_152

Test Sequence #02 Error: Disable Profile by an unknown ICCID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The Operational Profile identified by the ICCID #ICCID_OP_PROFX is not loaded

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			

V1.4 Page 222 of 777

IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(#ICCID_OP_PROFX, NO_PARAM, TRUE))	SW=0x6A82	RQ32_031 RQ32_033 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_151 RQ57_152
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	RQ32_031 RQ32_033 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_151 RQ57_152

Test Sequence #03 Error: Disable Profile (by ISD-P AID) is not possible when this Operational Profile is in Disabled state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT	_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	SW=0x6985	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_4 RQ57_142_15 RQ57_151 RQ57_153
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLE D } SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_4 RQ57_142_15 RQ57_151 RQ57_153

V1.4 Page 223 of 777

Test Sequence #04 Error: Disable Profile (by ICCID) is not possible when this Operational Profile is in Disabled state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_IS	DR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	SW=0x6985	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_4 RQ57_142_15 RQ57_151 RQ57_153
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISAB LED } SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_4 RQ57_142_15 RQ57_151 RQ57_153

Test Sequence #05 Error: Disable Profile (by ISD-P AID) not possible when PPR1 is set

The purpose of this test is to ensure that it is NOT possible to disable an Operational Profile4 with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded (this condition overrides the general initial condition defined in this test case)
eUICC The PROFILE_OPERATIONAL4 has been installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL4 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL4 corresponds to <isd_p_aid4></isd_p_aid4>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 224 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid4>, TRUE))</isd_p_aid4>	SW=0x6985	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_15 RQ57_151 RQ57_153
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid4>))</isd_p_aid4>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO4_ENABLED } SW=0x9000	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_15 RQ57_151 RQ57_153

Test Sequence #06 Error: Disable Profile (by ICCID) not possible when PPR1 is set

The purpose of this test is to ensure that it is NOT possible to disable an Operational Profile4 with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is not loaded (this condition overrides the general initial condition defined in this test case)
eUICC	The PROFILE_OPERATIONAL4 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL4 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(#ICCID_OP_PROF4, NO_PARAM, TRUE))	SW=0x6985	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_15 RQ57_151 RQ57_153
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF4,	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO4_ENABLED	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2

V1.4 Page 225 of 777

Test Sequence #07 Error: Disable Profile by ISDP-AID without refreshFlag while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELE	ECT_ISDR	
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	
IC4	Do not send F	FETCH command		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, FALSE))</isd_p_aid1>	SW=0x9300	RQ57_142 RQ57_153_1
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	

Test Sequence #08 Error: Disable Profile by ICCID with refreshFlag set while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

V1.4 Page 226 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SELE	ECT_ISDR	
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	
IC4	Do not send F	FETCH command		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	SW=0x9300	RQ57_142_10 RQ57_153_1
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW=0x9000	

4.2.22.2.3TC_eUICC_ES10c.DisableProfile_Case4

General Initial Conditions		
Entity	Entity Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	

Test Sequence #01 Nominal: Disable Profile by ISD-P AID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC	
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		

V1.4 Page 227 of 777

IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	#R_DISABLE_PROFILE_OK SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_149 RQ57_150 RQ24_010	
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14 RQ57_147	
3	Repeat IC1 ar	nd IC2			
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABL ED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_149 RQ57_150 RQ24_010	
5	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025	

Test Sequence #02 Nominal: Disable Profile by ICCID and "refreshFlag" set when Device supports "UICC Reset"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	#R_DISABLE_PROFILE_O K SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12	

V1.4 Page 228 of 777

				RQ57_149 RQ57_150	
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14 RQ57_147	
3	Repeat IC1 and IC2				
4	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABL ED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_149 RQ57_150	
5	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025	

Test Sequence #03 Nominal: Disable Profile by ISD-P AID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC	
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>	

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileStateChanged				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	#R_DISABLE_PROFILE_OK SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_149 RQ57_150 RQ24_010		
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State changed")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14 RQ57_147		

V1.4 Page 229 of 777

3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000			
4	Execute IC1 fi	ute IC1 from step 2 to step 4				
5	Repeat IC2					
6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_149 RQ57_150 RQ24_010		
7	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025		

Test Sequence #04 Nominal: Disable Profile by ICCID and "refreshFlag" set when Device supports "eUICC Profile State Change"

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileStateChanged				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELEC	CT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	#R_DISABLE_PROFILE_OK SW=0x91XX	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_149 RQ57_150	
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("eUICC Profile State changed")	RQ32_038 RQ32_039 RQ32_039_1 RQ32_041_2 RQ57_142_13 RQ57_142_14 RQ57_147	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000		
4	Execute IC1 from step 2 to step 4				
5	Repeat IC2				

V1.4 Page 230 of 777

6	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000	RQ32_031 RQ32_033 RQ32_037_1 RQ57_142_2 RQ57_142_3 RQ57_142_12 RQ57_149 RQ57_150
7	S_Device → eUICC	[SELECT_ICCID]	SW=6A82	RQ24_025

Test Sequence #05 Nominal: Disable Profile by ISD-P AID and "refreshFlag" no set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, FALSE))</isd_p_aid1>	#R_DISABLE_PROFILE_ OK SW=0x9000	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1 RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_149 RQ57_150
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISAB LED } SW=0x9000	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1 RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_149 RQ57_149
3	S_Device → eUICC	[SELECT_ICCID]	SW=0x6A82	RQ24_025

V1.4 Page 231 of 777

Test Sequence #06 Nominal: Disable Profile by ICCID and "refreshFlag" no set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, FALSE))	#R_DISABLE_PROFILE_ OK SW=0x9000	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1 RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_149 RQ57_150
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISAB LED } SW=0x9000	RQ32_031 RQ32_033 RQ32_038 RQ32_041_1 RQ57_142_1 RQ57_142_2 RQ57_142_3 RQ57_142_6 RQ57_142_9 RQ57_142_14 RQ57_149 RQ57_149
3	S_Device → eUICC	[SELECT_ICCID]	SW=0x6A82	RQ24_025

4.2.22.2.4TC_eUICC_ES10c.DisableProfile_ErrorCases_Case4

General Initial Conditions	
Entity Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC

Test Sequence #01 Error: Disable Profile by an unknown ISD-P AID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

V1.4 Page 232 of 777

eUICC The Operational Profile identified by the ISD-P AID <isd_p_a< th=""><th>_AIDX> is not loaded</th></isd_p_a<>	_AIDX> is not loaded
---	----------------------

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	CC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SI	ELECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aidx>, TRUE))</isd_p_aidx>	#R_DISABLE_PROFILE_ICCID_ISD P_NOTFOUND SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150

Test Sequence #02 Error: Disable Profile by an unknown ICCID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC
eUICC	The Operational Profile identified by the ICCID #ICCID_OP_PROFX is not loaded

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(#ICCID_OP_PROFX, NO_PARAM, TRUE))	#R_DISABLE_PROFILE_ICCID_IS DP_NOTFOUND SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1,	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4

V1.4 Page 233 of 777

		NO_PARAM))	} SW=0x9000	RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150	
--	--	------------	----------------	---	--

Test Sequence #03 Error: Disable Profile (by ISD-P AID) is not possible when this Operational Profile is in Disabled state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, TRUE))</isd_p_aid1>	#R_DISABLE_PROFILE_NOT_E NABLE_STATE SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150

Test Sequence #04 Error: Disable Profile (by ICCID) is not possible when this Operational Profile is in Disabled state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				

V1.4 Page 234 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	#R_DISABLE_PROFILE_NOT_ENA BLE_STATE SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000	RQ32_031 RQ32_032 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_2 RQ57_142_15 RQ57_149 RQ57_150

Test Sequence #05 Error: Disable Profile (by ISD-P AID) not possible when PPR1 is set

The purpose of this test is to ensure that it is NOT possible to disable an Operational Profile with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded (this condition overrides the general initial condition defined in this test case)
eUICC	The PROFILE_OPERATIONAL4 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL4 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL4 corresponds to <isd_p_aid4></isd_p_aid4>

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid4>, TRUE))</isd_p_aid4>	#R_DISABLE_PROFILE_DISA LLOWEDbyPOLICY SW=0x9000	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_15 RQ57_149 RQ57_150 RQ57_141 RQ57_141	

V1.4 Page 235 of 777

				RQ57_149 RQ57_150 RQ29_002 RQ29_022
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid4>))</isd_p_aid4>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO4_ENABLED } SW=0x9000	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_15 RQ57_149 RQ57_150

Test Sequence #06 Error: Disable Profile (by ICCID) not possible when PPR1 is set

The purpose of this test is to ensure that it is NOT possible to disable an Operational Profile4 with the Policy Rule "Disabling of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is not loaded (this condition overrides the general initial condition defined in this test case)
eUICC	The PROFILE_OPERATIONAL4 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL4 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_	_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(#ICCID_OP_PROF4, NO_PARAM, TRUE))	#R_DISABLE_PROFILE_DISA LLOWEDbyPOLICY SW=0x9000	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_15 RQ57_149 RQ57_150 RQ29_002 RQ29_002		
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF4, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO4_ENABLED }	RQ32_031 RQ32_032 RQ32_033 RQ32_034 RQ57_142_2 RQ57_142_3 RQ57_142_4 RQ57_142_15		

V1.4 Page 236 of 777

	SW=0x9000	RQ57_149
		RQ57_150

Test Sequence #07 Error: Disable Profile by ISD-P AID without refreshFlag while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SELE	CT_ISDR		
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX		
IC4	Do not send F	ETCH command			
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(NO_PARAM, <isd_p_aid1>, FALSE))</isd_p_aid1>	resp DisableProfileResponse ::= { disableResult catBusy } SW=0x9000 or 0x91XX	RQ57_142	
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK		
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000		
4	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000		

Test Sequence #08 Error: DisableProfile by ICCID with refreshFlag set while proactive session is ongoing

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled

V1.4 Page 237 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEI	LECT_ISDR	
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	
IC4	Do not send F	ETCH command		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DISABLE_PROFILE(#ICCID_OP_PROF1, NO_PARAM, TRUE))	resp DisableProfileResponse ::= { disableResult catBusy } SW=0x9000 or 0x91XX	RQ57_142_10
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
4	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1 } SW=0x9000	

4.2.23 ES10c (LPA -- eUICC): DeleteProfile

4.2.23.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_016, RQ24_020
- RQ29_002, RQ29_022
- RQ32_049, RQ32_050, RQ32_051, RQ32_052
- RQ57_119, RQ57_154, RQ57_155, RQ57_156, RQ57_157, RQ57_158, RQ57_159, RQ57_160, RQ57_161, RQ57_162

4.2.23.2 Test Cases

4.2.23.2.1TC_eUICC_ES10c.DeleteProfile_Case3

General Initial Conditions

V1.4 Page 238 of 777

Entity	Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	

Test Sequence #01 Nominal: Delete Profile by ISD-P AID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELE	CT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aid1>)</isd_p_aid1>	No response data is returned SW=0x9000	RQ24_016 RQ32_049 RQ32_051 RQ32_052 RQ57_154 RQ57_160 RQ24_010
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk: { } SW=0x9000	RQ57_119 RQ24_010

Test Sequence #02 Nominal: Delete Profile by ICCID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(#ICCID_OP_PROF1, NO_PARAM)	No response data is returned SW=0x9000	RQ24_016 RQ32_049 RQ32_051 RQ32_052 RQ57_154 RQ57_158 RQ57_160

V1.4 Page 239 of 777

2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { } SW=0x9000	RQ24_020 RQ57_119	
---	------------------	--	--	----------------------	--

4.2.23.2.2TC_eUICC_ES10c.DeleteProfile_ErrorCases_Case3

General Initial Conditions		
Entity Description of the initial condition		
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL2 has been installed on the eUICC	

Test Sequence #01 Error: Delete Profile not possible with unknown ISD-P AID

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile with an unknown ISD-P AID.

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The Operational Profile identified by the ISD-P AID <isd_p_aidx> is not loaded</isd_p_aidx>	
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC	
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>	
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC	
eUICC	The PROFILE_OPERATIONAL2 corresponds to <isd_p_aid2></isd_p_aid2>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	LECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aidx>)</isd_p_aidx>	SW=0x6A82	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_160 RQ57_161
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED } SW=0x9000	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_160 RQ57_161

V1.4 Page 240 of 777

Test Sequence #02 Error: Delete Profile not possible with unknown ICCID

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile with an unknown ICCID.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The Operational Profile identified by the ICCID #ICCID_OP_PROFX is not loaded
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(#ICCID_OP_PROFX, NO_PARAM)	SW=0x6A82	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_160 RQ57_161
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED } SW=0x9000	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_160 RQ57_161

Test Sequence #03 Error: Delete Profile (by ISD-P AID) not possible when this Operational Profile is in Enabled state

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile in Enabled state.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 corresponds to <isd_p_aid2></isd_p_aid2>

V1.4 Page 241 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aid2>)</isd_p_aid2>	SW=0x6985	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_160 RQ57_162
2	S_LPAd →eUICC	MTD_STORE_DATA (#GET_PROFILES_INFO_ALL)	profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED } SW=0x9000	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_160 RQ57_162

Test Sequence #04 Error: Delete Profile (by ICCID) not possible when this Operational Profile is in Enabled state

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile in Enabled state.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	LECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(#ICCID_OP_PROF2, NO_PARAM)	SW=0x6985	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_160 RQ57_162
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED } SW=0x9000	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_160 RQ57_162

V1.4 Page 242 of 777

Test Sequence #05 Error: Delete Profile (by ISD-P AID) not possible when PPR2 is set

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile with the Policy Rule "Deletion of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL3 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL3 corresponds to <isd_p_aid3></isd_p_aid3>
eUICC	The Nickname of the PROFILE_OPERATIONAL3 is equal to #NICKNAME3
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aid3>)</isd_p_aid3>	SW=0x6985	RQ24_016 RQ29_002 RQ29_022 RQ32_049 RQ32_050 RQ57_154 RQ57_156 RQ57_160 RQ57_160
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED, #PROFILE_INFO3 } SW=0x9000	RQ57_154 RQ57_156 RQ57_160 RQ57_162

Test Sequence #06 Error: Delete Profile (by ICCID) not possible when PPR2 is set

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile with the Policy Rule "Deletion of this Profile is not allowed".

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL3 is Disabled on the eUICC

V1.4 Page 243 of 777

eUICC	The Nickname of the PROFILE_OPERATIONAL3 is equal to #NICKNAME3
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	PROC_EUICC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELEC	T_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA_Case3(MTD_DELETE_PROFILE(#ICCID_OP_PROF3, NO_PARAM)	SW=0x6985	RQ24_016 RQ29_002 RQ29_022 RQ32_049 RQ32_050 RQ57_154 RQ57_156 RQ57_160 RQ57_160
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED, #PROFILE_INFO3 } SW=0x9000	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_156 RQ57_160 RQ57_162

4.2.23.2.3TC_eUICC_ES10c.DeleteProfile_Case4

General Initial Conditions		
Entity Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	

Test Sequence #01 Nominal: Delete Profile by ISD-P AID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 244 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aid1>)</isd_p_aid1>	#R_DELETE_PROFILE_OK SW=0x9000	RQ24_010 RQ24_016 RQ24_020 RQ32_049 RQ32_051 RQ32_052 RQ57_154 RQ57_158 RQ57_159 RQ57_160
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(NO_PARAM, <isd_p_aid1>))</isd_p_aid1>	response ProfileInfoListResponse::= profileInfoListOk: { } SW=0x9000	RQ24_010 RQ24_020 RQ57_119

Test Sequence #02 Nominal: Delete Profile by ICCID

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELI	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DELETE_PROFILE(#ICCID_OP_PROF1, NO_PARAM)	#R_DELETE_PROFILE_OK SW=0x9000	RQ24_016 RQ24_020 RQ32_049 RQ32_051 RQ32_052 RQ57_154 RQ57_158 RQ57_159
2	S_LPAd →eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	response ProfileInfoListResponse::= profileInfoListOk: { } SW=0x9000	RQ24_020 RQ57_119

4.2.23.2.4TC_eUICC_ES10c.DeleteProfile_ErrorCases_Case4

General Initial Conditions		
Entity Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	
eUICC The PROFILE_OPERATIONAL2 has been installed on the eUICC		

V1.4 Page 245 of 777

Test Sequence #01 Error: Delete Profile not possible with unknown ISD-P AID

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile with an unknown ISD-P AID.

Initial Conditions	
Entity	Description of the initial condition
eUICC	A Operational Profile identified by the ISD-P AID <isd_p_aidx> is not loaded</isd_p_aidx>
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 corresponds to <isd_p_aid2></isd_p_aid2>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUIC	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aidx>)</isd_p_aidx>	#R_DELETE_PROFILE_ICCID_IS DP_NOTFOUND SW=0x9000	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_158 RQ57_159
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED } SW=0x9000	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_158 RQ57_159

Test Sequence #02 Error: Delete Profile not possible with unknown ICCID

The purpose of this test is to ensure that it is NOT possible to delete an Operational with an ICCID unknown.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The Operational Profile identified by the ICCID #ICCID_OP_PROFX is not loaded
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC

V1.4 Page 246 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DELETE_PROFILE(#ICCID_OP_PROFX, NO_PARAM)	#R_DELETE_PROFILE_ICCID_IS DP_NOTFOUND SW=0x9000	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_158 RQ57_159
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED } SW=0x9000	RQ24_016 RQ32_049 RQ57_154 RQ57_157 RQ57_158 RQ57_159

Test Sequence #03 Error: Delete Profile (by ISD-P AID) not possible when this Operational Profile is in Enabled state

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile in Enabled state.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL1 corresponds to <isd_p_aid1></isd_p_aid1>
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 corresponds to <isd_p_aid2></isd_p_aid2>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	C_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aid2>)</isd_p_aid2>	#R_DELETE_PROFILE_NOTDIS ABLESTATE SW=0x9000	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_158 RQ57_159
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED,	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155

V1.4 Page 247 of 777

#PROFILE_INFO2_ENABLED	RQ57_158
1	RQ57_159
SW=0x9000	

Test Sequence #04 Error: Delete Profile (by ICCID) not possible when this Operational Profile is in Enabled state

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile in Enabled state.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_	ROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SELE	CT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DELETE_PROFILE(#ICCID_OP_PROF2, NO_PARAM)	#R_DELETE_PROFILE_NOTDISA BLESTATE SW=0x9000	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_158 RQ57_159	
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED } SW=0x9000	RQ24_016 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_158 RQ57_159	

Test Sequence #05 Error: Delete Profile (by ISD-P AID) not possible when PPR2 is set

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile with the Policy Rule "Deletion of this Profile is not allowed".

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL3 is Disabled on the eUICC	
eUICC	The PROFILE_OPERATIONAL3 corresponds to <isd_p_aid3></isd_p_aid3>	
eUICC	The Nickname of the PROFILE_OPERATIONAL3 is equal to #NICKNAME3	

V1.4 Page 248 of 777

Non-confidential

eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(MTD_DELETE_PROFILE(NO_PARAM, <isd_p_aid3>)</isd_p_aid3>	#R_DELETE_PROFILE_DISALLO WEDBYPOLICY SW=0x9000	RQ24_016 RQ29_002 RQ32_049 RQ32_050 RQ57_154 RQ57_156 RQ57_158 RQ57_159 RQ29_002 RQ29_002
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED, #PROFILE_INFO3 } SW=0x9000	RQ24_016 RQ29_002 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_158 RQ57_159

Test Sequence #06 Error: Delete Profile (by ICCID) not possible when PPR2 is set

The purpose of this test is to ensure that it is NOT possible to delete an Operational Profile with the Policy Rule "Deletion of this Profile is not allowed".

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL3 is Disabled on the eUICC	
eUICC	The Nickname of the PROFILE_OPERATIONAL3 is equal to #NICKNAME3	
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC	
eUICC	The PROFILE_OPERATIONAL2 is Enabled on the eUICC	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	I I WID STORE DATAL I ===>\range ==\range		RQ24_016 RQ29_002	

V1.4 Page 249 of 777

		MTD_DELETE_PROFILE(#ICCID_OP_PROF3, NO_PARAM)	SW=0x9000	RQ32_049 RQ32_050 RQ57_154 RQ57_156 RQ57_158 RQ57_159 RQ29_002 RQ29_002
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISABLED, #PROFILE_INFO2_ENABLED, #PROFILE_INFO3 } SW=0x9000	RQ24_016 RQ29_002 RQ32_049 RQ32_050 RQ57_154 RQ57_155 RQ57_158 RQ57_159

4.2.24 ES10c (LPA -- eUICC): eUICCMemoryReset

4.2.24.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_020
- RQ29_005
- RQ31_027, RQ31_028
- RQ33_011, RQ33_008, RQ33_009, RQ33_010, RQ33_012
- RQ35_006
- RQ57_051, RQ57_052, RQ57_054, RQ57_163, RQ57_165, RQ57_165_1, RQ57_166, RQ57_167, RQ57_167_1, RQ57_168, RQ57_169, RQ57_170

4.2.24.2 Test Cases

4.2.24.2.1TC_eUICC_ES10c.eUICCMemoryReset

General Initial Conditions		
Entity Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	
eUICC	The Default SM-DP+ Address #TEST_DP_ADDRESS1 has been set on the IS R.	

Test Sequence #01 Nominal: Reset All Operational Profiles (without Enabled Profile)

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC

V1.4 Page 250 of 777

eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL3 is Disabled on the eUICC	
eUICC	The Nickname of the PROFILE_OPERATIONAL3 is equal to #NICKNAME3	
eUICC	No Notification is stored in the eUICC's Pending Notifications List	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SELECT_I	SDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	Retrieve free non-volatile memory value (tag 0x82) from <ext_card_resource > in EUICCInfo2 as <free_mem_op_prof_ INSTALLED></free_mem_op_prof_ </ext_card_resource 	
2	S_LPAd → eUICC	MTD_STORE_DATA(#EUICC_MEMORY_RESET_OP_PR O)	#R_EUICC_MEMORY_RE SET_OK SW=0x9000	RQ57_163 RQ57_166 RQ57_169 RQ57_170 RQ33_010
3	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { } SW=0x9000	RQ33_011 RQ33_008 RQ33_012
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DE1 SW = 0x9000	RQ57_071 RQ57_071 _1 RQ57_071 _2 RQ57_072 _1 RQ57_072 _1 RQ57_072 _2 RQ57_074 RQ57_167 _1
5	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	Retrieve free non-volatile memory value (tag 0x82) from <ext_card_resource> in EUICCInfo2 as <free_memory_no_p rofile=""> Verify that <free_mem_op_prof_installed> is lower than <free_memory_no_p rofile=""></free_memory_no_p></free_mem_op_prof_installed></free_memory_no_p></ext_card_resource>	RQ31_027 RQ31_028 RQ57_051 RQ57_052 RQ57_054 RQ24_020

V1.4 Page 251 of 777

6	S_LPAd → eUICC	MTD_STORE_DATA(#R_ES10a_GECA_DS_DP	
		#GET_EUICC_CONFIGURED_ADDR	_1	RQ33_009
		ESSES)	SW = 0x9000	

Test Sequence #02 Nominal: Reset All Operational Profiles (with Enabled Profile)

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC	
eUICC	No Notification is stored in the eUICC's Pending Notifications List	

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE					
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR					
1	S_LPAd → eUICC	MTD_STORE_DATA(#EUICC_MEMORY_RESET_OP_PRO)	#R_EUICC_MEMORY_RE SET_OK SW=0x91XX	RQ57_163 RQ57_166 RQ57_169 RQ57_170 RQ33_010		
2	S_Device →eUICC	FETCH 'XX'	REFRESH Command ("UICC Reset")	RQ57_168		
3	Repeat IC1 and IC2					
4	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DE1 SW = 0x9000 Note : A Disable Notification for PROFILE_OPERATIONAL 1 MAY be also present in the response	RQ57_071 RQ57_071_1 RQ57_071_2 RQ57_072 RQ57_072_1 RQ57_072_2 RQ57_074 RQ57_167_1 RQ35_006		
5	S_LPAd → eUICC	MTD_STORE_DATA(#GET_RAT)	#R_DEFAULT_RAT SW = 0x9000	RQ29_005 RQ57_179 RQ57_180 RQ57_181 RQ57_182 RQ57_184		
6	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { } SW=0x9000	RQ33_011 RQ33_008 RQ33_012		

V1.4 Page 252 of 777

Test Sequence #03 Nominal: Reset the Default SM-DP+ Address only

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL3 is Disabled on the eUICC
eUICC	The Nickname of the PROFILE_OPERATIONAL3 is equal to #NICKNAME3

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SELECT_ISI	DR		
1	S_LPAd → eUICC	MTD_STORE_DATA(#EUICC_MEMORY_RESET_DEF_SMD PADDRESS)	#R_EUICC_MEMORY_RE SET_OK SW=0x9000	RQ57_163 RQ57_167 RQ57_169 RQ57_170 RQ33_010	
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1_DISAB LED, #PROFILE_INFO3 } SW=0x9000		
3	S_LPAd →eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADDRE SSES)	#R_ES10a_GECA_DS SW = 0x9000	RQ33_008	

Test Sequence #04 Nominal: Reset All Operational Profiles and the Default SM-DP+ Address

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Disabled on the eUICC
eUICC	The PROFILE_OPERATIONAL3 has been installed on the eUICC
eUICC	The PROFILE_OPERATIONAL3 is Disabled on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 253 of 777

1	S_LPAd → eUICC	MTD_STORE_DATA(#EUICC_MEMORY_RESET)	#R_EUICC_MEMORY_RE SET_OK SW=0x9000	RQ57_163 RQ57_166 RQ57_167 RQ57_169 RQ57_170 RQ33_010
2	S_LPAd →eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { } SW=0x9000	RQ33_011 RQ33_008 RQ33_012
3	S_LPAd →eUICC	MTD_STORE_DATA(#GET_EUICC_CONFIGURED_ADDRE SSES)	#R_ES10a_GECA_DS SW = 0x9000	RQ33_008

4.2.24.2.2TC_eUICC_ES10c.eUICCMemoryReset_ErrorCases

Test Sequence #01 Error: eUICC Memory Reset while proactive session is ongoing

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 has been installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL1 is Enabled on the eUICC	
eUICC	The PROFILE_OPERATIONAL2 has been installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL2 is Disabled on the eUICC	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	I_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
IC3	S_Device → eUICC	MTD_SEND_SMS_PP([GET_MNO_SD])	SW=0x91XX	
IC4	Do not send F	FETCH command		
1	S_LPAd → eUICC	MTD_STORE_DATA(#EUICC_MEMORY_RESET_O P_PRO)	resp EuiccMemoryResetResponse::= { resetResult catBusy } SW=0x9000 or 0x91XX	RQ57_165_ 1
2	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x00 – POR OK	
3	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	

V1.4 Page 254 of 777

4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1, #PROFILE_INFO2 } SW=0x9000	RQ57_165
---	-------------------	---	--	----------

Test Sequence #02 Error: Nothing to delete

Initial Conditions		
Entity	Description of the initial condition	
eUICC	No Profile is loaded on the eUICC	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_	INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#EUICC_MEMORY_RESET_O P_PRO)	resp EuiccMemoryResetResponse::= { resetResult nothingToDelete } SW=0x9000	RQ57_163

4.2.25 ES10c (LPA -- eUICC): GetEID

4.2.25.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ33_002
- RQ57_171, RQ57_172, RQ57_172_1

4.2.25.2 Test Cases

4.2.25.2.1TC_eUICC_ES10c.GetEID

Test Sequence #01 Nominal

The purpose of this test is to ensure that it is possible to retrieve the EID.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_	NITIALIZATION_SEQUENCE		

V1.4 Page 255 of 777

Non-confidential

IC2 PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1 S_LPAd → MTD_STORE_DATA(eUICC #GET_EID)		resp GetEuiccDataResponse ::= { eidValue #EID1 } SW=0x9000	RQ33_002 RQ57_171 RQ57_172	

Test Sequence #02 Error

The purpose of this test is to ensure that if the provided tagList is invalid or unsupported, the eUICC returns an error status word.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_IN	ITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EID_INVALID)	No response data return and SW different than 0x9000	RQ33_002 RQ57_172_1

4.2.26 ES10c (LPA -- eUICC): SetNickname

4.2.26.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

RQ57_173, RQ57_174, RQ57_175, RQ57_176, RQ57_177, RQ57_178

4.2.26.2 Test Cases

4.2.26.2.1TC_eUICC_ES10c.SetNickname

General Initial Conditions		
Entity Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 is loaded on the eUICC	

Test Sequence #01 Nominal: Add a Nickname to a Disabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is empty

V1.4 Page 256 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_NICKNAME_OP_PROF 1)	resp SetNicknameResponse ::= { setNicknameResult ok } SW=0x9000	RQ57_177 RQ57_178
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { profileNickname #NICKNAME2 } } SW=0x9000	RQ57_174

Test Sequence #02 Nominal: Update a Nickname of a Disabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is equal to #NICKNAME1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_NICKNAME_OP_PROF 1)	resp SetNicknameResponse ::= { setNicknameResult ok } SW=0x9000	RQ57_177 RQ57_178
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { profileNickname #NICKNAME2 } } SW=0x9000	RQ57_174

V1.4 Page 257 of 777

Test Sequence #03 Nominal: Remove a Nickname from a Disabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is equal to #NICKNAME1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICO	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN	_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_NICKNAME_EMPTY_O P_PROF1)	resp SetNicknameResponse ::= { setNicknameResult ok } SW=0x9000	RQ57_177 RQ57_178
2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { profileNickname SHALL not be present } } SW=0x9000	RQ57_175

Test Sequence #04 Nominal: Remove a non-existing Nickname from a Disabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is empty

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_NICKNAME_EMPTY_O P_PROF1)	resp SetNicknameResponse ::= { setNicknameResult ok } SW=0x9000	RQ57_177 RQ57_178

V1.4 Page 258 of 777

2	S_LPAd → eUICC	MTD_STORE_DATA(MTD_GET_PROFILE_INFO(#ICCID_OP_PROF1, NO_PARAM))	resp ProfileInfoListResponse ::= profileInfoListOk :{ { profileNickname SHALL not be present } } SW=0x9000	RQ57_176
---	-------------------	--	--	----------

Test Sequence #05 Nominal: Add a Nickname to an Enabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is empty

This test sequence SHALL be the same as the Test Sequence #01 defined in this section.

Test Sequence #06 Nominal: Update a Nickname of an Enabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is equal to #NICKNAME1

This test sequence SHALL be the same as the Test Sequence #02 defined in this section.

Test Sequence #07 Nominal: Remove a Nickname from an Enabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is equal to #NICKNAME1

This test sequence SHALL be the same as the Test Sequence #03 defined in this section.

Test Sequence #08 Nominal: Remove a non-existing Nickname from an Enabled Operational Profile

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Enabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is empty

This test sequence SHALL be the same as the Test Sequence #04 defined in this section.

V1.4 Page 259 of 777

Test Sequence #09 Error: ICCID not found

The purpose of this test is to ensure that the method ES10c.SetNickname returns an error in case the targeted Profile does not exist on the eUICC.

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Disabled
eUICC	The Profile identified by the ICCID #ICCID_UNKNOWN is not present on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#SET_NICKNAME_ICCID_UN KNOWN)	resp SetNicknameResponse ::= { setNicknameResult iccidNotFound } SW=0x9000	RQ57_173 RQ57_178

4.2.27 ES10b (LPA -- eUICC): GetRAT

4.2.27.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ28_001
- RQ29_006, RQ29_007, RQ29_007_1, RQ29_008, RQ29_008_1, RQ29_009,
 RQ29_010_1, RQ29_011, RQ29_012, RQ29_016, RQ29_022
- RQ57_179, RQ57_180, RQ57_181, RQ57_182, RQ57_184, RQ57_186

4.2.27.2 Test Cases

4.2.27.2.1TC_eUICC_ES10b.GetRAT

Test Sequence #01 Nominal: Get Default RAT

The purpose of this test is to verify that the eUICC can be configured with a RAT as defined in SGP.21 [3] Annex H.

V1.4 Page 260 of 777

Initial Conditions	
Entity	Description of the initial condition
eUICC	The EUM has configured the eUICC's RAT as defined in section G.2.4

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUIC	ROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SELE	CT_ISDR		
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_RAT)	#R_DEFAULT_RAT SW = 0x9000	RQ28_001 RQ29_007_1 RQ29_008 RQ29_009 RQ29_011 RQ29_016 RQ57_179 RQ57_180 RQ57_181 RQ57_182 RQ57_184 RQ57_186 RQ29_007	

Test Sequence #02 Nominal: With additional PPARs

The purpose of this test is to verify that the eUICC can be configured with a RAT that contains custom rules reflecting agreements between some Operators and OEMs. After having checked the content of the RAT, Profiles with PPR1 and PPR2 are installed in order to make sure that the eUICC accepts such PPRs.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The EUM has configured the eUICC's RAT as defined in section G.2.5
eUICC	There is no Profile installed in the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_RAT)	#R_RAT_WITH_OTHER_RULES with exact same structure and order SW = 0x9000	RQ28_001 RQ29_007_1 RQ29_008 RQ29_009 RQ29_010_1 RQ29_011 RQ29_016 RQ57_179 RQ57_180 RQ57_181

V1.4 Page 261 of 777

				RQ57_182 RQ57_184 RQ57_186 RQ29_007 RQ29_008_1
2	S_LPAd → eUICC	Install PROFILE_OPERATIONAL4	Profile successfully downloaded (i.e. ProfileInstallationResult contains a SuccessResult)	RQ29_010_1 RQ29_022 RQ29_008_1
3	S_LPAd → eUICC	Delete PROFILE_OPERATIONAL4		
4	S_LPAd → eUICC	Install PROFILE_OPERATIONAL3	Profile successfully downloaded (i.e. ProfileInstallationResult contains a SuccessResult)	RQ29_010_1 RQ29_022 RQ29_008_1

4.3 SM-DP+ interfaces

4.3.1 ES2+ (Operator -- SM-DP+): DownloadOrder

This test case is defined as FFS and not applicable for this version of test specification.

4.3.2 ES2+ (Operator -- SM-DP+): ConfirmOrder

This test case is defined as FFS and not applicable for this version of test specification.

4.3.3 ES2+ (Operator -- SM-DP+): CancelOrder

This test case is defined as FFS and not applicable for this version of test specification.

4.3.4 ES2+ (Operator -- SM-DP+): ReleaseProfile

This test case is defined as FFS and not applicable for this version of test specification.

4.3.5 ES2+ (Operator -- SM-DP+): HandleDownloadProgressInfo

This test case is defined as FFS and not applicable for this version of test specification.

4.3.6 ES2+ (Operator -- SM-DP+): TLS, Mutual Authentication, Server, Session Establishment

This test case is defined as FFS and not applicable for this version of test specification.

4.3.7 ES8+ (SM-DP+ -- eUICC): InitialiseSecureChannel

4.3.7.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

4.3.7.2 Test Cases

All testing for ES8+ functions is performed in section 4.3.13 ES9+ (LPA -- SM-DP+): GetBoundProfilePackage.

V1.4 Page 262 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

4.3.8 ES8+ (SM-DP+ -- eUICC): ConfigureISDP

4.3.8.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

4.3.8.2 Test Cases

All testing for ES8+ functions is performed in section 4.3.13 ES9+ (LPA -- SM-DP+): GetBoundProfilePackage.

4.3.9 ES8+ (SM-DP+ -- eUICC): StoreMetadata

4.3.9.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

4.3.9.2 Test Cases

All testing for ES8+ functions is performed in section 4.3.13 ES9+ (LPA -- SM-DP+): GetBoundProfilePackage.

4.3.10 ES8+ (SM-DP+ -- eUICC): ReplaceSessionKeys

4.3.10.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

4.3.10.2 Test Cases

All testing for ES8+ functions is performed in section 4.3.13 ES9+ (LPA -- SM-DP+): GetBoundProfilePackage.

4.3.11 ES8+ (SM-DP+ -- eUICC): LoadProfileElements

4.3.11.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

V1.4 Page 263 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

4.3.11.2 Test Cases

All testing for ES8+ functions is performed in section 4.3.13 ES9+ (LPA -- SM-DP+): GetBoundProfilePackage.

4.3.12 ES9+ (LPA -- SM-DP+): InitiateAuthentication

The test sequences defined in this section are intended for testing on both the SM-DP+ and the SM-DS.

4.3.12.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26_033
- RQ31_030, RQ31_033, RQ31_034, RQ31_035, RQ31_036, RQ31_037, RQ31_038, RQ31_039, RQ31_041, RQ31_042, RQ31_043, RQ31_073
- RQ45_006, RQ45_026, RQ45_026_1
- RQ56_004,RQ56_005, RQ56_006, RQ56_007, RQ56_008, RQ56_009, RQ56_010, RQ56_011, RQ56_012, RQ56_013, RQ56_014
- RQ57 106
- RQ62_001, RQ62_002, RQ62_004, RQ62_005, RQ62_006, RQ62_007
- RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_017, RQ65_018

4.3.12.2 Test Cases

General Initial Conditions for SM-DP + testing		
Entity	Description of the general initial condition	
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST	

4.3.12.2.1TC_SM-DP+_ES9+.InitiateAuthenticationNIST

Test Sequence #01 Nominal

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
1	S_LPAd → SERVER	MTD_HTTP_REQ(#SERVER_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #SERVER_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK) • Verify that <transaction_id_ia> matches <transaction_id_signed _ia=""> • Verify the validity of <server_signature1> using the public key</server_signature1></transaction_id_signed></transaction_id_ia>	Common: RQ31_030 RQ31_033 RQ31_034 RQ31_035 RQ31_037 RQ31_038 RQ31_039 RQ31_041 RQ31_042 RQ31_043

V1.4 Page 264 of 777

	#PK_SM_XXauth_ECDSA	RQ45_006
	contained in	RQ45_026
	#CERT_SM_XXauth_ECDSA	RQ45_026
	#OLITI_OW_/Madii_LODO/T	RQ57_106
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_017
		RQ65_018
		SM-DP+:
		RQ56_004
		RQ56_005
		RQ56_006
		RQ56_007
		RQ56_009
		RQ56_010
		RQ56_012
		RQ56_013
		SM-DS:
		RQ58_003
		RQ58_003 RQ58_004
		RQ58_005
		RQ58_006
		RQ58_008
		RQ58_010
		RQ58_012
		RQ58_013
		RQ58_014
		RQ58_015
		RQ58_016
		RQ58_017
		RQ58_018
		RQ58_019

Test Sequence #02 Nominal: Uniqueness of Transaction ID and Server Challenge

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
		MTD_HTTP_REQ(#SERVER_ADDRESS,		Common: RQ31_030	
S_LPAd →	#PATH_INITIATE_AUTH,	MTD_HTTP_RESP(RQ31_033		
	SERVER	MTD_INITIATE_AUTHENTICATION	#R_INITIATE_AUTH_OK)	RQ31_034 RQ31_035	
		(#S_EUICC_CHALLENGE,		RQ31_037 RQ31_038	

V1.4 Page 265 of 777

		#C_FUICO_INFO4		DO04 000
		#S_EUICC_INFO1, #SERVER_ADDRESS))		RQ31_039 RQ31_041 RQ31_042 RQ31_043 RQ45_006 RQ45_026 RQ45_026 RQ45_026_1 RQ57_106 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_017 RQ65_018 SM-DP+ RQ56_006 RQ56_010 RQ56_012 RQ56_010 RQ56_010 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_010 RQ56_012 RQ56_013 RQ58_010 RQ58_010 RQ58_010 RQ58_010 RQ58_010 RQ58_011 RQ58_011 RQ58_015 RQ58_016 RQ58_016 RQ58_017 RQ58_016 RQ58_017 RQ58_016 RQ58_017 RQ58_016
2	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on ES	9+	
3	S_LPAd → SERVER	MTD_HTTP_REQ(#SERVER_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION (#S_EUICC_CHALLENGE,	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK_2) Verify that: • <transaction_id_2> received in this step is different to the</transaction_id_2>	Common: RQ31_030 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006
-				

V1.4 Page 266 of 777

#S_EUICC_INFO1,	<transaction_id_ia> in</transaction_id_ia>	RQ62_007
#SERVER_ADDRESS))	Step 1	RQ62_009
		RQ65_001
	• <transaction_id_signe< td=""><td>RQ65_002</td></transaction_id_signe<>	RQ65_002
	D_2> received in this step is	RQ65_003
	different to the	RQ65_004
	<transaction_id_signe< td=""><td>RQ65_005</td></transaction_id_signe<>	RQ65_005
	D_IA> in Step 1	RQ65_007
	OFFICE OUTS I FNOT O	RQ65_008
	• <server_challenge_2></server_challenge_2>	RQ65_009
	received in this step is	RQ65_017
	different to the	RQ65_018
	<server_challenge> in</server_challenge>	SM-DP+:
	Step 1.	RQ56_009
		SM-DS:
		RQ56_008

Test Sequence #03 Error: Failed due to Invalid Server Address (Subject Code 8.8.1 Reason Code 3.8)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH on ES9-	+	
1	S_LPAd → SERVER	MTD_HTTP_REQ (#SERVER_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #UNKNOWN_SERVER_ADDRESS))	MTD_HTTP_RESP(#R_ERROR_SMXX_1_3_8)	Common RQ31_033 RQ31_034 RQ57_106 RQ62_001 RQ62_002 RQ65_018 SM-DP+: RQ56_004 RQ56_005 RQ56_008 RQ56_011 RQ56_014 SM-DS: RQ58_003 RQ58_004 RQ58_007 RQ58_0011 RQ58_0011 RQ58_0011

Test Sequence #04 Error: Failed due to Unsupported Public Key Identifiers (Subject Code 8.8.2 Reason Code 3.1)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
1	S_LPAd → SERVER	MTD_HTTP_REQ(#SERVER_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE,	MTD_HTTP_RESP(#R_ERROR_SMXX_2_3_1)	Common: RQ26_033 RQ31_033 RQ31_034 RQ31_035 RQ31_036

V1.4 Page 267 of 777

#EUICC_INFO1_8_8_2_3_1, #SERVER_ADDRESS))	RQ57_106 RQ62_001 RQ62_002 RQ65_018
	SM-DP+: RQ56_004 RQ56_005 RQ56_006 RQ56_008 RQ56_011 RQ56_014
	SM-DS: RQ58_003 RQ58_004 RQ58_005 RQ58_007 RQ58_011 RQ58_020

Test Sequence #05 Error: Failed due to Unsupported Specification Version Number (Subject Code 8.8.3 Reason Code 3.1)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES9+		
1	S_LPAd → SERVER	MTD_HTTP_REQ(#SERVER_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #EUICC_INFO1_8_8_3_3_1_LOWER, #SERVER_ADDRESS))	MTD_HTTP_RESP(#R_ERROR_SMXX_3_3_ 1)	Common: RQ31_033 RQ31_034 RQ57_106 RQ62_001 RQ62_002 RQ65_018 SM-DP+: RQ56_004 RQ56_008 RQ56_011 RQ56_014 SM-DS: RQ58_003 RQ58_007 RQ58_011 RQ58_020
2	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES9+		
3	S_LPAd → SERVER	MTD_HTTP_REQ(#SERVER_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #EUICC_INFO1_8_8_3_3_1_HIGHER, #SERVER_ADDRESS))	MTD_HTTP_RESP(#R_ERROR_SMXX_3_3_ 1)	Common: RQ31_033 RQ31_034 RQ57_106 RQ62_001 RQ62_002 RQ65_018 SM-DP+: RQ56_004 RQ56_008 RQ56_011 RQ56_014

V1.4 Page 268 of 777

		SM-DS:	
		RQ58_003	
		RQ58_007	
		RQ58_011	
		RQ58_020	

Test Sequence #06 Error: Failed due to Unavailable Server Auth Certificate (Subject Code 8.8.4 Reason Code 3.7)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES9+		
1	S_LPAd → SERVER	MTD_HTTP_REQ(#SERVER_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #EUICC_INFO1_8_8_4_3_7, #SERVER_ADDRESS))	MTD_HTTP_RESP(#R_ERROR_SMXX_4_3_ 7)	Common: RQ26_033 RQ31_034 RQ31_035 RQ31_036 RQ57_106 RQ62_001 RQ62_002 RQ65_018 SM-DP+: RQ56_004 RQ56_005 RQ56_006 RQ56_001 RQ56_011 RQ56_014 SM-DS: RQ58_003 RQ58_004 RQ58_005 RQ58_006 RQ58_007 RQ58_007 RQ58_011 RQ58_007

4.3.12.2.2TC_SM-DP+_ES9+.InitiateAuthenticationFRP

This test case is defined as FFS and not applicable for this version of test specification.

4.3.12.2.3TC_SM-DP+_ES9+.InitiateAuthenticationBRP

General Initial Conditions		
Entity	Description of the general initial condition	
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for BRP	

Test Sequence #01 Nominal

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.3.12.2.1 TC_SM-DP+_ES9+.InitiateAuthenticationNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

V1.4 Page 269 of 777

4.3.13 ES9+ (LPA -- SM-DP+): GetBoundProfilePackage

4.3.13.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_028
- RQ25_001, RQ25_002, RQ25_004, RQ25_005, RQ25_006, RQ25_009, RQ25_010, RQ25_011, RQ25_012, RQ25_013, RQ25_014, RQ25_015
- RQ26_018, RQ26_019, RQ26_020, RQ26_021, RQ26_022, RQ26_029, RQ26_031, RQ26_034, RQ26_035
- RQ31_143, RQ31_144, RQ31_146, RQ31_147, RQ31_148, RQ31_148_2,
 RQ31_148_3, RQ31_149, RQ31_150, RQ31_151, RQ31_152, RQ31_155,
 RQ31_162, RQ31_165, RQ31_166, RQ31_168, RQ31_170
- RQ32 069, RQ32 070
- RQ44_001
- RQ47 001
- RQ55_001, RQ55_002, RQ55_003, RQ55_004, RQ55_005, RQ55_006, RQ55_007, RQ55_008, RQ55_009, RQ55_017, RQ55_018, RQ55_020, RQ55_021, RQ55_022, RQ55_028, RQ55_033, RQ55_033_1, RQ55_037, RQ55_040, RQ55_041
- RQ56_015, RQ56_016, RQ56_017, RQ56_018, RQ56_019, RQ56_020, RQ56_021,
 RQ56_022, RQ56_023, RQ56_024, RQ56_025, RQ56_026, RQ56_027, RQ56_028
- RQ57_028, RQ57_039
- RQ62 001, RQ62 002, RQ62 004, RQ62 005, RQ62 006, RQ62 007
- RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_020, RQ65_021
- RQG0 001, RQG0 002, RQG0 003, RQG0 004, RQG0 005, RQG0 006

4.3.13.2 Test Cases

4.3.13.2.1TC_SM-DP+_ES9+.GetBoundProfilePackageNIST

General Initial Conditions			
Entity	Description of the general initial condition		
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. There have been no previous attempts to download the pending profile.		

V1.4 Page 270 of 777

Test Sequence #01 Nominal: Using S-ENC and S-MAC without Confirmation Code

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is loaded as an Unprotected Profile Package. Confirmation Code is not provided by the Operator to the SM-DP+.Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_U	C_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_SK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP _SK (#R_GET_BPP_RESP_OP1_S K, <s_mac>, <s_enc>, #SMDP_METADATA_OP_PR OF1)</s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_006 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_035 RQ31_143 RQ31_150 RQ31_151 RQ31_152 RQ31_155 RQ31_165 RQ31_165 RQ31_166 RQ31_170 RQ32_069 RQ32_070 RQ44_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_001 RQ55_001 RQ55_001 RQ55_002 RQ55_003 RQ55_004 RQ55_007 RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_018 RQ55_020 RQ55_021

V1.4 Page 271 of 777

		RQ55_022
		RQ55_028
		RQ55_033
		RQ55_033_1
		RQ55_037
		RQ55_041
		RQ56_015
		RQ56_016
		RQ56_017
		RQ56_023
		RQ56_024
		RQ56_026
		RQ56_027
		RQ57_039
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
		RQG0_005 RQG0_006
		NQG0_000

Test Sequence #02 Nominal: Using S-ENC and S-MAC with Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is loaded as an Unprotected Profile Package. Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_U	C_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS,	MTD_HTTP_RESP(#R_GET_B PP_RESP_OP1_SK)	RQ25_001 RQ25_002 RQ25_004 RQ25_006

V1.4 Page 272 of 777

	#PATH_GET_BPP,	Verify that	RQ25_010
	MTD_GET_BPP(<transaction_id_gbpp></transaction_id_gbpp>	RQ25_010
	·	matches	
	<s_transaction_id>,</s_transaction_id>		RQ25_012
		<s_transaction_id></s_transaction_id>	RQ25_013
	#PREP_DOWNLOAD_RESP_CC))	MTD_TEST_ES8+_GET_BPP_	RQ25_015
	#I KEI _BOWNEOAB_KEGI _GG))	SK	RQ26_018
		(#R_GET_BPP_RESP_OP1_S	RQ26_019
		K, <s_mac>, <s_enc>,</s_enc></s_mac>	RQ26_020
		#SMDP_METADATA_OP_PRO	RQ26_022
		F1)	RQ26_029
		,	RQ26_031
			RQ26_034
			RQ26_035
			RQ31_143
			RQ31_144
			RQ31_146
			RQ31_147
			RQ31_147
			RQ31_151
			RQ31_151 RQ31_152
			RQ31_152 RQ31_155
			RQ31_162
			RQ31_165
			RQ31_166
			RQ31_170
			RQ32_069
			RQ32_070
			DO44 004
			RQ44_001
			RQ45_006
			RQ45_026
			RQ45_026_1
			RQ47_001
			RQ55_001
			RQ55_002
			RQ55_003
			RQ55_004
			RQ55_005
			RQ55_006
			RQ55_007
			RQ55_008
			RQ55_009
			RQ55_017
			RQ55_018
			RQ55_020
			RQ55_021
			RQ55_022
			RQ55_028
			RQ55_033
			RQ55_033_1
			RQ55_037
			RQ55_041
			RQ56_015
			RQ56_016
			RQ56_017
			RQ56_023
			RQ56_024
			RQ56_026
			RQ56_027
			RQ57_039

V1.4 Page 273 of 777

		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001,
		RQG0_002,
		RQG0_003,
		RQG0_004,
		RQG0_005,
		RQG0_006

Test Sequence #03 Nominal: Using PPK-ENC and PPK-MAC without Confirmation Code

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRES	S_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_R ESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP _PPK (#R_GET_BPP_RESP_OP1_ PPK, <s_mac>, <s_enc>, <ppk_mac>, <ppk_enc>,</ppk_enc></ppk_mac></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_005 RQ25_006 RQ25_009 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_014 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_021 RQ26_021 RQ26_022 RQ26_022 RQ26_029 RQ26_031 RQ26_034

V1.4 Page 274 of 777

OF1)	RQ26_035 RQ31_143 RQ31_150 RQ31_151 RQ31_152 RQ31_155 RQ31_162 RQ31_165 RQ31_166
	RQ31_150 RQ31_151 RQ31_152 RQ31_155 RQ31_162 RQ31_165
	RQ31_151 RQ31_152 RQ31_155 RQ31_162 RQ31_165
	RQ31_152 RQ31_155 RQ31_162 RQ31_165
	RQ31_155 RQ31_162 RQ31_165
	RQ31_162 RQ31_165
	RQ31_165
	RQ31_168
	RQ31_170
	RQ32_069
	RQ32_070
	RQ44_001
	RQ45_006
	RQ45_026
	RQ45_026_1
	RQ55_001
	RQ55_002
	RQ55_003
	RQ55_004
	RQ55_005
	RQ55_006
	RQ55_007
	RQ55_008
	RQ55_009
	RQ55_017
	RQ55_018
	RQ55_020
	RQ55_021
	RQ55_022
	RQ55_028
	RQ55_033
	RQ55_033_1
	RQ55_037
	RQ55_040
	RQ55_041
	RQ56_015
	RQ56_016
	RQ56_017
	RQ56_023
	RQ56_024
	RQ56_026
	RQ56_027
	RQ57_039
	RQ62_001
	RQ62_002
	RQ62_003
	RQ62_004
	RQ62_005
	RQ62_006
	RQ62_007
	RQ62_009
	RQ65_001
	RQ65_002
	RQ65_003
	RQ65_004
	RQ65_005
	RQ65_007
	RQ65_008
	RQ65_009
	RQ65_020

V1.4 Page 275 of 777

		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
		RQG0_005
		RQG0_006

Test Sequence #04 Nominal: Using PPK-ENC and PPK-MAC with Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc>
	 Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_UC	_cc	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_B PP_RESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_ PPK (#R_GET_BPP_RESP_OP1_P PK, <s_mac>, <s_enc>, <ppk_mac>, <ppk_enc>, #SMDP_METADATA_OP_PRO F1)</ppk_enc></ppk_mac></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_005 RQ25_006 RQ25_009 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_014 RQ25_015 RQ26_019 RQ26_020 RQ26_021 RQ26_022 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_035 RQ31_143 RQ31_144 RQ31_144 RQ31_146 RQ31_147 RQ31_150 RQ31_151 RQ31_155 RQ31_155 RQ31_166 RQ31_166 RQ31_166 RQ31_166 RQ31_166 RQ31_170 RQ32_069 RQ32_070 RQ44_001

V1.4 Page 276 of 777

		<u> </u>	DO45 000
			RQ45_006
			RQ45_026
			RQ45_026_1
			RQ55_001
			RQ55_002
			RQ55_003
			RQ55_004
			RQ55_005
			RQ55_006
			RQ55_007
			RQ55_008
			RQ55_009
			RQ55_017
			RQ55_018
			RQ55_020
			RQ55_021
			RQ55_022
			RQ55_028
			RQ55_033
			RQ55_033_1
			RQ55_037
			RQ55_040
			RQ55_041
			RQ56_015
			RQ56_016
			RQ56_017
			RQ56_023
			RQ56_024 RQ56_026R
			Q56_027
			RQ57_039
			RQ62_001
			RQ62_001
			RQ62_002
			RQ62_004
			RQ62_005
			RQ62_006
			RQ62_007
			RQ62_009
			RQ65_001
			RQ65_002
			RQ65_003
			RQ65_004
			RQ65_005
			RQ65_007
			RQ65_008
			RQ65_009
			RQ65_020R
			Q65_021
			RQG0_001
			RQG0_002
			RQG0_003
			RQG0_004
			RQG0_005
			RQG0_006
-	-	-	

V1.4 Page 277 of 777

Non-confidential

Test Sequence #05 Nominal: Using S-ENC and S-MAC with Metadata split over 2 segments without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package using the S-ENC and S-MAC with the metadata split over two sequenceOf88 segments without a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1_2_SEG is loaded as an Unprotected Profile Package. Confirmation Code is not provided by the Operator to the SM-DP+.

This test sequence SHALL be the same as the Test Sequence #01 defined in this section except that #SMDP_METADATA_OP_PROF1_2_SEG replaces #SMDP METADATA OP PROF1.

NOTE:

There is no testing required in addition to Test Sequence #01 as the R_GET_BPP_RESP_OP1_SK constants allow for 1 or 2 segments and for the SM-DP+ to successfully pass this test sequence it SHALL use 2 segments to deliver the metadata.

Test Sequence #06 Nominal: Using PPK-ENC and PPK-MAC with Metadata split over 2 segments without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package using the PPK-ENC and PPK-MAC with the metadata split over two sequenceOf88 segments without a Confirmation Code.

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured #SMDP_METADATA_OP_PROF1_2_SEG is securely loaded Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	with as a

This test sequence SHALL be the same as the Test Sequence #03 defined in this section except that #SMDP_METADATA_OP_PROF1_2_SEG replaces #SMDP METADATA OP PROF1.

NOTE:

There is no testing required in addition to Test Sequence #03 as the R_GET_BPP_RESP_OP1_PPK constants allow for 1 or 2 segments and for the SM-DP+ to successfully pass this test sequence it SHALL use 2 segments to deliver the metadata.

4.3.13.2.2TC_SM-DP+_ES9+.GetBoundProfilePackageFRP

This test case is defined as FFS and not applicable for this version of test specification.

V1.4 Page 278 of 777

4.3.13.2.3TC_SM-DP+_ES9+.GetBoundProfilePackageBRP

General Initial Conditions			
Entity	Description of the general initial condition		
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for BRP PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. There have been no previous attempts to download the pending profile. 		

Test Sequence #01 Nominal: Using S-ENC and S-MAC without Confirmation Code

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.3.13.2.1 TC_SM-DP+_ES9+.GetBoundProfilePackageNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #02 Nominal: Using PPK-ENC and PPK-MAC without Confirmation Code

This test sequence SHALL be the same as the Test Sequence #03 defined in section 4.3.13.2.1 TC_SM-DP+_ES9+.GetBoundProfilePackageNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.3.13.2.4TC_SM-DP+_ES9+.GetBoundProfilePackage_RetryCases_ReuseOTPK_NIST

General Initial Conditions				
Entity Description of the general initial condition				
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. The EID is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.			

Test Sequence #01 Nominal: Retry with same otPK.eUICC.ECKA using S-ENC and S-MAC without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt for the same otPK.eUICC.ECKA using S-ENC and S-MAC for Profile protection without a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is loaded as an Unprotected Profile Package. Confirmation Code is not provided by the Operator to the SM-DP+. There have been no previous attempts to download the pending profile.

V1.4 Page 279 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Extract <otpk< th=""><th>PROF_DOWNLOAD_DEF_DP_U C_SM_DP+_ECKA> from #INIT_S ilePackage Response in Step 4.</th><th>USE_CASE_CANCEL_SESSION_SK</th><th></th></otpk<>	PROF_DOWNLOAD_DEF_DP_U C_SM_DP+_ECKA> from #INIT_S ilePackage Response in Step 4.	USE_CASE_CANCEL_SESSION_SK	
IC2	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRES	S_UC_NO_CC_RETRY	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_SK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_SK (#R_GET_BPP_RESP_OP1_SK, <s_mac>, <s_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 matches the value previously received in the GetBoundProfilePackage response in step 4 of the procedure in IC1</otpk_sm_dp+_ecka></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_006 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_022 RQ26_029 RQ26_031 RQ26_034 RQ26_035 RQ31_143 RQ31_144 RQ31_146 RQ31_147 RQ31_148_3 RQ31_149 RQ31_155 RQ31_165 RQ31_166 RQ31_170 RQ32_069 RQ32_070 RQ44_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_007 RQ55_001 RQ55_001 RQ55_001 RQ55_002 RQ55_001 RQ55_002 RQ55_001 RQ55_002 RQ55_003 RQ55_004 RQ55_005 RQ55_005 RQ55_007 RQ55_008 RQ55_007 RQ55_008 RQ55_009 RQ55_007 RQ55_008 RQ55_009 RQ55_0017 RQ55_008 RQ55_009 RQ55_009 RQ55_0017 RQ55_008 RQ55_009 RQ55_0017 RQ55_008 RQ55_009

V1.4 Page 280 of 777

		RQ56_016
		RQ56_017
		RQ56_017 RQ56_021
		RQ56_023
		RQ56_024
		RQ56_026
		RQ56_027
		RQ57_039
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
		RQG0_005
		RQG0_006
		· _

Test Sequence #02 Nominal: Retry with same otPK.eUICC.ECKA using S-ENC and S-MAC with Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt for the same otPK.eUICC.ECKA using the S-ENC and S-MAC for Profile protection with a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is loaded as an Unprotected Profile Package. Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+. There have been no previous attempts to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_PROF_DOWNLOAD_DEF_DP_USE_CASE_CC_CANCEL_SESSION_S K			
	Extract <otpk_sm_dp+_ecka> from #INIT_SC_PROF1 in the GetBoundProfilePackage Response in Step 4.</otpk_sm_dp+_ecka>			
IC2	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_CC_RETRY			

V1.4 Page 281 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_R ESP_OP1_SK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_SK (#R_GET_BPP_RESP_OP1_SK, <s_mac>, <s_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 matches the value previously received in the GetBoundProfilePackage response in step 4 of the procedure in IC1</otpk_sm_dp+_ecka></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_022 RQ26_029 RQ26_031 RQ26_035 RQ31_143 RQ31_144 RQ31_146 RQ31_146 RQ31_146 RQ31_165 RQ31_165 RQ31_165 RQ31_165 RQ31_165 RQ31_166 RQ31_166 RQ31_170 RQ32_069 RQ32_070 RQ44_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_001 RQ55_001 RQ55_001 RQ55_001 RQ55_001 RQ55_002 RQ55_003 RQ55_007 RQ55_008 RQ55_009 RQ55_009 RQ55_017 RQ55_018 RQ55_020 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_033 RQ55_022 RQ55_033 RQ55_033_1
			#INIT_SC_PROF1 matches the value previously received in the GetBoundProfilePackage response in	RQ55_001 RQ55_002 RQ55_003 RQ55_004 RQ55_005 RQ55_006 RQ55_007 RQ55_008
				RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_028 RQ55_033
				RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_021 RQ56_023 RQ56_024 RQ56_026

V1.4 Page 282 of 777

		RQ56_027
		RQ57_039
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
		RQG0_005
		RQG0_006

Test Sequence #03 Nominal: Retry with same otPK.eUICC.ECKA using PPK-ENC and PPK-MAC without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt for the same otPK.eUICC.ECKA using the PPK-ENC and PPK-MAC for Profile protection without a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. There has been no previous attempts to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_ K Extract <otpk GetBoundProf</otpk 			
IC2	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_NO_CC_RETRY			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_005 RQ25_006 RQ25_009 RQ25_010

V1.4 Page 283 of 777

	<s_transaction_id>,</s_transaction_id>	MTD_TEST_ES8+_GET_BPP_PP	RQ25_011
	#PREP_DOWNLOAD_RESP)	K	RQ25_012
	,	(#R_GET_BPP_RESP_OP1_PPK,	RQ25_013
	,	<s_mac>, <s_enc>,</s_enc></s_mac>	RQ25_014
		<ppk_mac>, <ppk_enc>,</ppk_enc></ppk_mac>	RQ25_015
		#SMDP_METADATA_OP_PROF1)	RQ26_018
		· ·	RQ26_019
		• Verify that	RQ26_020
		<otpk_sm_dp+_ecka> in</otpk_sm_dp+_ecka>	RQ26_021
		#INIT_SC_PROF1 matches the	RQ26_022
		value previously received in the	RQ26_029
		GetBoundProfilePackage response	RQ26_031
		in step 4 of the procedure in IC1	RQ26_034
			RQ26_035
			RQ31_143
			RQ31_148_3
			RQ31_149
			RQ31_155
			RQ31_162
			RQ31_165
			RQ31_166
			RQ31_168
			RQ31_170
			RQ32_069
			RQ32_070
			RQ44_001
			RQ45_006
			RQ45_026
			RQ45_026_1
			RQ55_001
			RQ55_002
			RQ55_003
			RQ55_004
			RQ55_005
			RQ55_006
			RQ55_007
			RQ55_008
			RQ55_009
			RQ55_017
			RQ55_018
			RQ55_020
			RQ55_021
			RQ55_022
			RQ55_028
			RQ55_033
			RQ55_033_1
			RQ55_037
			RQ55_040
			RQ55_041
			RQ56_015
			RQ56_016
			RQ56_017
			RQ56_021
			RQ56_023
			RQ56_024
			RQ56_026
			RQ56_027
			RQ57_039
			RQ62_001
			RQ62_002
			RQ62_003
			.1902_000

V1.4 Page 284 of 777

	RQ62_004
	RQ62_005
	RQ62_006
	RQ62_007
	RQ62_009
	RQ65_001
	RQ65_002
	RQ65_003
	RQ65_004
	RQ65_005
	RQ65_007
	RQ65_008
	RQ65_009
	RQ65_020
	RQ65_021
	RQG0_001
	RQG0_002
	RQG0_003
	RQG0_004
	RQG0_005
	RQG0_006

Test Sequence #04 Nominal: Retry with same otPK.eUICC.ECKA using PPK-ENC and PPK-MAC with Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package with a retry attempt for the same otPK.eUICC.ECKA using the PPK-ENC and PPK-MAC for Profile protection with a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+. There has been no previous attempts to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_PROF_DOWNLOAD_DEF_DP_USE_CASE_CC_CANCEL_SESSION_ PPK Extract <otpk_sm_dp+_ecka> from #INIT_SC_PROF1 in the GetBoundProfilePackage Response in Step 4.</otpk_sm_dp+_ecka>			
IC2	PROC_ES9+_	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_CC_RETRY		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_PPK (#R_GET_BPP_RESP_OP1_PPK, <s_mac>, <s_enc>,</s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_005 RQ25_006 RQ25_009 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_014

V1.4 Page 285 of 777

	<ppk_mac>, <ppk_enc>,</ppk_enc></ppk_mac>	RQ25_015
	#SMDP_METADATA_OP_PROF1)	RQ26_018
		RQ26_019
	Verify that CTRK SM RR FOKA in	RQ26_020
	<otpk_sm_dp+_ecka> in</otpk_sm_dp+_ecka>	RQ26_021
	#INIT_SC_PROF1 matches the	RQ26_022
	value previously received in the	RQ26_029
	GetBoundProfilePackage response in step 4 of the procedure in IC1	RQ26_031
	in step 4 of the procedure in ici	RQ26_034
		RQ26_035
		RQ31_143
		RQ31_144
		RQ31_146
		RQ31_147
		RQ31_148_3
		RQ31_149
		RQ31_155
		RQ31_162
		RQ31_165
		RQ31_166
		RQ31_168
		RQ31_170
		RQ32_069
		RQ32_070
		RQ44_001
		RQ45_006
		RQ45_026
		RQ45_026_1
		RQ47_001
		RQ55_001
		RQ55_002
		RQ55_003 RQ55_004
		RQ55_004 RQ55_005
		RQ55_006
		RQ55_007
		RQ55_008
		RQ55_009
		RQ55_017
		RQ55 018
		RQ55_020
		RQ55_021
		RQ55_022
		RQ55_028
		RQ55_033
		RQ55_033_1
		RQ55_037
		RQ55_040
		RQ55_041
		RQ56_015
		RQ56_016
		RQ56_017
		RQ56_021
		RQ56_023
		RQ56_024
		RQ56_026
		RQ56_027
		RQ57_039
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004

V1.4 Page 286 of 777

		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
		RQG0_005
		RQG0_006

Test Sequence #05 Nominal: Retry with same otPK.EUICC.ECKA rejected by eUICC using S-ENC and S-MAC without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt with the same otPK.EUICC.ECKA rejected by the eUICC using the S-ENC and S-MAC without a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is loaded as an Unprotected Profile Package. Confirmation Code is not provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_PROF_DOWNLOAD_DEF_DP_USE_CASE_CANCEL_SESSION_SK Extract <otpk_sm_dp+_ecka> from #INIT_SC_PROF1 in the GetBoundProfilePackage Response in Step 4.</otpk_sm_dp+_ecka>			
IC2	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRES	S_UC_NO_CC_RETRY	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ NEW_OTPK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_3_7) OR MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_SK) • Verify that <transaction_id_gbpp> matches <s_transaction_id></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_006 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_015 RQ26_018 RQ26_019 RQ26_020

V1.4 Page 287 of 777

			RQ26_022
		MTD_TEST_ES8+_GET_BPP_SK	RQ26_029
		(#R_GET_BPP_RESP_OP1_SK,	RQ26_031
		<s_mac>, <s_enc>,</s_enc></s_mac>	RQ26_034
		#SMDP_METADATA_OP_PROF1)	RQ26_035
		 Verify that <otpk dp+="" ecka="" sm=""></otpk> 	RQ31_143
		in #INIT_SC_PROF1 is different from	RQ31_148_3
			RQ31_150
		the value previously received in the	RQ31_151
		GetBoundProfilePackage response in step 4 of the procedure in IC1	RQ31_152
		step 4 of the procedure in IC1	RQ31_155
			RQ31_162
			RQ31_165
			RQ31_166
			RQ31_170
			RQ32_069
			RQ32_070
			RQ44_001
			RQ45_006
			RQ45_026
			RQ45_026_1
			RQ55_001
			RQ55_002
			RQ55_003
			RQ55_004
			RQ55_005
			RQ55_006
			RQ55_007
			RQ55_008
			RQ55_009
			RQ55_017
			RQ55_018
			RQ55_020
			RQ55_021
			RQ55_022
			RQ55_028
			RQ55_033
			RQ55_033_1
			RQ55_037
			RQ55_041
			RQ56_015
			RQ56_016
			RQ56_017
			RQ56_022
			RQ56_023
			RQ56_024
			RQ56_026
			RQ56_027
			RQ57_039
			RQ62_001
			RQ62_002
			RQ62_003
			RQ62_004 RQ62_005
			RQ62_005 RQ62_006
			RQ62_006 RQ62_007
			RQ62_007 RQ62_009
			RQ62_009 RQ65_001
			RQ65_001 RQ65_002
			RQ65_002 RQ65_003
			RQ65_003
			RQ65_005
<u> </u>			11400_000

V1.4 Page 288 of 777

_			
			RQ65_007
			RQ65_008
			RQ65_009
			RQ65_020
			RQ65_021
			RQG0_001
			RQG0_002
			RQG0_003
			RQG0_004
			RQG0_005
			RQG0_006

Test Sequence #06 Nominal: Retry with same otPK.EUICC.ECKA rejected by eUICC using S-ENC and S-MAC with Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt with the same otPK.EUICC.ECKA rejected by the eUICC using the S-ENC and S-MAC with a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is loaded as an Unprotected Profile Package. Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Extract <otpk< td=""><td>PROF_DOWNLOAD_DEF_DP_U K_SM_DP+_ECKA> from #INIT_ ilePackage Response in Step 4</td><td>SE_CASE_CC_CANCEL_SESSION_SK SC_PROF1 in the</td><td></td></otpk<>	PROF_DOWNLOAD_DEF_DP_U K_SM_DP+_ECKA> from #INIT_ ilePackage Response in Step 4	SE_CASE_CC_CANCEL_SESSION_SK SC_PROF1 in the	
IC2	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRES	S_UC_CC_RETRY	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ NEW_OTPK_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_3_7) OR MTD_HTTP_RESP(#R_GET_BPP_RES P_OP1_SK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_SK (#R_GET_BPP_RESP_OP1_SK, <s_mac>, <s_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 is different from the value previously received in the</otpk_sm_dp+_ecka></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_006 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_020 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_035 RQ31_143 RQ31_144 RQ31_146 RQ31_147

V1.4 Page 289 of 777

step 4 of the procedure in IC1 RQ31 150 RQ31 151 RQ31 152 RQ32 RQ32 RQ32 RQ32 RQ32 RQ32 RQ32 RQ3		GetBoundProfilePackage response in	RQ31_148_3
RO31_151 RO31_152 RO31_155 RO31_156 RO31_166 RO31_166 RO31_166 RO31_170 RO32_069 RO32_070 RO44_001 RO45_006 RO45_006 RO45_006 RO45_006 RO45_006 RO55_001 RO55_001 RO55_002 RO55_008 RO55_007 RO35_008 RO55_007 RO35_008 RO55_007 RO55_008 RO55_009 RO55_007 RO55_009 RO55_007 RO55_009 RO55_007 RO55_009 RO55_000 RO55_000			
RO31 155 RO31 165 RO31 165 RO31 165 RO31 166 RO31 170 RO32 090 RO45 006 RO45 006 RO45 006 RO55 001 RO55 002 RO55 001 RO55 001 RO55 001 RO55 002 RO55 001 RO55 002 RO55 001 RO55 002 RO56 002 RO56 003 RO56 002 RO56 003 RO56 004 RO56 007 RO57 009 RO55 001 RO5			
RO31_155 RO31 162 RO31 165 RO31 170 RO32_059 RO32_070 RO44_001 RO45_006 RO45_006 RO45_006 RO45_006 RO45_006 RO55_001 RO55_001 RO55_002 RO55_003 RO55_009 RO55_009 RO55_009 RO55_001 RO55_001 RO55_002 RO55_003 RO55_003 RO55_003 RO55_003 RO55_004 RO55_006 RO55_007 RO55_008 RO55_009 RO55_000 RO5			
RC31_165 RC31_165 RC31_170 RC32_069 RC32_070 RC44_001 RC45_006 RC45_006 RC45_006 RC45_006 RC45_006 RC45_006 RC55_001 RC55_001 RC55_001 RC55_001 RC55_002 RC55_003 RC55_003 RC55_007 RC55_008 RC65_008			
RO31_166 RO31_170 RO32_069 RO32_070 RO44_001 RO45_006 RO45_006 RO45_006 RO45_006 RO45_006 RO45_006 RO55_001 RO55_001 RO55_001 RO55_006 RO55_007 RO55_008 RO55_007 RO55_008 RO55_007 RO55_008			
R031 170 R032 099 R032 070 R044 001 R045 006 R045 026 R045 026 R045 026 R055 001 R055 001 R055 001 R055 001 R055 007 R056 007 R066 007			
R331_170 R332_099 R322_099 R322_099 R322_090 R324_001 R044_001 R045_006 R445_026_1 R047_001 R045_001 R055_001 R055_002 R055_003 R055_006 R055_007 R055_008 R055_009 R055_017 R055_018 R055_008 R055_009 R055_017 R055_018 R055_020 R055_017 R055_018 R055_033_1 R055_031			
R332_099 R332_070 R244_001 R245_006 R244_001 R245_006 R245_026 R445_026 R445_026 R447_001 R055_001 R055_003 R055_003 R055_007 R055_008 R055_007 R055_008 R055_007 R055_008 R055_007 R055_008 R055_007 R055_008 R055_017 R056_016 R056_020 R056_021 R05			
R032_070 R044_001 R045_006 R045_026_1 R047_026_1 R047_001 R045_001 R045_001 R055_001 R055_002 R055_003 R055_006 R055_007 R055_008 R055_009 R055_009 R055_017 R055_021 R055_022 R055_023 R055_024 R055_025 R055_021 R055_022 R055_021 R055_022 R055_023 R055_021 R055_022 R055_023 R055_021 R055_022 R055_023 R055_023 R056_024 R056_026 R056_016 R056_016 R056_016 R056_017 R056_016 R056_017 R066_017 R066_017 R066_017 R066_017 R066_017 R066_017 R066_017 R066_007			
RQ44, 001 RQ45, 006 RQ45, 006 RQ45, 006 RQ45, 006 RQ45, 006 RQ47, 001 RQ65, 001 RQ65, 001 RQ65, 002 RQ55, 003 RQ55, 004 RQ55, 006 RQ55, 007 RQ55, 006 RQ55, 007 RQ55, 008 RQ55, 009 RQ55, 017 RQ55, 020 RQ55, 033 RQ55, 033, 1 RQ56, 021 RQ56, 024 RQ56, 024 RQ56, 026 RQ56, 026 RQ56, 027 RQ56, 026 RQ56, 026 RQ56, 027 RQ57, 039 RQ62, 001 RQ62, 002 RQ62, 004 RQ62, 005 RQ62, 007 RQ62, 009 RQ65, 001 RQ65, 001 RQ65, 001 RQ65, 004 RQ65, 007 RQ65, 004 RQ65, 004 RQ65, 004 RQ65, 007 R			
RC45_006 RC45_026_1 RC45_026_1 RC47_001 RC45_001 RC45_001 RC45_002 RC45_003 RC55_003 RC55_004 RC55_006 RC65_007 RC65_007 RC65_007 RC65_008 RC55_009 RC65_007 RC65_008 RC65_009 RC65_007 RC65_008 RC65_009 RC65_009 RC65_008 RC65_009 RC65_009 RC65_009 RC66_009 RC66_009 RC66_009 RC66_0009 RC66_0007 RC66_0001 RC66_0007 RC66			
RC45 (226_1 RO46_(226_1) RO45_(201) RO45_(201) RO55_(201) RO55_(201) RO55_(202) RO55_(203) RO55_(204) RO55_(204) RO55_(201) RO55_(201) RO55_(201) RO55_(201) RO55_(201) RO55_(202) RO55_(202) RO55_(203) RO55_(201) RO55_(201) RO55_(202) RO55_(203) RO55_(201) RO56_(201) RO56_(201) RO56_(201) RO56_(201) RO62_(201) RO62_(20			
RC45_026_1 RC47_001 RC55_001 RC55_001 RC55_002 RC55_004 RC56_005 RC55_006 RC25_007 RC55_008 RC55_009 RC65_018 RC65_009 RC65_021 RC65_022 RC65_022 RC65_022 RC65_023 RC65_033_RC65_033_RC65_033 RC65_033 RC65_033 RC65_033 RC65_034 RC65_035 RC65_036 RC65_036 RC65_037 RC66_037 R			
RQ47_001 RQ55_001 RQ55_001 RQ55_002 RQ55_003 RQ55_004 RQ55_006 RQ65_007 RQ55_006 RQ65_007 RQ55_008 RQ55_017 RQ55_018 RQ55_019 RQ55_019 RQ55_019 RQ55_019 RQ55_022 RQ55_022 RQ55_022 RQ55_022 RQ55_022 RQ55_023 RQ55_023 RQ55_024 RQ56_023 RQ56_024 RQ56_027 RQ56_041 RQ56_016 RQ56_017 RQ56_026 RQ56_027 RQ56_027 RQ56_028 RQ56_028 RQ56_029 RQ56_029 RQ56_020 RQ56_020 RQ56_020 RQ56_020 RQ56_020 RQ56_020 RQ56_020 RQ56_020 RQ56_020 RQ66_020 RQ66_020 RQ66_020 RQ66_001 RQ66_002 RQ66_001 RQ66_002 RQ66_001 RQ66_001 RQ66_002 RQ66_001			
RG55_001 RQ55_002 RQ55_003 RQ55_004 RQ55_005 RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_018 RQ55_018 RQ55_021 RQ55_021 RQ55_022 RQ55_022 RQ55_022 RQ55_023 RQ55_021 RQ55_021 RQ55_021 RQ55_022 RQ56_023 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ66_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_005 RQ62_006 RQ62_006 RQ66_007 RQ65_002 RQ66_003 RQ66_001			
RO55_002 RQ55_003 RQ55_004 RQ55_005 RQ55_006 RQ55_007 RQ55_008 RQ55_007 RQ55_009 RQ55_017 RQ55_009 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_028 RQ55_023 RQ55_033_1 RQ55_033_1 RQ55_033 RQ55_033 RQ55_031 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_005 RQ65_003 RQ66_007 RQ65_003 RQ66_007 RQ65_003 RQ66_007 RQ65_003 RQ66_007 RQ65_003 RQ66_007 RQ65_003 RQ66_007 RQ65_008			
RO55_004 RQ55_004 RQ55_005 RQ55_006 RQ55_007 RQ55_008 RQ55_007 RQ55_008 RQ65_007 RQ55_018 RQ55_017 RQ55_018 RQ55_012 RQ55_012 RQ55_021 RQ55_022 RQ55_028 RQ55_023 RQ55_033 RQ55_033 RQ55_031 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ66_024 RQ66_026 RQ66_027 RQ57_039 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_001 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ66_001 RQ65_002 RQ66_007			
RQ55_005 RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_009 RQ55_018 RQ55_019 RQ55_011 RQ55_020 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033 RQ55_033 RQ55_031 RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ66_026 RQ66_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_005 RQ62_006 RQ62_007 RQ65_009 RQ66_007 RQ65_008 RQ66_007			
RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_011 RQ55_011 RQ55_012 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033 RQ55_033 RQ55_031 RQ55_031 RQ55_041 RQ56_016 RQ66_017 RQ66_022 RQ56_024 RQ56_026 RQ56_027 RQ55_041 RQ56_026 RQ56_027 RQ57_039 RQ62_006 RQ56_027 RQ57_039 RQ62_006 RQ62_006 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_009 RQ66_007			
RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_009 RQ55_017 RQ55_018 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_023 RQ55_033 1 RQ55_033 1 RQ55_031 RQ55_015 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ67_039 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ66_001 RQ66_001 RQ66_002 RQ66_000 RQ66_000 RQ66_000			
RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_017 RQ55_021 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ55_037 RQ55_041 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_002 RQ62_003 RQ62_006 RQ62_006 RQ62_007 RQ62_009 RQ65_008 RQ66_003			
RQ55_008 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_033_1 RQ55_033_1 RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ56_027 RQ62_003 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ65_001			
RQ55_009 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ56_015 RQ66_015 RQ66_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ66_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ62_000 RQ65_000 RQ66_000 RQ66_000 RQ66_000 RQ66_000 RQ66_000 RQ66_000 RQ66_000 RQ66_000 RQ66_000			
RQ55_017 RQ55_018 RQ55_020 RQ55_021 RG55_021 RG55_028 RQ55_028 RQ55_033 RG55_031 RG55_037 RG55_041 RG56_016 RG66_016 RG66_017 RG66_022 RQ56_023 RQ56_024 RG56_026 RQ56_027 RG57_039 RG62_001 RG62_002 RG62_001 RG62_002 RG62_003 RQ62_001 RG62_002 RG62_003 RQ62_004 RG62_005 RG62_006 RQ62_007 RG62_006 RQ62_007 RG65_001 RQ66_002 RG65_001 RG65_001 RG65_002 RG65_001 RG65_002 RG65_001 RG65_002 RG65_003 RG65_004 RG65_007 RG65_008 RG65_007 RG65_008 RG65_007 RG65_008 RG65_007 RG65_008 RG65_007 RG65_008			
RQ55_018 RQ55_021 RQ55_021 RQ55_021 RQ55_022 RQ55_023 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_006 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007			
RQ55_020 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033_1 RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_022 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_007			
RC55_021 RC055_022 RC055_028 RC055_033 RC055_033_1 RC055_031 RC055_041 RC056_015 RC066_016 RC066_017 RC066_016 RC066_017 RC066_022 RC066_023 RC056_023 RC056_024 RC056_026 RC056_027 RC057_039 RC062_001 RC062_002 RC062_003 RC062_004 RC062_007 RC062_006 RC062_007 RC062_007 RC062_008 RC062_007 RC062_009 RC065_001 RC065_002 RC065_003 RC065_005 RC065_006			
RQ55_022 RQ55_028 RQ55_033 RQ55_033_1 RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_001 RQ65_006 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008			
RQ55_028 RQ55_033 RQ55_0331 RQ55_037 RQ55_041 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ67_039 RQ62_001 RQ62_002 RQ62_003 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ65_001 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ66_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008			
RQ55_033_1 RQ55_033_1 RQ55_033_1 RQ55_037 RQ55_041 RQ56_015 RQ56_015 RQ56_017 RQ56_022 RQ56_023 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_010 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_007			
RQ55_033_1 RQ55_037 RQ55_041 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007			
RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007			
RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_01 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007			
RQ56_015 RQ56_016 RQ56_017 RQ56_027 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_008			
RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_005 RQ65_007 RQ65_007			
RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_009			
RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_009			
RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008			
RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008			
RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_005			
RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_006 RQ65_007 RQ65_008 RQ65_009			RQ57_039
RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_006 RQ65_007 RQ65_008 RQ65_009			
RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007			
RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_007 RQ65_008			
RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_007 RQ65_008			
RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007			RQ62_005
RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ65_005 RQ65_007 RQ65_008 RQ65_009			
RQ65_007 RQ65_008 RQ65_009			RQ65_004
RQ65_007 RQ65_008 RQ65_009			RQ65_005
RQ65_008 RQ65_009			
RQ65_009			
RQ65_021			

V1.4 Page 290 of 777

		RQG0_001	
		RQG0_002	
		RQG0_003	
		RQG0_004	
		RQG0_005	
		RQG0_006	

Test Sequence #07 Nominal: Retry with same otPK.EUICC.ECKA rejected by eUICC using PPK-ENC and PPK-MAC without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt with the same otPK.EUICC.ECKA rejected by the eUICC using the PPK-ENC and PPK-MAC without a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Extract <otp< td=""><td>PROF_DOWNLOAD_DEF_DP_U K_SM_DP+_ECKA> from #INIT_ filePackage Response in Step 4</td><td></td><td></td></otp<>	PROF_DOWNLOAD_DEF_DP_U K_SM_DP+_ECKA> from #INIT_ filePackage Response in Step 4		
IC2	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRES	SS_UC_NO_CC_RETRY	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ NEW_OTPK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_3_7) OR MTD_HTTP_RESP(#R_GET_BPP_R ESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_PPK (#R_GET_BPP_RESP_OP1_PPK, <s_mac>, <s_enc>, <ppk_mac>, <ppk_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 is different from the value previously received in the GetBoundProfilePackage response in step 4 of the procedure in IC1</otpk_sm_dp+_ecka></ppk_enc></ppk_mac></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_005 RQ25_006 RQ25_009 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_014 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_021 RQ26_022 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_035 RQ31_143 RQ31_148_3 RQ31_150 RQ31_150 RQ31_151 RQ31_152 RQ31_155 RQ31_162 RQ31_165

V1.4 Page 291 of 777

T .		DO21 166
		RQ31_166
		RQ31_168
		RQ31_170
		RQ32_069
		RQ32_070
		RQ44_001
		RQ45_006
		RQ45_026
		RQ45_026_1
		RQ55_001
		RQ55_002
		RQ55_003
		RQ55_004
		RQ55_005
		RQ55_006
		RQ55_007
		RQ55_008
		RQ55_009
		RQ55_017
		RQ55_018
		RQ55_020
		RQ55_021
		RQ55_022
		RQ55_028
		RQ55_028
		RQ55_033_1
		RQ55_037
		RQ55_040
		RQ55_041
		RQ56_015
		RQ56_016
		RQ56_017
		RQ56_022
		RQ56_023
		RQ56_024
		RQ56_026
		RQ56_027
		RQ57_039
		RQ62 001
		· -
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
 <u> </u>		

V1.4 Page 292 of 777

		RQG0_005	
		RQG0_006	

Test Sequence #08 Nominal: Retry with same otPK.EUICC.ECKA rejected by eUICC using PPK-ENC and PPK-MAC with Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt with the same otPK.EUICC.ECKA rejected by the eUICC using the PPK-ENC and PPK-MAC.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_ES9+_ PK Extract <otpk GetBoundProf</otpk 				
IC2	PROC_ES9+_	S9+_CMA_PD_DEF_SMDP_ADDRESS_UC_CC_RETRY			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ NEW_OTPK_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_3_7) OR MTD_HTTP_RESP(#R_GET_BPP_R ESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_PPK (#R_GET_BPP_RESP_OP1_PPK, <s_mac>, <s_enc>, <ppk_mac>, <ppk_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 is different from the value previously received in the GetBoundProfilePackage response in step 4 of the procedure in IC1</otpk_sm_dp+_ecka></ppk_enc></ppk_mac></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_005 RQ25_006 RQ25_009 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_014 RQ25_015 RQ26_018 RQ26_020 RQ26_021 RQ26_020 RQ26_021 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_035 RQ31_143 RQ31_144 RQ31_144 RQ31_144 RQ31_145 RQ31_145 RQ31_150 RQ31_151 RQ31_152 RQ31_155 RQ31_155 RQ31_155	

V1.4 Page 293 of 777

RG31_168 RG31_170 RG32_090 RG32_070 RC44_006 RG45_006 RG55_007 RG55_007 RG55_008 RG55_007 RG55_008 RG55_009 RG65_009 RG66_009 RG6			
RG31 168 RG31 170 RG32 069 RG32 069 RG32 067 RG44 001 RG45 006 RG45 026 RG45 026 RG45 026 RG45 026 RG45 026 RG5 001 RG55 001 RG55 001 RG55 001 RG55 001 RG55 001 RG55 001 RG56 022 RG56 023 RG56 024 RG56 026 RG56 027 RG56 026 RG56 027 RG56 027 RG56 028 RG56 029 RG56 029 RG56 021 RG56 021 RG56 022 RG56 023 RG56 024 RG56 026 RG56 027 RG56 026 RG56 027 RG56 027 RG56 028 RG56 028 RG56 028 RG56 029 RG56 029 RG56 029 RG56 029 RG56 020			RQ31_165
RG31 170 RG32 069 RG32 070 RG44 001 RG45 006 RG45 007 RG55 001 RG56 002 RG55 001 RG56 002 RG56 001 RG56 002 RG56 002 RG56 003 RG56 004 RG56 006 RG56 007 RG56 006 RG56 007 RG56 006 RG56 007 RG56 006 RG56 007 RG56 007 RG56 008 RG56 007 RG56 008 RG66 008 RG56 008 RG66 008			RQ31_166
R331_079 R332_079 R332_079 R344_001 R245_006 R245_026 R245_026 R245_026 R245_026 R345_001 R355_002 R355_003 R355_004 R355_007 R355_008 R355_007 R355_008 R355_007 R355_008 R355_007 R355_008 R355_009 R355_007 R355_008 R355_007 R355_008 R355_007 R355_008 R355_009 R355_007 R355_008 R355_007 R355_008 R355_009 R355_007 R355_008 R355_009 R355_007 R355_008 R355_009 R355_007 R355_008 R355_009 R35			RQ31 168
R032_099 R034_001 R044_001 R045_006 R045_006 R045_008 R045_008 R045_008 R045_009 R055_001 R055_001 R055_001 R055_001 R055_001 R055_008 R056_002 R056_003 R056_004 R055_040 R055_041 R056_017 R056_016 R056_017 R056_016 R056_017 R056_016 R056_017 R056_016 R056_017 R056_016 R056_017 R056_018 R056_017 R056_018 R056_019 R056_001 R057_039 R066_024 R056_027 R066_024 R056_006 R066_027 R066_008 R066_007 R066_008 R066_009 R066_001 R066_001 R066_001 R066_002 R066_003 R066_004 R066_001 R066_001 R066_001 R066_002 R066_001			
R032.070 R044.001 R045.006 R045.026 R045.026 R045.026 R045.026 R045.026 R045.026 R045.026 R045.001 R035.001 R035.003 R035.004 R035.004 R035.006 R055.006 R055.007 R055.008 R055.007 R055.008 R055.007 R055.008 R055.007 R055.008 R055.009 R055.011 R055.021 R055.022 R055.023 R055.033 R055.041 R055.031 R055.041 R056.041			
RQ44 001 RQ45 006 RQ45 026 1 RQ47_001 RQ47_001 RQ50_002 RQ50_003 RQ56_003 RQ56_004 RQ56_006 RQ56_007 RQ56_008 RQ56_008 RQ56_008 RQ66_008 RQ66_008 RQ66_008 RQ66_008 RQ66_008 RQ66_008 RQ66_008 RQ66_008 RQ66_008 RQ66_009 RQ66_008 RQ66_009			
RC45 006 RC45 026 RC45 026 RC45 026 RC45 026 RC45 026 RC45 026 RC47 021 RC47 001 RC65 001 RC65 003 RC65 003 RC65 006 RC65 006 RC65 007 RC65 008 RC65 020 RC65 021 RC65 022 RC65 033 RC65 031 RC65 031 RC65 031 RC65 040 RC65 040 RC65 041 RC66 045 RC66 046 RC66 047 RC66 046 RC66 047 RC66 023 RC66 024 RC66 026 RC66 027 RC66 026 RC66 026 RC66 026 RC66 026 RC66 027 RC66 027 RC66 028 RC66 029 RC66 020			
R046_026_126_1 R047_001 R045_001 R045_001 R045_002 R055_002 R055_003 R055_004 R055_005 R055_006 R055_007 R055_008 R055_009 R055_017 R055_018 R055_021 R055_022 R055_023 R055_024 R055_023 R055_024 R055_024 R055_024 R055_025 R056_028 R045_033 R056_037 R055_040 R056_041 R056_0			
RA45 (024 RA55 001 RQ55 001 RQ55 002 RQ55 003 RQ55 004 RQ55 005 RQ55 006 RQ55 006 RQ55 007 RQ55 006 RQ55 007 RQ55 008 RQ55 009 RQ55 009 RQ55 018 RQ55 020 RQ55 022 RQ55 022 RQ55 023 RQ55 024 RQ55 021 RQ55 021 RQ55 022 RQ55 023 RQ55 024 RQ55 027 RQ55 029 RQ55 033 RQ55 034 RQ55 041 RQ55 040 RQ55 041 RQ55 040 RQ55 041 RQ55 040 RQ55 041 RQ56 015 RQ56 016 RQ56 017 RQ56 022 RQ56 023 RQ56 024 RQ56 026 RQ56 027 RQ52 001 RQ57 039 RQ62 001 RQ57 039 RQ62 001 RQ57 039 RQ62 001 RQ65 001 RQ65 001 RQ65 007 RQ62 003 RQ65 007 RQ62 009 RQ65 000 RQ65 004 RQ65 007 RQ			RQ45_006
RA45 (024 RA55 001 RQ55 001 RQ55 002 RQ55 003 RQ55 004 RQ55 005 RQ55 006 RQ55 006 RQ55 007 RQ55 006 RQ55 007 RQ55 008 RQ55 009 RQ55 009 RQ55 018 RQ55 020 RQ55 022 RQ55 022 RQ55 023 RQ55 024 RQ55 021 RQ55 021 RQ55 022 RQ55 023 RQ55 024 RQ55 027 RQ55 029 RQ55 033 RQ55 034 RQ55 041 RQ55 040 RQ55 041 RQ55 040 RQ55 041 RQ55 040 RQ55 041 RQ56 015 RQ56 016 RQ56 017 RQ56 022 RQ56 023 RQ56 024 RQ56 026 RQ56 027 RQ52 001 RQ57 039 RQ62 001 RQ57 039 RQ62 001 RQ57 039 RQ62 001 RQ65 001 RQ65 001 RQ65 007 RQ62 003 RQ65 007 RQ62 009 RQ65 000 RQ65 004 RQ65 007 RQ			RQ45_026
RG47_001 RG55_001 RG55_002 RG65_003 RG55_004 RG55_005 RG55_006 RG55_006 RG55_007 RG55_008 RG55_009 RG55_007 RG55_008 RG55_009 RG55_007 RG55_018 RG55_009 RG55_011 RG55_018 RG55_011 RG55_018 RG55_011 RG55_018 RG55_021 RG55_022 RG55_021 RG55_023 RG55_021 RG55_024 RG55_024 RG55_025 RG55_025 RG55_026 RG55_027 RG55_041 RG65_041 RG6			
RG55, 001 RG55, 003 RG55, 003 RG55, 004 RG55, 005 RG55, 006 RG55, 007 RG56, 008 RG55, 007 RG56, 008 RG55, 007 RG56, 008 RG55, 007 RG55, 001 RG55, 001 RG55, 001 RG55, 002 RG55, 021 RG55, 022 RG55, 022 RG55, 023 RG55, 023 RG55, 033 RG55, 033 RG55, 033 RG56, 034 RG56, 041 RG56, 041 RG56, 041 RG56, 041 RG56, 041 RG56, 041 RG56, 042 RG56, 022 RG56, 023 RG56, 024 RG56, 024 RG56, 027 RG66, 026 RG66, 027 RG66, 027 RG62, 007 RG65, 007 RG67,			
RG55_002 RG55_004 RG55_004 RG55_006 RG55_006 RG55_007 RG55_008 RG55_009 RG55_017 RG55_008 RG55_017 RG55_018 RG55_019 RG55_011 RG55_021 RG55_021 RG55_022 RG55_023 RG55_023 RG55_023 RG55_024 RG55_028 RG55_029 RG55_041 RG55_033 RG55_033 RG55_031 RG55_031 RG56_015 RG56_015 RG56_017 RG56_017 RG56_022 RG66_023 RG66_024 RG56_026 RG66_027 RG62_001 RG65_007 RG62_000 RG62_006 RG62_007 RG62_000 RG65_001 RG65_002 RG65_001 RG65_002 RG65_001 RG65_002 RG65_007 RG62_006 RG62_007 RG62_006 RG62_007 RG62_007 RG65_008 RG65_007 RG65_008 RG65_007 RG65_008 RG65_007 RG65_008 RG65_007 RG65_008 RG66_007 RG65_008 RG65_007 RG65_007 RG65_008 RG65_007 RG65_007 RG65_007 RG65_008 RG66_007 RG65_007 RG6			
RQ55_003 RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_008 RQ55_017 RQ55_009 RQ55_017 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_023 RQ55_024 RQ55_024 RQ55_033 RQ55_041 RQ55_040 RQ55_040 RQ55_041 RQ56_016 RQ66_016 RQ66_017 RQ56_022 RQ56_023 RQ66_024 RQ56_026 RQ56_027 RQ66_0201 RQ57_039 RQ66_0201 RQ67_003 RQ62_002 RQ62_001 RQ67_003 RQ62_004 RQ62_007 RQ66_006 RQ62_007 RQ66_001 RQ66_007 RQ66_008 RQ65_007 RQ66_008 RQ65_008 RQ65_008 RQ65_009 RQ65_009 RQ65_000 RQ66_0001 RQ66_0001 RQ66_0001 RQ66_0001 RQ66_0001 RQ66_0001 RQ66_0001 RQ66_0001 RQ60_0002			
RQ55_004 RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_018 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_033 RQ55_033 RQ55_037 RQ55_040 RQ55_041 RQ56_016 RQ56_017 RQ66_017 RQ66_017 RQ66_022 RQ66_022 RQ66_023 RQ66_024 RQ66_026 RQ66_027 RQ62_001 RQ62_001 RQ62_001 RQ62_002 RQ62_001 RQ62_007 RQ62_001 RQ66_002 RQ62_007 RQ66_003 RQ66_001 RQ66_002 RQ66_002 RQ66_003 RQ66_004 RQ66_007 RQ66_006 RQ62_007 RQ66_007 RQ66_007 RQ66_007 RQ66_007 RQ66_008 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_000 RQ66_000			
RQ55_006 RQ55_007 RQ55_008 RQ55_008 RQ55_017 RQ55_009 RQ55_011 RQ55_021 RQ55_021 RQ55_022 RQ55_023 RQ55_023 RQ55_028 RQ55_033_1 RQ55_033_1 RQ55_037 RQ55_041 RQ56_016 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ66_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ66_026 RQ56_027 RQ66_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ66_002 RQ66_002 RQ66_003 RQ62_004 RQ66_006 RQ62_007 RQ66_007 RQ66_007 RQ66_007 RQ66_007 RQ66_008 RQ66_007 RQ66_008 RQ66_007 RQ66_008 RQ66_007 RQ66_008 RQ66_007 RQ66_009 RQ66_007 RQ66_008 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_000			
RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_009 RQ55_018 RQ55_021 RQ55_021 RQ55_022 RQ55_022 RQ55_033 RQ55_033 RQ55_033 RQ55_031 RQ55_040 RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_006 RQ62_007 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_005 RQ62_007 RQ62_001 RQ66_001 RQ66_002 RQ66_002 RQ66_003 RQ66_006 RQ62_007 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ66_007 RQ66_008 RQ66_007 RQ66_007 RQ66_007 RQ66_008 RQ66_007 RQ6			
RQ55_007 RQ55_008 RQ55_009 RQ55_019 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_028 RQ55_033 RQ55_033_1 RQ55_037 RQ55_040 RQ55_041 RQ66_015 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_001 RQ67_009 RQ62_005 RQ62_006 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_007 RQ65_008 RQ65_007 RQ62_009 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_000 RQ65_001 RQ65_000 RQ65_001 RQ65_000 RQ65_001 RQ66_0000 RQ65_001 RQ60_0001 RQ60_0001			RQ55_005
RQ55_007 RQ55_008 RQ55_009 RQ55_019 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_028 RQ55_033 RQ55_033_1 RQ55_037 RQ55_040 RQ55_041 RQ66_015 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_001 RQ67_009 RQ62_005 RQ62_006 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_007 RQ65_008 RQ65_007 RQ62_009 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_000 RQ65_001 RQ65_000 RQ65_001 RQ65_000 RQ65_001 RQ66_0000 RQ65_001 RQ60_0001 RQ60_0001			RQ55_006
RQ55_009 RQ55_017 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_021 RQ55_028 RQ55_028 RQ55_028 RQ55_033_1 RQ55_033_1 RQ55_037 RQ55_040 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_022 RQ56_022 RQ66_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_007 RQ62_007 RQ65_008 RQ66_007 RQ65_008 RQ66_007 RQ65_009 RQ66_007 RQ65_009 RQ66_007 RQ65_009 RQ66_007 RQ65_009 RQ66_007 RQ65_009 RQ66_007 RQ65_009 RQ66_0000 RQ66_00000 RQ66_00000			
RQ55_017 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_021 RQ55_022 RQ55_033 RQ55_033 RQ55_033 RQ55_033 RQ55_031 RQ55_041 RQ56_037 RQ55_040 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ52_001 RQ57_039 RQ62_002 RQ62_001 RQ62_007 RQ62_007 RQ62_007 RQ62_007 RQ62_007 RQ62_008 RQ65_001 RQ65_003 RQ66_004 RQ66_004 RQ66_006 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_008 RQ65_0008 RQ66_0008 RQ66_0008 RQ66_0008 RQ66_0008 RQ66_0008 RQ66_0008 RQ66_0008			
RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033_1 RQ55_033_1 RQ55_037 RQ55_041 RQ55_041 RQ56_015 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_006 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_006 RQ62_006 RQ62_007 RQ65_001 RQ65_001 RQ65_001 RQ65_007 RQ66_007			
RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033 RQ55_033 RQ55_037 RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_024 RQ56_027 RQ62_001 RQ56_027 RQ62_001 RQ62_005 RQ62_002 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ66_007			
RQ55_020 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033_1 RQ55_037 RQ55_040 RQ55_041 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ66_007			
RQ55_021 RQ55_022 RQ55_028 RQ65_033 RQ55_033_1 RQ55_031 RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_015 RQ56_016 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ66_026 RQ56_027 RQ66_006 RQ57_039 RQ62_001 RQ62_002 RQ62_002 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_005 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ66_009			
RQ55_022 RQ55_028 RQ55_033_1 RQ55_033_1 RQ55_031 RQ55_041 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ66_022 RQ66_023 RQ56_024 RQ66_026 RQ66_027 RQ62_001 RQ57_039 RQ62_001 RQ67_039 RQ62_004 RQ62_003 RQ62_004 RQ62_006 RQ62_007 RQ62_007 RQ62_007 RQ62_007 RQ65_007			
RG55_028 RQ55_033_1 RQ55_033_1 RQ55_037 RQ65_040 RQ55_041 RQ56_015 RQ56_015 RQ56_017 RQ56_022 RQ66_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ65_0201 RQ62_002 RQ62_003 RQ62_002 RQ62_003 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_007 RQ62_007 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ665_002 RQ65_003 RQ65_001 RQ665_001 RQ665_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_006 RQ65_007 RQ65_008 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_001 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_000000000000000000000000000000000000			RQ55_021
RG55_028 RQ55_033_1 RQ55_033_1 RQ55_037 RQ65_040 RQ55_041 RQ56_015 RQ56_015 RQ56_017 RQ56_022 RQ66_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ65_0201 RQ62_002 RQ62_003 RQ62_002 RQ62_003 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_007 RQ62_007 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ665_002 RQ65_003 RQ65_001 RQ665_001 RQ665_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_006 RQ65_007 RQ65_008 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_001 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_000000000000000000000000000000000000			RQ55_022
RQ55_033_1 RQ55_033_1 RQ55_037 RQ55_040 RQ55_041 RQ55_041 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_001 RQ62_002 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_000			
RQ55_033_1 RQ55_040 RQ55_041 RQ55_041 RQ56_015 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_001 RQ66_0001 RQ66_001 RQ66_001 RQ66_001			
RQ55_037 RQ55_040 RQ55_041 RQ56_015 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_000 RQ65_001 RQ65_0008 RQ65_001 RQ65_0008 RQ66_0009 RQ65_001 RQ65_0008 RQ66_0009 RQ65_001 RQ60_001 RQ60_001			
RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_007 RQ65_008 RQ65_009 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_021 RQ60_001			
RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_022 RQ56_023 RQ56_026 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_009 RQ65_021 RQ60_001 RQ60_001 RQ60_002 RQ60_002 RQ60_003			
RQ56_015 RQ56_017 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_007 RQ62_007 RQ62_007 RQ62_007 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_0001 RQ60_001 RQG0_001			
RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_024 RQ56_027 RQ62_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_001 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ60_0000 RQ60_0000			
RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_026 RQ56_027 RG62_001 RQ57_039 RG62_002 RQ62_003 RG62_004 RQ62_005 RQ62_006 RG62_007 RQ62_009 RG65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_0201 RQG0_001 RQG0_001 RQG0_002 RQG0_002			RQ56_015
RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_026 RQ56_027 RG62_001 RQ57_039 RG62_002 RQ62_003 RG62_004 RQ62_005 RQ62_006 RG62_007 RQ62_009 RG65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_0201 RQG0_001 RQG0_001 RQG0_002 RQG0_002			RQ56_016
RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_020			
RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_0001 RQG0_0001 RQG0_0002 RQ60_003			
RQ56_024 RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_0001 RQG0_0002 RQ60_0003			
RQ56_026 RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ665_007 RQ65_008 RQ65_009 RQ65_020 RQ60_001 RQG0_001			
RQ56_027 RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_0001 RQ65_0001 RQ65_0001 RQ60_0002 RQ60_0003			
RQ62_001 RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ66_008 RQ65_007 RQ60_001 RQ65_021 RQG0_001 RQG0_002 RQG0_002			
RQ57_039 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_0001 RQG0_001 RQG0_002 RQG0_003			
RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ60_001 RQG0_002 RQ60_002 RQ60_003			
RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ60_001 RQG0_002 RQ60_002 RQ60_003			RQ57_039
RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ60_001 RQG0_001 RQG0_002 RQG0_003			
RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ60_001 RQG0_001 RQG0_002 RQ60_003			
RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_002			
RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_001 RQG0_002 RQG0_003			
RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			RQ65_001
RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_001 RQG0_002 RQG0_003			
RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_021 RQG0_001 RQG0_002 RQG0_003			
RQ65_021 RQG0_001 RQG0_002 RQG0_003			RQ65_020
RQG0_001 RQG0_002 RQG0_003			
RQG0_002 RQG0_003			
RQG0_003			
RQG0_003			
			NGG0_003
RQG0_004	<u></u>		KQGU_UU4

V1.4 Page 294 of 777

RQG0_005	
RQG0_006	

Test Sequence #09 Nominal: Confirmation Code retry

The purpose of this test is to test that the SM-DP+ accepts a subsequent correct Confirmation Code after the initial Confirmation Code supplied in the GetBoundProfilePackageRequest ASN.1 euiccSigned2 element is unknown.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and PPK_MAC>.</ppk_enc> Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+. The SM-DP+ is configured with two retries allowed for the receipt of a valid Confirmation Code There have been no previous attempts to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS	_UC_INVALID_CC	
IC2	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS	_UC_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_C C))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_PPK (#R_GET_BPP_RESP_OP1_PPK, <s_mac>, <s_enc>, <ppk_mac>, <ppk_enc>, #SMDP_METADATA_OP_PROF1)</ppk_enc></ppk_mac></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_006 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_015 RQ26_018 RQ26_020 RQ26_022 RQ26_022 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_034 RQ26_035 RQ31_143 RQ31_144 RQ31_144 RQ31_146 RQ31_147 RQ31_148 RQ31_148 RQ31_148 RQ31_148 RQ31_165 RQ31_165 RQ31_166 RQ31_170 RQ32_069 RQ32_070 RQ44_001 RQ45_006 RQ45_026

V1.4 Page 295 of 777

 T		
		RQ45_026_1
		RQ47_001
		RQ55_001
		RQ55_002
		RQ55_003
		RQ55_004
		RQ55_005
		RQ55_006
		RQ55_007
		RQ55_008
		RQ55_009
		RQ55_017
		RQ55_018
		RQ55_020
		RQ55_021
		RQ55_022
		RQ55_028
		RQ55_033
		RQ55_033_1
		RQ55_037
		RQ55_041
		RQ56_015
		RQ56_016
		RQ56_017
		RQ56_020
		RQ56_025
		RQ56_026
		RQ56_028
		RQ57_039
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
		RQG0_005
		RQG0_006
 1		

V1.4 Page 296 of 777

4.3.13.2.5 VOID

4.3.13.2.6VOID

4.3.13.2.7TC_SM-

DP+_ES9+.GetBoundProfilePackage_RetryCases_DifferentOTPK_NIST

General Initial Condition	General Initial Conditions			
Entity	Description of the general initial condition			
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. The EID is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.			

Test Sequence #01 Nominal: Retry without otPK.EUICC.ECKA using S-ENC and S-MAC without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt without otPK.EUICC.ECKA using the S-ENC and S-MAC without a Confirmation Code.

Initial Conditions				
Entity	Description of the initial condition			
SM-DP+	 PROFILE_OPERATIONAL1 is loaded as an Unprotected Profile Package. Confirmation Code is not provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile. 			

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_ Extract <otpk 4.</otpk 			
IC2	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRES	S_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ NEW_OTPK))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_SK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_SK (#R_GET_BPP_RESP_OP1_SK, <s_mac>, <s_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 is different from the value previously received in the</otpk_sm_dp+_ecka></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_006 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_022 RQ26_029

V1.4 Page 297 of 777

	GetBoundProfilePackage response in	RQ26_031
	step 4 of the procedure in IC1	RQ26_034
		RQ26_035
		RQ31_143
		RQ31_150
		RQ31_151
		RQ31_151
		RQ31_155
		RQ31_162
		RQ31_165
		RQ31_166
		RQ31_170
		RQ32_069
		RQ32_070
		RQ44_001
		RQ45_006
		RQ45_026
		RQ45_026_1
		RQ55_001
		RQ55_002
		RQ55_003
		RQ55_004
		RQ55_005
		RQ55_006
		RQ55_007
		RQ55_008
		RQ55_009
		RQ55_017
		RQ55_018
		RQ55_020
		RQ55_021
		RQ55_022
		RQ55_028
		RQ55_033
		RQ55_033_1
		RQ55_037
		RQ55_041
		RQ56_015
		RQ56_016
		RQ56_017
		RQ56_023
		RQ56_024
		RQ56_026
		RQ56_027
		RQ57_039
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
	•	

V1.4 Page 298 of 777

		RQ65_021	
		RQG0_001	
		RQG0_002	
		RQG0_003	
		RQG0_004	
		RQG0_005	
		RQG0_006	
		1	

Test Sequence #02 Nominal: Retry without otPK.EUICC.ECKA using S-ENC and S-MAC with Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt without otPK.EUICC.ECKA using the S-ENC and S-MAC with a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is loaded as an Unprotected Profile Package. Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+. SK Extract <otp GetBoundPro PROC_ES9+.</otp 			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ NEW_OTPK_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_SK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_SK (#R_GET_BPP_RESP_OP1_SK, <s_mac>, <s_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 is different from the value previously received in the GetBoundProfilePackage response in step 4 of the procedure in IC1</otpk_sm_dp+_ecka></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_004 RQ25_006 RQ25_010 RQ25_011 RQ25_013 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_020 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_035 RQ31_143 RQ31_144 RQ31_146 RQ31_147 RQ31_150 RQ31_151 RQ31_150 RQ31_151 RQ31_155 RQ31_155 RQ31_165 RQ31_165 RQ31_166

V1.4 Page 299 of 777

R331_370 R322_069 R322_070 R44_001 R45_006 R45_007 R45_006 R45_007 R45	T		
R032_070 R044_001 R045_006 R045_026 R046_026_1 R047_001 R055_001 R055_001 R055_001 R055_003 R055_003 R055_004 R055_006 R055_007 R055_009 R055_017 R055_009 R055_017 R055_009 R055_017 R055_009 R055_017 R055_028 R055_021 R055_028 R055_023 R055_021 R055_028 R055_023 R055_028 R055_027 R055_028 R055_028 R055_028 R055_029 R056_027 R057_039 R062_001 R062_002 R065_003 R062_004 R065_006 R062_007 R062_009 R065_001 R065_001 R065_002 R065_003 R065_001 R065_001 R065_001 R065_001 R065_001 R065_002 R065_003 R065_003 R065_003 R065_004 R065_006 R065_007 R065_008 R065_007 R065_008 R065_007 R065_009 R065_001 R065_001 R065_001 R065_002 R065_003 R065_003 R065_004 R065_006 R065_007 R			RQ31_170
RQ44_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ65_001 RQ65_001 RQ65_003 RQ65_003 RQ65_004 RQ65_005 RQ65_006 RQ26_006 RQ26_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ65_007 RQ66_007			
RQ45,026 RQ45,026 RQ45,026 RQ45,026 RQ45,026 RQ45,001 RQ65,001 RQ65,001 RQ65,003 RQ50,003 RQ50,004 RQ65,005 RQ65,007 RQ65,008 RQ65,009 RQ65,001 RQ65,007 RQ65,001 RQ66,001 RQ66,001 RQ66,001 RQ66,001 RQ66,001 RQ66,001 RQ66,001 RQ66,001 RQ62,001 RQ63,001 RQ63,001 RQ65,001 RQ60,003 RQ65,001			
RQ45_026_1 RQ47_001 RQ65_001 RQ65_001 RQ65_002 RQ56_003 RQ65_004 RQ65_006 RQ65_007 RQ65_008 RQ65_008 RQ65_009 RQ66_016 RQ65_007 RQ66_022 RQ66_024 RQ66_024 RQ66_024 RQ66_026 RQ66_026 RQ66_026 RQ66_027 RQ66_026 RQ66_027 RQ66_027 RQ66_028 RQ66_029 RQ66_029 RQ66_029 RQ66_029 RQ66_020 RQ66_001 RQ62_001 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_007 RQ66_006 RQ62_007 RQ66_006 RQ62_007 RQ66_007			RQ44_001
RO45_026_1 RO47_001 RO55_001 RO55_002 RO55_003 RO55_004 RO55_005 RO55_006 RO55_007 RO55_008 RO55_007 RO55_008 RO55_009 RO55_017 RO55_008 RO55_009 RO55_017 RO55_008 RO55_009 RO55_017 RO55_008 RO55_021 RO55_022 RO55_021 RO55_022 RO55_021 RO55_022 RO55_021 RO55_033_1 RO55_033_1 RO55_033_1 RO55_031 RO55_031 RO55_031 RO56_031 RO56_031 RO56_031 RO56_032 RO56_036 RO66_001 RO66_002 RO66_003 RO66_004 RO66_007 RO66_006 RO66_007 RO66			RQ45_006
RO45_026_1 RO47_001 RO55_001 RO55_002 RO55_003 RO55_004 RO55_005 RO55_006 RO55_007 RO55_008 RO55_007 RO55_008 RO55_009 RO55_017 RO55_008 RO55_009 RO55_017 RO55_008 RO55_009 RO55_017 RO55_008 RO55_021 RO55_022 RO55_021 RO55_022 RO55_021 RO55_022 RO55_021 RO55_033_1 RO55_033_1 RO55_033_1 RO55_031 RO55_031 RO55_031 RO56_031 RO56_031 RO56_031 RO56_032 RO56_036 RO66_001 RO66_002 RO66_003 RO66_004 RO66_007 RO66_006 RO66_007 RO66			RQ45_026
R047.001 R055.001 R055.002 R055.003 R055.003 R055.004 R055.006 R055.007 R065.008 R065.007 R065.007 R065.008 R065.001 R065.001 R065.001 R065.001 R065.001 R065.001 R066.002 R0662.001 R0662.006 R062.003 R0662.004 R0662.006 R062.007 R0665.007 R0665.007 R0660.001 R0660.001 R0660.001 R0665.001 R0665.002 R0665.003 R0665.004 R0665.004 R0665.007 R0665.006 R0665.007			
RG55_001 RG55_002 RG55_003 RG55_004 RG55_005 RG55_006 RG55_007 RG55_008 RG55_007 RG55_008 RG55_017 RG55_008 RG55_017 RG55_017 RG55_017 RG55_020 RG55_017 RG55_022 RG55_021 RG55_022 RG55_023 RG55_021 RG56_022 RG55_033 RG55_033 RG55_033 RG55_033 RG55_033 RG55_033 RG55_033 RG55_033 RG55_037 RG56_016 RG56_017 RG56_016 RG56_017 RG66_016 RG66_017 RG66_022 RG66_024 RG66_027 RG67_039 RG62_001 RG62_001 RG62_001 RG62_001 RG62_001 RG62_002 RG62_003 RG62_004 RG65_007 RG66_007			
RQ55_002 RQ55_003 RQ65_004 RQ65_006 RQ65_007 RQ65_008 RQ65_009 RQ55_018 RQ55_018 RQ55_021 RQ65_022 RQ55_022 RQ55_023 RQ55_023 RQ55_023 RQ56_024 RQ66_015 RQ66_016 RQ66_024 RQ66_027 RQ66_026 RQ66_027 RQ66_026 RQ66_027 RQ66_026 RQ66_027 RQ66_027 RQ66_026 RQ66_027 RQ66_027 RQ66_027 RQ66_026 RQ66_027 RQ66_036 RQ66_076 RQ6			
RG55_003 RG55_005 RG55_006 RG55_006 RG55_007 RG55_008 RG55_007 RG55_008 RG55_017 RG55_017 RG55_018 RG55_020 RG55_021 RG55_022 RG55_023 RG55_023 RG55_023 RG55_033 1 RG55_033 1 RG55_033 1 RG56_037 RG56_024 RG56_016 RG66_016 RG66_016 RG66_017 RG66_022 RG66_024 RG66_026 RG66_024 RG66_026 RG66_026 RG66_026 RG62_007 RG62_001 RG62_005 RG62_007 RG62_006 RG65_007 RG65_001 RG65_001 RG65_001 RG65_002 RG65_001 RG65_002 RG65_002 RG65_003 RG65_004 RG65_007 RG65_009 RG65_001 RG65_000			
RQ55_004 RQ55_005 RQ55_006 RQ55_007 RQ55_007 RQ55_008 RQ55_009 RQ55_018 RQ55_021 RQ55_021 RQ55_022 RQ55_023 RQ55_023 RQ55_024 RQ55_028 RQ55_033_1 RQ55_033_1 RQ55_037 RQ56_015 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_020 RQ56_020 RQ56_020 RQ56_027 RQ66_007			RQ55_003
RQ55_006 RQ55_007 RQ55_007 RQ55_007 RQ55_007 RQ55_007 RQ55_009 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_023 RQ55_033 RQ55_033 RQ55_031 RQ55_031 RQ55_031 RQ55_031 RQ55_041 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_022 RQ56_023 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_007 RQ65_007 RQ66_007			
RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_018 RQ55_019 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033_1 RQ55_033_1 RQ55_031 RQ55_031 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ66_006 RQ62_007 RQ62_009 RQ65_001 RQ66_006 RQ62_007 RQ62_009 RQ65_001 RQ66_006 RQ66_006 RQ66_006 RQ66_007 RQ66_006 RQ66_007 RQ66_006 RQ66_007 RQ66_006 RQ66_007 RQ66_006 RQ66_007 RQ66_007 RQ66_008 RQ66_008 RQ66_008 RQ66_009 RQ66_001 RQ66_001 RQ60_001 RQ60_001 RQ60_001 RQ60_002 RQ66_001 RQ60_001 RQ60_002 RQ66_001			
RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_023 RQ55_023 RQ55_033 RQ55_033 RQ55_031 RQ55_031 RQ55_031 RQ55_031 RQ55_041 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ65_007 RQ66_007			
RQ55_008 RQ55_017 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ56_015 RQ66_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_007 RQ62_006 RQ62_007 RQ62_007 RQ62_008 RQ62_007 RQ62_009 RQ65_001 RQ66_007 RQ62_009 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_006 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_0000 RQ65_000000000000000000000000000000000000			
RQ55_009 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ56_016 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_006 RQ62_007 RQ65_003 RQ62_006 RQ62_007 RQ65_003 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ66_007 RQ65_008 RQ65_009 RQ65_001 RQ66_007 RQ65_008 RQ65_000 RQ66_007 RQ65_000 RQ60_0002 RQ60_0003 RQ60_0003 RQ60_0003			
RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ66_015 RQ56_022 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RG62_001 RQ62_003 RQ62_004 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_002 RQ65_003 RQ65_004 RQ65_002 RQ65_003 RQ65_004 RQ65_002 RQ65_003 RQ65_004 RQ65_004 RQ65_006 RQ62_007 RQ65_008 RQ65_001 RQ60_001 RQ60_001 RQ60_001			
RQ55_020 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033 RQ55_033_1 RQ55_037 RQ55_041 RQ56_016 RQ66_016 RQ66_016 RQ66_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_026 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_006 RQ62_007 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_009 RQ65_001 RQ65_0000 RQ65_000000000000000000000000000000000000			
RQ55_020 RQ55_021 RQ55_021 RQ55_022 RQ55_028 RQ55_033_1 RQ55_033_1 RQ55_031 RQ55_031 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_024 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_007 RQ62_008 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_006 RQ65_007 RQ65_007 RQ65_008 RQ65_007 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ66_001 RQ60_001 RQ60_001			
RQ55_021 RQ55_028 RQ55_028 RQ55_033 RQ55_033,1 RQ55_031 RQ55_037 RQ55_041 RQ56_016 RQ66_016 RQ66_017 RQ56_022 RQ56_023 RQ56_024 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_008 RQ66_001 RQ60_001			
RO55_022 RQ55_028 RQ55_033 1 RQ55_033 1 RQ55_041 RQ56_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_024 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_007 RQ62_009 RQ65_001 RQ62_007 RQ63_007			
RC55_028 RQ55_033 RQ55_033_1 RG55_037 RG55_041 RG56_015 RG56_016 RG56_016 RG56_017 RQ56_022 RG56_023 RG56_023 RG56_024 RG56_026 RG56_027 RG57_039 RG62_001 RG62_002 RG62_001 RG62_002 RG62_001 RG62_002 RG62_003 RG62_006 RG62_007 RG65_001 RG65_001 RG65_002 RG65_003 RG65_004 RG65_003 RG65_004 RG65_005 RG65_007 RG65_008 RG65_007 RG65_008 RG65_001 RG65_001 RG65_002 RG65_001 RG65_002 RG65_003 RG65_004 RG65_005 RG65_007 RG65_007 RG65_007 RG65_008 RG65_009 RG65_001 RG65_000000000000000000000000000000000000			
RC55_033_1 RC55_033_1 RC55_037 RC55_041 RC56_015 RC56_015 RC56_016 RC56_017 RC56_022 RC56_022 RC56_023 RC56_024 RC56_026 RC56_027 RC57_039 RC62_001 RC62_001 RC62_002 RC62_003 RC62_004 RC62_005 RC62_006 RC62_007 RC67_009 RC65_001 RC65_002 RC65_001 RC65_007 RC65_008 RC65_007 RC65_008 RC65_007 RC65_008 RC65_009			
RQ65_033_1 RQ55_031 RQ55_041 RQ56_015 RQ66_015 RQ66_017 RQ66_022 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_006 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_001 RQ65_00008 RQ65_001 RQ66_00008 RQ65_000008 RQ65_000008 RQ65_000008 RQ60_0001 RQ60_0001 RQ60_0003			
RQ55_037 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_009 RQ65_001 RQ65_0006 RQ65_001 RQ65_002 RQ65_003 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_000000000000000000000000000000000000			
RQ55_041 RQ56_015 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_002 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_0008 RQ65_0008 RQ65_00008 RQ65_00008 RQ60_0001 RQG0_0002 RQ60_0003 RQG0_0004			
RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_006 RQ62_007 RQ62_008 RQ62_007 RQ63_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_000 RQ65_001 RQ66_0000 RQ60_0000 RQ60_0000			
RQ56_016 RQ56_027 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_006 RQ62_007 RQ62_007 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_0008 RQ66_0008 RQ66_0008 RQ60_0008			
RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_007 RQ62_007 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_001 RQ60_001 RQ60_001 RQ60_002 RQG0_003 RQG0_004 RQ60_003			
RQ56_022 RQ36_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ66_008 RQ65_007 RQ66_008 RQ65_009 RQ65_020 RQ65_020 RQ66_020 RQ66_020 RQ66_0003 RQ66_020 RQ66_001 RQ60_001 RQ60_002 RQ60_003 RQ60_003 RQ60_003			
RQ56_023 RQ36_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_001 RQ60_00000000000000000000000000000000000			
RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RG62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_007 RQ60_008 RQ60_007 RQ60_003 RQG0_004			
RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_007 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_006 RQ65_007 RQ65_007 RQ65_008 RQ65_008 RQ65_009 RQ65_009 RQ65_0000 RQ65_000000000000000000000000000000000000			RQ56_023
RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_000005 RQ60_0003 RQG0_0003 RQG0_0005			RQ56_024
RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_000005 RQ60_0003 RQG0_0003 RQG0_0005			RQ56_026
RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_009			
RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_004 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_020 RQ60_001 RQG0_001 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ60_001 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_001 RQG0_003 RQG0_004 RQG0_005			
RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			RQ62 009
RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQG0_003 RQG0_004 RQG0_005			
RQG0_004 RQG0_005			
RQG0_005			
			KQG0_006

V1.4 Page 300 of 777

Test Sequence #03 Nominal: Retry without otPK.EUICC.ECKA using PPK-ENC and PPK-MAC without Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt without otPK.EUICC.ECKA using the PPK-ENC and PPK-MAC without a Confirmation Code.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	K Extract <otpk GetBoundProf</otpk 	ROF_DOWNLOAD_DEF_DP_USE_CASE_CANCEL_SESSION_PP SM_DP+_ECKA> from #INIT_SC_PROF1 in the Package Response in Step 4. MA_PD_DEF_SMDP_ADDRESS_UC_NO_CC		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_ NEW_OTPK))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_PP K (#R_GET_BPP_RESP_OP1_PPK, <s_mac>, <s_enc>, <ppk_mac>, <ppk_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 is different from the value previously received in the GetBoundProfilePackage response in step 4 of the procedure in IC1</otpk_sm_dp+_ecka></ppk_enc></ppk_mac></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_005 RQ25_006 RQ25_009 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_014 RQ25_015 RQ26_019 RQ26_021 RQ26_020 RQ26_021 RQ26_022 RQ26_029 RQ26_031 RQ26_031 RQ26_035 RQ31_143 RQ31_148_3 RQ31_148_3 RQ31_150 RQ31_151 RQ31_152 RQ31_155 RQ31_155 RQ31_166 RQ31_168 RQ31_168 RQ31_170 RQ32_069 RQ32_070 RQ44_001

V1.4 Page 301 of 777

		RQ45_006
		RQ45_026
		RQ45_026_1
		RQ55_001
		RQ55_002 RQ55_003
		RQ55_004
		RQ55_005
		RQ55_006
		RQ55_007
		RQ55_008
		RQ55_009
		RQ55_017
		RQ55_018
		RQ55_020
		RQ55_021
		RQ55_022
		RQ55_028
		RQ55_033
		RQ55_033_1
		RQ55_037
		RQ55_040
		RQ55_041
		RQ56_015
		RQ56_016
		RQ56_017
		RQ56_022
		RQ56_023 RQ56_024
		RQ56_026
		RQ56_027
		RQ57_039
		RQ62_001
		RQ62_001
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_007
		RQ65_001
		RQ65_001
		RQ65_002
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_020
		RQ65_021
		RQG0_001
		RQG0_002
		RQG0_003
		RQG0_004
		RQG0_005
		RQG0_006
	<u> </u>	

V1.4 Page 302 of 777

Test Sequence #04 Nominal: Retry without otPK.EUICC.ECKA using PPK-ENC and PPK-MAC with Confirmation Code

The purpose of this test is to test that the LPAd can request the delivery and the binding of a Profile Package for a retry attempt without otPK.EUICC.ECKA using the PPK-ENC and PPK-MAC with a Confirmation Code.

Initial Conditions		
Entity	Description of the initial condition	
	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> 	
SM-DP+	Confirmation Code #CONFIRMATION_CODE1 associated PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+. There have been no previous attempt to download the pending profile.	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_PROF_DOWNLOAD_DEF_DP_USE_CASE_CC_CANCEL_SESSION _PPK Extract <otpk_sm_dp+_ecka> from #INIT_SC_PROF1 in the GetBoundProfilePackage Response in Step 4. PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_CC</otpk_sm_dp+_ecka>			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP _NEW_OTPK_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_R ESP_OP1_PPK) • Verify that <transaction_id_gbpp> matches <s_transaction_id> MTD_TEST_ES8+_GET_BPP_PPK (#R_GET_BPP_RESP_OP1_PPK, <s_mac>, <s_enc>, <ppk_mac>, <ppk_enc>, #SMDP_METADATA_OP_PROF1) • Verify that <otpk_sm_dp+_ecka> in #INIT_SC_PROF1 is different from the value previously received in the GetBoundProfilePackage response in step 4 of the procedure in IC1.</otpk_sm_dp+_ecka></ppk_enc></ppk_mac></s_enc></s_mac></s_transaction_id></transaction_id_gbpp>	RQ25_001 RQ25_002 RQ25_006 RQ25_009 RQ25_010 RQ25_011 RQ25_012 RQ25_013 RQ25_014 RQ25_015 RQ26_018 RQ26_019 RQ26_020 RQ26_021 RQ26_021 RQ26_022 RQ26_021 RQ26_031 RQ26_035 RQ31_143 RQ31_144 RQ31_144 RQ31_146 RQ31_147 RQ31_148_3 RQ31_150 RQ31_151 RQ31_150 RQ31_151 RQ31_152 RQ31_155 RQ31_162 RQ31_165 RQ31_166 RQ31_166 RQ31_166

V1.4 Page 303 of 777

RO32_098 RO32_098 RO32_070 RO34_001 RO45_008 RO45_008 RO45_008 RO45_028_RO45_028_RO45_028_RO45_028_RO45_028_RO45_028_RO45_028_RO45_008 RO55_003 RO55_004 RO55_005 RO55_006 RO55_006 RO55_007 RO55_008 RO55_009 RO55_009 RO55_017 RO55_008 RO55_009 RO55_001 RO65_001 RO65_001 RO65_001 RO66_001 RO66_001 RO66_002 RO66_004 RO62_007 RO62_009 RO66_001 RO62_007 RO62_009 RO66_001 RO62_007 RO62_009 RO66_001		1	
RO32_070 RQ44_001 RQ45_006 RQ45_026_1 RQ47_001 RQ55_002 RQ55_002 RQ55_003 RQ55_004 RQ55_006 RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_008 RQ55_009 RQ55_009 RQ55_001 RQ55_002 RQ55_008 RQ55_008 RQ55_008 RQ55_008 RQ55_008 RQ55_008 RQ55_001 RQ55_007 RQ55_018 RQ55_033 RQ55_033_1 RQ55_006 RQ56_001 RQ66_002 RQ56_001 RQ66_002 RQ56_003 RQ66_004 RQ66_005 RQ62_006 RQ62_006 RQ62_007 RQ62_009 RQ62_009 RQ62_009 RQ62_009 RQ65_001 RQ65_001 RQ65_001 RQ65_000 RQ66_000			
RO44_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_027 RQ55_003 RQ55_007 RQ55_008 RQ65_007 RQ56_008 RQ66_008 RQ66_008 RQ66_008 RQ66_009			RQ32_069
RO44_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_026 RQ45_027 RQ55_003 RQ55_007 RQ55_008 RQ65_007 RQ56_008 RQ66_008 RQ66_008 RQ66_008 RQ66_009			RQ32 070
RQ45_006 RQ45_026_1 RQ45_026_1 RQ47_001 RQ55_002 RQ55_002 RQ55_003 RQ55_004 RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_001 RQ55_001 RQ55_001 RQ55_001 RQ55_001 RQ55_002 RQ55_002 RQ55_003 RQ55_003 RQ56_004 RQ56_006 RQ66_006 RQ66_007 RQ66_007 RQ66_008 RQ66_007 RQ66_008 RQ66_001 RQ66_007 RQ66_000 RQ66_001 RQ66_001 RQ66_001 RQ66_001 RQ66_002 RQ66_004 RQ66_006 RQ66_007 RQ66_008 RQ66_007 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_009 RQ66_000			
RO45 026 1 RO47_001 RQ55 001 RQ55 001 RQ55 002 RQ55 003 RQ55 006 RQ55 007 RQ55 008 RQ56 001 RQ66 001 RQ66 002 RQ62 003 RQ62 001 RQ62 002 RQ65 004 RQ65 007 RQ65 008 RQ66 001 RQ66 006 RQ62 007 RQ66 008 RQ66 007 RQ66 008 RQ66 001 RQ66 000			
RQ45_026_1 RQ47_001 RQ55_001 RQ55_001 RQ55_003 RQ55_003 RQ55_006 RQ55_006 RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_018 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_022 RQ55_023 RQ55_033_1 RQ55_033_1 RQ55_033_1 RQ56_037 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_027 RQ56_023 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ52_007 RQ52_007 RQ52_007 RQ52_007 RQ52_007 RQ52_007 RQ52_007 RQ56_003 RQ66_003 RQ66_007 RQ66			
RQ47, 001 RQ55, 002 RQ55, 002 RQ55, 003 RQ55, 004 RQ55, 006 RQ55, 006 RQ55, 006 RQ55, 007 RQ55, 008 RQ55, 009 RQ55, 017 RQ55, 018 RQ55, 018 RQ55, 020 RQ55, 021 RQ55, 022 RQ55, 022 RQ55, 023 RQ55, 023 RQ55, 023 RQ55, 023 RQ56, 023 RQ56, 023 RQ56, 024 RQ56, 024 RQ56, 027 RQ56, 022 RQ56, 023 RQ56, 024 RQ56, 024 RQ56, 027 RQ57 RQ57 RQ57 RQ57 RQ57 RQ57 RQ57 RQ5			
RQ55_001 RQ55_002 RQ55_003 RQ55_004 RQ55_006 RQ55_006 RQ55_006 RQ55_007 RQ55_008 RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_008 RQ55_017 RQ55_018 RQ55_022 RQ55_022 RQ55_023 RQ55_033 RQ55_033 RQ55_033 RQ55_031 RQ55_040 RQ55_041 RQ56_016 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_006 RQ52_007 RQ52_007 RQ62_009 RQ65_007 RQ66_006 RQ66_007 RQ66_007 RQ66_006 RQ66_007 RQ6			
RQ55. 002 RQ55. 003 RQ55. 004 RQ55. 004 RQ55. 006 RQ55. 007 RQ55. 008 RQ55. 009 RQ55. 009 RQ55. 017 RQ55. 018 RQ55. 020 RQ55. 021 RQ55. 022 RQ55. 022 RQ55. 023 RQ55. 033 RQ55. 033 RQ55. 033 RQ55. 034 RQ55. 041 RQ56. 015 RQ56. 016 RQ56. 017 RQ56. 017 RQ56. 022 RQ56. 024 RQ56. 027 RQ57. 039 RQ58. 001 RQ58. 002 RQ62. 004 RQ56. 001 RQ62. 002 RQ62. 003 RQ65. 001 RQ65. 001 RQ65. 001 RQ65. 002 RQ65. 001 RQ65. 002 RQ65. 007 RQ65. 002 RQ65. 007 RQ65. 009 RQ65. 001 RQ66. 004 RQ66. 007 RQ66. 008 RQ65. 007 RQ66. 009 RQ65. 001 RQ60. 001 RQ60. 002 RQ60. 003 RQ66. 004 RQ66. 007 RQ66. 008 RQ65. 007 RQ65. 009 RQ65. 001 RQ60. 001 RQ60. 002 RQ60. 003 RQ66. 003 RQ66. 004 RQ60. 003 RQ66. 003 RQ66. 004 RQ60. 003			
RQ55. 003 RQ55. 004 RQ55. 005 RQ55. 007 RQ55. 008 RQ55. 007 RQ55. 008 RQ55. 009 RQ55. 009 RQ55. 017 RQ55. 018 RQ55. 017 RQ55. 018 RQ55. 022 RQ55. 022 RQ55. 022 RQ55. 023 RQ55. 033.1 RQ55. 033.1 RQ55. 033.1 RQ55. 033.1 RQ56. 037 RQ56. 016 RQ56. 017 RQ56. 017 RQ56. 016 RQ56. 017 RQ56. 017 RQ56. 016 RQ56. 017 RQ56. 022 RQ56. 023 RQ56. 023 RQ56. 024 RQ56. 027 RQ57. 039 RQ62. 001 RQ62. 005 RQ62. 004 RQ62. 005 RQ62. 007 RQ65. 008 RQ65. 009 RQ65. 009 RQ65. 000 RQ66. 000 RQ60. 000			
RG55_006 RC95_006 RC95_006 RC95_007 RC95_008 RC95_007 RC95_008 RC95_009 RC95_017 RC95_018 RC95_020 RC95_021 RC95_022 RC95_022 RC95_023 RC95_023 RC95_033_1 RC95_033_1 RC95_033_1 RC95_033_1 RC95_041 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_023 RC96_023 RC96_024 RC96_026 RC96_027 RC97_039 RC96_027 RC97_039 RC96_020 RC96_003 RC96_004 RC96_006 RC96_006 RC96_006 RC96_007 RC96_006 RC96_007 RC96			RQ55_002
RG55_006 RC95_006 RC95_006 RC95_007 RC95_008 RC95_007 RC95_008 RC95_009 RC95_017 RC95_018 RC95_020 RC95_021 RC95_022 RC95_022 RC95_023 RC95_023 RC95_033_1 RC95_033_1 RC95_033_1 RC95_033_1 RC95_041 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_016 RC96_023 RC96_023 RC96_024 RC96_026 RC96_027 RC97_039 RC96_027 RC97_039 RC96_020 RC96_003 RC96_004 RC96_006 RC96_006 RC96_006 RC96_007 RC96_006 RC96_007 RC96			RQ55_003
ROS5.006 RQS5.006 RQS5.007 ROS5.008 RGS5.009 ROS5.009 ROS5.017 RQS5.008 ROS5.009 ROS5.017 RQS5.018 RGS5.021 RGS5.022 ROS5.022 ROS5.022 ROS5.023 ROS5.023 ROS5.033 ROS5.033 ROS5.033 ROS5.041 ROS5.037 ROS5.041 RQS5.041 RQS5.041 RQS6.016 RQS6.016 RQS6.016 RQS6.016 RQS6.016 RQS6.016 RQS6.016 RQS6.022 RQS6.023 RQS6.023 RQS6.024 RQS6.024 RQS6.026 RQS6.027 RQS7.039 RQS2.001 RQS2.001 RQS2.001 RQS2.001 RQS2.002 RQS6.003 RQS2.006 RQS2.007 RQS5.001 RQS5.001 RQS5.001 RQS5.001 RQS5.001 RQS5.001 RQS5.001 RQS5.001 RQS5.002 RQS5.003 RQS5.001 RQS5.001 RQS5.001 RQS5.002 RQS5.003 RQS5.004 RQS5.006 RQS2.007 RQS5.008 RQS5.009 RQS5.001 RQS5.001 RQS5.001 RQS5.001 RQS5.002 RQS5.000 RQS5.001 RQS65.001 RQS65.002 RQS5.000 RQS5.001 RQS0.001 RQS0.001 RQS0.001 RQS0.001			
RQ55_006 RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_018 RQ55_021 RQ55_022 RQ55_022 RQ55_022 RQ55_023 RQ55_023 RQ55_023 RQ55_023 RQ55_033 RQ55_033 RQ55_033 RQ55_031 RQ55_041 RQ56_016 RQ56_016 RQ56_016 RQ56_017 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ66_006 RQ62_006 RQ62_006 RQ66_006 RQ66_007 RQ62_007 RQ62_009 RQ65_001 RQ65_007 RQ65_009 RQ65_001 RQ65_007 RQ65_009 RQ65_001 RQ65_007 RQ65_009 RQ65_001 RQ65_000 RQ665_000			
RQ55_007 RQ55_008 RQ55_009 RQ55_017 RQ55_018 RQ55_020 RQ55_021 RQ55_022 RQ55_022 RQ55_023 RQ55_033 RQ55_033 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ55_041 RQ56_015 RQ56_016 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ56_026 RQ56_027 RQ56_027 RQ56_020 RQ66_000 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ65_005 RQ65_007 RQ65_006 RQ65_007 RQ65_009 RQ65_007 RQ65_009 RQ65_001 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ665_001 RQ60_0001 RQ60_0001 RQ60_0001 RQ60_0001 RQ60_0001			
ROS5_008 RQ55_007 ROS5_017 ROS5_018 ROS5_021 ROS5_021 ROS5_022 ROS5_023 ROS5_023 ROS5_033_1 ROS5_033_1 ROS5_033_1 ROS5_040 ROS5_041 ROS6_015 ROS6_016 ROS6_016 ROS6_017 ROS6_022 ROS6_024 ROS6_024 ROS6_026 ROS6_027 ROS5_040 ROS6_027 ROS5_041 ROS6_028 ROS6_029 ROS6_020 ROS6_001 ROS6_007 ROS6_003 ROS6_007 ROS6_003 ROS6_007 ROS6_006			
RG55_099 RQ55_017 RQ65_018 RQ55_020 RG55_021 RQ55_022 RG55_028 RG55_028 RG55_033_RG55_033_RG55_037 RG55_041 RQ55_041 RQ56_046 RG56_046 RG56_046 RG56_047 RG56_023 RG56_024 RG56_024 RG56_026 RG56_027 RG57_039 RG62_001 RG62_003 RG62_001 RG62_003 RG62_001 RG62_003 RG66_007 RG62_006 RG62_006 RG62_007 RG62_007 RG62_008 RG65_007 RG65_009 RG65_001 RG65_002 RG65_001 RG65_002 RG65_003 RG65_004 RG65_006 RG65_007 RG65_007 RG65_008 RG65_009 RG65_009 RG65_007 RG65_008 RG65_009 RG66_009			
RG55_017 RQ55_018 RQ55_021 RG55_022 RG55_022 RG55_028 RG55_033 RG55_033 RG55_033 RG55_031 RG55_031 RG55_031 RG55_040 RG55_041 RG56_016 RG56_016 RG56_017 RG56_021 RG56_022 RG56_022 RG56_022 RG56_022 RG56_022 RG56_022 RG56_026 RG56_027 RG57_039 RG62_001 RG62_001 RG62_002 RG62_007 RG62_007 RG62_006 RG62_007 RG62_007 RG62_008 RG65_007 RG65_008 RG65_009 RG65_007 RG65_009 RG65_001 RG65_001 RG65_001 RG65_001 RG65_002 RG65_007 RG65_000 RG65_001 RG65_001 RG65_001 RG65_001 RG65_001 RG65_002 RG65_007 RG65_000 RG65_001 RG65_000 RG65_001 RG65_000 RG65_001 RG65_000 RG65_001 RG65_000 RG65_001 RG65_000 RG65_002 RG65_000			
RQ65_018 RQ65_021 RQ65_021 RQ65_022 RQ65_028 RQ65_033 RQ65_033 RQ65_033 RQ65_031 RQ65_040 RQ65_041 RQ66_046 RQ66_046 RQ66_046 RQ66_046 RQ66_022 RQ66_023 RQ66_024 RQ66_026 RQ66_027 RQ67_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ65_008 RQ66_009 RQ65_001 RQ65_002 RQ65_003 RQ66_004 RQ65_006 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ66_009 RQ65_007 RQ65_008 RQ66_009 RQ66_001 RQ66_000 RQ66_001 RQ66_001 RQ66_001 RQ66_002 RQ66_003 RQ66_001 RQ66_001 RQ66_002 RQ66_003 RQ66_001 RQ66_001 RQ66_002 RQ66_003 RQ66_001 RQ66_001 RQ66_002 RQ66_003 RQ66_001			
RQ65_020 RQ65_021 RQ65_022 RQ65_022 RQ65_028 RQ65_033 RQ65_033 RQ65_033 RQ65_037 RQ65_040 RQ65_041 RQ66_016 RQ66_016 RQ66_016 RQ66_022 RQ66_023 RQ66_022 RQ66_023 RQ66_024 RQ66_026 RQ62_006 RQ62_001 RQ62_001 RQ62_006 RQ62_001 RQ62_006 RQ62_006 RQ62_006 RQ62_007 RQ62_006 RQ66_001			RQ55_017
RQ65_021 RQ65_028 RQ65_033_1 RQ65_033_1 RQ65_033_1 RQ65_031 RQ65_041 RQ66_016 RQ66_016 RQ66_016 RQ66_017 RQ66_022 RQ66_023 RQ66_023 RQ66_024 RQ66_026 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_001 RQ62_005 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ66_0001 RQ66_0002 RQ65_001 RQ66_00000000000000000000000000000000000			RQ55_018
RQ65_021 RQ65_028 RQ65_033_1 RQ65_033_1 RQ65_033_1 RQ65_031 RQ65_041 RQ66_016 RQ66_016 RQ66_016 RQ66_017 RQ66_022 RQ66_023 RQ66_023 RQ66_024 RQ66_026 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_001 RQ62_005 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ66_0001 RQ66_0002 RQ65_001 RQ66_00000000000000000000000000000000000			
RQ55_028 RQ55_028 RQ55_033 RQ55_033 RQ55_031 RQ55_031 RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ62_007 RQ66_001 RQ65_002 RQ66_003 RQ66_004 RQ65_005 RQ66_007 RQ66_008 RQ65_0000 RQ66_001 RQ66_001 RQ66_001 RQ66_002 RQ66_001			
RQ55_028 RQ55_033 RQ55_033 RQ55_037 RQ55_041 RQ56_015 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_000 RQ65_001 RQ66_005 RQ65_000 RQ65_001 RQ66_005			
RQ55_033 RQ65_037 RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_006 RQ62_006 RQ62_007 RQ62_007 RQ62_008 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ66_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_009 RQ65_009 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ66_0000 RQ66_0000			
RQ55_033_1 RQ55_037 RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RR62_002 RQ62_001 RR62_002 RQ62_001 RQ62_001 RQ62_005 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_001 RQ65_001 RQ66_002 RQ65_001 RQ66_000 RQ66_001 RQ66_002 RQ66_000 RQ66_001 RQ66_002 RQ66_000 RQ66_001 RQ66_001 RQ60_001 RQ60_001			
RQ55_037 RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_001 RQ62_005 RQ62_001 RQ62_006 RQ62_007 RQ62_007 RQ65_008 RQ62_007 RQ65_008 RQ65_008 RQ65_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_000 RQ65_000 RQ60_001 RQG0_001 RQG0_002 RQG0_003 RQG0_004			
RQ55_040 RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ65_008 RQ62_007 RQ65_008 RQ65_008 RQ65_008 RQ65_009 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_001 RQ65_000			
RQ55_041 RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RG62_003 RQ62_004 RQ62_005 RQ62_005 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_006 RQ65_007 RQ65_007 RQ65_008 RQ65_008 RQ65_009 RQ65_001 RQ65_009 RQ65_001 RQ65_000000000000000000000000000000000000			
RQ56_015 RQ56_016 RQ56_017 RQ56_022 RQ56_023 RQ56_023 RQ56_026 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_001 RQ65_0000 RQ65_001 RQ60_001 RQ60_001 RQG0_001 RQG0_002 RQG0_003 RQ60_003			
RQ56_016 RQ65_017 RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RG62_001 RQ62_002 R662_003 RQ62_004 RG62_005 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_002 RQ65_001 RQ60_001 RQ60_002 RQ60_003 RQ60_003			RQ55_041
RQ56_017 RQ66_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 R662_001 RQ62_002 RG62_003 RQ62_004 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_0000 RQ65_001 RQ65_0000 RQ65_001 RQ65_0000 RQ65_001 RQ65_000000 RQ65_000000000000000000000000000000000000			RQ56_015
RQ56_017 RQ66_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 R662_001 RQ62_002 RG62_003 RQ62_004 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_0000 RQ65_001 RQ65_0000 RQ65_001 RQ65_0000 RQ65_001 RQ65_000000 RQ65_000000000000000000000000000000000000			RQ56_016
RQ56_022 RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_008 RQ62_006 RQ62_007 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_021 RQ60_001 RQ60_001 RQ60_002 RQ60_003 RQ60_003 RQ60_003 RQ60_003 RQ60_003 RQ60_003 RQ60_003			
RQ56_023 RQ56_024 RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_007 RQ62_007 RQ62_007 RQ65_002 RQ65_001 RQ65_002 RQ65_007 RQ65_002 RQ65_001 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_009 RQ65_001 RQ60_001 RQ60_001 RQ60_002 RQ60_003 RQ60_003 RQ60_003			
RQ56_024 RQ56_026 RQ56_027 RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_004 RQ65_005 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_001 RQ60_001 RQG0_001 RQG0_001 RQG0_003 RQG0_003			
RQ56_026 RQ56_027 RQ57_039 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_006 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_004 RQ65_005 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_0000 RQ65_001 RQ60_0001 RQG0_0001 RQG0_0001 RQG0_0003 RQG0_0004 RQG0_0005			
RQ56_027 RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ60_001 RQG0_001 RQG0_001 RQG0_002 RQ60_003 RQ60_004 RQG0_005			
RQ57_039 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_0000 RQ65_001 RQ65_000000 RQ65_000000000000000000000000000000000000			
RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_001 RQ65_009 RQ65_001 RQ65_0000 RQ65_000000 RQ65_000000 RQ65_000000000000000000000000000000000000			
RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_009 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ60_001 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			RQ62_002
RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			RQ62_003
RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ62_009 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_007 RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			RQ65_005
RQ65_008 RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_009 RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_020 RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQ65_021 RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQG0_001 RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQG0_002 RQG0_003 RQG0_004 RQG0_005			
RQG0_003 RQG0_004 RQG0_005			
RQG0_004 RQG0_005			
RQG0_005			
RQG0_005			RQG0_004
1.200_500			
	<u> </u>		1 1 1 <u>-</u> 3 - 3

V1.4 Page 304 of 777

4.3.13.2.8 VOID

4.3.13.2.9VOID

4.3.13.2.10 TC_SM-DP+_ES9+.GetBoundProfilePackage_ErrorCasesNIST

General Initial Conditions			
Entity	Description of the general initial condition		
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. The EID is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. There have been no previous attempts to download the pending profile. 		

Test Sequence #01 Error: Invalid eUICC Signature (Subject Code 8.1 Reason Code 6.1)

The purpose of this test is to test that the SM-DP+ returns the correct error code for an invalid eUICC signature supplied in GetBoundProfilePackageRequest.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_UC_NO	D_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_8_1_6_1))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	RQ26_029 RQ26_031 RQ31_143 RQ31_148_2 RQ56_015 RQ56_016 RQ56_017 RQ56_018 RQ56_025 RQ56_026 RQ56_026 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006

V1.4 Page 305 of 777

		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009

Test Sequence #02 Error: Unknown TransactionID in JSON transport layer (Subject Code 8.10.1 Reason Code 3.9)

The purpose of this test is to test that the SM-DP+ returns the correct error code when the TransactionID supplied in GetBoundProfilePackageRequest JSON transport layer is unknown.

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	Confirmation Code is not provided by the Operator to the SM-DP+.	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_UC_N	D_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<invalid_transaction_id>, #PREP_DOWNLOAD_RESP))</invalid_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_ 9)	RQ26_029 RQ26_031 RQ31_143 RQ31_148_2 RQ56_015 RQ56_016 RQ56_017 RQ56_018 RQ56_025 RQ56_026 RQ56_026 RQ56_028 RQ62_001 RQ62_002

Test Sequence #03 Error: Unknown TransactionID in ASN.1 euiccSigned2 element (Subject Code 8.10.1 Reason Code 3.9)

The purpose of this test is to test that the SM DP+ returns the correct error code when the TransactionID supplied in the GetBoundProfilePackageRequest ASN.1 euiccSigned2 element is unknown.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Confirmation Code is not provided by the Operator to the SM-DP+.

V1.4 Page 306 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9	+_CMA_PD_DEF_SMDP_ADDRESS_UC_NC)_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_8_10_1_3_9))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_ 9)	RQ26_029 RQ26_031 RQ31_143 RQ31_148_2 RQ56_015 RQ56_016 RQ56_017 RQ56_018 RQ56_025 RQ56_026 RQ56_026 RQ56_028 RQ62_001 RQ62_002

Test Sequence #04 Error: Missing Confirmation Code (Subject Code 8.2.7 Reason Code 2.2)

The purpose of this test is to test that the SM-DP+ returns the correct error code when the Confirmation Code is missing in the PrepareDownloadResponse request ASN.1 euiccSigned2 element.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Confirmation Code #CONFIRMATION_CODE1 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_CC		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_7_2_2)	RQ26_029 RQ26_031 RQ31_143 RQ31_144 RQ31_146 RQ31_147 RQ31_148_2 RQ56_015 RQ56_016 RQ56_017 RQ56_018 RQ56_025 RQ56_026 RQ56_026 RQ56_028 RQ62_001 RQ62_002

V1.4 Page 307 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #05 Error: Refused Confirmation Code (Subject Code 8.2.7 Reason Code 3.8)

The purpose of this test is to test that the SM-DP+ returns the correct error code when the Confirmation Code supplied in the GetBoundProfilePackageRequest ASN.1 euiccSigned2 element is unknown.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Confirmation Code #CONFIRMATION_CODE2 associated to PROFILE_OPERATIONAL1 is provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_U	C_CC	
IC2	<pre><s_hashed_cc> = MTD_GENERATE_HASHED_CC(#CONFIRMATION_CODE1, <s_transaction_id>)</s_transaction_id></s_hashed_cc></pre>			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_7_3_8)	RQ26_029 RQ26_031 RQ31_143 RQ31_144 RQ31_146 RQ31_147 RQ31_148_2 RQ56_015 RQ56_016 RQ56_017 RQ56_018 RQ56_025 RQ56_026 RQ56_026 RQ56_028 RQ56_028 RQ62_001 RQ62_002

Test Sequence #06 VOID 4.3.13.2.11 VOID

4.3.13.2.12 **VOID**

4.3.14 ES9+ (LPA -- SM-DP+): AuthenticateClient

4.3.14.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

• RQ26_033

V1.4 Page 308 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

- RQ31_025, RQ31_058RQ31_058, RQ31_059, RQ31_060, RQ31_061, RQ31_067,
 RQ31_080, RQ31_081, RQ31_082, RQ31_083, RQ31_085, RQ31_086, RQ31_089,
 RQ31_090, RQ31_091, RQ31_092, RQ31_093, RQ31_094, RQ31_095
- RQ41_001, RQ41_006, RQ41_007, RQ41_008
- RQ42_001
- RQ45_006, RQ45_017, RQ45_026, RQ45_026_1, RQ45_027, RQ45_028, RQ45_029
- RQ47_001
- RQ56_029, RQ56_030, RQ56_031, RQ56_032, RQ56_033, RQ56_034, RQ56_035, RQ56_036, RQ56_036_1, RQ56_037, RQ56_038, RQ56_039, RQ56_040, RQ56_041, RQ56_041_1, RQ56_041_2
- RQ57_037, RQ57_057, RQ57_057_1, RQ57_108
- RQ62_001, RQ62_002, RQ62_004, RQ62_005, RQ62_006, RQ62_007
- RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_007, RQ65_008
 RQ65_009, RQ65_022, RQ65_023

4.3.14.2 Test Cases

4.3.14.2.1TC_SM-DP+_ES9+.AuthenticateClientNIST

General Initial Conditions		
Entity	Description of the general initial condition	
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST and #CERT_SM_DPpb_ECDSA for NIST PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. 	

Test Sequence #01 Nominal for Default SM-DP+ Address Use Case without Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. EID #EID1 is not known to the SM-DP+ and is not associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES	9+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(MTD_HTTP_RESP(#R_INITI ATE_AUTH_OK)	

V1.4 Page 309 of 777

		#S_EUICC_CHALLENGE, #S_EUICC_INFO1,		
		#IUT_SM_DP_ADDRESS))		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_ UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUT H_CLIENT_OK) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPpb_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_025 RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_081 RQ31_092 RQ31_091 RQ31_092 RQ31_094 RQ31_095 RQ41_006 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_029 RQ56_032 RQ56_032 RQ56_034 RQ56_035 RQ56_036 RQ56_036 RQ56_036 RQ56_037 RQ56_039 RQ56_039 RQ56_030 RQ56_040 RQ56_041_1 RQ56_041_2 RQ57_057_1 RQ57_108 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_002 RQ65_0006 RQ65_0007 RQ65_0008 RQ65_0007 RQ65_0008 RQ65_0009

V1.4 Page 310 of 777

GSM Association
Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #02 Nominal for Default SM-DP+ Address Use Case with Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code #CONFIRMATION_CODE1 is provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_II	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITI ATE_AUTH_OK)			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK_CC) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPpb_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_025 RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_082 RQ31_091 RQ31_092 RQ31_093 RQ31_094 RQ31_095 RQ41_006 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_027 RQ45_029 RQ47_001 RQ56_029 RQ56_032 RQ56_034 RQ56_035 RQ56_036 RQ56_036 RQ56_037 RQ56_037 RQ56_039 RQ56_040 RQ56_041_1 RQ56_041_2		

V1.4 Page 311 of 777

		RQ57_037
		RQ57_057_1
		RQ57_108
		RQ62_001
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_022
		RQ65_023
	l .	

Test Sequence #03 Nominal for Default SM-DP+ Use Case Second Attempt without Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	AUTH_CLIENT_FAIL_DEF_DP_USE_	CASE_INVALID_MATCHING_ID)
IC2	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
IC3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_AUTH_CLIENT_OK) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2</s_transaction_id></transaction_id_ac>	RQ31_025 RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_081 RQ31_082 RQ31_091

V1.4 Page 312 of 777

	<smdp_signature2></smdp_signature2>	RQ31_092
	using the	RQ31_093
	#PK_SM_DPpb_ECDSA	RQ31_094
	·	RQ31_095
	Verify that the SM-DP+	RQ41_006
	Address in the	RQ42_001
	#SMDP_METADATA_OP_P	RQ45_006
	ROF1 matches	RQ45_026
	#IUT_SM_DP_ADDRESS.	RQ45_026_1
	Verify that	RQ45_027
	<transaction_id_signe< td=""><td>RQ45_029</td></transaction_id_signe<>	RQ45_029
	D_AC> matches	RQ56_029
	<s_transaction_id></s_transaction_id>	RQ56_032
		RQ56_034
		RQ56_035
		RQ56_036
		RQ56_036_1
		RQ56_037
		RQ56_039
		RQ56_040
		RQ56_041_1
		RQ56_041_2
		RQ57_037
		RQ57_057_1
		RQ57_108
		RQ62_001
		RQ62_001
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_006 RQ62_007
		RQ62_007 RQ62_009
		RQ65_001
		RQ65_001
		RQ65_002
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_007
		RQ65_009
		RQ65_009
		RQ65_023
		.1900_020

Test Sequence #04 VOID VODIVOIDVOIDTest Sequence #05 Nominal for SM-DS Use Case without Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 in the 'Released' state with a MatchingID equal to <matching_id_event>.</matching_id_event> EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+.

V1.4 Page 313 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS_U C_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUT H_CLIENT_OK) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPpb_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_025 RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_081 RQ31_091 RQ31_092 RQ31_093 RQ31_094 RQ31_095 RQ41_006 RQ41_007 RQ41_008 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026_1 RQ45_027 RQ45_029 RQ56_032 RQ56_032 RQ56_032 RQ56_032 RQ56_036 RQ56_036 RQ56_036 RQ56_037 RQ56_037 RQ56_037 RQ56_037 RQ56_037 RQ56_037 RQ56_037 RQ56_030 RQ56_040 RQ56_041_1 RQ56_041_2 RQ57_057_1 RQ57_108 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_0003 RQ65_004 RQ65_0005

V1.4 Page 314 of 777

		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_022
		RQ65_023
		1

Test Sequence #06 Nominal for SM-DS Use Case with Confirmation Code

Initial Conditions	
Entity Description of the initial condition	
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 in the 'Released' state with a MatchingID equal to <matching_id_event>.</matching_id_event> EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code #CONFIRMATION_CODE1 is provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITI ATE_AUTH_OK)		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS_U C_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK_CC) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPpb_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_025 RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_081 RQ31_091 RQ31_092 RQ31_093 RQ31_094 RQ31_095 RQ41_006 RQ41_007 RQ41_008 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026_1 RQ45_027 RQ45_029 RQ45_029 RQ47_001 RQ56_029 RQ56_032 RQ56_034 RQ56_036 RQ56_036_1	

V1.4 Page 315 of 777

		RQ56_037
		RQ56_039
		RQ56_040
		RQ56_041_1
		RQ56_041_2
		RQ57_037
		RQ57_057_1
		RQ57_108
		RQ62_001R
		Q62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_022
		RQ65_023
		11300_020

Test Sequence #07 VOID Test Sequence #08 Nominal for Activation Code Use Case with Matching ID without Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with the MatchingID set as an Activation Code Token with the value #MATCHING_ID_1. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH on E	S9+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>,</s_transaction_id>	MTD_HTTP_RESP(#R_AUT H_CLIENT_OK) • Verify that <transaction_id_ac></transaction_id_ac>	RQ31_025 RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081

V1.4 Page 316 of 777

	#AUTH_SERVER_RESP_ACT_CO	matches	RQ31_082
	DE_UC_OK))	<s_transaction_id></s_transaction_id>	RQ31_002
		<pre><s_ikansaction_id></s_ikansaction_id></pre>	RQ31_091
		V '6 (I P P) 6 (I	RQ31_093
		Verify the validity of the	RQ31_094
		smdpSignature2	RQ31_095
		<smdp_signature2></smdp_signature2>	RQ41 001
		using the	RQ41_006
		#PK_SM_DPpb_ECDSA	RQ41_000
		#1 1C_0M_D1 pb_E0D0/C	RQ41_007 RQ41_008
		Verify that the SM-DP+	RQ41_006 RQ42_001
			RQ45_006
		Address in the	RQ45_006
		#SMDP_METADATA_OP_P	RQ45_026_1
		ROF1 matches	
		#IUT_SM_DP_ADDRESS.	RQ45_027
		_	RQ45_029
		Verify that	RQ56_029
		<transaction_id_signe< td=""><td>RQ56_032</td></transaction_id_signe<>	RQ56_032
		D_AC> matches	RQ56_034 RQ56_035
			RQ56_036
		<s_transaction_id></s_transaction_id>	RQ56_036_1
			RQ56_037
			RQ56_039 RQ56_040
			RQ56_041_1
			RQ56_041_2 RQ57_037
			RQ57_057_1
			RQ57_037_1 RQ57_108
			RQ62_001
			RQ62_002
			RQ62_003
			RQ62_004
			RQ62_005
			RQ62_006
			RQ62 007
			RQ62_009
			RQ65_001
			RQ65_002
			RQ65_003
			RQ65_004
			RQ65_005
			RQ65_007
			RQ65_008
			RQ65_009
			RQ65_022
			RQ65_023

Test Sequence #09 Nominal for Activation Code Use Case with Matching ID with Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with the MatchingID set as an Activation Code Token with the value #MATCHING_ID_1. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code #CONFIRMATION_CODE1 is provided by the Operator to the SM-DP+.

V1.4 Page 317 of 777

Ste p	Directio n	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_COD E_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK_CC) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPpb_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_025 RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_082 RQ31_091 RQ31_092 RQ31_093 RQ31_094 RQ31_095 RQ41_001 RQ41_006 RQ41_007 RQ41_008 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_0261 RQ45_027 RQ45_029 RQ47_001 RQ56_032 RQ56_032 RQ56_034 RQ56_035 RQ56_036 RQ56_036 RQ56_036 RQ56_037 RQ56_039 RQ56_041_1 RQ56_037 RQ56_039 RQ56_041_1 RQ56_041_2 RQ57_037 RQ56_041 RQ56_041_2 RQ57_037 RQ56_041 RQ56_041_1 RQ56_041_2 RQ57_057_1 RQ57_108 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001

V1.4 Page 318 of 777

	RQ65_002
	RQ65_003
	RQ65_004
	RQ65_005
	RQ65_007
	RQ65_008
	RQ65_009
	RQ65_022
	RQ65_023

Test Sequence #10 VOID Test Sequence #11 Nominal for Activation Code Use Case with Matching ID without Confirmation Code not associated to EID

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with the MatchingID set as an Activation Code Token with the value #MATCHING_ID_1. EID #EID1 is not known to the SM-DP+ and is not associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+. 	

This test sequence SHALL be the same as the Test Sequence #08 defined in this section.

Test Sequence #12 Nominal for Activation Code Use Case with Matching ID and Confirmation Code not associated to EID

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with the MatchingID set as an Activation Code Token with the value #MATCHING_ID_1. EID #EID1 is not known to the SM-DP+ and is not associated to PROFILE_OPERATIONAL1. Confirmation Code #CONFIRMATION_CODE1 is provided by the Operator to the SM-DP+.

This test sequence SHALL be the same as the Test Sequence #9 defined in this section.

Test Sequence #13 VOID Void

4.3.14.2.2TC_SM-DP+_ES9+.AuthenticateClientNIST_ErrorCases

General Initial Conditions			
Entity	Description of the general initial condition		
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST and #CERT_SM_DPpb_ECDSA for NIST Confirmation Code is not provided by the Operator to the SM-DP+ for the pending profile. 		

V1.4 Page 319 of 777

Test Sequence #1 Error: Invalid EUM Certificate (Subject Code 8.1.2 Reason Code 6.1)

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_2_6_1_SIG))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002
2	S_LPAd → SM-DP+	Close TLS session (unless SM-DP+ has already closed TLS session)		
3	PROC_TLS_I	NITIALIZATION_SERVER_AUTH on E	S9+	
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
5	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002

V1.4 Page 320 of 777

6	S_LPAd → SM-DP+	Close TLS session (unless SM-DP+ has already closed TLS session)		
7	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
8	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
9	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_2_6_1_EX_CP))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002
10	S_LPAd → SM-DP+	Close TLS session (unless SM-DP+ has already closed TLS session)		
11	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
12	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
13	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002
14	S_LPAd → SM-DP+	Close TLS session (unless SM-DP+ has already closed TLS session)		
15	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
16	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
17	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT,	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ31_061 RQ45_028 RQ56_030

V1.4 Page 321 of 777

MTD_AUTHENTICATE_CLIENT(RQ56_038
<s_transaction_id>,</s_transaction_id>	RQ56_041
#AUTH_SERVER_RESP_DEF_DP	RQ62_001
_UC_8_1_2_6_1_EX_BC_PLC))	RQ62_002

Test Sequence #2 Error: Expired EUM Certificate (Subject Code 8.1.2 Reason Code 6.3)

Initial Conditions	
Entity	Description of the initial state
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_2_6_3))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_3)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002

Test Sequence #3 Error: Invalid eUICC Certificate (Subject Code 8.1.3 Reason Code 6.1)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a

V1.4 Page 322 of 777

Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>
There have been no previous attempts to download the pending profile.
1 31
 EID #EID1 is known to the SM-DP+ and associated to
PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1		I NITIALIZATION_SERVER_AUTH on E	•		
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_3_6_1_SIG))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002	
2	S_LPAd → SM-DP+	Close TLS session (unless SM-DP+ has already closed TLS session)			
3	PROC_TLS_I	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
5	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_3_6_1_EX_KU))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002	
6	S_LPAd → SM-DP+	Close TLS session (unless SM-DP+ has already closed TLS session)			
7	PROC_TLS_I	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
8	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH,	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		

V1.4 Page 323 of 777

		MTD INITIATE ALITHENTICATIO		
		MTD_INITIATE_AUTHENTICATION(
		#S_EUICC_CHALLENGE, #S_EUICC_INFO1,		
		#IUT_SM_DP_ADDRESS))		
		MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS,		RQ31_061 RQ45_028
	S LPAd \rightarrow	#PATH_AUTH_CLIENT,	MTD_HTTP_RESP(RQ56_030
9	SM-DP+	MTD_AUTHENTICATE_CLIENT(<s_transaction_id>,</s_transaction_id>	#R_ERROR_8_1_3_6_1)	RQ56_038 RQ56_041
		#AUTH_SERVER_RESP_DEF_DP _UC_8_1_3_6_1_EX_CP))		RQ62_001 RQ62_002
10	$\begin{array}{c} \text{S_LPAd} \rightarrow \\ \text{SM-DP+} \end{array}$	Close TLS session (unless SM-DP+ has already closed TLS session)		
11	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
		MTD_HTTP_REQ(
		#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH,		
12	$\begin{array}{c} \text{S_LPAd} \rightarrow \\ \text{SM-DP+} \end{array}$	MTD_INITIATE_AUTHENTICATION(MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
		#S_EUICC_CHALLENGE, #S_EUICC_INFO1,		
		#IUT_SM_DP_ADDRESS))		
		MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS,		RQ31_061 RQ45_028
13	$S_LPAd \to$	#PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(RQ56_030 RQ56_038
	SM-DP+	<s_transaction_id>,</s_transaction_id>	#R_ERROR_8_1_3_6_1)	RQ56_041
		#AUTH_SERVER_RESP_DEF_DP _UC_8_1_3_6_1_SUB_ORG))		RQ62_001 RQ62_002
14	S_LPAd → SM-DP+	Close TLS session (unless SM-DP+ has already closed TLS session)		
15	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
		MTD_HTTP_REQ(
		#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH,		
16	$\begin{array}{c} \text{S_LPAd} \rightarrow \\ \text{SM-DP+} \end{array}$	MTD_INITIATE_AUTHENTICATIO	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
		#S_EUICC_CHALLENGE, #S_EUICC_INFO1,		
		#JEDIOG_INTOT; #IUT_SM_DP_ADDRESS))		
		MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS,		RQ31_061 RQ45_028
17	$S_LPAd \to$	#PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(RQ56_030 RQ56_038
''	SM-DP+	<s_transaction_id>,</s_transaction_id>	#R_ERROR_8_1_3_6_1)	RQ56_041
		#AUTH_SERVER_RESP_DEF_DP _UC_8_1_3_6_1_SUB_SN))		RQ62_001 RQ62_002
		I .		

V1.4 Page 324 of 777

GSM Association
Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #4 Error: Expired eUICC Certificate (Subject Code 8.1.3 Reason Code 6.3)

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE OPERATIONAL1. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_3_6_3))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_3)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002

Test Sequence #5 Error: Invalid eUICC Signature (Subject Code 8.1 Reason Code 6.1)

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. 	

V1.4 Page 325 of 777

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_6_1_SIG))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_04 RQ62_001 RQ62_002	

Test Sequence #6 Error: Invalid Server Challenge (Subject Code 8.1 Reason Code 6.1)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH on ES	59+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>,</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	RQ31_061 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002

V1.4 Page 326 of 777

#AUTH_SERVER_RESP_DEF_DP	
_UC_8_1_6_1_CHA))	

Test Sequence #7 Error: Unknown Cl Public Key (Subject Code 8.11.1 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, S_LPAd → SM-DP+ MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_D P_UC_8_11_1_3_9))</s_transaction_id>		MTD_HTTP_RESP(#R_ERROR_8_11_1_3_9)	RQ26_033 RQ31_061 RQ45_028 RQ56_030 RQ56_038 RQ56_041 RQ62_001 RQ62_002

Test Sequence #8 Error: Profile not released (Subject Code 8.2 Reason Code 1.2)

Initial Conditions	
Entity Description of the initial condition	
SM-DP+	Pending Profile PROFILE_OPERATIONAL1 is not in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 iconfigured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>

V1.4 Page 327 of 777

•	There have been no previous attempts to download the pending profile.
•	EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

Step	Direction Sequence / Description		Expected result	REQ	
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_O K)		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC_ OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_1_2)	RQ31_061 RQ31_083 RQ56_033 RQ56_038 RQ56_041 RQ62_001 RQ62_002	

Test Sequence #9 Error: Unknown Transaction ID in JSON transport layer (Subject Code 8.10.1 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	IITIALIZATION_SERVER_AUTH on ES	9+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 328 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<invalid_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_OK))</invalid_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ31_061 RQ56_038 RQ56_041 RQ62_001 RQ62_002
---	--------------------	--	--	--

Test Sequence #10 Error: Unknown Transaction ID in ASN.1 euiccSigned1 payload (Subject Code 8.10.1 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>
	 There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_10_1_3_9))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ31_061 RQ56_038 RQ56_041 RQ62_001 RQ62_002

V1.4 Page 329 of 777

Test Sequence #11 Error: Invalid Matching ID for Profile Download Default DP+ Address Use Case (Subject Code 8.2.6 Reason Code 3.8)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_CO DE_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_6_3_8)	RQ31_061 RQ41_006 RQ41_008 RQ56_033 RQ56_038 RQ56_041 RQ62_001 RQ62_002

Test Sequence #12 Error: Invalid Matching ID for Profile Download Activation Code Use Case (Subject Code 8.2.6 Reason Code 3.8)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_1. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

V1.4 Page 330 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	$\begin{array}{c} \text{S_LPAd} \rightarrow \\ \text{SM-DP+} \end{array}$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	$\begin{array}{c} \text{S_LPAd} \rightarrow \\ \text{SM-DP+} \end{array}$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_6_3_8)	RQ31_061 RQ41_006 RQ41_007 RQ41_008 RQ56_033 RQ56_038 RQ56_041 RQ62_001 RQ62_002
2	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES9+		
3	$\begin{array}{c} \text{S_LPAd} \rightarrow \\ \text{SM-DP+} \end{array}$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
4	$\begin{array}{c} \text{S_LPAd} \rightarrow \\ \text{SM-DP+} \end{array}$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_CODE_2_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_6_3_8)	RQ31_061 RQ41_006 RQ41_007 RQ41_008 RQ56_033 RQ56_038 RQ56_041 RQ62_001 RQ62_002

Test Sequence #13 Error: Invalid Matching ID for Profile Download SM-DS Use Case (Subject Code 8.2.6 Reason Code 3.8)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 in the 'Released' state with a MatchingID equal to <matching_id_event>.</matching_id_event> Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1.

V1.4 Page 331 of 777

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_6_3_8)	RQ31_061 RQ41_006 RQ41_007 RQ41_008 RQ56_033 RQ56_038 RQ56_041 RQ62_001 RQ62_002	
2	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+		
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_CO DE_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_6_3_8)	RQ31_061 RQ41_006 RQ41_007 RQ41_008 RQ56_033 RQ56_038 RQ56_041 RQ62_001 RQ62_002	

Test Sequence #14 Error: Un-matched EID (Subject Code 8.1.1 Reason Code 3.8)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>. There have been no previous attempts to download the pending profile.</ppk_mac></ppk_enc>

V1.4 Page 332 of 777

•	EID #EID1 is known to the SM-DP+ and associated to
	PROFILE_OPERATIONAL1.
•	EID #EID2 is not known to the SM-DP+ and is not associated
	to PROFILE_OPERATIONAL1

Non-confidential

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH on E	S9+	
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_8_1_1_3_8))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_1_3_8)	RQ31_061 RQ56_033 RQ56_038 RQ56_041 RQ62_001 RQ62_002

Test Sequence #15 Error: No Eligible Profile (Subject Code 8.2.5 Reason Code 4.3)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL3 configured with #SMDP_METADATA_OP_PROF3 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Pending Profile PROFILE_OPERATIONAL3 is in the 'Released' state, with an empty MatchingID. There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL3.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+		
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 333 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_U C_8_2_5_4_3))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_5_4_3)	RQ31_061 RQ31_086 RQ31_090 RQ42_001 RQ56_033 RQ56_038 RQ56_041 RQ57_057 RQ62_001 RQ62_002
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL			RQ31_089

Test Sequence #16 Error: Download Order Expired (Subject Code 8.8.5 Reason Code 4.10)

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. The SM-DP+ has expired Profile download order. NOTE: this is expected to be done through proprietary means.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES9+		
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_8_5_4_10)	RQ31_061 RQ56_031 RQ56_038 RQ56_041 RQ62_001 RQ62_002

V1.4 Page 334 of 777

GSM Association
Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #17 Error: Maximum number of retries for Profile download order exceeded (Subject Code 8.8.5 Reason Code 6.4)

Non-confidential

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. Pending Profile PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac li="" tc_sm-dp+_es9+.authenticateclientbrp.<=""> EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. All previous attempts to download the pending Profile have been unsuccessful. The SM-DP+'s maximum number of attempts as defined in #IUT_SM-DP+_MAX_NUMBER_DOWNLOAD_ATTEMPTS for the Profile download order has been reached. </ppk_mac></ppk_enc>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES9+		
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_8_5_6_4)	RQ31_061 RQ31_067 RQ31_085 RQ56_031_1 RQ56_038 RQ56_041 RQ62_001 RQ62_002

Test Sequence #18 VOID

4.3.14.2.3TC_SM-DP+_ES9+.AuthenticateClientFRP

This test case is defined as FFS and not applicable for this version of test specification.

V1.4 Page 335 of 777

4.3.14.2.4VOID

4.3.14.2.5TC_SM-DP+_ES9+.AuthenticateClientBRP

General Initial Conditions			
Entity	Description of the general initial condition		
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for BRP PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There have been no previous attempts to download the pending profile. 		

Test Sequence #01 Nominal for Default SM-DP+ Address Use Case without Confirmation Code

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.3.14.2.1 TC_SM-DP+_ES9+.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.3.14.2.6TC_SM-DP+_ES9+.AuthenticateClient_RetryCases_Reuse_OTPK

Test Sequence #01 Nominal Default SM-DP+ Use Case Retry Attempt without Confirmation Code for reuse of OTPK

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with #MATCHING_ID_EMPTY. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_ES9+_PROF_DOWNLOAD_DEF_DP_USE_CASE_CANCEL_SESSION_PPK				
IC2	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		

V1.4 Page 336 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_RETRY _OK) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPauth_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_082 RQ31_091 RQ31_092 RQ31_093 RQ31_094 RQ31_095 RQ41_006 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_029 RQ56_032 RQ56_032 RQ56_032 RQ56_035 RQ56_036 RQ56_036 RQ56_037 RQ56_039 RQ56_041_1 RQ56_037 RQ56_041_2 RQ57_037 RQ56_041_2 RQ57_057_1 RQ57_108 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_000 RQ62_000 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_000 RQ65_001 RQ65_000
---	--------------------	--	--	--

V1.4 Page 337 of 777

Test Sequence #02 Nominal SM-DS Use Case Retry Attempt without Confirmation Code for reuse of OTPK

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Pending Profile PROFILE_OPERATIONAL1 in the 'Released' state with a MatchingID equal to <matching_id_event>.</matching_id_event> EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_ES9+_PROF_DOWNLOAD_SM_DS_USE_CASE_CANCEL_SESSION				
IC2	PROC_TLS_II	NITIALIZATION_SERVER_AUTH on E	S9+		
IC3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS_U C_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_RETRY _OK) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPauth_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_082 RQ31_091 RQ31_092 RQ31_093 RQ31_094 RQ31_095 RQ41_006 RQ41_007 RQ41_008 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_029 RQ56_032 RQ56_034 RQ56_036 RQ56_036 RQ56_036 RQ56_037 RQ56_039	

V1.4 Page 338 of 777

		RQ56_040
		RQ56_041_1
		RQ56_041_2
		RQ57_037
		RQ57_057_1
		RQ57_108
		RQ62_002
		RQ62_003
		RQ62_004
		RQ62_005
		RQ62_006
		RQ62_007
		RQ62_009
		RQ65_001
		RQ65_002
		RQ65_003
		RQ65_004
		RQ65_005
		RQ65_007
		RQ65_008
		RQ65_009
		RQ65_022
		RQ65_023

Test Sequence #03 Nominal Activation Code Use Case with Matching ID Retry Attempt without Confirmation Code for reuse of OTPK

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with the MatchingID set as an Activation Code Token with the value #MATCHING_ID_1. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROF_DOWNLOAD_ACT_CODE_US	E_CASE_CANCEL_SESSION	
IC2	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on E	S9+	
IC3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 339 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_CO DE_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUT H_CLIENT_RETRY_OK) • Verify that <transaction_id_ac> matches <s_transaction_id> • Verify the validity of the smdpSignature2 <smdp_signature2> using the #PK_SM_DPauth_ECDSA • Verify that the SM-DP+ Address in the #SMDP_METADATA_OP_P ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches <s_transaction_id></s_transaction_id></transaction_id_signe></smdp_signature2></s_transaction_id></transaction_id_ac>	RQ31_058 RQ31_059 RQ31_060 RQ31_080 RQ31_081 RQ31_081 RQ31_091 RQ31_092 RQ31_093 RQ31_094 RQ31_095 RQ41_001 RQ41_006 RQ41_007 RQ41_008 RQ42_001 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_027 RQ45_029 RQ56_032 RQ56_032 RQ56_032 RQ56_034 RQ56_035 RQ56_036 RQ56_036 RQ56_037 RQ56_039 RQ56_037 RQ56_039 RQ56_041_1 RQ56_037 RQ56_039 RQ56_041_1 RQ56_041_2 RQ57_037 RQ57_057_1 RQ57_108 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_007 RQ62_009 PQ65_001
			ROF1 matches #IUT_SM_DP_ADDRESS. • Verify that <transaction_id_signe d_ac=""> matches</transaction_id_signe>	RQ56_041_1 RQ56_041_2 RQ57_037 RQ57_057_1 RQ57_108 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007

V1.4 Page 340 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #04 Nominal Activation Code Use Case with Matching ID for Retry Attempt without Confirmation Code not associated to EID for reuse of OTPK

Initial Conditions		
Entity	Entity Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with the MatchingID set as an Activation Code Token with the value #MATCHING_ID_1. EID #EID1 is not known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+. 	

This test sequence SHALL be the same as the Test Sequence #03 defined in this section.

4.3.15 ES9+ (LPA -- SM-DP+): HandleNotification

4.3.15.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ25_016, RQ25_018, RQ25_023
- RQ25 024, RQ25 025, RQ25 026
- RQ31_171, RQ31_176, RQ31_177, RQ31_177_1, RQ31_178, RQ31_181
- RQ35_017, RQ35_019, RQ35_022
- RQ45_006, RQ45_026, RQ45_026_1
- RQ55 048 1
- RQ56_042, RQ56_042_1, RQ56_042_2
- RQ57 075
- RQ62_001, RQ62_002, RQ62_003, RQ62_004, RQ62_005, RQ62_006, RQ62_007, RQ62_009
- RQ63_005
- RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_006, RQ65_007, RQ65_008, RQ65_009, RQ65_024

4.3.15.2 Test Cases

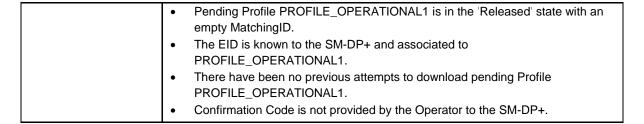
4.3.15.2.1TC_SM-DP+_ES9+_HandleNotificationNIST

General Initial Conditions		
Entity Description of the general initial condition		
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST	

V1.4 Page 341 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification



Test Sequence #01 Nominal: All Notifications

The purpose of this test is to verify that the SM-DP+ acknowledges the incoming ProfileInstallationResult and OtherSignedNotification for all types of Profile notifications.

Initial Conditions			
Entity Description of the initial condition			
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SN	MDP_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_OK1))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ31_171 RQ31_176 RQ31_177 RQ31_177_1 RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026_1 RQ55_048_1 RQ56_042_2 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ57_075 RQ62_001 RQ62_002 RQ62_003 RQ62_001 RQ62_002 RQ62_003 RQ62_007 RQ62_006 RQ62_007 RQ62_009 RQ63_005 RQ65_001 RQ65_002 RQ65_001

V1.4 Page 342 of 777

2		VERIFY_CMA_PD_DEF_SMDP_A		RQ65_004 RQ65_005 RQ65_006 RQ65_007 RQ65_008 RQ65_009 RQ65_024 RQ31_178
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PENDING_NOTIF_OTHER _INST1))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ31_176 RQ31_177 RQ31_177_1 RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026_1 RQ56_042_1 RQ56_042_1 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ57_075 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_005 RQ62_007 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000 RQ65_000
5	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH C	on ES9+	
6	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PENDING_NOTIF_EN1))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ31_176 RQ31_177 RQ31_177_1 RQ31_178

V1.4 Page 343 of 777

	1			
				RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026_1 RQ55_048_1 RQ56_042_1 RQ56_042_2 RQ57_075 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_005 RQ62_009 RQ63_005 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_006 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009
7	PROC TIS IN	I NITIALIZATION_SERVER_AUTH (n FS9+	_
8	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PENDING_NOTIF_DIS1))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ31_176 RQ31_177 RQ31_1771 RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026_1 RQ55_048_1 RQ56_042_1 RQ56_042_1 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ57_075 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009

V1.4 Page 344 of 777

Non-confidential

9	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH o	on ES9+	RQ63_005 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_006 RQ65_007 RQ65_008 RQ65_009 RQ65_024
10	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PENDING_NOTIF_DE1))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ31_171 RQ31_176 RQ31_177 RQ31_177 RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ45_0261 RQ55_048_1 RQ56_042 RQ56_042_1 RQ56_042_2 RQ57_075 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_007 RQ62_009 RQ63_005 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_006 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_009 RQ65_009

Test Sequence #02 Nominal: Successful PIR, no install OtherSignedNotification and then Enable OtherSignedNotification Notifications

The purpose of this test is to verify that the SM-DP+ acknowledges the incoming ProfileInstallationResult and OtherSignedNotification for Profile enable.

V1.4 Page 345 of 777

Initial Conditions			
Entity Description of the initial condition			
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1_EN is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC_EN	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_OK1))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ31_171 RQ31_176 RQ31_177 RQ31_177_1 RQ31_178 RQ31_181 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ45_026_1 RQ55_048_1 RQ56_042_2 RQ56_042_1 RQ56_042_2 RQ57_075 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_007 RQ62_006 RQ62_007 RQ62_009 RQ63_005 RQ65_001 RQ65_002 RQ65_001 RQ65_002 RQ65_007 RQ65_006 RQ65_007 RQ65_006 RQ65_007 RQ65_008 RQ65_008 RQ65_009 RQ65_009
2		VERIFY_CMA_PD_DEF_SMDP_AD		RQ31_178
3	PROC_TLS_II	NITIALIZATION_SERVER_AUTH on	ES9+	ī
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF,	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024

V1.4 Page 346 of 777

#S_PENDING_NOTIF_EN1)) RQ31_176 RQ31_177 RQ31_177 RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ55_048 RQ56_042 RQ56_042 RQ56_042 RQ57_075 RQ62_001 RQ62_002
RQ31_177_ RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ55_048 RQ56_042 RQ56_042 RQ56_042 RQ57_075 RQ62_001 RQ62_002
RQ31_177_ RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ55_048 RQ56_042 RQ56_042 RQ56_042 RQ57_075 RQ62_001 RQ62_002
RQ31_178 RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ55_048 RQ56_042 RQ56_042 RQ56_042 RQ57_075 RQ62_001 RQ62_002
RQ31_181 RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ55_048 RQ56_042 RQ56_042 RQ56_042 RQ56_042 RQ57_075 RQ62_001 RQ62_002
RQ35_017 RQ35_019 RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ45_026 RQ55_048 RQ56_042 RQ56_042 RQ56_042 RQ57_075 RQ62_001 RQ62_002
RQ35_022 RQ45_006 RQ45_026 RQ45_026 RQ55_048_ RQ56_042 RQ56_042_ RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ45_006 RQ45_026 RQ45_026_ RQ55_048_ RQ56_042 RQ56_042_ RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ45_026 RQ45_026 RQ55_048 RQ56_042 RQ56_042 RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ45_026_ RQ55_048_ RQ56_042 RQ56_042_ RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ55_048_ RQ56_042 RQ56_042_ RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ56_042 RQ56_042_ RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ56_042_ RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ56_042_ RQ57_075 RQ62_001 RQ62_002
RQ57_075 RQ62_001 RQ62_002
RQ62_001 RQ62_002
RQ62_002
I DOGO 000
RQ62_003
RQ62_004
RQ62_005
RQ62_006
RQ62_007
RQ62_009
RQ63_005
RQ65_001
RQ65_002
RQ65_003
RQ65_004
RQ65_005
RQ65_006
RQ65_007
RQ65_008
RQ65_009
RQ65_024

Test Sequence #03 Error: Invalid Transaction ID

Initial Conditions			
Entity Description of the initial condition			
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package.		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMDP	_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_INVALID_TRANS_ID))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176

V1.4 Page 347 of 777

				RQ31_177
				RQ31_177_1
				RQ31_178
				RQ35_017
				RQ35_019
				RQ35_022
				RQ56_042
				RQ56_042_1
				RQ56_042_2
				RQ62_001
				RQ62_002
				RQ63_005
				RQ65_006
	DD00 500		4 D D D D D D D D D D D D D D D D D D D	D004 470
2	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMDP	_ADDRESS_UC_NO_CC	RQ31_178

Test Sequence #04 Error: PIR Error Reason - incorrect Input Values

Initial Conditions				
Entity Description of the initial condition				
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>			

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_ES9+_	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC_NO_CC			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_INCORRECT_INP UT_VALUES))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_1771 RQ35_017 RQ35_017 RQ35_019 RQ35_022 RQ56_042 RQ56_042 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006	
2	PROC_ES9+_	VERIFY_CMA_PD_DEF_SMDP_AD	DDRESS_NO_CC_FAIL	RQ31_178	

V1.4 Page 348 of 777

Test Sequence #05 Error: PIR Error Reason – invalid signature

Initial Conditions				
Entity Description of the initial condition				
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> 			

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_INVALID_SIGN))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_177 RQ31_178 RQ35_017 RQ35_019 RQ35_022 RQ56_042_1 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_	VERIFY_CMA_PD_DEF_SMDP_AD	DDRESS_NO_CC_FAIL	RQ31_178

Test Sequence #06 Error: PIR Error Reason – unsupported Crt Values

Initial Conditions			
Entity Description of the initial condition			
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc>		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC_NO_CC			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025

V1.4 Page 349 of 777

	#S_PN_PIR_UNSUPPORTED_C	RQ25_026
	RT))	RQ31_171
		RQ31_176
		RQ31_177
		RQ31_177_1
		RQ31_178
		RQ35_017
		RQ35_019
		RQ35_022
		RQ56_042
		RQ56_042_1
		RQ56_042_2
		RQ62_001
		RQ62_002
		RQ62_009
		RQ63_005
		RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_	FAIL RQ31_178

Test Sequence #07 Error: PIR Error Reason – unsupported Remote Operation Type

Initial Conditions			
Entity	Description of the initial condition		
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> 		

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_ES9+	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC_NO_CC				
1	S_LPAd → SMDP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_UNSUP_REMOTE_ OP_TYPE))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 1 RQ31_178 RQ35_017 RQ35_019 RQ35_022 RQ56_042 RQ56_042 1 RQ56_042_1 RQ56_042_2 RQ56_042_2 RQ56_042_2		

V1.4 Page 350 of 777

		RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL	RQ31_178

Test Sequence #08 Error: PIR Error Reason – unsupported Profile Class

Initial Conditions			
Entity Description of the initial condition			
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_UNSUP_PROFILE_ CLASS))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_177_1 RQ31_178 RQ35_017 RQ35_019 RQ35_022 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL			RQ31_178

Test Sequence #09 Error: PIR Error Reason – SCP03t Structure Error

Initial Conditions			
Entity Description of the initial condition			
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>		

V1.4 Page 351 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_P	ROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_SCP03T_STRUC TURE_ERROR))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_177 RQ35_017 RQ35_017 RQ35_019 RQ35_022 RQ56_042_1 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL			RQ31_178

Test Sequence #10 Error: PIR Error Reason – SCP03t Security Error

Initial Conditions			
Entity Description of the initial condition			
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc>		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_SCP03T_SECURIT Y_ERROR))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_176 RQ31_177 RQ31_177_1 RQ31_178 RQ35_017 RQ35_019 RQ35_019 RQ35_022 RQ56_042 RQ56_042_1 RQ56_042_2

V1.4 Page 352 of 777

		RQ62_001 RQ62_002
		RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL	RQ31_178

Test Sequence #11 Error: PIR Error Reason – install Failed Due To Iccid Already Exists On eUICC

Initial Conditions		
Entity Description of the initial condition		
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_ICCID_ALREADY_ EXISTS))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_1771 RQ31_178 RQ35_017 RQ35_019 RQ35_022 RQ56_042_1 RQ56_042_2 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL RQ31_178			

V1.4 Page 353 of 777

Test Sequence #12 Error: PIR Error Reason – install Failed Due To Insufficient Memory For Profile

Initial Conditions		
Entity Description of the initial condition		
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_INSUFFICIENT_ME MORY))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_1771 RQ35_017 RQ35_017 RQ35_019 RQ35_022 RQ56_042 RQ56_042 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL RQ31_178			

Test Sequence #13 Error: PIR Error Reason – install Failed Due To Interruption

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024

V1.4 Page 354 of 777

		#S_PN_PIR_INSTALL_INTERR		RQ25_025
		UPTION))		RQ25_026
				RQ31_171
				RQ31_176
				RQ31_177
				RQ31_177_1
				RQ31_178
				RQ35_017
				RQ35_019
				RQ35_022
				RQ56_042
				RQ56_042_1
				RQ56_042_2
				RQ62_001
				RQ62_002
				RQ62_009
				RQ63_005
				RQ65_006
2	PROC_ES9+_V	/ERIFY_CMA_PD_DEF_SMDP_AD	DRESS_NO_CC_FAIL	RQ31_178

Test Sequence #14 Error: PIR Error Reason – install Failed Due To PE Processing Error

Initial Conditions		
Entity Description of the initial condition		
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_PE_PROCESSING _ERROR))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_1771 RQ35_017 RQ35_017 RQ35_019 RQ35_022 RQ56_042 RQ56_042 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006

V1.4 Page 355 of 777

Test Sequence #15 Error: PIR Error Reason – install Failed Due To Data Mismatch

Initial Conditions		
Entity Description of the initial condition		
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_DATA_MISMATCH))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_177 RQ35_019 RQ35_017 RQ35_019 RQ35_022 RQ56_042 RQ56_042 RQ56_042_1 RQ56_042_2 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL RQ31_178			

Test Sequence #16 Error: PIR Error Reason – test Profile Install Failed Due To Invalid Naa Key

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	

V1.4 Page 356 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_TEST_PROFILE_IN VALID_NAA_KEY))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_177_1 RQ31_178 RQ35_017 RQ35_019 RQ35_022 RQ56_042_2 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL RQ31_178			RQ31_178

Test Sequence #17 Error: PIR Error Reason – PPR Not Allowed

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_PPR_NOT_ALLOW ED))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_177 RQ31_178 RQ35_017 RQ35_019 RQ35_022 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009

V1.4 Page 357 of 777

		RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL	RQ31_178

Test Sequence #18 Error: PIR Error Reason – install Failed Due To Unknown Error

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac></ppk_mac></ppk_enc>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMD	P_ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#S_PN_PIR_UNKNOWN_ERRO R))	#R_HTTP_204_OK	RQ25_016 RQ25_018 RQ25_023 RQ25_024 RQ25_025 RQ25_026 RQ31_171 RQ31_176 RQ31_177 RQ31_177 RQ35_017 RQ35_019 RQ35_022 RQ56_042_1 RQ56_042_1 RQ56_042_2 RQ62_001 RQ62_002 RQ62_009 RQ63_005 RQ65_006
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL RQ31_178			

4.3.15.2.2TC_SM-DP+_ES9+_HandleNotificationFRP

This test case is defined as FFS and not applicable for this version of test specification.

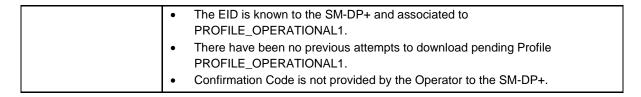
4.3.15.2.3TC_SM-DP+_ES9+_HandleNotificationBRP

General Initial Conditions		
Entity	Description of the general initial condition	
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for BRP Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. 	

V1.4 Page 358 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification



Test Sequence #01 Nominal: All Notifications

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.3.15.2.1 TC_SM-DP+_ES9+_HandleNotificationNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.3.16 ES9+ (LPA -- SM-DP+): CancelSession

4.3.16.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_118, RQ31_119, RQ31_120, RQ31_121, RQ31_122, RQ31_123,
 RQ31_123_1, RQ31_124, RQ31_125, RQ31_126, RQ31_129, RQ31_160
- RQ45_006, RQ45_026, RQ45_026_1
- RQ55 048
- RQ56_043, RQ56_044, RQ56_045, RQ56_046, RQ56_047, RQ56_048, RQ56_049
- RQ57 114 1, RQ57 116
- RQ62_001, RQ62_002, RQ62_003, RQ62_004, RQ62_005, RQ62_006, RQ62_007, RQ62_009
- RQ63_004
- RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_025

4.3.16.2 Test Cases

4.3.16.2.1TC_SM-DP+_ES9+.CancelSession_After_AuthenticateClientNIST

General Initial Conditions		
Entity	Description of the general initial condition	
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. The EID is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. There have been no previous attempts to download the pending profile. 	

V1.4 Page 359 of 777

Test Sequence #01 Nominal: End User Rejection after Authenticate Client

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'End User Rejection' reason after Authenticate Client, and that the RSP session is terminated by the SM-DP+.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	ROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_NO_CC			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_EU_REJ))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_129 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_045 RQ56_046 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_005 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_008 RQ65_007
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL			RQ57_114_1

V1.4 Page 360 of 777

Test Sequence #02 Nominal: End User Postponed after Authenticate Client

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'End User postponed' reason after Authenticate Client, and the SM-DP+ keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions			
Entity	Description of the initial condition		
SM-DP+	 PROFILE_OPERATIONAL1 #SMDP_METADATA_OP_PROF1 is Package using <ppk_enc> and <p< li=""> Confirmation Code is not provided by </p<></ppk_enc>	PK_MAC>.	with rofile

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+	_CMA_PD_DEF_SMDP_ADDRESS_UC	NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_122 RQ31_124 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_045 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_005 RQ65_005 RQ65_005 RQ65_005
2	PROC_ES9+	_VERIFY_PROFILE_DOWNLOAD_DEF	_SMDP_ADDRESS_UC	RQ57_114_1

Test Sequence #03 Nominal: Timeout after Authenticate Client

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'Timeout' reason after Authenticate Client, and the SM-DP+ keeps

V1.4 Page 361 of 777

the RSP session's corresponding Profile download order in the 'Released' state available for

a further retry.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_UC	_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_TIMEOUT))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_122 RQ31_124 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_045 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_0001
2	PROC_ES9+_	VERIFY_PROFILE_DOWNLOAD_DEF	_SMDP_ADDRESS_UC	RQ57_114_1

Test Sequence #04 Nominal: PPR Not Allowed after Authenticate Client

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'PPR Not Allowed' reason after Authenticate Client, and that the RSP session is terminated by the SM-DP+.

V1.4 Page 362 of 777

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 is configured with #SMDP_METADATA_OP_PROF1_PPR2 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1_PPR2 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1		CMA_PD_DEF_SMDP_ADDRESS_UC_ LIENT_OK_PPR2 instead of #R_AUTH_C		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_PPR_NOT_ALLOWE D))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_126 RQ31_129 RQ45_006 RQ45_026 RQ45_026 RQ45_026_1 RQ56_045 RQ56_045 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_005 RQ62_007 RQ62_009 RQ63_004 RQ65_001
2	PROC_ES9+	_VERIFY_CMA_PD_DEF_SMDP_ADDRE	ESS_NO_CC_FAIL	RQ57_114_1

Test Sequence #05 Nominal: Undefined Reason after Authenticate Client

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'Undefined Reason' reason after Authenticate Client, and that the RSP session is terminated by the SM-DP+.

V1.4 Page 363 of 777

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	CMA_PD_DEF_SMDP_ADDRESS_UC_	NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_UNDEFINED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_126 RQ31_129 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_045 RQ56_046 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_007 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009
2	PROC_ES9+_	VERIFY_CMA_PD_DEF_SMDP_ADDRI	ESS_NO_CC_FAIL	RQ57_114_1

Test Sequence #06 Error: Unknown Transaction ID in JSON transport layer (Subject Code 8.10.1, Reason Code 3.9) after Authenticate Client

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using an Invalid Transaction ID after Authenticate Client, that the SM-DP+ returns a function execution status 'Failed' Subject Code 8.10.1, Reason Code 3.9, and keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

V1.4 Page 364 of 777

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_NO_CC		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<invalid_transaction_id>, #CS_RESP_OK_POSTPONED))</invalid_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_001 RQ62_002 RQ65_009
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_001 RQ62_002 RQ63_004 RQ65_009
3	PROC_ES9+	_VERIFY_PROFILE_DOWNLOAD_DEF_	SMDP_ADDRESS_UC	RQ57_114_1

Test Sequence #07 Error: Unknown Transaction ID in ASN.1 CancelSessionResponse Element (Subject Code 8.10.1, Reason Code 3.9) after Authenticate Client

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using an Invalid Transaction ID in the ASN.1 CancelSessionResponse element after Authenticate Client, that the SM-DP+ returns a function execution status 'Failed' with Subject Code 8.10.1, Reason Code 3.9, and keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc>

V1.4 Page 365 of 777

• Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+	_CMA_PD_DEF_SMDP_ADDRESS_UC_	NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_ERROR_8_10_1_3_9))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_002 RQ65_009
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ63_004 RQ65_009
3	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC			RQ57_114_1

Test Sequence #08 Error: Invalid eUICC Signature (Subject Code 8.1 Reason Code 6.1) after Authenticate Client

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using an Invalid Signature after Authenticate Client that the SM-DP+ returns a function execution status 'Failed' with Subject Code 8.1 Reason Code 6.1 and that the RSP session is stopped by the SM-DP+ and keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions		
Entity	escription of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_NO_CC			

V1.4 Page 366 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_ERROR_8_1_6_1))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	RQ31_118 RQ31_119 RQ31_121 RQ31_123 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_002 RQ65_009
2	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC			RQ57_114_1

Test Sequence #09 Error: Invalid OID (Subject Code 8.8 Reason Code 3.10) after Authenticate Client

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using an Invalid OID after Authenticate Client that the SM-DP+ returns a function execution status 'Failed' with Subject Code 8.8 Reason Code 3.10 and that the RSP session is stopped by the SM-DP+ and keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+	_CMA_PD_DEF_SMDP_ADDRESS_UC_	NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_ERROR_8_8_3_10))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_8_3_10)	RQ31_118 RQ31_119 RQ31_121 RQ31_123_1 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_001 RQ62_002 RQ65_009
2	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC		RQ57_114_1	

V1.4 Page 367 of 777

4.3.16.2.2TC_SM-DP+_ES9+.CancelSession_After_GetBoundProfilePackageNIST

General Initial Conditions		
Entity	Description of the general initial condition	
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST	

Test Sequence #01 Nominal: End User Rejection after GetBoundProfilePackage

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'End User Rejection' reason after GetBoundProfilePackage, and that the RSP session is terminated by the SM-DP+.

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMDP_	ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_EU_REJ))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_126 RQ31_129 RQ31_160 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_045 RQ56_046 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_005 RQ65_005

V1.4 Page 368 of 777

				RQ65_008 RQ65_009 RQ65_025
2	PROC_ES9+_	VERIFY_CMA_PD_DEF_SMDP_ADDF	RESS_NO_CC_FAIL	RQ57_114_1

Test Sequence #02 Nominal: End User Postponed after GetBoundProfilePackage

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'End User postponed' reason after GetBoundProfilePackage, and the SM-DP+ keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMDP_A	DDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_124 RQ31_160 RQ45_006 RQ45_026 RQ45_026_1 RQ56_045 RQ56_045 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_000

V1.4 Page 369 of 777

	2	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC	RQ57_114_1	l
--	---	---	------------	---

Test Sequence #03 Nominal: Timeout after GetBoundProfilePackage

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'Timeout' reason after GetBoundProfilePackage , and the SM-DP+ keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC_NO_CC		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_TIMEOUT))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_122 RQ31_124 RQ31_160 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_045 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ65_001 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007 RQ65_008 RQ65_007 RQ65_008 RQ65_009 RQ65_009
2	PROC_ES9+	RQ57_114_1		

V1.4 Page 370 of 777

Test Sequence #04 Nominal: PPR Not Allowed after GetBoundProfilePackage

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'PPR Not Allowed' reason after GetBoundProfilePackage, and that the RSP session is terminated by the SM-DP+.

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 is configured with #SMDP_METADATA_OP_PROF1_PPR2 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1_PPR2 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC_NO_CC using #R_AUTH_CLIENT_OK_PPR2 instead of #R_AUTH_CLIENT_OK			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_PPR_NOT_ALLOWE D))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_126 RQ31_129 RQ31_160 RQ45_006 RQ45_026 RQ45_026 RQ45_026_1 RQ56_045 RQ56_045 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_007
2	PROC_ES9+	_VERIFY_CMA_PD_DEF_SMDP_ADDRE	ESS_NO_CC_FAIL	RQ57_114_1

V1.4 Page 371 of 777

Test Sequence #05 Nominal: Metadata Mismatch after GetBoundProfilePackage

The purpose of this test is to verify that the LPAd can request the cancellation of an on-going RSP session using the 'Metadata Mismatch' reason after GetBoundProfilePackage, and that the RSP session is terminated by the SM-DP+.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMDP_A	DDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_M_DATA_MISMAT CH))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_126 RQ31_129 RQ31_160 RQ45_006 RQ45_026 RQ45_026_1 RQ56_043 RQ56_045 RQ56_046 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_006 RQ62_007 RQ65_001 RQ65_0005
2	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_NO_CC_FAIL			RQ57_114_1

V1.4 Page 372 of 777

Test Sequence #06 Nominal: Load BPP Execution Error after GetBoundProfilePackage

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using that the 'loadBppExecutionError' reason after GetBoundProfilePackage, that the RSP session is terminated by the SM-DP+.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMDP_	ADDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_L_BPP_EXE_ERR OR))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_126 RQ31_129 RQ31_160 RQ45_006 RQ45_026 RQ45_026_1 RQ55_048 RQ56_045 RQ56_047 RQ56_046 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_005 RQ65_005
2	PROC_ES9+_	VERIFY_CMA_PD_DEF_SMDP_ADDF	RESS_NO_CC_FAIL	RQ57_114_1

V1.4 Page 373 of 777

Test Sequence #07 Nominal: Undefined Reason after GetBoundProfilePackage

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using the 'Undefined Reason' reason after GetBoundProfilePackage, and that the RSP session is terminated by the SM-DP+.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC_NO_CC			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_UNDEFINED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_121 RQ31_125 RQ31_126 RQ31_126 RQ31_129 RQ31_160 RQ45_006 RQ45_026 RQ45_026_1 RQ55_048 RQ56_045 RQ56_045 RQ56_047 RQ56_048 RQ57_116 RQ62_001 RQ62_002 RQ62_003 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_009 RQ63_004 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_000 RQ65_0005 RQ65_0000 RQ65_000000000000000000000000000000000000
2	PROC_ES9+_V	ERIFY_CMA_PD_DEF_SMDP_ADDR	ESS_NO_CC_FAIL	RQ57_114_1

V1.4 Page 374 of 777

GSM Association
Official Document SGP.23 - SGP.23 RSP Test Specification

Non-confidential

Test Sequence #08 Error: Unknown Transaction ID in JSON transport layer (Subject Code 8.10.1, Reason Code 3.9) after GetBoundProfilePackage

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using an Invalid Transaction ID after GetBoundProfilePackage that the SM-DP+ returns a function execution status 'Failed' Subject Code 8.10.1, Reason Code 3.9 and keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_ES9+_	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC_NO_CC			
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<invalid_transaction_id>, #CS_RESP_OK_POSTPONED))</invalid_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_001 RQ62_002 RQ65_009	
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ31_160 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_001 RQ62_002 RQ63_004 RQ65_009	
3	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC				

Test Sequence #09 Error: Unknown Transaction ID in ASN.1 CancelSessionResponse Element (Subject Code 8.10.1, Reason Code 3.9) after GetBoundProfilePackage

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using an Invalid Transaction ID in the ASN.1 CancelSessionResponse element

V1.4 Page 375 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

after GetBoundProfilePackage that the SM-DP+ returns a function execution status 'Failed' with Subject Code 8.10.1, Reason Code 3.9 and keeps the RSP session's corresponding Profile download order in the 'Released' state available for a further retry.

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+_	PROFILE_DOWNLOAD_DEF_SMDP_A	DDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_ERROR_8_10_1_3_9))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_002 RQ65_009
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS)	RQ31_118 RQ31_119 RQ31_120 RQ31_121 RQ31_160 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_001 RQ62_002 RQ63_004 RQ65_009
3	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC RQ5			RQ57_114_1

Test Sequence #10 Error: Invalid eUICC Signature (Subject Code 8.1 Reason Code 6.1) after GetBoundProfilePackage

The purpose of this test is to verify that if the LPAd can request the cancellation of an ongoing RSP session using an Invalid Signature after GetBoundProfilePackage using S-ENC and S-MAC. But the SM-DP+ returns a function execution status 'Failed' with Subject Code 8.1 Reason Code 6.1 and that the RSP session is stopped by the SM-DP+ and keeps the RSP session's corresponding Profile download order in the 'Downloaded' state available for a further retry.

V1.4 Page 376 of 777

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+	_PROFILE_DOWNLOAD_DEF_SMDP_AI	DDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_ERROR_8_1_6_1))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	RQ31_118 RQ31_119 RQ31_121 RQ31_123 RQ56_043 RQ56_044 RQ56_047 RQ56_048 RQ56_049 RQ62_001 RQ62_001 RQ62_002 RQ63_004 RQ65_009
2	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC RQ5			RQ57_114_1

Test Sequence #11 Error: Invalid OID (Subject Code 8.8 Reason Code 3.10) after **GetBoundProfilePackage**

The purpose of this test is to verify that if the LPAd requests the cancellation of an on-going RSP session using an Invalid OID after GetBoundProfilePackage that the SM-DP+ returns a function execution status 'Failed' with Subject Code 8.8 Reason Code 3.10 and that the RSP session is stopped by the SM-DP+ and keeps the RSP session's corresponding Profile download order in the 'Downloaded' state available for a further retry..

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	 PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Confirmation Code is not provided by the Operator to the SM-DP+. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_ES9+	_PROFILE_DOWNLOAD_DEF_SMDP_AD	DDRESS_UC_NO_CC	
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(MTD_HTTP_RESP(#R_ERROR_8_8_3_10)	RQ31_118 RQ31_119 RQ31_121 RQ31_123_1 RQ56_043

V1.4 Page 377 of 777

	<s_transaction_id>,</s_transaction_id>	RQ56_044
	#CS_RESP_ERROR_8_8_3_10))	RQ56_047
		RQ56_048
		RQ56_049
		RQ62_001
		RQ62_002
		RQ63_004
		RQ65_009
2	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_ADDRESS_UC	RQ57_114_1

4.3.16.2.3TC_SM-DP+_ES9+.CancelSession_After_AuthenticateClientFRP

This test case is defined as FFS and not applicable for this version of test specification.

4.3.16.2.4TC_SM-DP+_ES9+.CancelSession_After_GetBoundProfilePackageFRP

This test case is defined as FFS and not applicable for this version of test specification.

4.3.16.2.5TC_SM-DP+_ES9+.CancelSession_After_AuthenticateClientBRP

General Initial Conditions		
Entity	Description of the general initial condition	
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for BRP PROFILE_OPERATIONAL1 configured with #SMDP_METADATA_OP_PROF1 Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. The EID is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. There have been no previous attempts to download the pending profile.	

Test Sequence #01 Nominal: End User Rejection after Authenticate Client

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.3.16.2.1 TC_SM-DP+_ES9+.CancelSession_After_AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #02 Nominal: End User Postponed after Authenticate Client

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.3.16.2.1 TC_SM-DP+_ES9+.CancelSession_After_AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.3.16.2.6TC_SM-DP+_ES9+.CancelSession_After_GetBoundProfilePackageBRP

General Initial Conditions		
Entity	Description of the general initial condition	
SM-DP+	SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for BRP	

V1.4 Page 378 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #01 Nominal: End User Rejection after GetBoundProfilePackage

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.3.16.2.2 TC_SM-DP+_ES9+.CancelSession_After_GetBoundProfilePackageNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #02 Nominal: End User Postponed after GetBoundProfilePackage

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.3.16.2.2 TC_SM-DP+_ES9+.CancelSession_After_GetBoundProfilePackageNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.3.17 ES9+ (LPA -- SM-DP+): TLS, Server Authentication, Session Establishment

4.3.17.1 TC_SM-DP+_ES9+_Server_Authentication_for_HTTPS_EstablishmentNIST

Perform all test sequences defined in section 4.6.3.2.1 with the following variables set as follows:

- SERVER = SM-DP+ under test
 - CERT_SERVER_TLS = #CERT_SM_DP_TLS

4.3.17.2 TC_SM-DP+_ES9+_Server_Authentication_for_HTTPS_EstablishmentBRP

Perform all test sequences defined in section 4.6.3.2.2 with the following variables set as follows:

- SERVER = SM-DP+ under test
 - CERT_SERVER_TLS = #CERT_SM_DP_TLS

4.3.18 ES12 (SM-DP+ -- SM-DS): RegisterEvent

This test case is defined as FFS and not applicable for this version of test specification.

4.3.19 ES12 (SM-DP+ -- SM-DS): DeleteEvent

This test case is defined as FFS and not applicable for this version of test specification.

4.3.20 ES12 (SM-DP+ -- SM-DS): TLS, Mutual Authentication, Client, Session Establishment

4.3.20.1 TC_SM-

DP+_ES12_Client_Mutual_Authentication_for_HTTPS_EstablishmentNIST

Perform all test sequences defined in section 4.6.1.2.1 with the following variables set as follows:

- CLIENT = SM-DP+ under test
 - CERT CLIENT TLS = #CERT SM DP TLS for NIST
- SERVER = S_SM-DS

V1.4 Page 379 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

CERT_S_SERVER_TLS = #CERT_S_SM_DS_TLS for NIST

4.3.20.2 TC_SM-

DP+_ES12_Client_Mutual_Authentication_for_HTTPS_EstablishmentBRP

Perform all test sequences defined in section 4.6.1.2.2 with the following variables set as follows:

- CLIENT = SM-DP+ under test
 - O CERT CLIENT TLS = #CERT SM DP TLS for BRP
- SERVER = S_SM-DS
 - CERT_S_SERVER_TLS = #CERT_S_SM_DS_TLS for BRP

4.4 LPAd Interfaces

4.4.1 ES10a (LPA -- eUICC): GetEuiccConfiguredAddresses

This test case is defined as FFS and not applicable for this version of test specification.

4.4.2 ES10a (LPA -- eUICC): SetDefaultDpAddress

This test case is defined as FFS and not applicable for this version of test specification.

4.4.3 ES10b (LPA -- eUICC): PrepareDownload

This test case is defined as FFS and not applicable for this version of test specification.

4.4.4 ES10b (LPA -- eUICC): LoadBoundProfilePackage

This test case is defined as FFS and not applicable for this version of test specification.

4.4.5 ES10b (LPA -- eUICC): GetEUICCChallenge

This test case is defined as FFS and not applicable for this version of test specification.

4.4.6 ES10b (LPA -- eUICC): GetEUICCInfo

This test case is defined as FFS and not applicable for this version of test specification.

4.4.7 ES10b (LPA -- eUICC): ListNotification

This test case is defined as FFS and not applicable for this version of test specification.

4.4.8 ES10b (LPA -- eUICC): RetrieveNotificationsList

This test case is defined as FFS and not applicable for this version of test specification.

4.4.9 ES10b (LPA -- eUICC): RemoveNotificationFromList

This test case is defined as FFS and not applicable for this version of test specification.

4.4.10 ES10b (LPA -- eUICC): LoadCRL

This test case is defined as FFS and not applicable for this version of test specification.

V1.4 Page 380 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

4.4.11 ES10b (LPA -- eUICC): AuthenticateServer

This test case is defined as FFS and not applicable for this version of test specification.

4.4.12 ES10b (LPA -- eUICC): CancelSession

This test case is defined as FFS and not applicable for this version of test specification.

4.4.13 ES10c (LPA -- eUICC): GetProfilesInfo

This test case is defined as FFS and not applicable for this version of test specification.

4.4.14 ES10c (LPA -- eUICC): EnableProfile

This test case is defined as FFS and not applicable for this version of test specification.

4.4.15 ES10c (LPA -- eUICC): DisableProfile

This test case is defined as FFS and not applicable for this version of test specification.

4.4.16 ES10c (LPA -- eUICC): DeleteProfile

This test case is defined as FFS and not applicable for this version of test specification.

4.4.17 ES10c (LPA -- eUICC): eUICCMemoryReset

This test case is defined as FFS and not applicable for this version of test specification.

4.4.18 ES10c (LPA -- eUICC): GetEID

This test case is defined as FFS and not applicable for this version of test specification.

4.4.19 ES10c (LPA -- eUICC): SetNickname

This test case is defined as FFS and not applicable for this version of test specification.

4.4.20 ES10b (LPA -- eUICC): GetRAT

This test case is defined as FFS and not applicable for this version of test specification.

4.4.21 ES9+ (LPA -- SM-DP+): InitiateAuthentication

4.4.21.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ21_001
- RQ31_028, RQ31_033, RQ31_034, RQ31_035, RQ31_036, RQ31_043, RQ31_045, RQ31_052, RQ31_075
- RQ56_004, RQ56_005, RQ56_006, RQ56_007, RQ56_008, RQ56_011, RQ56_012, RQ56_009, RQ56_010
- RQ62_001, RQ62_002, RQ62_004, RQ62_005, RQ62_006, RQ62_007, RQ62_008
- RQ63_001_1, RQ63_004, RQ63_006

V1.4 Page 381 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

 RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_017

4.4.21.2 Test Cases

4.4.21.2.1TC_LPAd_InitiateAuthentication_Nominal

General Initial Conditions	
Entity Description of the general initial condition	
Device	The protection of access to the LUI is disabled
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)
eUICC	There is no default SM-DP+ address configured
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.

Test Sequence #01 Nominal: Initiate Authentication

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
1	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	RQ31_028 RQ31_033 RQ56_004 RQ56_005 RQ56_006 RQ56_007 RQ56_012
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_OK)	No error: Next step of common mutual authentication procedure is performed.	RQ31_043 RQ56_009 RQ56_010 RQ62_001 RQ62_002 RQ62_004 RQ62_005 RQ62_006 RQ62_007 RQ62_008 RQ63_001_1 RQ63_004 RQ63_006 RQ65_001 RQ65_002 RQ65_003 RQ65_004 RQ65_005 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_017

V1.4 Page 382 of 777

4.4.21.2.2TC_LPAd_InitiateAuthentication_ErrorCases

General Initial Conditions		
Entity	Description of the general initial condition	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)	
Device	The protection of access to the LUI is disabled	
eUICC	There is no default SM-DP+ address configured	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	

Test Sequence #01 Error: Invalid SM-DP+ Address

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH on ES9	+	
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_8_1_3_8)	LPAd aborts AddProfile procedure	RQ31_034 RQ56_008 RQ56_011
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE _TIMEOUT in Annex F.	RQ31_034 RQ56_008 RQ56_011

Test Sequence #02 Error: Unsupported Security Configuration

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	NITIALIZATION_SERVER_AUTH on ES9	+	
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_8_2_3_1)	LPAd aborts AddProfile procedure	RQ31_035 RQ56_008 RQ56_011

V1.4 Page 383 of 777

2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE _TIMEOUT in Annex F.	RQ31_035 RQ56_008 RQ56_011
---	--------------------	----------------------------	--	----------------------------------

Test Sequence #03 Error: Unsupported SVN

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+		
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_8_3_3_1)	LPAd aborts AddProfile procedure	RQ56_008, RQ56_011
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ56_008, RQ56_011

Test Sequence #04 Error: Unavailable SM-DP+ Certificate

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on ES	9+	
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_8_4_3_7)	LPAd aborts AddProfile procedure	RQ31_036, RQ56_008, RQ56_011
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_036, RQ56_008, RQ56_011

V1.4 Page 384 of 777

Test Sequence #05 Error: Invalid SM-DP+ Certificate

Ste p	Directio n	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES	9+	
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_INV_CERT)	LPAd aborts AddProfile procedure	RQ31_052
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication or ES9+.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_052

Test Sequence #06 Error: Invalid SM-DP+ Signature

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+		
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_INV_SIGN)	LPAd aborts AddProfile procedure	RQ31_052
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication or ES9+.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_052

Test Sequence #07 Error: Invalid SM-DP+ Address sent by the SM-DP+

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_II	NITIALIZATION_SERVER_AUTH on ES9	+	

V1.4 Page 385 of 777

IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_INV_SMDP+_ADD RESS)	LPAd informs the S_EndUser and aborts the AddProfile procedure	RQ31_045
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication or ES9+.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_045

Test Sequence #08 Error: Unsupported CI Key ID

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_II	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+		
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_INV_CI)	LPAd aborts AddProfile procedure	RQ31_052
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication or ES9+.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_052

Test Sequence #09 Error: Invalid SM-DP+ OID

Initial Conditions	
Entity	Description of the initial condition
LPAd	Add Profile operation is initiated, #ACTIVATION_CODE_2 is provided to the LPAd on request from the S_EndUser
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_2 (PROFILE_OPERATIONAL1)

V1.4 Page 386 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+		
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_INV_OID)	LPAd informs the S_EndUser and aborts the AddProfile procedure	RQ31_075
2	LPAd → S_SM-DP+	No Profile download action	No ES9+.InitiateAuthentication or ES9+.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_075

4.4.22 ES9+ (LPA -- SM-DP+): GetBoundProfilePackage

4.4.22.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_112, RQ31_113, RQ31_141, RQ31_146, RQ31_147, RQ31_148_2
- RQ56_015, RQ56_018, RQ56_022, RQ56_024, RQ56_025, RQ56_026, RQ56_027, RQ56_028
- RQ65_020

4.4.22.2 Test Cases

4.4.22.2.1TC_LPAd_ES9+_GetBoundProfilePackage_Nominal

General Initial Conditions			
Entity Description of the general initial condition			
Device	The protection of access to the LUI is disabled		
eUICC	eUICC There is no default SM-DP+ address configured		

Test Sequence #01 Nominal: Get BPP using S-ENC and S-MAC without Confirmation Code

V1.4 Page 387 of 777

Initial Conditions		
Entity Description of the initial condition		
LPAd Add Profile operation is initiated by using #ACTIVATION_CODE_1.		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_	INIT_AUTH			
IC3	PROC_ES9+_	AUTH_CLIENT			
1	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePacka ge method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transacti on_id="">, #R_PREP_DOWNLOAD_NO_CC)) Verify: • If <s_transaction_id> is the same as in #R_PREP_DOWNLOAD_NO_CC • <euicc_signature2> using the #PK_EUICC_ECDSA</euicc_signature2></s_transaction_id></s_transacti>	RQ31_113 RQ31_141 RQ31_148_ 2 RQ56_024 RQ56_026 RQ65_020	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_B PP_OK)	No error, see Note 1.	RQ56_027	

Test Sequence #02 Nominal: Get BPP using S-ENC and S-MAC with Confirmation Code

Initial Conditions		
Entity Description of the initial condition		
LPAd Add Profile operation is initiated by using #ACTIVATION_CODE_3.		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH or	ES9+	
IC2	PROC_ES9+_INIT_AUTH			

V1.4 Page 388 of 777

IC3	PROC_ES9+_AUTH_CLIENT_CC			
IC4	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_EndUser.	#CONFIRMATION_CODE1 is provided by manual entry.	
1	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transact ion_id="">, #R_PREP_DOWNLOAD_WITH_ CC)) Verify if: •<s_transaction_id> is the same as in #R_PREP_DOWNLOAD_WITH_ CC •<euicc_signature2> using the #PK_EUICC_ECDSA •<s_hashed_cc> = MTD_GENERATE_HASHED_CC (#CONFIRMATION_CODE1, <s_transaction_id>)</s_transaction_id></s_hashed_cc></euicc_signature2></s_transaction_id></s_transact>	RQ31_112 RQ31_113 RQ31_141 RQ31_148_ 2 RQ31_146 RQ31_147 RQ56_015 RQ56_024
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_BPP _OK)	No error, see Note 1.	RQ56_027

Test Sequence #03 Nominal: Get BPP using PPK-ENC and PPK-MAC without Confirmation Code

Initial Conditions		
Entity Description of the initial condition		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_INIT_AUTH			
IC3	PROC_ES9+_AUTH	PROC_ES9+_AUTH_CLIENT		
1	LPAd → S_SM- DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transa ction_id="">, #R_PREP_DOWNLOAD_NO_ CC))</s_transa>	RQ31_113 RQ31_141 RQ31_148_ 2 RQ56_024 RQ56_026 RQ65_020

V1.4 Page 389 of 777

			Verify: • If <s_transaction_id> is the same as in #R_PREP_DOWNLOAD_NO_CC • <euicc_signature2></euicc_signature2></s_transaction_id>	
			using the #PK_EUICC_ECDSA	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_BP P_OK_PPK)	No error, see Note 1.	RQ56_027

Test Sequence #04 Nominal: Get BPP using PPK-ENC and PPK-MAC with Confirmation Code

Initial Conditions		
Entity Description of the initial condition		
LPAd Add Profile operation is initiated by using #ACTIVATION_CODE_3.		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_I	NIT_AUTH		
IC3	PROC_ES9+_A	AUTH_CLIENT_CC		
IC4	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_EndUser.	#CONFIRMATION_CODE1 is provided by manual entry.	
1	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transact ion_id="">, #R_PREP_DOWNLOAD_WITH_CC)) Verify if: • <s_transaction_id> is the same as in #R_PREP_DOWNLOAD_WITH_CC • <euicc_signature2> using the #PK_EUICC_ECDSA • <s_hashed_cc> = MTD_GENERATE_HASHED_CC (#CONFIRMATION_CODE1, <s_transaction_id>)</s_transaction_id></s_hashed_cc></euicc_signature2></s_transaction_id></s_transact>	RQ31_112 RQ31_113 RQ31_141 RQ31_148_2 RQ31_146 RQ31_147 RQ56_015 RQ56_024 RQ56_026

V1.4 Page 390 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

2	S_SM-DP+ \rightarrow LPAd	MTD_HTTP_RESP(#GET_BPP _OK_PPK)	No error, see Note 1.	RQ56_027
---	-----------------------------	------------------------------------	-----------------------	----------

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. Request for Authenticated Confirmation, if not requested before and not aborted.

4.4.22.2.2TC_LPAd_ES9+_GetBoundProfilePackage_Retry

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	
eUICC	There is no default SM-DP+ address configured	

Test Sequence #01 Nominal: Get BPP Retry after incorrect Confirmation Code

Initial Conditions			
Entity Description of the initial condition			
LPAd Add Profile operation is initiated by using #ACTIVATION_CODE_3.			
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL1)		

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+					
IC2	PROC_ES9+_	INIT_AUTH				
IC3	PROC_ES9+_	AUTH_CLIENT_CC				
IC4	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_EndUser.	#CONFIRMATION_CODE2 is provided by manual entry.			
IC5	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transa ction_id="">, #R_PREP_DOWNLOAD_WIT H_CC)) Verify if: <s_hashed_cc> = MTD_GENERATE_HASHED_CC(#CONFIRMATION_CODE 2, <s_transaction_id>)</s_transaction_id></s_hashed_cc></s_transa>			
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8 _2_7_3_8)	Continue to step 2	RQ31_148_ 2 RQ56_022		
2	S_SM-DP+ closes TLS session (unless ,LPAd has already closed TLS session)					
3	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+					

V1.4 Page 391 of 777

4	PROC_ES9+_INIT_AUTH				
5	PROC_ES9+_AUTH_CLIENT_CC				
6	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_EndUser.	#CONFIRMATION_CODE1 is provided by manual entry.	RQ31_148_ 3 RQ56_022	
7	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transa ction_id="">, #R_PREP_DOWNLOAD_WIT H_CC)) Verify if: • If <s_transaction_id> is the same as in #R_PREP_DOWNLOAD_WIT H_CC • <euicc_signature2> using the #PK_EUICC_ECDSA • <s_hashed_cc> = MTD_GENERATE_HASHED_ CC(#CONFIRMATION_CODE</s_hashed_cc></euicc_signature2></s_transaction_id></s_transa>	RQ31_148_ 3 RQ56_022 RQ56_026	
			1, <s_transaction_id>)</s_transaction_id>		
8	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_BPP_O K)	No error, see Note 1.	RQ56_024 RQ56_027	

4.4.22.2.3TC_LPAd_ES9+_GetBoundProfilePackage_Error

General Initial Condit	General Initial Conditions			
Entity	Description of the general initial condition			
Device	The protection of access to the LUI is disabled			
eUICC	There is no default SM-DP+ address configured			
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)			
LPAd Add Profile operation is initiated by using #ACTIVATION_CODE_1.				

Test Sequence #01 Error: Wrong eUICC Signature

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_INIT_AUTH				
IC3	PROC_ES9+	_AUTH_CLIENT			

V1.4 Page 392 of 777

IC4	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #R_PREP_DOWNLOAD_NO_CC))</s_transaction_id>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	LPAd aborts AddProfile procedure Note: the LPAd MAY retry by restarting the Profile download and installation procedure.	RQ56_018 RQ56_025 RQ56_028

Test Sequence #02 Error: BPP Not Available

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+	_INIT_AUTH		
IC3	PROC_ES9+_AUTH_CLIENT			
IC4	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #R_PREP_DOWNLOAD_NO_CC))</s_transaction_id>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_2_3_7)	LPAd aborts AddProfile procedure Note: the LPAd MAY retry by restarting the Profile download and installation procedure.	RQ56_028

Test Sequence #03 Error: Unknown TransactionID received by SM-DP+

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES	59+	
IC2	PROC_ES9+	_INIT_AUTH		
IC3	PROC_ES9+	_AUTH_CLIENT		
IC4	LPAd → S_SM-DP+	Send ES9+.GetBundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #R_PREP_DOWNLOAD_NO_CC))</s_transaction_id>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	LPAd aborts AddProfile procedure Note: the LPAd MAY retry by restarting the Profile download and installation procedure.	RQ56_018 RQ56_025 RQ56_028

Test Sequence #04 Error: Missing Confirmation Code

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES	9+	

V1.4 Page 393 of 777

IC2	PROC_ES9+_INIT_AUTH				
IC3	PROC_ES9+	AUTH_CLIENT			
IC4	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #R_PREP_DOWNLOAD_NO_CC))</s_transaction_id>		
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_2_7_2_2)	LPAd aborts AddProfile procedure Note: the LPAd MAY retry by restarting the Profile download and installation procedure.	RQ56_018 RQ56_025 RQ56_028	

Test Sequence #05 Error: Download Order Expired

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH on E	S9+	
IC2	PROC_ES9+	_INIT_AUTH		
IC3	PROC_ES9+	_AUTH_CLIENT		
IC4	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #R_PREP_DOWNLOAD_NO_CC))</s_transaction_id>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_8_5_4_10)	LPAd aborts AddProfile procedure Note: the LPAd MAY retry by restarting the Profile download and installation procedure.	RQ56_018 RQ56_025 RQ56_028

Test Sequence #06 Error: Wrong Confirmation Code

Initial Conditions		
Entity Description of the initial condition		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_3.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_INIT_AUTH			
IC3	PROC_ES9+_AUTH_CLIENT_CC			
IC4	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_EndUser.	#CONFIRMATION_CODE2 is provided by manual entry.	

V1.4 Page 394 of 777

IC5	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #R_PREP_DOWNLOAD_WITH_CC))</s_transaction_id>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_2_7_3_8)	LPAd aborts AddProfile procedure Note: the LPAd MAY retry by restarting the Profile download and installation procedure	RQ56_018 RQ56_025 RQ56_028

Test Sequence #07 Error: Maximum number of Confirmation Code retries exceeded

Initial Conditions		
Entity	Description of the initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_3.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+	PROC_ES9+_INIT_AUTH			
IC3	PROC_ES9+_AUTH_CLIENT_CC				
IC4	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_EndUser.	#CONFIRMATION_CODE2 is provided by manual entry.		
IC5	$\begin{array}{c} LPAd \to \\ S_SM\text{-DP\text{+}} \end{array}$	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #R_PREP_DOWNLOAD_WITH_CC))</s_transaction_id>		
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_2_7_6_4)	LPAd aborts AddProfile procedure The LPAd SHALL NOT retry by restarting the Profile download and installation procedure.	RQ56_018 RQ56_025 RQ56_028 RQ31_148_2	

4.4.23 ES9+ (LPA -- SM-DP+): AuthenticateClient

4.4.23.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

• RQ21_001, RQ21_002

V1.4 Page 395 of 777

- RQ31_032, RQ31_033, RQ31_043, RQ31_046, RQ31_055, RQ31_056, RQ31_057, RQ31_060, RQ31_061, RQ31_073, RQ31_076, RQ31_083, RQ31_085, RQ31_090, RQ31_091, RQ31_095, RQ31_136
- RQ42_001, RQ42_002, RQ42_003, RQ42_004, RQ42_005, RQ42_006, RQ42_007, RQ42_008, RQ42_009, RQ42_010, RQ42_011, RQ42_012, RQ42_013, RQ42_014, RQ42_015, RQ42_016, RQ42_017, RQ42_018, RQ42_019, RQ42_020, RQ43_001
- RQ56_001, RQ56_004, RQ56_005, RQ56_009, RQ56_010, RQ56_029, RQ56_030, RQ56_031_1, RQ56_033, RQ56_037, RQ56_038, RQ56_039, RQ56_040, RQ56_041, RQ56_041_1, RQ56_041_2
- RQ57_031
- RQ62 001, RQ62 002, RQ62 004, RQ62 005, RQ62 006, RQ62 007, RQ62 008
- RQ63_001_1, RQ63_004, RQ63_006
- RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_019, RQ65_022

4.4.23.2 Test Cases

4.4.23.2.1TC_LPAd_AuthenticateClient_Nominal

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	
eUICC	There is no default SM-DP+ address configured	

Test Sequence #01 Nominal: Authenticate Client without Confirmation Code

Initial Conditions		
Entity	Entity Description of the initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICAT ION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	

V1.4 Page 396 of 777

	I			
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_OK)	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT (<s_transaction_id>, #R_AUTH_SERVER_MATCH_I D_DEV_INFO)) Verify: • if #R_AUTH_SERVER_MATCH_I D_DEV_INFO used with the #MATCHING_ID_1 • If <s_transaction_id> is the same as in #INITIATE_AUTH_OK • <euicc_signature1> using the #PK_EUICC_ECDSA • if <s_smdp_challenge> present in the #R_AUTH_SERVER_MATCH_I D_DEV_INFO is the same as in <s_smdp_signed1> present in #INITIATE_AUTH_OK • for #DEVICE_INFO: - TAC is BCD coded as 4 octets acc. to 3GPP_TS 23.003 - if IMEI is present then it is BCD coded as 8 octets acc. to 3GPP TS 23.003 - if O_D_GSM_GERAN then gsmSupportedRelease is set to the highest release as defined in #IUT_GSM_GERAN_REL if O_D_UMTS_UTRAN then utranSupportedRelease is set to the highest release as defined in #IUT_UMTS_UTRAN_REL.</s_smdp_signed1></s_smdp_challenge></euicc_signature1></s_transaction_id></s_transaction_id>	RQ21_001 RQ21_002 RQ31_043 RQ31_046 RQ31_055 RQ31_056 RQ31_057 RQ31_060 RQ31_076 RQ42_001 RQ42_002 RQ42_003 RQ42_004 RQ42_005 RQ42_006 RQ42_007 RQ42_008 RQ42_009 RQ42_010 RQ42_011 RQ42_011 RQ42_011 RQ42_012 RQ42_013, RQ42_014, RQ42_014, RQ42_015, RQ42_015, RQ42_016, RQ42_017, RQ42_018, RQ42_019, RQ42_019, RQ42_019, RQ42_010 RQ42_010 RQ42_010 RQ42_010 RQ42_010 RQ42_010, RQ42_010 RQ42_010, RQ42_010 RQ42_010, RQ56_009 RQ56_009 RQ56_001, RQ62_001, RQ62_002,
			_	
			if <s_smdp_challenge></s_smdp_challenge>	
				RQ42_010
			=	
			-	
			=	
1	_	·		
	→ LPAd	AUTH_OK)		
			· · · · · · · · · · · · · · · · · · ·	
				RQ56_010
			•	
			- if O_D_CDMA2000_1X then	RQ62_002,
			cdma2000onexSupportedReleas	RQ62_005,
			e is set to the highest release as	RQ62_006,
			defined in	RQ62_007,
			#IUT_CDMA2000_1X_REL.	RQ62_008,
			if O_D_CDMA2000_HRPD then	RQ63_001_1 RQ63_004,
			cdma2000hrpdSupportedReleas	RQ63_004, RQ63_006,
			e is set to the highest release as	RQ65_001,
			defined in	RQ65_002,
			#IUT_CDMA2000_HRPD_REL.	RQ65_003,
			The value R is either 1, 2 or 3 for Rev 0, A or B respectively.	RQ65_004,
			- if O_D_CDMA2000_EHRPD	RQ65_005, RQ65_007,
			then	RQ65_008,
			cdma2000ehrpdSupportedRelea	RQ65_009
			se is set to the highest release	RQ65_019
			as defined in #IUT_CDMA2000_EHRPD_REL	RQ65_022
			#IO1_ODIVIAZUUU_ERKFU_REL	
			– if O_D_LTE then	
	<u></u>		eutranSupportedRelease is set	
B				

V1.4 Page 397 of 777

			to the highest release as defined in #IUT_LTE_EUTRAN_REL. — if O_D_NFC_TS26 then contactlessSupportedRelease is set to the highest release as defined in #IUT_NFC_REL. — if O_D_CRL then rspCrlSupportedVersion is set to the highest release as defined in #IUT_RSP_VERSION . For each of the options O_D_GSM_GERAN, O_D_UMTS_UTRAN, O_D_CDMA2000_1X, O_D_CDMA2000_HRPD, O_D_CDMA2000_EHRPD, O_D_LTE, O_D_NFC_TS26 or O_D_CRL, if the option is not set, verify that the corresponding field in DeviceCapabilities is not present.	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_OK)	No Error	RQ31_073 RQ31_095 RQ56_037 RQ56_040 RQ56_041_1 RQ56_041_2

Test Sequence #02 Nominal: Authenticate Client with Confirmation Code

Initial Conditions				
Entity	Description of the initial condition			
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_3.			
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL1)			

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH o	n ES9+	
IC2	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICAT ION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_ AUTH_OK)	MTD_HTTP_REQ(#TEST_DP_ADDRESS1,	RQ21_001 RQ21_002

V1.4 Page 398 of 777

		#PATH_AUTH_CLIENT,	RQ31_043
		MTD_AUTHENTICATE_CLIENT	RQ31_043 RQ31_046
		(<s_transaction_id>,</s_transaction_id>	· -
			RQ31_055
		#R_AUTH_SERVER_MATCH_I	RQ31_056
		D_DEV_INFO))	RQ31_057
			RQ31_060
		\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	RQ31_076
		Verify:	RQ42_001
		• if	RQ42_002
		#R_AUTH_SERVER_MATCH_I	RQ42_003
		D_DEV_INFO used with the	RQ42_004
		#MATCHING_ID_3	RQ42_005
		• If <s id="" transaction=""> is</s>	RQ42_006
		the same as in	RQ42_007
			RQ42_008
		#INITIATE_AUTH_OK	RQ42_009
		• <euicc_signature1> using</euicc_signature1>	RQ42_010
		the #PK_EUICC_ECDSA	RQ42_011
		• if <s challenge="" smdp=""></s>	RQ42_012
		present in the	RQ42_013
		#R_AUTH_SERVER_MATCH_I	RQ42_014
		D_DEV_INFO is the same as in	RQ42_015
		<s_smdp_signed1> present</s_smdp_signed1>	RQ42_016
		in #INITIATE_AUTH_OK	RQ42_017
			RQ42_018
		• for #DEVICE_INFO:	RQ42_019
		- TAC is BCD coded as 4 octets	RQ42_020
		acc. to 3GPP TS 23.003	RQ43_001
		- if IMEI is present then it is	RQ56_009
		BCD coded as 8 octets acc. to	RQ56_010
		3GPP TS 23.003	RQ56_029
			RQ56_039
		- if O_D_GSM_GERAN then	RQ62_001
		gsmSupportedRelease is set to	RQ62_002
		the highest release as defined in	RQ62_004
		#IUT_GSM_GERAN_REL.	RQ62_005
		- if O_D_UMTS_UTRAN then	RQ62_006
		utranSupportedRelease is set to	RQ62_007
		the highest release as defined in	RQ62_008
		#IUT_UMTS_UTRAN_REL.	RQ63_001_1 RQ63_004
		- if O_D_CDMA2000_1X then	RQ63_004 RQ63_006
		cdma2000onexSupportedReleas	RQ65_000
		e is set to the highest release as	RQ65_001 RQ65_002
		defined in	RQ65_002 RQ65_003
		#IUT_CDMA2000_1X_REL.	RQ65_003 RQ65_004
		- if O_D_CDMA2000_HRPD	RQ65_005
		then	RQ65_005
		cdma2000hrpdSupportedReleas	RQ65_007 RQ65_008
		e is set to the highest release as	RQ65_008 RQ65_022
		defined in	11000_022
		#IUT_CDMA2000_HRPD_REL.	
		The value R is either 1, 2 or 3 for	
		Rev 0, A or B respectively.	
		· · ·	
		- if O_D_CDMA2000_EHRPD	
		then	
		cdma2000ehrpdSupportedRelea	
		se is set to the highest release	
		as defined in	
		#IUT_CDMA2000_EHRPD_REL	
<u> </u>	1	1	l .

V1.4 Page 399 of 777

			- if O_D_LTE then eutranSupportedRelease is set to the highest release as defined in #IUT_LTE_EUTRAN_REL. - if O_D_NFC_TS26 then contactlessSupportedRelease is set to the highest release as defined in #IUT_NFC_REL.	
			- if O_D_CRL then rspCrlSupportedVersion is set to the highest release as defined in #IUT_RSP_VERSION.	
			For each of the options O_D_GSM_GERAN, O_D_UMTS_UTRAN, O_D_CDMA2000_1X, O_D_CDMA2000_HRPD, O_D_CDMA2000_EHRPD, O_D_LTE, O_D_NFC_TS26 or O_D_CRL, if the option is not set, verify that the corresponding field in DeviceCapabilities is not present.	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_OK_CC)	No Error	RQ31_073 RQ31_095 RQ56_037 RQ56_040 RQ56_041_1 RQ56_041_2

Test Sequence #03 Nominal: Authenticate Client with Confirmation Code Retry

Initial Conditions			
Entity Description of the initial condition			
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_3.		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL1)		

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+	_INIT_AUTH				
IC3	PROC_ES9+_AUTH_CLIENT_CC					
IC4	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_EndUser.	#CONFIRMATION_CODE2 is provided by manual entry.			
IC5	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePack age method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transactio n_id="">,</s_transactio>			

V1.4 Page 400 of 777

			#R_PREP_DOWNLOAD_WITH_CC)) Verify if: <s_hashed_cc> = MTD_GENERATE_HASHED_CC(# CONFIRMATION_CODE2, <s_transaction_id>)</s_transaction_id></s_hashed_cc>		
IC6	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ER ROR_8_2_7_3_8)			
IC7	Restart Add Profile procedure if O_D_CC_RETRY not supported				
IC8	PROC_TLS_I	NITIALIZATION_SERVER_AUT	TH on ES9+		
IC9	PROC_ES9+	_INIT_AUTH			
IC10	S_SM-DP+ → LPAd	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(< S_TRANSACTION_ID>, #R_AUTH_SERVER_MATCH_ID_ DEV_INFO))		
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_OK_CC)	No Error	RQ31_091	

4.4.23.2.2TC_LPAd_AuthenticateClient_ErrorCases

General Initial Conditions			
Entity Description of the general initial condition			
S_SM-DP+	There is a pending Profile download order for MATCHING_ID_1 (PROFILE_OPERATIONAL1)		
eUICC	There is no default SM-DP+ address configured		
Device	The protection of access to the LUI is disabled		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.		

Test Sequence #01 Error: Invalid EUM Certificate

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+					
IC2	PROC_ES9+_IN	PROC_ES9+_INIT_AUTH				
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>			

V1.4 Page 401 of 777

2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	LPAd aborts AddProfile procedure	RQ31_061 RQ56_030 RQ56_038
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041

Test Sequence #02 Error: Expired EUM Certificate

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_	INIT_AUTH				
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>			
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_3)	LPAd aborts AddProfile procedure	RQ31_061 RQ56_030		
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041		

Test Sequence #03 Error: Invalid eUICC Certificate

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_INIT	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_IN	IIT_AUTH				
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>			
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	LPAd aborts AddProfile procedure	RQ31_061 RQ56_030		
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041		

V1.4 Page 402 of 777

Test Sequence #04 Error: Expired eUICC Certificate

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_	INIT_AUTH				
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>			
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_3)	LPAd aborts AddProfile procedure	RQ31_061 RQ56_030		
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041		

Test Sequence #05 Error: Invalid eUICC Signature or serverChallenge

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_	INIT_AUTH			
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>		
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	LPAd aborts AddProfile procedure	RQ31_061 RQ56_030	
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041	

Test Sequence #06 Error: Insufficient Memory

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_INIT_AUTH			
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT,	

V1.4 Page 403 of 777

			MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_4_8)	LPAd aborts AddProfile procedure	RQ56_030
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041

Test Sequence #07 Error: Unknown CI Root Key

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_	INIT_AUTH				
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>			
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_11_1_3_9)	LPAd aborts AddProfile procedure	RQ56_030		
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041		

Test Sequence #08 Error: Profile not Allowed (Not in 'released' State)

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_	INIT_AUTH				
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>			
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_2_1_2)	LPAd aborts AddProfile procedure	RQ31_083 RQ56_030		
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_033 RQ56_041		

V1.4 Page 404 of 777

Test Sequence #09 Error: Unknown TransactionID

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_	INIT_AUTH				
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>			
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	LPAd aborts AddProfile procedure	RQ56_030		
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041		

Test Sequence #10 Error: Refused MatchingID

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_2_6_3_8)	LPAd aborts AddProfile procedure	RQ31_083 RQ31_090 RQ56_030
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_033 RQ56_041

Test Sequence #11 Error: Refused EID

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_INIT_AUTH			
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT,	

V1.4 Page 405 of 777

			MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_1_1_3_8)	LPAd aborts AddProfile procedure	RQ31_083 RQ56_030
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041

Test Sequence #12 Error: No Eligible Profile for this eUICC/Device

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_2_5_4_3)	LPAd aborts AddProfile procedure	RQ31_090 RQ31_083 RQ56_030
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_041

Test Sequence #13 Error: Expired Download Order

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _transaction_id="">, #R_AUTH_SERVER_MATCH_ID_D EV_INFO))</s>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_8_5_4_10)	LPAd aborts AddProfile procedure	RQ31_090 RQ56_030 RQ56_031

V1.4 Page 406 of 777

3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT in Annex F.	RQ56_030 RQ56_033 RQ56_041
---	--------------------	----------------------------	--	----------------------------------

Test Sequence #14 Error: Maximum Number of Retries Exceeded

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(< S_TRANSACTION_ID>, #R_AUTH_SERVER_MATCH_ID_ DEV_INFO))	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_8_5_6_4)	LPAd aborts AddProfile procedure	RQ31_085 RQ56_030 RQ56_031_1
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_T IMEOUT in Annex F.	RQ56_030 RQ56_041

Test Sequence #15 Error: Invalid SM-DP+(pb) certificate

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #R_AUTH_SERVER_MATCH_ID _DEV_INFO))</s_transaction_id>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#AUTH_CLIENT_INV_PB_CE RT)	LPAd aborts AddProfile procedure (See Note)	RQ31_136 RQ57_031
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_T IMEOUT in Annex F.	RQ31_136 RQ57_031

V1.4 Page 407 of 777

Note: Before the AddProfile procedure is aborted, the LPAd may request for Authenticated Confirmation from the S_EndUser. In this case the S_EndUser SHALL give the Authenticated confirmation.

Test Sequence #16 Error: Different OID for SM-DP+ Certificates (CERT.DPpb.ECDSA and CERT.DPauth.ECDSA not belonging to the same entity)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH or	ES9+	
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	AuthenticateClient	MTD_HTTP_REQ(#TEST_DP_AD DRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(< S_TRANSACTION_ID>, #R_AUTH_SERVER_MATCH_ID _DEV_INFO))	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#AUTH_CLI ENT_INV_CI)	LPAd aborts AddProfile procedure (See Note)	RQ31_136 RQ57_031
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_T IMEOUT in Annex F.	RQ31_136 RQ57_031

Note: Before the AddProfile procedure is aborted, the LPAd may request for Authenticated Confirmation from the S_EndUser. In this case the S_EndUser SHALL give the Authenticated confirmation.

Test Sequence #17 Error: Invalid SM-DP+ signature (smdpSignature2)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(< S_TRANSACTION_ID>, #R_AUTH_SERVER_MATCH_ID _DEV_INFO))	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#AUTH_CLIENT_INV_SIGN)	LPAd aborts AddProfile procedure (See Note)	RQ31_136 RQ57_031

V1.4 Page 408 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_T IMEOUT in Annex F.	RQ31_136 RQ57_031
---	--------------------	----------------------------	--	----------------------

Note: Before the AddProfile procedure is aborted, the LPAd may request for Authenticated Confirmation from the S_EndUser. In this case the S_EndUser SHALL give the Authenticated confirmation.

Test Sequence #18 Error: Invalid TransactionID sent by SM-DP+

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+_	INIT_AUTH		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient Method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(< S_TRANSACTION_ID>, #R_AUTH_SERVER_MATCH_ID _DEV_INFO))	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#AUTH_CLIENT_INV_TRANS ACTION_ID)	LPAd aborts AddProfile procedure (See Note)	RQ31_136 RQ57_031
3	LPAd → S_SM-DP+	No Profile download action	No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_T IMEOUT in Annex F.	RQ31_136 RQ57_031

Note: Before the AddProfile procedure is aborted, the LPAd may request for Authenticated Confirmation from the S_EndUser. In this case the S_EndUser SHALL give the Authenticated confirmation.

4.4.24 ES9+ (LPA – SM-DP+): HandleNotification

4.4.24.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_171, RQ31_173, RQ31_176, RQ32_001
- RQ35_008, RQ35_012, RQ35_013, RQ35_014, RQ35_014_3, RQ35_017, RQ35_018, RQ35_022
- RQ56_042, RQ62_003, RQ62_009, RQ63_005, RQ65_024, RQC3_003

V1.4 Page 409 of 777

4.4.24.2 Test Cases

4.4.24.2.1TC_LPAd_ES9+_HandleNotification_Nominal

Throughout all the test cases the maximum number of Notifications simultaneously tested has been set as to two as there is not minimum defined in SGP.21 [3] or SGP.22 [2] for the number of Notifications that can be stored by the eUICC.

General Initial Conditions			
Entity	Description of the general initial condition		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)		
S_SM-DP+	S_SM-DP+(1) is configured with #TEST_DP_ADDRESS1 and #CERT_S_SM_DP_TLS S_SM-DP+(2) is configured with #TEST_DP_ADDRESS2 and #CERT_S_SM_DP2_TLS		
Device	The protection of access to the LUI is disabled		
eUICC	There is no default SM-DP+ address configured		

Test Sequence #01 Nominal: Successful PIR and Install Notifications to the Same SM-DP+ Address

Initial Conditions		
Entity	Description of the initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1 for PROFILE_OPERATIONAL1	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	ITIALIZATION_SERVER_AUTH on ES9	+	
IC2	PROC_ES9+_II	NIT_AUTH		
IC3	PROC_ES9+_A	AUTH_CLIENT		
IC4	PROC_ES9+_GET_BPP (s. Note 1)			
1	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ32_001
2	LPAd → S_SM-DP+(1)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_PIR _OK)) • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ31_171 RQ31_176 RQ35_008 RQ35_013 RQ35_017 RQ35_018 RQ62_003

V1.4 Page 410 of 777

			Т	D005 00:
				RQ65_024
				RQC3_003
3	S_SM-DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd. The LPAd MAY inform the End User of the success status indicated by the Profile Installation Result.	RQ35_008 RQ35_014 RQ35_017 RQ56_042 RQ62_003 RQ62_009 RQ63_005
4	$\begin{array}{c} LPAd \to \\ S_SM\text{-DP\text{+}(1)} \end{array}$	Establish an HTTPs connection if prev	iously closed	
5	LPAd → S_SM-DP+(1)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#PENDING_NOTIF_INST1)) sent within the timeout #IUT_LPAd_NOTIFICATION_TI MEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ35_008 RQ35_013 RQ35_014 RQ35_022 RQ35_018 RQ62_003 RQ65_024 RQC3_003
6	S_SM-DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd	RQ35_008 RQ35_022 RQ56_042 RQ62_003 RQ62_009 RQ63_005

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the session.

Note 2: the timeout SHALL start after the PIR is received

Test Sequence #02 Nominal: Successful PIR and Enable Notifications to the Same SM-DP+ Address

Initial Conditions		
Entity	Description of the initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1 for PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_EN instead of #METADATA_OP_PROF1.	

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_INIT_AUTH				
IC3	PROC_ES9+_A	PROC_ES9+_AUTH_CLIENT			

V1.4 Page 411 of 777

IC4	PROC_ES9+_GET_BPP (s. Note 1)			
1	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ32_001
2	LPAd → S_SM-DP+(1)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_PIR_OK)) • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ31_171 RQ31_176 RQ35_008 RQ35_013 RQ35_017 RQ35_018
3	S_SM-DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd. The LPAd MAY inform the End User of the success status indicated by the Profile Installation Result.	RQ35_008 RQ35_014 RQ35_017
4	S_EndUser → LPAd	Initiate the Enable Profile operation for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation PROFILE_OPERATIONAL1 is enabled	
5	LPAd → S_SM-DP+(1)	Establish an HTTPs connection	if previously closed	
6	LPAd → S_SM-DP+(1)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#PENDING_NOTIF_EN1)) sent within the timeout #IUT_LPAd_NOTIFICATION_TIMEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ35_008 RQ35_013 RQ35_014 RQ35_022 RQ35_018
7	S_SM-DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd	RQ35_008 RQ35_022

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the session.

Note 2: the timeout SHALL start after the End User Intent verification.

Test Sequence #03 Nominal: Disable and Delete Notifications to the Same SM-DP+ Address

Initial Conditions		
Entity Description of the initial condition		
eUICC	PROFILE_OPERATIONAL1 is installed on the eUICC	
eUICC	PROFILE_OPERATIONAL1 is in the Enabled state	

V1.4 Page 412 of 777

Step	Direction	Sequence / Description	Expected result	REQ	
1	S_EndUser → LPAd	Initiate the Disable Profile operation for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation PROFILE_OPERATIONAL1 is disabled	RQ32_001	
2	LPAd → S_SM- DP+(1)	Establish an HTTPs connection i	if previously closed		
3	LPAd → S_SM- DP+(1)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#PENDING _NOTIF_DIS1)) sent within the timeout #IUT_LPAd_NOTIFICATION_TIME OUT Verify the euiccNotificationSignature	RQ35_008 RQ35_013 RQ35_017 RQ35_018	
			<tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>		
4	S_SM- DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd	RQ35_008 RQ35_014 RQ35_017	
5	LPAd → S_SM- DP+(1)	Establish an HTTPs connection if previously closed			
6	S_EndUser → LPAd	Initiate the Delete Profile operation for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation End User acknowledges the consequences of deleting the Profile (it MAY be done in one single step combined with the End User Intent verification) PROFILE_OPERATIONAL1 is deleted		
7	LPAd → S_SM- DP+(1)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#PENDING _NOTIF_DEL1)) sent within the timeout #IUT_LPAd_NOTIFICATION_TIME OUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ35_008 RQ35_013 RQ35_014 RQ35_022 RQ35_018	
8	S_SM- DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd	RQ35_008 RQ35_022	
Note 1:	Note 1: the timeout SHALL start after the End User Intent verification.				

V1.4 Page 413 of 777

Test Sequence #04 Nominal: Enable and Disable Notifications with Different SM-DP+ Addresses

Initial Conditions		
Entity	Description of the initial condition	
eUICC	PROFILE_OPERATIONAL1 is installed on the eUICC	
eUICC	PROFILE_OPERATIONAL2 is installed on the eUICC	
eUICC	PROFILE_OPERATIONAL1 is in the Enabled state	

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Enable Profile operation for PROFILE_OPERATIONAL2	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation PROFILE_OPERATIONAL2 is enabled	RQ32_001
2	LPAd → S_SM-DP+(1)	Establish an HTTPs connection if	previously closed	
3	LPAd → $S_SM-DP+(1)$	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#PENDING _NOTIF_DIS1)) sent within the timeout #IUT_LPAd_NOTIFICATION_TIME OUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ35_012 RQ35_008 RQ35_013 RQ35_014_3 RQ35_017 RQ35_018
4	S_SM-DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd	RQ35_008 RQ35_014 RQ35_017
5	$\begin{array}{c} LPAd \to \\ S_SM\text{-DP\text{+}(2)} \end{array}$	Establish an HTTPs connection		
6	LPAd → S_SM-DP+(2)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS2, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#PENDING _NOTIF_EN2)) sent within the timeout #IUT_LPAd_NOTIFICATION_TIME OUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ35_012 RQ35_008 RQ35_013 RQ35_014 RQ35_014_3 RQ35_022 RQ35_018
7	S_SM-DP+(2) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd	RQ35_008 RQ35_022

V1.4 Page 414 of 777

Note 1: Steps 2,3 and 4 can be executed in parallel to the steps 5, 6 and 7

Note 2: the timeout SHALL start after the End User Intent verification.

Test Sequence #05 Nominal: Different SM-DP+ Addresses in PIR and Install Notifications

Initial Conditions		
Entity	Description of the initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1 for PROFILE_OPERATIONAL1 with #METADATA_OP_PROF1_INST_DIFF instead of #METADATA_OP_PROF1.	

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_I	NIT_AUTH			
IC3	PROC_ES9+_A	AUTH_CLIENT			
IC4	PROC_ES9+_0	GET_BPP(s. Note 1)			
IC5	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.		
1	$\begin{array}{c} LPAd \to \\ S_SM-DP+(1) \end{array}$	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_PIR_O K))	RQ35_012 RQ35_008 RQ35_013 RQ35_017 RQ35_018	
2	S_SM-DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd. The LPAd MAY inform the End User of the success status indicated by the Profile Installation Result.	RQ35_008 RQ35_014 RQ35_017	
3	$\begin{array}{c} LPAd \to \\ S_SM\text{-DP\text{+}(2)} \end{array}$	Establish an HTTPs connection			
4	LPAd → S_SM-DP+(2)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS2, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#PENDIN G_NOTIF_INST_ADDRESS2)) sent within the timeout #IUT_LPAd_NOTIFICATION_TIM EOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	RQ35_012 RQ35_008 RQ35_013 RQ35_014 RQ35_022 RQ35_018	
5	S_SM-DP+(2) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd	RQ35_008 RQ35_022	

V1.4 Page 415 of 777

- Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the session.
- Note 2: Steps 1 and 2 can be executed in parallel to the steps 3,4 and 5
- Note 3: the timeout SHALL start after the End User Intent verification.

Test Sequence #06 Nominal: Profile Download with PIR Failed

Initial Conditions		
Entity	Description of the initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1 for PROFILE_OPERATIONAL1.	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_IN	NIT_AUTH		
IC3	PROC_ES9+_A	UTH_CLIENT		
IC4	LPAd → S_SM- DP+(1)	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transacti on_id="">, #R_PREP_DOWNLOAD_NO_CC))</s_transacti>	
IC5	S_SM-DP+(1) → LPAd	MTD_HTTP_RESP(#GET_BPP _INV)	No error exhibited by the LPAd, s. note 1.	
IC6	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	
1	LPAd → S_SM- DP+(1)	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_PIR_S ECU_INVALID)) • Verify the euiccSignPIR <euicc_sign_pir> using the #PK_EUICC_ECDSA</euicc_sign_pir>	RQ31_171 RQ31_173 RQ31_176 RQ35_008 RQ35_012 RQ35_013 RQ35_014
2	S_SM-DP+(1) → LPAd	#R_HTTP_204_OK	No error exhibited by the LPAd. The LPAd MAY inform the End User of the error status indicated by the Profile Installation Result.	RQ35_008

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the session.

V1.4 Page 416 of 777

Test Sequence #07 Nominal: Successful PIR and Install Notifications after Connectivity Interruption

This Test Sequence is FFS

Test Sequence #08 Nominal: No Acknowledge for Successful PIR results in No Further Notifications

The purpose of this test case is to verify that the next Notification of a group is not sent until LPA receives a successful response from the SM-DP+ for the previous Notification

Initial Conditions	
Entity	Description of the initial condition
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1 for PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_II	NIT_AUTH			
IC3	PROC_ES9+_A	AUTH_CLIENT with #MATCHING_II	D_1 as <matching_id></matching_id>		
IC4	PROC_ES9+_0 (s. Note 1)	GET_BPP			
1	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.		
2	$\begin{array}{c} LPAd \to \\ S_SM-DP+(1) \end{array}$	Send ES9+.HandleNotification method initiated	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_PIR _OK))		
3	LPAd → S_SM-DP+(1)	No ES9+.HandleNotification method sent	No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_NOTIFICATION_TI MEOUT OR TLS Session closed independent of timeout.	RQ35_014	

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the session.

Note 2: The timeout in Step 3 SHALL start after the End User Intent verification.

4.4.25 ES9+ (LPA - SM-DP+): CancelSession

4.4.25.1 Conformance Requirements

References

V1.4 Page 417 of 777

GSMA RSP Technical Specification [2]

Requirements

- RQ29_011, RQ29_012, RQ29_013, RQ29_014, RQ29_018, RQ29_007_1, RQ29_008, RQ29_008_1, RQ29_009, RQ29_015
- RQ31_071, RQ31_096, RQ31_099, RQ31_100, RQ31_101, RQ31_102, RQ31_103, RQ31_105, RQ31_111, RQ31_114, RQ31_117, RQ31_118, RQ31_120, RQ31_121, RQ31_123, RQ31_123_1, RQ31_124, RQ31_129, RQ31_159, RQ31_160, RQ31_162_1, RQ31_186_1
- RQ56_044, RQ56_047
- RQ65_025

4.4.25.2 Test Cases

4.4.25.2.1TC_LPAd_ES9+_CancelSession_Nominal

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	
eUICC	There is no default SM-DP+ address configured	

Test Sequence #01 Nominal: Profile Download with PPR1 not allowed due to Operational Profile already present

Initial Conditions		
Entity Description of the initial condition		
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_4.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_4 (associated with PROFILE_OPERATIONAL4)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_IN	PROC_ES9+_INIT_AUTH		
IC3	PROC_ES9+_AUTH_CLIENT Extract <s_transaction_id></s_transaction_id>			
IC4	PROC_ES9+_GET_BPP with #METADATA_OP_PROF4 used in #GET_BPP_OK This step is conditional – occurs only if ES9+.CancelSession method was not sent before (e.g. request for Confirmation was required after ES9+.AuthenticateClient method)			

V1.4 Page 418 of 777

1	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_PPR_NOT_ALLOWED)) Verify: •<euicc_cancel_session_si gnature=""> with the #PK_EUICC_ECDSA •<s_transaction_id> is the same as in IC3</s_transaction_id></euicc_cancel_session_si></s_transaction_id>	RQ31_099 RQ56_044 RQ56_047 RQ65_025 RQ31_114 RQ31_117 RQ31_118 RQ31_120
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCCE SS)	If Step 1 was performed directly after IC3: No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT. OR If Step 1 was performed after IC4: No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT.	RQ31_099

Test Sequence #02 Nominal: End User rejection due to PPR1 set

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL4 with PPR1 is installed and enabled on the eUICC	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_	_INIT_AUTH		
IC3	PROC_ES9+_AUTH_CLIENT Extract <s_transaction_id></s_transaction_id>			
IC4	PROC_ES9+_GET_BPP This step is conditional – occurs only if ES9+.CancelSession method was not sent before (e.g. request for Confirmation was required after ES9+.AuthenticateClient method)			
1	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation	RQ31_071 RQ31_096

V1.4 Page 419 of 777

			OR Simple End User Confirmation/Rejection if Authenticated Confirmation was requested before. End User advised about a Profile with PPR1 already present and the End User consent is requested if not requested before.	
2	S_EndUser → LPAd	End User Rejection (or failed confirmation) is performed within the period as defined in #IUT_EU_CONFIRMATION_TI MEOUT		
3	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_EU_REJ)) Verify: •<euicc_cancel_session_si gnature=""> with the #PK_EUICC_ECDSA •<s_transaction_id> is the same as in IC3</s_transaction_id></euicc_cancel_session_si></s_transaction_id>	RQ56_044 RQ56_047 RQ65_025 RQ31_114 RQ31_117 RQ31_118 RQ31_120
4	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCCESS)	If Step 1 was performed directly after IC3: No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT. OR If Step 1 was performed after IC4: No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT.	RQ31_114

Test Sequence #03 Nominal: Load BPP Error

Initial Conditions		
Entity	Description of the initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			

V1.4 Page 420 of 777

IC2	PROC_ES9+_INIT_AUTH			
IC3	PROC_ES9+_AUTH_CLIENT Extract <s_transaction_id></s_transaction_id>			
IC4	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transacti on_id="">, #R_PREP_DOWNLOAD_NO_CC))</s_transacti>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_BPP_LOAD_ERROR)	Continue to step 2 (End User Confirmation) if requested, otherwise continue with Step 3	
2	LPAd → S_EndUser	Request for Confirmation if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before OR Simple End User Confirmation if Authenticated Confirmation was requested before.	
3	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_EU_LOAD_BPP_ERRO R)) Verify: •<euicc_cancel_session_si gnature=""> with the #PK_EUICC_ECDSA •<s_transaction_id> is the same as in IC3</s_transaction_id></euicc_cancel_session_si></s_transaction_id>	RQ31_129 RQ56_044 RQ56_047 RQ65_025 RQ31_114 RQ31_117 RQ31_118 RQ31_120 RQ31_162 _1
4	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCCESS)	No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT.	RQ31_129

Test Sequence #04 Nominal: End User Timeout due to PPR1 set

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL4 with PPR1 set is installed and enabled on the eUICC	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)	

V1.4 Page 421 of 777

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_INIT_AUTH				
IC3	PROC_ES9+_AUTH_CLIENT Extract <s_transaction_id></s_transaction_id>				
	PROC_ES9+_	_GET_BPP			
IC4		onditional – occurs only if ES9+.Car onfirmation was required after ES9+	ncelSession method was not sent befo AuthenticateClient method)	re (e.g.	
1	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation OR Simple End User Confirmation if Authenticated Confirmation was requested before. End User advised about a Profile with PPR1 already present and the End User consent is requested if not requested before.	RQ31_071 RQ31_096 RQ31_159	
2	S_EndUser → LPAd	No End User Rejection or Confirmation is performed within the period as defined in #IUT_EU_CONFIRMATION_TI MEOUT			
3	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_TIMEOUT)) Verify: •<euicc_cancel_session_si gnature=""> with the #PK_EUICC_ECDSA •<s_transaction_id> is the same as in IC3</s_transaction_id></euicc_cancel_session_si></s_transaction_id>	RQ56_044 RQ56_047 RQ65_025 RQ31_114 RQ31_124 RQ56_044 RQ56_047 RQ65_025 RQ31_117 RQ31_118 RQ31_120 RQ31_111	
4	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCCESS)	If Step 1 was performed directly after IC3: No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_T IMEOUT. OR If Step 1 was performed after IC4: No ES9+.HandleNotification requests are sent within the timeout	RQ31_114	

V1.4 Page 422 of 777

#IUT_LPAd_SESSION_CLOSE_T	
IMEOUT.	

Test Sequence #05 Nominal: Load BPP Error due to unknown TAG

Initial Conditions			
Entity	Description of the initial condition		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_INIT_AUTH			
IC3	PROC_ES9+_A Extract <s_tra< td=""><td>UTH_CLIENT .NSACTION_ID></td><td></td><td></td></s_tra<>	UTH_CLIENT .NSACTION_ID>		
IC4	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transacti on_id="">, #R_PREP_DOWNLOAD_NO_CC))</s_transacti>	
1	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_BPP _LOAD_ERROR_UNKNOWN_ TAG)	Continue to step 2 (End User Confirmation) if requested, otherwise continue with Step 3	
2	LPAd → S_EndUser	Request for Confirmation if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before OR Simple End User Confirmation if Authenticated Confirmation was requested before.	
3	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_EU_LOAD_BPP_ERRO R)) Verify: •<euicc_cancel_session_si gnature=""> with the #PK_EUICC_ECDSA •<s_transaction_id> is the same as in IC3</s_transaction_id></euicc_cancel_session_si></s_transaction_id>	RQ31_129 RQ56_044 RQ56_047 RQ65_025 RQ31_114 RQ31_186 _1 RQ31_162 _1
4	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCCE SS)	No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT.	RQ31_129

V1.4 Page 423 of 777

4.4.25.2.2TC_LPAd_ES9+_CancelSession_EndUserPostponed_Nominal

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	
eUICC There is no default SM-DP+ address configured		

Test Sequence #01 Nominal: End User Postponed due to PPR1 set

Initial Conditions		
Entity Description of the initial condition		
eUICC	The PROFILE_OPERATIONAL4 with PPR1 set is installed and enabled on the eUICC	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_I	NIT_AUTH		
IC3	PROC_ES9+_AUTH_CLIENT Extract <s_transaction_id></s_transaction_id>			
IC4	PROC_ES9+_GET_BPP This step is conditional – occurs only if ES9+.CancelSession method was not sent before (e.g. request for Confirmation was required after ES9+.AuthenticateClient method)			
1	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation OR Simple End User Confirmation/Rejection if Authenticated Confirmation was requested before. End User advised about a Profile with PPR1 already present and the End User consent is requested if not requested before.	RQ31_071 RQ31_096
2	S_EndUser → LPAd	End User Postpone is performed within the period as defined in #IUT_EU_CONFIRMATION_TI MEOUT		
3	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1,	RQ56_044 RQ56_047

V1.4 Page 424 of 777

			#PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(RQ65_025 RQ31_114
4	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCCESS)	If Step 1 was performed directly after IC3: No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT. OR If Step 1 was performed after IC4: No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TI MEOUT.	RQ31_114

4.4.25.2.3TC_LPAd_ES9+_CancelSession_Error

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	
eUICC	There is no default SM-DP+ address configured	

Test Sequence #01 Error: Unknown TransactionID after End User Rejection/Postpone

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL4 with PPR1 set is installed and enabled on the eUICC	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH	on ES9+	
IC2	PROC_ES9+_INIT_AUTH			
IC3	PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_1 as <matching_id> Extract <s_transaction_id></s_transaction_id></matching_id>			

V1.4 Page 425 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

	PROC_ES9+_	_GET_BPP			
IC4	This step is conditional – occurs only if ES9+.CancelSession method was not sent before (e.g. request for Confirmation was required after ES9+.AuthenticateClient method)				
IC5	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation OR Simple End User Confirmation/Rejection if Authenticated Confirmation was requested before. End User advised about a Profile with PPR1 already present and the End User consent is requested if not requested before.		
IC6	S_EndUser → LPAd	End User Postpone/Rejection (or failed confirmation) is performed within the period as defined in #IUT_EU_CONFIRMATION_T IMEOUT			
1	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	No error after receiving the HTTPs response. (See Note)	RQ56_044 RQ56_047 RQ56_049 RQ31_121	

Test Sequence #02 Error: Invalid eUICC Signature after End User Rejection/Postpone

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL4 with PPR1 set is installed and enabled on the eUICC	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)	

V1.4 Page 426 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_INIT_AUTH			
IC3		AUTH_CLIENT with #MATCHING	G_ID_1 as <matching_id></matching_id>	
IC4			ancelSession method was not sent befor P+.AuthenticateClient method)	e (e.g.
IC5	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation OR Simple End User Confirmation/Rejection if Authenticated Confirmation was requested before. End User advised about a Profile with PPR1 already present and the End User consent is requested if not requested before.	
IC6	S_EndUser → LPAd	End User Postpone/Rejection (or failed confirmation) is performed within the period as defined in #IUT_EU_CONFIRMATION_T IMEOUT		
1	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_EU_REJ)) OR MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_EU_POSTPONED))</s_transaction_id></s_transaction_id>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERR OR_8_1_6_1)	No error after receiving the HTTPs response. The LPA SHALL stop the procedure: no ES9+.CancelSession requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT	RQ56_044 RQ56_047 RQ56_049 RQ31_123

V1.4 Page 427 of 777

Test Sequence #03 Error: Invalid SM-DP+ OID after End User Rejection/Postpone

Initial Conditions	Initial Conditions		
Entity	Description of the initial condition		
eUICC	The PROFILE_OPERATIONAL4 with PPR1 set is installed and enabled on the eUICC		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (associated with PROFILE_OPERATIONAL1)		

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
IC2	PROC_ES9+_INIT_AUTH				
IC3		_AUTH_CLIENT with #MATCHING	G_ID_1 as <matching_id></matching_id>		
IC4			ancelSession method was not sent beforenter. A+.AuthenticateClient method)	re (e.g.	
IC5	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation OR Simple End User Confirmation/Rejection if Authenticated Confirmation was requested before. End User advised about a Profile with PPR1 already present and the End User consent is requested if not requested before.		
IC6	S_EndUser → LPAd	End User Postpone/Rejection (or failed confirmation) is performed within the period as defined in #IUT_EU_CONFIRMATION_T IMEOUT			
1	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_EU_REJ)) OR MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION(</s_transaction_id>		

V1.4 Page 428 of 777

			<s_transaction_id>, #CS_OK_EU_POSTPONED))</s_transaction_id>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_ERR OR_8_8_3_10)	No error after receiving the HTTPs response. The LPA SHALL stop the procedure: no ES9+.CancelSession requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT	RQ56_044 RQ56_047 RQ56_049 RQ31_123_ 1

4.4.25.2.4TC_LPAd_ES9+_CancelSession_PPRs

General Initial Conditions		
Entity Description of the general initial condition		
Device	Device The protection of access to the LUI is disabled	
eUICC There is no default SM-DP+ address configured		

Test Sequence #01 Nominal: End User rejection/postpone after PPR1 consent requested

Initial Conditions			
Entity Description of the initial condition			
eUICC	The eUICC's RAT is configured as detailed SGP.21 Annex H: one PPAR authorizing PPR1 and PPR2 for all MNOs with End User consent required (i.e. #PPRS_ALLOWED) no additional rules		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_4.		
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_4 (associated with PROFILE_OPERATIONAL4)		

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH or	n ES9+			
IC2	PROC_ES9+_IN	IIT_AUTH				
IC3		PROC_ES9+_AUTH_CLIENT Extract <s_transaction_id></s_transaction_id>				
IC4	PROC_ES9+_GET_BPP with #METADATA_OP_PROF4 used in #GET_BPP_OK This step is conditional – occurs only if ES9+.CancelSession method was not sent before (e.g. request for Confirmation was required after ES9+.AuthenticateClient method)					
1	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation OR Simple End User	RQ31_102 RQ31_103 RQ29_007 _1 RQ29_008 RQ29_009 RQ29_015		

V1.4 Page 429 of 777

			Confirmation/Rejection if Authenticated Confirmation was requested before. Relevant information about PPRs is shown, including consequences for the End User, and the End User consent is requested if not requested before.	RQ29_011 RQ29_013 RQ29_018
2	S_EndUser → LPAd	End User Postpone/Rejection (or failed confirmation) is performed within the period as defined in #IUT_EU_CONFIRMATION_TI MEOUT		
3	LPAd → S_SM-DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(RQ31_100 RQ31_105 RQ31_160
4	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCC ESS)	If Step 1 was performed directly after IC3: No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TIMEOUT. OR If Step 1 was performed after IC4: No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TIMEOUT.	RQ31_100 RQ31_160

V1.4 Page 430 of 777

Test Sequence #02 Nominal: End User rejection/posptone after PPR2 consent requested

Initial Conditions	Initial Conditions			
Entity	Description of the initial condition			
eUICC	The eUICC's RAT is configured as detailed SGP.21 Annex H:			
	 one PPAR authorizing PPR1 and PPR2 for all MNOs with End User consent required (i.e. #PPRS_ALLOWED) 			
	no additional rules			
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_3_NO_CC.			
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL3)			

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+					
IC2	PROC_ES9+_INIT	Γ_AUTH				
IC3		PROC_ES9+_AUTH_CLIENT Extract <s_transaction_id></s_transaction_id>				
IC4	This step is condit	PROC_ES9+_GET_BPP with #METADATA_OP_PROF3 used in #GET_BPP_OK This step is conditional – occurs only if ES9+.CancelSession method was not sent before (e.g. request for Confirmation was required after ES9+.AuthenticateClient method)				
1	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation OR Simple End User Confirmation/Rejection if Authenticated Confirmation was requested before. Relevant information about PPRs is shown, including consequences for the End User, and the End User consent is requested if not requested before.	RQ31_102 RQ31_103 RQ29_007 _1 RQ29_008 RQ29_009 RQ29_015 RQ29_011 RQ29_013 RQ29_018		
2	S_EndUser → LPAd	End User Postpone/Rejection (or failed confirmation) is performed within the period as defined in #IUT_EU_CONFIRMATION_T IMEOUT				
3	LPAd → S_SM- DP+	Send ES9+.CancelSession method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(RQ31_100 RQ31_105 RQ31_160		

V1.4 Page 431 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

			<pre><s_transaction_id>, #CS_OK_EU_REJ)) OR MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_OK_EU_POSTPONED))</s_transaction_id></s_transaction_id></pre>	
			Verify: • <euicc_cancel_session_s ignature=""> with the #PK_EUICC_ECDSA •<s_transaction_id> is the same as in IC3</s_transaction_id></euicc_cancel_session_s>	
4	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#R_SUCC ESS)	If Step 1 was performed directly after IC3: No ES9+.GetBoundProfilePackage requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_TIMEOUT.	RQ31_100
			If Step 1 was performed after IC4: No ES9+.HandleNotification requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE_ TIMEOUT.	

4.4.26 ES9+ (LPA - SM-DP+): HTTPS

4.4.26.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ21_001
- RQ26_023, RQ26_024, RQ26_026, RQ26_027, RQ26_029
- RQ31_032, RQ31_032_1
- RQ45_026, RQ45_031
- RQ56_001, RQ56_003
- RQ60_001, RQ60_002, RQ60_004
- RQ61_001

V1.4 Page 432 of 777

4.4.26.2 Test Cases

4.4.26.2.1TC_LPAd_HTTPS_Nominal

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	
eUICC	There is no default SM-DP+ address configured	
LPAd Add Profile operation is initiated by using #ACTIVATION_CODE_1.		

Test Sequence #01 Nominal: HTTPS Session Establishment

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>) Verify if: •#IUT_TLS_VERSION SHALL be 1.2 or higher •<tls_cipher_suites> SHALL contain at least TLS_ECDHE_ECDSA_WITH_ AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_ AES_128_CBC_SHA256 •<ext_sha256_ecdsa> SHALL have at least the 'supported_signature_algorith ms' extension set with HashAlgorithm sha256 (04) and SignatureAlgorithm ecdsa (03).</ext_sha256_ecdsa></tls_cipher_suites></ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_024 RQ26_026 RQ31_032 RQ56_001
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DP_TLS)</session_id_random>	MTD_TLS_CLIENT_KEY_EXC H_ETC(<client_tls_ephe M_KEY>)</client_tls_ephe 	RQ26_027 RQ31_032 RQ45_026 RQ56_003
3	S_SM-DP+ → LPAd	Finalize TLS Handshake (send Server ChangeCipherSpec and Finished messages)	HTTPS connection established	RQ31_032 RQ56_001 RQ60_001 RQ60_002 RQ61_001

Test Sequence #02 Nominal: non-reuse of session keys

The purpose of this test sequence is to verify that the LPAd is not reusing ephemeral keys from the previous session.

V1.4 Page 433 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+ Extract <client_tls_ephem_key></client_tls_ephem_key>			
IC2	Terminate TLS s	session and restart "Add Profile" Proced	dure as define in the initial condition	ns.
			MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
1	LPAd → S_SM-DP+	Send TLS Client Hello	Verify if: •#IUT_TLS_VERSION SHALL be 1.2 or higher • <tls_cipher_suites> SHALL be at least TLS_ECDHE_ECDSA_WITH_A ES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_A ES_128_CBC_SHA256 • <ext_sha256_ecdsa> SHALL have at least the 'supported_signature_algorithm s' extension set with HashAlgorithm sha256 (04) and SignatureAlgorithm ecdsa (03).</ext_sha256_ecdsa></tls_cipher_suites>	RQ31_032
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC (#TLS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DP_TLS)</session_id_random>	MTD_TLS_CLIENT_KEY_EXC H_ETC(<client_tls_ephe m_key="">) Verify if CCLIENT_TLS_EPHEM_KEY> is different from the one used by LPAd in IC1</client_tls_ephe>	RQ31_032
3	S_SM-DP+ → LPAd	Finalize TLS Handshake (send Server ChangeCipherSpec and Finished messages)	HTTPS connection established	RQ31_032 RQ60_001 RQ60_002 RQ60_004 RQ61_001

4.4.26.2.2TC_LPAd_HTTPS_ErrorCases

General Initial Condit	General Initial Conditions	
Entity	Description of the general initial condition	
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_1.	

Test Sequence #01 Error: Invalid (SM-DP+) TLS Certificate signature

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>,</tls_cipher_suites>	

V1.4 Page 434 of 777

			#SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa>	
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DP_TLS_INV_SIG)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_026
3	LPDd → S_SM-DP+	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ56_003

Test Sequence #02 Error: Expired TLS Certificate

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DP_TLS_EXPIRED)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_026
3	LPDd → S_SM-DP+	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ56_003

Test Sequence #03 Error: Invalid TLS Certificate with critical extension not set

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	I Send II S Client Hello I TI C CIDUED CUITEC		
2	S_SM-DP+ → LPAd	,	LPAd aborts AddProfile procedure	RQ31_032 RQ45_026
3	LPDd → S_SM-DP+	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ56_003

V1.4 Page 435 of 777

Test Sequence #04 Error: Invalid TLS Certificate with invalid 'key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC(# TLS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DP_TLS_INV_KEY_ USAGE)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_031
3	LPDd → S_SM-DP+	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ56_003

Test Sequence #05 Error: Invalid TLS Certificate with invalid 'extended key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC(# TLS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DP_TLS_INV_EXT_K EY_USAGE)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_031
3	LPDd → S_SM-DP+	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ56_003

Test Sequence #06 Error: Invalid TLS Certificate with invalid 'Certificate Policies' extensions

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC(# TLS_VERSION_1_2, #S_TLS_CIPHER_SUITE,	LPAd aborts AddProfile procedure	RQ31_032 RQ45_031

V1.4 Page 436 of 777

		<pre><session_id_random>, #CERT_S_SM_DP_TLS_INV_CERT _POL)</session_id_random></pre>		
3	$\begin{array}{c} LPDd \to \\ S_SM\text{-DP\text{+}} \end{array}$	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ56_003

Test Sequence #07 Error: Invalid TLS Certificate based on Invalid CI (Invalid Curve)

Step	Direction	Sequence / Description	Expected result	REQ
IC1	Power-on the	Device		
1	LPAd → S_SM-DP+	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DP+ → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DP_TLS_INV_CURVE)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_031
3	LPDd → S_SM-DP+	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_029 RQ56_003

4.4.27 ES11 (LPA – SM-DS): InitiateAuthentication

4.4.27.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_033, RQ31_034, RQ31_035, RQ31_036, RQ31_043, RQ31_045, RQ31_048, RQ31_052, RQ31_075
- RQ58_013, RQ58_020
- RQ65_026

4.4.27.2 Test Cases

4.4.27.2.1TC_LPAd_ES11_InitiateAuthentication_Nominal

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	
Device	The Profile Download is initiated using SM-DS (see section 2.2.4.1).	

V1.4 Page 437 of 777

S_SM-DS	S_SM-DP+ (#TEST_DP_ADDRESS1) performed Profile download Event Registration to the S_SM-DS (#TEST_ROOT_DS_ADDRESS) with #EVENT_ID_1
eUICC	There is no default SM-DP+ address configured
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #EVENT_ID_1 (PROFILE_OPERATIONAL1) (see Note)

Note: in order to avoid potentially misleading errors on LUI, the S_SM-DP+ SHALL be available to the LPAd for profile download during test sequence execution. The test tool SHALL NOT check the ES9+ communication.

Test Sequence #01 Nominal: Initiate Authentication

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITI	ALIZATION_SERVER_AUTH on	ES11	
1	LPAd → S_SM- DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	RQ31_033
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_DS_OK)	No error: Next step of common mutual authentication procedure is performed.	RQ31_043 RQ58_013, RQ58_020, RQ65_026

4.4.27.2.2TC_LPAd_ES11_InitiateAuthentication_ErrorCases

General Initial Conditions			
Entity Description of the general initial condition			
Device	The protection of access to the LUI is disabled		
Device	The Profile Download is initiated using SM-DS (see section 2.2.4.1)		
S_SM-DP+ (#TEST_DP_ADDRESS1) performed Profile download Event S_SM-DS Registration to the S_SM-DS (#TEST_ROOT_DS_ADDRESS) with #EVENT_II (see Note)			
eUICC	There is no default SM-DP+ address configured		
Note: the S_SM_DP+ does not need to be available to the LPAd for profile download during test sequence execution, as the LPAd is not expected to receive the smdpAddress.			

V1.4 Page 438 of 777

Test Sequence #01 Error: Invalid SM-DS Address

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH or	ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS , #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERRO R_8_9_1_3_8)	LPAd aborts AddProfile procedure	RQ31_034, RQ58_020
2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_034, RQ58_020

Test Sequence #02 Error: Unsupported Security Configuration

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH on E	ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS , #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERROR _8_9_2_3_1)	LPAd aborts AddProfile procedure	RQ31_035, RQ58_020
2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_035, RQ58_020

Test Sequence #03 Error: Unsupported SVN

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH on E	ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS , #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA	

V1.4 Page 439 of 777

			TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERROR _8_9_3_3_1)	LPAd aborts AddProfile procedure	RQ58_020
2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ58_020

Test Sequence #04 Error: Unavailable SM-DS Certificate

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH on ES	511	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERROR_8_ 9_4_3_7)	LPAd aborts AddProfile procedure	RQ31_036, RQ58_020
2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE _TIMEOUT in Annex F.	RQ31_036, RQ58_020

Test Sequence #05 Error: Invalid SM-DS Certificate

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH on E	ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS , #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_INV_CERT_ DS)	LPAd aborts AddProfile procedure	RQ31_052 RQ58_013

V1.4 Page 440 of 777

	2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication or ES11.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_052 RQ58_013	
--	---	-------------------	----------------------------	---	----------------------	--

Test Sequence #06 Error: Invalid SM-DS Signature

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INIT	TALIZATION_SERVER_AUTH or	n ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIAT E_AUTH_INV_SIGN_DS)	LPAd aborts AddProfile procedure	RQ31_052 RQ58_013
2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication or ES11.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE _TIMEOUT in Annex F.	RQ31_052 RQ58_013

Test Sequence #07 Error: Invalid SM-DS Address sent by the SM-DS

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH or	ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS , #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE _AUTH_INV_SMDS_ADDRES S)	LPAd informs the S_EndUser and aborts the AddProfile procedure	RQ31_045 RQ31_052 RQ58_013
2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication or ES11.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOS E_TIMEOUT in Annex F.	RQ31_045 RQ31_052 RQ58_013

V1.4 Page 441 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #08 Error: Unsupported CI Key ID

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH o	n ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS , #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE _AUTH_INV_CI_DS)	LPAd aborts AddProfile procedure	RQ31_048 RQ31_052 RQ58_013
2	LPAd → S_SM-DS	No Profile download action	No ES11.InitiateAuthentication or ES11.AuthenticateClient requests are sent within the timeout #IUT_LPAd_SESSION_CLOSE _TIMEOUT in Annex F.	RQ31_048 RQ31_052 RQ58_013

4.4.28 ES11 (LPA - SM-DS): AuthenticateClient

4.4.28.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_046, RQ31_056, RQ31_057, RQ31_061, RQ31_062, RQ31_065, RQ31_078,
 RQ31_083, RQ31_085, RQ31_090, RQ31_095, RQ31_136, RQ36_018, RQ36_019,
 RQ36_020
- RQ42_001, RQ42_002, RQ42_003, RQ42_004, RQ42_005, RQ42_006, RQ42_007, RQ42_008, RQ42_009, RQ42_010, RQ42_011, RQ42_012, RQ42_013, RQ42_014, RQ42_015, RQ42_016, RQ42_017, RQ42_018, RQ42_019, RQ42_020
- RQ58_021, RQ58_030, RQ58_036, RQ58_037, RQ58_038, RQ58_039
- RQ62_001, RQ62_002, RQ62_003, RQ62_004, RQ62_005, RQ62_006, RQ62_007, RQ62_008, RQ62_009
- RQ63_001_1, RQ63_004, RQ63_005, RQ63_006
- RQ65_001, RQ65_002, RQ65_003, RQ65_004, RQ65_005, RQ65_006, RQ65_007, RQ65_008, RQ65_009, RQ65_022, RQ65_028

V1.4 Page 442 of 777

4.4.28.2 Test Cases

4.4.28.2.1 TC_LPAd_ES11_AuthenticateClient_Nominal

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	
Device	The Profile Download is initiated using SM-DS (see section 2.2.4.1)	
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state	
eUICC	There is no default SM-DP+ address configured	

Test Sequence #01 Nominal: Authenticate Client with empty MatchingID

Initial Conditions	Initial Conditions		
Entity	Description of the initial condition		
S_SM-DS	S_SM-DP+ (#TEST_DP_ADDRESS1) performed Profile download Event Registration to the root S_SM-DS (#TEST_ROOT_DS_ADDRESS) with #EVENT_ID_1 for #EID1		
S_SM-DP+	There is a pending Profile download order for #EVENT_ID_1 (PROFILE_OPERATIONAL1) (see Note)		

Note: in order to avoid potentially misleading errors on LUI, the S_SM-DP+ SHALL be available to the LPAd for profile download during test sequence execution. The test tool SHALL NOT check the ES9+ communication.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES11		
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICAT ION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE_ AUTH_DS_OK)	MTD_HTTP_REQ(#TEST_ROO T_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT (<s_transaction_id>, #R_AUTH_SERVER_DS_MATC H_ID_DEV_INFO)) Verify: • If <s_transaction_id> is the same as in</s_transaction_id></s_transaction_id>	RQ31_046 RQ31_056 RQ31_057 RQ31_078 RQ36_018, RQ36_019 RQ42_001 RQ42_002 RQ42_002 RQ42_003 RQ42_004 RQ42_005 RQ42_005

V1.4 Page 443 of 777

Official Document SGF.23 - SGF.23 KSF Test Specific		
	#INITIATE_AUTH_DS_OK	RQ42_007
	• <euicc_signature1> using</euicc_signature1>	RQ42_008
	the #PK_EUICC_ECDSA	RQ42_009
	 if <matching_id> is empty</matching_id> 	RQ42_010
	• if <s_smds_challenge></s_smds_challenge>	RQ42_011
	present in the	RQ42_012 RQ42_013
	#R_AUTH_SERVER_MATCH_I	RQ42_013 RQ42_014
	D_DEV_INFO is the same as in	RQ42_015
	<s_smds_signed1> present</s_smds_signed1>	RQ42 016
	in #INITIATE_AUTH_DS_OK • for #DEVICE_INFO:	RQ42_017
	- TAC is BCD coded as 4 octets	RQ42_018
	acc. To 3GPP TS 23.003	RQ42_019
	- if IMEI is present then it is BCD	RQ42_020
	coded as 8 octets acc. To 3GPP	RQ58_021
	TS 23.003	RQ58_036
	- if O_D_GSM_GERAN then	RQ58_037 RQ58_038
	gsmSupportedRelease is set to	RQ62_001
	the highest release as defined in	RQ62_002
	#IUT_GSM_GERAN_REL if O_D_UMTS_UTRAN then	RQ62_003
	utranSupportedRelease is set to	RQ62_004
	the highest release as defined in	RQ62_005
	#IUT_UMTS_UTRAN_REL.	RQ62_006
	- if O_D_CDMA2000_1X then	RQ62_007
	cdma2000onexSupportedReleas	RQ62_008
	e is set to the highest release as	RQ62_009 RQ63_001_
	defined in	1
	#IUT_CDMA2000_1X_REL.	RQ63_004
	- if O_D_CDMA2000_HRPD then	RQ63_005
	cdma2000hrpdSupportedReleas	RQ63_006
	e is set to the highest release as	RQ65_001
	defined in	RQ65_002
	#IUT_CDMA2000_HRPD_REL.	RQ65_003
	The value R is either 1, 2 or 3 for	RQ65_004
	Rev 0, A or B respectively.	RQ65_005 RQ65_006
	– if O_D_CDMA2000_EHRPD	RQ65_007
	then cdma2000ehrpdSupportedRelea	RQ65_008
	se is set to the highest release	RQ65_009
	as defined in	RQ65_022
	#IUT_CDMA2000_EHRPD_REL	RQ65_028
	if O_D_LTE then	
	eutranSupportedRelease is set	
	to the highest release as defined	
	in #IUT_LTE_EUTRAN_REL.	
	- if O_D_NFC_TS26 then	
	contactlessSupportedRelease is set to the highest release as	
	defined in #IUT_NFC_REL.	
	- if O_D_CRL then	
	rspCrlSupportedVersion is set to	
	the highest release as defined in	
	#IUT_RSP_VERSION .	
	For each of the options	
	O_D_GSM_GERAN,	
	O_D_UMTS_UTRAN,	
	O_D_CDMA2000_1X,	

V1.4 Page 444 of 777

			O_D_CDMA2000_HRPD, O_D_CDMA2000_EHRPD, O_D_LTE, O_D_NFC_TS26 or O_D_CRL, if the option is not set, verify that the corresponding field in DeviceCapabilities is not present.	
2	S_SM-DS → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_DS_OK1)	No Error	RQ31_062, RQ31_065, RQ31_095

Test Sequence #02 Nominal: Authenticate Client with MatchingID set to EventID

Initial Conditions	Initial Conditions		
Entity	Description of the initial condition		
S_SM-DS	The Alternative S_SM-DS(2) (#TEST_DS_ADDRESS1) performed Profile download Event Registration to the root S_SM-DS(1) (#TEST_ROOT_DS_ADDRESS) with #EVENT_ID_1 for #EID1		
S_SM-DS	S_SM-DP+ (#TEST_DP_ADDRESS1) performed Profile download Event Registration to the Alternative S_SM-DS(2) (#TEST_DS_ADDRESS1) with #EVENT_ID_2 for #EID1		
S_SM-DP+	There is a pending Profile download order for #EVENT_ID_2 (PROFILE_OPERATIONAL1) (see Note)		

Note: in order to avoid potentially misleading errors on LUI, the S_SM-DP+ SHALL be available to the LPAd for profile download during test sequence execution. The test tool SHALL NOT check the ES9+ communication.

Step	Direction	Sequence/ Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTI	H on ES11	
IC2	LPAd → S_SM-DS(1)	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	
1	S_SM-DS(1) → LPAd	MTD_HTTP_RESP(#INITIAT E_AUTH_DS_OK)	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #R_AUTH_SERVER_DS_MATCH _ID_DEV_INFO)) Verify: • if <matching_id> is empty</matching_id></s_transaction_id>	RQ31_078
2	S_SM-DS(1) → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_DS_OK_D SADDR1)	No Error	RQ31_062 RQ31_065 RQ31_095

V1.4 Page 445 of 777

3	PROC_TLS_INITIALIZATION_SERVER_AUTH on with #TEST_DS_ADDRESS1 and #CERT_S_SM_DS2_TLS			ES11
4	LPAd → S_SM-DS(2)	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DS_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DS_ADDRESS1)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	
5	S_SM-DS(2) → LPAd	MTD_HTTP_RESP(#INITIAT E_AUTH_DS_OK_1)	MTD_HTTP_REQ(#TEST_DS_AD DRESS1 , #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(< S_TRANSACTION_ID>, #R_AUTH_SERVER_DS_MATCH_ID_DEV_INFO_1)) Verify: • if <matching_id> is set to #EVENT_ID_1</matching_id>	RQ31_078 RQ36_018 RQ36_020
6	S_SM-DS(2) → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_DS_OK2)	No Error	RQ31_062 RQ31_065 RQ31_095

4.4.28.2.2TC_LPAd_ES11_AuthenticateClient_ErrorCases

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	
Device	The Profile Download is initiated using SM-DS (see section 2.2.4.1)	
S_SM-DP+	There is a pending Profile download order for #EVENT_ID_1 (PROFILE_OPERATIONAL1) (see Note)	
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state	
eUICC	There is no default SM-DP+ address configured	
No. 11 COMPD 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		

Note: the S_SM_DP+ does not need to be available to the LPAd for profile download during test sequence execution, as the LPAd is not expected to receive the smdpAddress.

Test Sequence #01 Error: Invalid EUM Certificate

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES11			
IC2	PROC_ES11_INIT_AUTH				
1	LPAd → S_SM-DS	Send ES11.AuthenticateClient method	MTD_HTTP_REQ(#TEST_ROOT_D S_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_ TRANSACTION_ID>,</s_ 		

V1.4 Page 446 of 777

			#R_AUTH_SERVER_DS_MATCH_I D_DEV_INFO))	
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERRO R_8_1_2_6_1)	LPAd aborts AddProfile procedure	RQ31_061
3	LPAd → S_SM-DS	No Profile download action	No requests are sent on ES11 within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT in Annex F.	RQ58_030 RQ58_039

Test Sequence #02 Error: Expired EUM Certificate

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH	on ES11	
IC2	PROC_ES11_	INIT_AUTH		
1	LPAd → S_SM-DS	Send ES11.AuthenticateClient method	MTD_HTTP_REQ(#TEST_ROOT_D S_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s _TRANSACTION_ID>, #R_AUTH_SERVER_DS_MATCH_I D_DEV_INFO))</s 	
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERRO R_8_1_2_6_3)	LPAd aborts AddProfile procedure	RQ31_061
3	LPAd → S_SM-DS	No Profile download action	No requests are sent on ES11 within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT in Annex F.	RQ58_030 RQ58_039

Test Sequence #03 Error: Invalid eUICC Certificate

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH	on ES11	
IC2	PROC_ES11_	INIT_AUTH		
1	LPAd → S_SM-DS	Send ES11.AuthenticateClient method	MTD_HTTP_REQ(#TEST_ROOT_D S_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_ TRANSACTION_ID>, #R_AUTH_SERVER_DS_MATCH_I D_DEV_INFO))</s_ 	
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERRO R_8_1_3_6_1)	LPAd aborts AddProfile procedure	RQ31_061
3	LPAd → S_SM-DS	No Profile download action	No requests are sent on ES11 within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT in Annex F.	RQ58_030 RQ58_039

V1.4 Page 447 of 777

Test Sequence #04 Error: Expired eUICC Certificate

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH or	n ES11	
IC2	PROC_ES11_IN	IIT_AUTH		
1	LPAd → S_SM-DS	Send ES11.AuthenticateClient method	MTD_HTTP_REQ(#TEST_ROOT_D S_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_ TRANSACTION_ID>, #R_AUTH_SERVER_DS_MATCH_I D_DEV_INFO))</s_ 	
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERRO R_8_1_3_6_3)	LPAd aborts AddProfile procedure	RQ31_061
3	LPAd → S_SM-DS	No Profile download action	No requests are sent on ES11 within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT in Annex F.	RQ58_030 RQ58_039

Test Sequence #05 Error: Invalid eUICC signature or serverChallenge

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INIT	TIALIZATION_SERVER_AUTH	on ES11	
IC2	PROC_ES11_IN	IT_AUTH		
1	LPAd → S_SM-DS	Send ES11.AuthenticateClient method	MTD_HTTP_REQ(#TEST_ROOT_D S_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_ TRANSACTION_ID>, #R_AUTH_SERVER_DS_MATCH_I D_DEV_INFO))</s_ 	
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ER ROR_8_1_6_1)	LPAd aborts AddProfile procedure	RQ58_030 RQ58_039
3	LPAd → S_SM-DS	No Profile download action	No requests are sent on ES11 within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT in Annex F.	RQ58_030 RQ58_039

Test Sequence #06 Error: Unknown TransactionID

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES11			
IC2	PROC_ES11_INIT_AUTH			
1	LPAd → S_SM-DS	Send ES11.AuthenticateClient method	MTD_HTTP_REQ(#TEST_ROOT_D S_ADDRESS, #PATH_AUTH_CLIENT,	

V1.4 Page 448 of 777

			MTD_AUTHENTICATE_CLIENT(<s_ TRANSACTION_ID>,</s_ 	
			#R_AUTH_SERVER_DS_MATCH_I D_DEV_INFO))	
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERRO R_8_10_1_3_9)	LPAd aborts AddProfile procedure	RQ56_030
3	LPAd → S_SM-DS	No Profile download action	No requests are sent on ES11 within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT in Annex F.	RQ56_030 RQ56_041

Test Sequence #07 Error: Unknown Event Record

Initial Conditions		
Entity	Description of the initial condition	
S_SM-DS	The Alternative S_SM-DS (#TEST_DS_ADDRESS1) performed Profile download Event Registration to the root S_SM-DS (#TEST_ROOT_DS_ADDRESS) with #EVENT_ID_1 for #EID1	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_SERVER_AUTH	on ES11	
IC2	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	
IC3	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE _AUTH_DS_OK)	MTD_HTTP_REQ(#TEST_ROOT_DS _ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_ transaction_id="">, #R_AUTH_SERVER_DS_MATCH_ID _DEV_INFO))</s_>	
IC4	S_SM-DS → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_DS_OK_DS ADDR1)	No Error	
IC5		NITIALIZATION_SERVER_AUTH S_ADDRESS1 and #CERT_S_SN	on //_DS2_TLS	ES11
IC6	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DS_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DS_ADDRESS1)) • Extract <euicc_challenge></euicc_challenge></euicc_challenge>	

V1.4 Page 449 of 777

IC7	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE _AUTH_DS_OK_1)	MTD_HTTP_REQ(#TEST_DS_ADDR ESS1 , #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_ TRANSACTION_ID>, #R_AUTH_SERVER_DS_MATCH_ID _DEV_INFO_1))</s_ 	
1	S_SM-DS → LPAd	MTD_HTTP_RESP(#R_ERRO R_8_9_5_3_9)	LPAd aborts AddProfile procedure	RQ31_090 RQ31_083
2	LPAd → S_SM-DS	No Profile download action	No requests are sent on ES11 within the timeout #IUT_LPAd_SESSION_CLOSE_TIM EOUT in Annex F.	RQ58_035

4.4.29 ES11 (LPA -- SM-DS): HTTPS

4.4.29.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26_023, RQ26_024, RQ26_026, RQ26_027, RQ26_029, RQ31_032, RQ36_017
- RQ45_026, RQ45_028, RQ45_033
- RQ58_001, RQ58_002
- RQ60_001, RQ60_002, RQ61_001

4.4.29.2 Test Cases

4.4.29.2.1TC_LPAd_ES11_HTTPS_Nominal

General Initial Conditio	General Initial Conditions			
Entity	Description of the general initial condition			
Device	The protection of access to the LUI is disabled			
Device	The Profile Download is initiated using SM-DS (see section 2.2.4.1)			
S_SM-DS	S_SM-DP+ (#TEST_DP_ADDRESS1) performed Profile download Event Registration to the S_SM-DS (#TEST_ROOT_DS_ADDRESS) with #EVENT_ID_1			
eUICC	There is no default SM-DP+ address configured			

Test Sequence #01 Nominal: HTTPS Session Establishment

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#I UT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>) Verify if: • #IUT_TLS_VERSION SHALL be 1.2 or higher • <tls_cipher_suites></tls_cipher_suites></ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_024 RQ26_026 RQ31_032 RQ58_001

V1.4 Page 450 of 777

			SHALL contain at least TLS_ECDHE_ECDSA_WITH_ AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_ AES_128_CBC_SHA256	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS)</session_id_random>	MTD_TLS_CLIENT_KEY_EXC H_ETC(<client_tls_ephe M_KEY>)</client_tls_ephe 	RQ26_027 RQ31_032 RQ36_017 RQ45_026 RQ45_028 RQ45_033 RQ58_002
3	S_SM-DS → LPAd	Finalize TLS Handshake (send Server ChangeCipherSpec and Finished messages)	HTTPS connection established	RQ31_032 RQ58_001 RQ60_001 RQ60_002 RQ61_001

Test Sequence #02 Nominal: non-reuse of session keys

The purpose of this test sequence is to verify that the LPAd is not reusing ephemeral keys from the previous session.

Step	Direction	Sequence / Description	Expected result	REQ
IC1		PROC_TLS_INITIALIZATION_SERVER_AUTH on ES11 Extract <client_tls_ephem_key></client_tls_ephem_key>		
IC2	Power-off and	d Power-on the Device.		
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION,	RQ31_032
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE,	MTD_TLS_CLIENT_KEY_EXC H_ETC(<client_tls_ephe M_KEY>) Verify if</client_tls_ephe 	RQ31_032

V1.4 Page 451 of 777

		<pre><session_id_random>, #CERT_S_SM_DS_TLS)</session_id_random></pre>	• <client_tls_ephem_key> is different from the one used by LPAd in IC1</client_tls_ephem_key>	
З	S_SM-DS → LPAd	Finalize TLS Handshake (send Server ChangeCipherSpec and Finished messages)	HTTPS connection established	RQ31_032 RQ58_001 RQ60_001 RQ60_002 RQ61_001

4.4.29.2.2TC_LPAd_ES11_HTTPS_Error

General Initial Conditions			
Entity	Description of the general initial condition		
Device	The protection of access to the LUI is disabled		
Device	The Profile Download is initiated using SM-DS (see section 2.2.4.1)		
S_SM-DS	S_SM-DP+ (#TEST_DP_ADDRESS1) performed Profile download Event Registration to the S_SM-DS (#TEST_ROOT_DS_ADDRESS) with #EVENT_ID_1		
eUICC	There is no default SM-DP+ address configured		

Test Sequence #01 Error: Invalid (SM-DS) TLS Certificate signature

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS_INV_SIG)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_026 RQ45_028
3	LPDd → S_SM-DS	TLS 1.2 close	A TLS alert is sent with Fatal-level	RQ26_023 RQ58_002

Test Sequence #02 Error: Expired TLS Certificate

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS_EXPIRED)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_026

V1.4 Page 452 of 777

	3	$\begin{array}{cc} LPDd & \to \\ S_SM\text{-DS} \end{array}$	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ58_002	
--	---	---	---------------	--	----------------------	--

Test Sequence #03 Error: Invalid TLS Certificate with critical extension not set

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS_INV_CRITIC AL_EXT)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_026
3	LPDd → S_SM-DS	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ58_002

Test Sequence #04 Error: Invalid TLS Certificate with invalid 'key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS_INV_KEY_U SAGE)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_033
3	LPDd → S_SM-DS	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ58_002

Test Sequence #05 Error: Invalid TLS Certificate with invalid 'extended key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS_INV_EXT_K EY_USAGE)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_033

V1.4 Page 453 of 777

Non-confidential

3	$\begin{array}{c} LPDd & \to \\ S_SM\text{-DS} \end{array}$	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ58_002	
---	--	---------------	---	----------------------	--

Test Sequence #06 Error: Invalid TLS Certificate with invalid 'Certificate Policies' extensions

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS_INV_CERT_POL)</session_id_random>	LPAd aborts AddProfile procedure	RQ31_032 RQ45_033
3	LPDd → S_SM-DS	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ58_002

Test Sequence #07 Error: Invalid TLS Certificate based on Invalid CI (Invalid Curve)

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SM-DS → LPAd	MTD_TLS_SERVER_HELLO_ETC(#T LS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SM_DS_TLS_INV_CURVE)</session_id_random>	LPAd aborts AddProfile procedure	RQ26_029 RQ31_032 RQ45_033
3	LPDd → S_SM-DS	TLS 1.2 close	The TLS connection is rejected. A TLS alert MAY be sent.	RQ26_023 RQ58_002

4.5 SM-DS Interfaces

4.5.1 ES12 (SM-DP+ -- SM-DS): RegisterEvent

4.5.1.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

 RQ36_004, RQ36_005, RQ36_006, RQ36_007, RQ36_008, RQ36_009, RQ36_010, RQ36_011, RQ36_012, RQ36_013,

V1.4 Page 454 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

- RQ59_003, RQ59_004, RQ59_005, RQ59_006, RQ59_007, RQ59_009, RQ59_010, RQ59_011, RQ59_012, RQ59_013, RQ59_014, RQ59_015
- RQ62_001, RQ62_002, RQ62_004, RQ62_005, RQ62_006, RQ62_007
- RQ65_001, RQ65_002, RQ65_003, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_030

4.5.1.2 Test Cases

4.5.1.2.1 TC_ROOT_SM_DS_ES12.RegisterEvent

General Initial Conditions			
Entity	ntity Description of the general initial condition		
Root SM-DS	 No TLS connections are established between the Root SM-DS and any of the simulator test tools. 		

Test Sequence #01 Nominal: EventID Registration to SM-DS without Event forwarding

The purpose of this test is to verify that the SM-DS can perform Event Registration without Event forwarding set.

Initial Conditions	
Entity	Description of the initial condition
Root SM-DS	#EVENT_ID_1 is not already used by the Root SM-DS

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	NITIALIZATION_MUTUAL_AUTH	on ES12	
1	S_SM-DP+ → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, FALSE))	MTD_HTTP_RESP(#R_SUCCES S)	RQ36_004 RQ36_005 RQ59_004 RQ59_006 RQ59_009 RQ59_011 RQ59_013 RQ59_014 RQ62_001 RQ62_002 RQ62_005 RQ62_006 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_030
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL		RQ36_004 RQ59_006

V1.4 Page 455 of 777

Test Sequence #02 Nominal: EventID Registration to SM-DS with Event forwarding

The purpose of this test is to verify that the SM-DS ignores the ForwardingIndicator and successfully performs Event Registration with Event forwarding set.

Initial Conditions		
Entity	Description of the initial condition	
Root SM-DS	#EVENT_ID_1 is not already used by the Root SM-DS	

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12				
1	S_SM-DP+ → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))	MTD_HTTP_RESP(#R_SUCCESS)	RQ59_003 RQ59_012 RQ62_001 RQ62_002		
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL		RQ36_004 RQ59_006		

Test Sequence #03 Error: Event Record Already Exists without Event Forwarding (Subject Code 8.9.5 Reason Code 3.3)

Initial Conditions		
Entity	Description of the initial condition	
Root SM-DS	#EVENT_ID_1 is already used by the Root SM-DS	

Step	Directio n	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_MUTUAL_AUTH	on ES12	
1	S_SM-DP+ → Root SM- DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, FALSE))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_3)	RQ59_005 RQ59_010 RQ59_015 RQ62_001 RQ62_002
2	S_LPAd → Root SM- DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL_ERROR		RQ59_005

V1.4 Page 456 of 777

4.5.1.2.2 TC_ALT_SM_DS_ES12.RegisterEvent

The test sequences in this section test the Alternative SM-DS acting as a Server on ES12 and a Client on ES15.

General Initial Conditions				
Entity Description of the general initial condition				
Alt. SM-DS	 No TLS connections are established between the Alternative SM-DS and any of the simulator test tools. 			

Test Sequence #01 Nominal: EventID Registration on Alternative SM-DS with Event forwarding

The purpose of this test is to verify that Alternative SM-DS can perform Event Registration with Event forwarding set.

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 is not already used by the Alternative SM-DS

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12		
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))		
2	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15		
3	Alt. SM-DS → S_SM-DS	Call ES15.RegisterEvent	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(<function_req_id>, <function_call_id>, #EID1, #IUT_SM_DS_ADDRESS, <event_id>, FALSE))</event_id></function_call_id></function_req_id>	RQ36_007 RQ36_008 RQ36_009 RQ36_010 RQ36_011 RQ36_012 RQ36_013 RQ59_002 RQ59_004 RQ59_006 RQ59_011 RQ62_001 RQ62_001 RQ62_004 RQ62_006 RQ62_006 RQ62_007

V1.4 Page 457 of 777

	S_SM-DS →	MTD_HTTP_RESP(#R_SUCCE		RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_030
4	S_SM-DS → Alt. SM-DS	SS) on ES15	No Error	
5	Alt. SM-DS → S_SM-DP+	Successful result is sent to the S_SM-DP+	MTD_HTTP_RESP(#R_SUCCES S) on ES12	RQ36_007 RQ36_008 RQ36_009 RQ36_010 RQ36_011 RQ36_012 RQ36_013 RQ59_009 RQ59_013 RQ59_014 RQ62_001 RQ62_002 RQ62_005 RQ62_006 RQ65_001 RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009
6	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_3)	RQ36_009 RQ59_006

Test Sequence #02 Nominal: Uniqueness of EventID Registration by Alternative SM-DS with Event forwarding

The purpose of this test is to verify that Alternative SM-DS can perform Event Registration using a unique EventID2 value with Event forwarding set.

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 is not already used by the Alternative SM-DS

V1.4 Page 458 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	TUAL_AUTH on ES12	
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))		
2	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MU	TUAL_AUTH on ES15	
3	Alt. SM-DS → S_SM-DS	Call ES15.RegisterEvent	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(<function_req_id>, <function_call_id>, #EID1, #IUT_SM_DS_ADDRESS, <event_id>, FALSE)) Extract the value of <event_id></event_id></event_id></function_call_id></function_req_id>	RQ36_006 RQ62_001 RQ62_002
4	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_SUCCE SS) on ES15	No Error	
5	Alt. SM-DS → S_SM-DP+	Successful result is sent to the S_SM-DP+	MTD_HTTP_RESP(#R_SUCCES S) on ES12	RQ36_006 RQ62_001 RQ62_002
6	S_SM-DP+ → Alt. SM-DS	Close TLS session on ES12 (unles closed TLS session)	ss Alternative SM-DS has already	
7	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	TUAL_AUTH on ES12	
8	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_2, TRUE))		
9	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MU	TUAL_AUTH on ES15	
10	Alt. SM-DS → S_SM-DS	Call ES15.RegisterEvent	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(<function_req_id>,</function_req_id>	RQ36_006 RQ62_001 RQ62_002

V1.4 Page 459 of 777

	<function_call_id>, #EID1,</function_call_id>	
	#IUT_SM_DS_ADDRESS,	
	<event_id>,</event_id>	
	FALSE))	
	Verify that <event_id> in step 3</event_id>	
	is not equal to <event_id></event_id>	

Test Sequence #03 Error: SM-DS registration failed, Root SM-DS unavailable (Subject Code 8.9 Reason Code 5.1)

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 is not already used by the Alternative SM-DS

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12		
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))		
2	Alt. SM-DS → S_SM-DS	TLS communication is initiated with S_SM-DS	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, <ext_sha256_ecdsa>) No TLS response from S_SM-DS</ext_sha256_ecdsa>	RQ36_010
3	Alt. SM-DS → S_SM-DP+	Wait for #IUT_SM_DS_TLS_TIMEOUT to expire.	MTD_HTTP_RESP(#R_ERROR_8_9_5_1)	RQ59_005 RQ59_007 RQ59_010 RQ59_015 RQ62_001 RQ62_002
4	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12		
5	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1,		

V1.4 Page 460 of 777

		#EVENT_ID_1, TRUE))		
6	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15		
7	Alt. SM-DS → S_SM-DS	Call ES15.RegisterEvent	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(<function_req_id>, <function_call_id>, #EID1, #IUT_SM_DS_ADDRESS, <event_id>, FALSE))</event_id></function_call_id></function_req_id>	RQ59_007 RQ62_001 RQ62_002
8	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_SUCCE SS) on ES15	No Error	
9	Alt. SM-DS → S_SM-DP+	Successful result is sent to the S_SM-DP+	MTD_HTTP_RESP(#R_SUCCES S) on ES12	RQ59_007 RQ62_001 RQ62_002

Test Sequence #04 Error: SM-DS registration failed, Root SM-DS error (Subject Code 8.9 Reason Code 4.2)

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 is not already used by the Alternative SM-DS for #EID1

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM- DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12		
1	S_SM-DP+ → Alt. SM- DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))		
2	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15		
3	Alt. SM-DS → S_SM-DS	Call ES15.RegisterEvent	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(<function_req_id>, <function_call_id>,</function_call_id></function_req_id>	RQ36_007 RQ36_008 RQ36_009 RQ36_010 RQ36_011

V1.4 Page 461 of 777

			#EID1, #IUT_SM_DS_ADDRESS,	RQ36_012 RQ36_013
			<event_id>, FALSE))</event_id>	RQ59_002 RQ59_004 RQ59_006 RQ59_011 RQ62_001
				RQ62_002 RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_030
4	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_ERROR_1_2_4_2)	No Error	
5	Alt. SM-DS → S_SM- DP+	SM-DS forwards error response back to S_SM-DP+	MTD_HTTP_RESP(#R_ERROR_8_9_4_2)	RQ59_005 RQ59_007 RQ59_010 RQ59_015 RQ62_001 RQ62_002
6	S_SM-DP+ → Alt. SM- DS	Close TLS session on ES12 (unl closed TLS session)	ess Alternative SM-DS has already	
7	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12		
8	S_SM-DP+ → Alt. SM- DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))		
9	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15		
10	Alt. SM-DS → S_SM-DS	Call ES15.RegisterEvent	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(<function_req_id>, <function_call_id>, #EID1, #IUT_SM_DS_ADDRESS, <event_id>, FALSE))</event_id></function_call_id></function_req_id>	RQ36_009 RQ62_001 RQ62_002

V1.4 Page 462 of 777

Non-confidential

11	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_SUCC ESS) on ES15	No Error	
12	Alt. SM-DS → S_SM- DP+	Successful result is sent to the S_SM-DP+	MTD_HTTP_RESP(#R_SUCCES S) on ES12	RQ36_009 RQ62_001 RQ62_002

Test Sequence #05 Error: Event Record Already Exists on Alternative SM-DS (Subject Code 8.9.5 Reason Code 3.3)

Initial Conditions	
Entity	Description of the initial condition
SM-DS	#EVENT_ID_1 is already used by the Alternative SM-DS.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	TUAL_AUTH on ES12	
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_DP_ADDRESS1, #EVENT_ID_1, TRUE))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_3)	RQ59_005 RQ59_007 RQ59_010 RQ59_015 RQ62_001 RQ62_002

4.5.2 ES12 (SM-DS -- SM-DP+): DeleteEvent

4.5.2.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ36_024, RQ36_025, RQ36_025_1, RQ36_027, RQ36_028, RQ36_029, RQ36_030, RQ36_031, RQ36_032
- RQ510_019, RQ510_020
- RQ59_016, RQ59_016_1, RQ59_017, RQ59_017_1, RQ59_017_2, RQ59_018, RQ59_019, RQ59_021, RQ59_022, RQ59_023, RQ59_024, RQ59_025
- RQ62_001, RQ62_002, RQ62_004, RQ62_005, RQ62_006, RQ62_007
- RQ65_001, RQ65_002, RQ65_003, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_031

V1.4 Page 463 of 777

4.5.2.2 Test Cases

4.5.2.2.1 TC_ROOT_SM_DS_ES12.DeleteEvent

Test Sequence #01 Nominal: Event Deletion

The purpose of this test is to verify that the Root SM-DS can perform Event Deletion.

Initial Conditions	
Entity	Description of the initial condition
Root SM-DS	#EVENT_ID_1 was registered for #EID1 and #TEST_DP_ADDRESS1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	ITIALIZATION_MUTUAL_AUTH or	ES12	
1	S_SM-DP+ → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_SUCCE SS)	RQ36_024 RQ36_025 RQ36_025_1 RQ36_029 RQ36_030 RQ59_016 RQ59_021 RQ59_023 RQ59_024 RQ510_019 RQ62_001 RQ62_002 RQ62_005 RQ62_006 RQ65_001 RQ65_002 RQ65_003 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_031
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_I	RETRIEVAL_ERROR	RQ36_025 RQ36_029 RQ59_017_1

Test Sequence #02 Error: Event Record Does Not Exist (Subject Code 8.9.5 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
Root SM-DS	#EVENT_ID_1 is not registered

V1.4 Page 464 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	ITIALIZATION_MUTUAL_AUTH on	ES12	
1	S_SM-DP+ → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ59_016_1 RQ59_022 RQ59_025 RQ510_020 RQ62_001 RQ62_002

Test Sequence #03 Error: Event Record Does Not Match OID (Subject Code 8.9.5 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 was registered for #EID1 and #TEST_DP_ADDRESS1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Root SM-DS	PROC_TLS_INITIALIZATION_MU	ITUAL_AUTH_INV_OID on ES12	
1	S_SM-DP+ → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ59_016_1 RQ59_022 RQ59_025 RQ510_020 RQ62_001 RQ62_002
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL		RQ59_016_1

4.5.2.2.2 TC_ALT_SM_DS_ES12.DeleteEvent

The test sequences in this section test the Alternative SM-DS acting as a Server on ES12 and a Client on ES15.

General Initial Conditions		
Entity	Description of the general initial condition	
Alt. SM-DS	 No TLS connections are established between the Alternative SM-DS and any of the simulator test tools. 	

Test Sequence #01 Nominal: Cascaded Event Deletion on Alternative SM-DS

The purpose of this test is to verify that Alternative SM-DS can perform cascaded Event Deletion.

V1.4 Page 465 of 777

Non-confidential

Initial Conditions		
Entity	Description of the initial condition	
Alt. SM-DS	#EVENT_ID_1 registration for #EID1 and #TEST_DP_ADDRESS1 was cascaded using <event_id_r> to the Root SM-DS</event_id_r>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12	
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))		
2	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MU	ITUAL_AUTH on ES15	
3	Alt. SM-DS → S_SM-DS	Call ES15.DeleteEvent	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(<function_req_id>, <function_call_id>, #EID1, <event_id>)) Verify that <event_id> is equal to <event_id_r></event_id_r></event_id></event_id></function_call_id></function_req_id>	RQ36_027 RQ36_028 RQ36_031 RQ36_032 RQ59_016 RQ59_017 RQ59_017_2 RQ59_023 RQ62_001 RQ62_002 RQ62_004 RQ62_006 RQ62_007 RQ65_001 RQ65_002 RQ65_003 RQ65_003 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_009 RQ65_031
4	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_SUCCESS) on ES15	No Error	RQ510_019
5	Alt. SM-DS → S_SM-DP+	SM-DS sends response back to S_SM-DP+	MTD_HTTP_RESP(#R_SUCCESS) on ES12	RQ36_027 RQ36_028 RQ36_031 RQ36_032 RQ59_016 RQ59_021 RQ59_024 RQ510_019 RQ62_001 RQ62_001 RQ62_005 RQ62_005

V1.4 Page 466 of 777

				RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_031
6	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ36_031 RQ59_019 RQ510_020 RQ62_001 RQ62_002

Test Sequence #02 Nominal: Cascaded Event Deletion, Event Record not found on Root SM-DS

The purpose of this test is to verify that if cascaded deletion fails because the Event Record was not found in the Root SM-DS the Alternative SM-DS can ignore this error case and continue.

Initial Conditions		
Entity	Description of the initial condition	
Alt. SM-DS	#EVENT_ID_1 registration for #EID1 and #TEST_DP_ADDRESS1 was cascaded using <event_id_r> to the Root SM-DS</event_id_r>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12		
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))		
2	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15		
3	Alt. SM-DS → S_SM-DS	Call ES15.DeleteEvent	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(<function_req_id>, <function_call_id>, #EID1, <event_id>))</event_id></function_call_id></function_req_id>	RQ36_027 RQ36_028 RQ36_031 RQ36_032 RQ59_016 RQ59_017 RQ59_017_2 RQ59_023 RQ62_001 RQ62_002

V1.4 Page 467 of 777

			Verify that <event_id> is equal to <event_id_r></event_id_r></event_id>	RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_031
4	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	No Error	RQ510_020 RQ62_001 RQ62_002
5	Alt. SM-DS → S_SM-DP+	SM-DS sends response back to S_SM-DP+	MTD_HTTP_RESP(#R_SUCCESS) on ES12	RQ59_021 RQ59_024 RQ510_019 RQ62_001 RQ62_002
6	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ36_031 RQ59_018 RQ510_020 RQ62_001 RQ62_002

Test Sequence #03 Error: Cascaded Event Deletion failed, Root SM-DS Unavailable (Subject Code 8.9 Reason Code 5.1)

Initial Conditions		
Entity	Description of the initial condition	
Alt. SM-DS	#EVENT_ID_1 registration for #EID1 and #TEST_DP_ADDRESS1 was cascaded using <event_id_r> to the Root SM-DS</event_id_r>	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES12		
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))		
2	Alt. SM-DS → S_SM-DS	TLS communication is initiated with S_SM-DS	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, <ext_sha256_ecdsa>) No TLS response from S_SM-DS</ext_sha256_ecdsa>	RQ36_028

V1.4 Page 468 of 777

3	Alt. SM-DS → S_SM-DP+	Wait for #IUT_SM_DS_TLS_TIMEOUT to expire.	MTD_HTTP_RESP(#R_ERROR_8_9_5_1)	RQ59_016_1 RQ59_018 RQ59_022 RQ59_025 RQ62_001 RQ62_002
4	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	ITUAL_AUTH on ES12	
5	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))		
6	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15		
7	Alt. SM-DS → S_SM-DS	Call ES15.DeleteEvent	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(<function_req_id>, <function_call_id>, #EID1, <event_id>)) Verify that <event_id> is equal to <event_id_r></event_id_r></event_id></event_id></function_call_id></function_req_id>	RQ59_018 RQ62_001 RQ62_002
8	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_SUCCESS) on ES15	No Error	RQ510_019 RQ62_001 RQ62_002
9	Alt. SM-DS → S_SM-DP+	SM-DS sends response back to S_SM-DP+	MTD_HTTP_RESP(#R_SUCCESS) on ES12	RQ59_018 RQ510_019 RQ62_001 RQ62_002

Test Sequence #04 Error: Cascaded Event Deletion failed, Root SM-DS execution error (Subject Code 8.9 Reason Code 4.2)

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 registration for #EID1 and #TEST_DP_ADDRESS1 was cascaded using <event_id_r> to the Root SM-DS</event_id_r>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	TUAL_AUTH on ES12	

V1.4 Page 469 of 777

1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))		
2	Alt. SM-DS → S_SM-DS	PROC_TLS_INITIALIZATION_MU	TUAL_AUTH on ES15	
3	Alt. SM-DS → S_SM-DS	Call ES15.DeleteEvent	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(<function_req_id>, <function_call_id>, #EID1, <event_id>))</event_id></function_call_id></function_req_id>	RQ36_027 RQ36_028 RQ36_031 RQ36_032 RQ59_016 RQ59_017 RQ59_017_2 RQ59_023 RQ62_001 RQ62_002 RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009
4	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_ERROR_1_2_4_2)	No Error	RQ510_020 RQ62_001 RQ62_002
5	Alt. SM-DS → S_SM-DP+	SM-DS sends response back to S_SM-DP+	MTD_HTTP_RESP(#R_ERROR_8_9_4_2)	RQ59_018 RQ59_022 RQ59_025 RQ510_020 RQ62_001 RQ62_002

Test Sequence #05 Error: Event Record Does Not Match OID (Subject Code 8.9.5 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 registration for #EID1 and #TEST_DP_ADDRESS1 was cascaded using <event_id_r> to the Root SM-DS.</event_id_r>

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	ITUAL_AUTH_INV_OID on ES12	

V1.4 Page 470 of 777

1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ59_016_1 RQ59_022 RQ59_025 RQ510_020 RQ62_001 RQ62_002
2	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	JTUAL_AUTH on ES12	
3	Alt. SM-DS → S_SM-DS	Call ES15.DeleteEvent	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(<function_req_id>, <function_call_id>, #EID1, <event_id>))</event_id></function_call_id></function_req_id>	RQ59_016_1 RQ62_001 RQ62_002
4	S_SM-DS → Alt. SM-DS	MTD_HTTP_RESP(#R_SUCCESS) on ES15	No Error	RQ510_019 RQ62_001 RQ62_002
5	Alt. SM-DS → S_SM-DP+	SM-DS sends response back to S_SM-DP+	MTD_HTTP_RESP(#R_SUCCESS) on ES12	RQ59_016_1 RQ510_019 RQ62_001 RQ62_002

4.5.2.2.3 TC_ALT_SM_DS_ES12.DeleteEvent_Error_Nonexistant_EventID

General Initial Condition	General Initial Conditions	
Entity	Description of the general initial condition	
Alt. SM-DS	 No TLS connections are established between the Alternative SM-DS and any of the simulator test tools. 	

Test Sequence #01 Error: Event Record Does Not Exist (Subject Code 8.9.5 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 is not registered

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DP+ → Alt. SM-DS	PROC_TLS_INITIALIZATION_MU	ITUAL_AUTH on ES12	
1	S_SM-DP+ → Alt. SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DP+_F_REQ_ID,	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ59_016_1 RQ59_022 RQ59_025 RQ510_020

V1.4 Page 471 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

#FUNCTION_CALL_ID_1,	RQ62_001
#EID1,	RQ62_002
#EVENT_ID_1))	

4.5.3 ES15 (SM-DS -- SM-DS): RegisterEvent

4.5.3.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ36_005, RQ36_010, RQ36_011, RQ36_012
- RQ62_001, RQ62_002, RQ62_005, RQ62_006
- RQ65_001, RQ65_002, RQ65_003, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_030
- RQ510_003, RQ510_004, RQ510_005, RQ510_006, RQ510_009, RQ510_010, RQ510_011, RQ510_012, RQ510_013, RQ510_014, RQ510_015

4.5.3.2 Test Cases

4.5.3.2.1 TC_ROOT_SM_DS_ES15.RegisterEvent

General Initial Conditions		
Entity	Description of the general initial condition	
Root SM-DS	 No TLS connections are established between the Root SM-DS and any of the simulator test tools. 	

Test Sequence #01 Nominal: EventID Registration to SM-DS with Event forwarding

The purpose of this test is to verify that the Root SM-DS ignores the ForwardingIndicator and successfully performs Event Registration with Event forwarding set.

Initial Conditions	
Entity	Description of the initial condition
Root SM-DS	#EVENT_ID_1 is not already used by the Root SM-DS

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15			
1	S_SM-DS → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DS_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_ALT_DS_ADDRESS,	MTD_HTTP_RESP(#R_SUCCESS)	RQ510_003 RQ510_012 RQ62_001 RQ62_002

V1.4 Page 472 of 777

		#EVENT_ID_1, TRUE))	
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL	RQ36_011

Test Sequence #02 Nominal: EventID Registration to SM-DS without Event forwarding

The purpose of this test is to verify that the Root SM-DS successfully performs Event Registration with Event without Event forwarding set.

Initial Conditions	
Entity	Description of the initial condition
Root SM-DS	#EVENT_ID_1 is not already used by the Root SM-DS

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_IN	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15			
1	S_SM-DS → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DS_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_ALT_DS_ADDRESS, #EVENT_ID_1, FALSE))	MTD_HTTP_RESP(#R_SUCCESS)	RQ36_010 RQ36_011 RQ36_012 RQ510_004 RQ510_006 RQ510_009 RQ510_011 RQ510_014 RQ62_001 RQ62_002 RQ62_005 RQ62_006 RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_008 RQ65_009 RQ65_009	
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_F	RETRIEVAL	RQ36_011	

Test Sequence #03 Error: Event Record Already Exists without Event Forwarding (Subject Code 8.9.5 Reason Code 3.3)

Initial Conditions		
Entity	Description of the initial condition	
Root SM-DS	#EVENT_ID_1 is already used by the Root SM-DS	

V1.4 Page 473 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15			
1	S_SM-DS → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#S_SM_DS_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #TEST_ALT_DS_ADDRESS, #EVENT_ID_1, FALSE))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_3)	RQ510_005 RQ510_010 RQ510_015 RQ62_001 RQ62_002
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL_ERROR		RQ36_005

4.5.4 ES15 (SM-DS -- SM-DS): DeleteEvent

4.5.4.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ36_028, RQ36_029, RQ36_030, RQ36_031
- RQ62_001, RQ62_002, RQ62_005, RQ62_006
- RQ65_001, RQ65_002, RQ65_003, RQ65_005, RQ65_007, RQ65_008, RQ65_009, RQ65_031
- RQ510_016, RQ510_016_1, RQ510_021, RQ510_022, RQ510_023, RQ510_024, RQ510_025

4.5.4.2 Test Cases

4.5.4.2.1 TC_ROOT_SM_DS_ES15.DeleteEvent

General Initial Conditions			
Entity	ntity Description of the general initial condition		
Root SM-DS	No TLS connections are established between the Alternative SM-DS and any of the simulator test tools.		

Test Sequence #01 Nominal: Event Deletion

The purpose of this test is to verify that the Root SM-DS can perform Event Deletion.

Initial Conditions		
Entity	Description of the initial condition	
Root SM-DS	#EVENT_ID_1 was registered for #EID1 and #TEST_DP_ADDRESS1.	

V1.4 Page 474 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15			
1	S_SM-DS → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DS_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_SUCCESS)	RQ36_028 RQ36_029 RQ36_030 RQ62_001 RQ62_002 RQ62_006 RQ65_001 RQ65_002 RQ65_003 RQ65_005 RQ65_007 RQ65_007 RQ65_008 RQ65_009 RQ65_031 RQ510_016 RQ510_021 RQ510_023 RQ510_024
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL_ERROR		RQ36_031

Test Sequence #02 Error: Event Record Does Not Exist (Subject Code 8.9.5 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
Root SM-DS	#EVENT_ID_1 is not registered

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_MUTUAL_AUTH on ES15			
1	S_SM-DS → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DS_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ510_016_1 RQ510_022 RQ510_025 RQ62_001 RQ62_002

Test Sequence #03 Error: Event Record Does Not Match OID (Subject Code 8.9.5 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
Alt. SM-DS	#EVENT_ID_1 was registered for #EID1 and #TEST_DP_ADDRESS1.

V1.4 Page 475 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_SM-DS → Root SM-DS	PROC_TLS_INITIALIZATION_MUTUAL_AUTH_INV_OID on ES15		
1	S_SM-DS → Root SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_DELETE_EVENT, MTD_DELETE_EVENT(#S_SM_DS_F_REQ_ID, #FUNCTION_CALL_ID_1, #EID1, #EVENT_ID_1))	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ510_016_1 RQ510_022 RQ510_025 RQ62_001 RQ62_002
2	S_LPAd → Root SM-DS	PROC_ES11_VERIFY_EVENT_RETRIEVAL		RQ510_016_1

4.5.5 ES11 (LPA -- SM-DS): InitiateAuthentication

4.5.5.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26_033
- RQ31_030, RQ31_033, RQ31_034, RQ31_035, RQ31_036, RQ31_037, RQ31_038, RQ31_039, RQ31_041, RQ31_042, RQ31_043, RQ31_073
- RQ57_106
- RQ58_003, RQ58_004, RQ58_005, RQ58_006, RQ58_007, RQ58_008, RQ58_010, RQ58_011, RQ58_012, RQ58_013, RQ58_014, RQ58_015, RQ58_016, RQ58_017, RQ58_018, RQ58_019, RQ58_020
- RQ62_001, RQ62_002
- RQ65_018

4.5.5.2 Test Cases

4.5.5.2.1 TC_SM_DS_ES11.InitiateAuthenticationNIST

General Initial Conditions for SM-DS testing			
Entity	Description of the general initial condition		
SM-DS	SM-DS is configured with the #CERT_SM_DSauth_ECDSA for NIST		

Perform all test sequences defined in 4.3.12.2.1 with the following variables:

- Test Environment = TE_S1
- SERVER = SM-DS
 - CERT_SM_XXauth_ECDSA = CERT_SM_DSauth_ECDSA
 - PK_SM_XXauth_ECDSA = PK_SM_DSauth_ECDSA

V1.4 Page 476 of 777

4.5.6 ES11 (LPA -- SM-DS): Authenticate Client

4.5.6.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26_005, RQ26_006, RQ26_012, RQ26_014
- RQ31 058, RQ31 059, RQ31 060
- RQ36_017, RQ36_021, RQ36_022
- RQ45 006, RQ45 026, RQ45 026 1, RQ45 027, RQ45 028, RQ45 029
- RQ57_037, RQ57_108
- RQ58_025, RQ58_026, RQ58_027, RQ58_028, RQ58_029, RQ58_031, RQ58_036, RQ58_036_1, RQ58_037, RQ58_038, RQ58_039
- RQ62_001, RQ62_002
- RQ65_27, RQ65_028, RQ65_029

4.5.6.2 Test Cases

4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST

General Initial Conditions			
Entity	Entity Description of the general initial condition		
SM-DS	SM-DS is configured with the #CERT_SM_DSauth_ECDSA for NIST		

Test Sequence #01 Nominal Matching ID Empty for one pending Event

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with an empty Matching ID, and that Event Retrieval occurs for one pending Event.

Initial Conditions			
Entity	Description of the initial condition		
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	NITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE,	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 477 of 777

		#S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))		
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_MATC HING_ID_EMPTY))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVENT_ ENTRY_1_OK)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ36_021 RQ36_022 RQ45_026 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_025 RQ58_025 RQ58_025 RQ58_025 RQ58_027 RQ58_026 RQ58_027 RQ58_028 RQ58_027 RQ58_031 RQ58_031 RQ58_036 RQ58_037 RQ58_038 RQ58_037 RQ58_038 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #02 Nominal Matching ID Empty for two pending Events

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with an empty Matching ID, and that Event Retrieval occurs for any pending Events.

Initial Conditions			
Entity	Description of the initial condition		
SM-DS	 #EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1. #EVENT_ID_2 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS2. 		

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	INITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 478 of 777

		ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))		
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVENT_ ENTRY_MULTI_OK)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ36_021 RQ36_022 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_025 RQ58_026 RQ58_027 RQ58_026 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_029 RQ58_031 RQ58_036 RQ58_037 RQ58_036 RQ58_037 RQ58_038 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #03 Nominal Matching ID Empty for no pending Events

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with an empty Matching ID, and that Event Retrieval returns no pending Events.

Initial Conditions	
Entity	Description of the initial condition
SM-DS	No Events have been registered in the SM-DS for #EID1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH			
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 479 of 777

		#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))		
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_MATC HING_ID_EMPTY))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVENT_ ENTRY_EMPTY_OK)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ36_021 RQ36_022 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ57_108 RQ57_108 RQ58_025 RQ58_025 RQ58_025 RQ58_026 RQ58_027 RQ58_028 RQ58_027 RQ58_031 RQ58_032 RQ65_029

Test Sequence #04 Nominal Matching ID Omitted for one pending Event

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with the Matching ID omitted, and that Event Retrieval occurs for one pending Event.

Initial Conditions	
Entity	Description of the initial condition
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH			
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 480 of 777

		ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))		
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<\$_TRANSACTION_ID>, #AUTH_SERVER_RESP_MATC HING_ID_OMITTED))	MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVENT_ ENTRY_1_OK)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ36_021 RQ36_022 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ57_108 RQ58_025 RQ58_025 RQ58_025 RQ58_027 RQ58_026 RQ58_027 RQ58_028 RQ58_027 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_036 RQ58_037 RQ58_038 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #05 Nominal Matching ID Omitted for two pending Events

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with the Matching ID omitted, and that Event Retrieval occurs for any pending Events.

Initial Conditions	
Entity Description of the initial condition	
SM-DS	 #EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1. #EVENT_ID_2 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS2.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH			
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS,	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 481 of 777

		#PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))		
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_MATC HING_ID_OMITTED))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVENT_ ENTRY_MULTI_OK)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ36_021 RQ36_022 RQ45_026 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ57_037 RQ57_108 RQ57_037 RQ57_108 RQ58_025 RQ58_026 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_029 RQ58_031 RQ58_036 RQ58_037 RQ58_036 RQ58_037 RQ58_038 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #06 Nominal Matching ID Omitted for no pending Events

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with the Matching ID omitted, and that Event Retrieval returns no pending Events.

Initial Conditions		
Entity	Description of the initial condition	
SM-DS	No Events have been registered in the SM-DS for #EID1.	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH			
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS,	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 482 of 777

		#PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))		
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_MATC HING_ID_OMITTED))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVENT_ ENTRY_EMPTY_OK)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ36_021 RQ36_022 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_027 RQ57_037 RQ57_108 RQ57_037 RQ57_108 RQ58_025 RQ58_025 RQ58_025 RQ58_026 RQ58_027 RQ58_028 RQ58_027 RQ58_031 RQ58_031 RQ58_033 RQ58_031 RQ58_033 RQ58_031 RQ58_033 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_031 RQ58_032 RQ58_034 RQ58_035 RQ58_035 RQ58_036

Test Sequence #07 Nominal Matching ID containing EventID with one pending Event

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with a Matching ID containing an EventID, and that Event Retrieval occurs for the requested pending Event.

Initial Conditions		
Entity	ntity Description of the initial condition	
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_I	NITIALIZATION_SERVER_AUTH		

V1.4 Page 483 of 777

IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_MATC HING_ID_EVENT_ID))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVENT_ ENTRY_1_OK)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ36_021 RQ36_022 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_025 RQ58_025 RQ58_025 RQ58_027 RQ58_026 RQ58_027 RQ58_028 RQ58_027 RQ58_028 RQ58_027 RQ58_034 RQ58_034 RQ58_037 RQ58_038 RQ58_037 RQ58_038 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #08 Nominal Matching ID containing EventID with two pending Events

The purpose of this test is to verify that common mutual authentication between the SM-DS and the S_LPAd is performed successfully with a Matching ID containing an EventID, and that Event Retrieval occurs for only the requested pending Event.

Initial Conditions		
Entity	Description of the initial condition	
SM-DS	 #EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1. #EVENT_ID_2 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS2. 	

Repeat Test Sequence #07 Nominal Matching ID containing one Event with one pending Event.

V1.4 Page 484 of 777

Test Sequence #09 Error: Invalid EUM Certificate (Subject Code 8.1.2 Reason Code 6.1)

Initial Conditions				
Entity	Description of the initial condition			
SM-DS	 #EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1. 			

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	PROC_TLS_	PROC_TLS_INITIALIZATION_SERVER_AUTH				
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)			
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_2_6_1_SIG))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_0261 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_037 RQ58_039 RQ62_001 RQ62_001 RQ62_002 RQ65_028 RQ65_029		
2	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)			
3	PROC_TLS_	NITIALIZATION_SERVER_AUTH				
4	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE,	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)			

V1.4 Page 485 of 777

		#S_EUICC_INFO1,		
		#IUT_SM_DS_ADDRESS))		
5	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_2_6_1_EX_KU))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_030 RQ58_030 RQ58_030 RQ58_039 RQ65_028 RQ62_001 RQ62_002 RQ65_029
6	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)	
7	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
8	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
9	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_2_6_1_EX_CP))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_030 RQ58_037 RQ58_039 RQ62_001

V1.4 Page 486 of 777

				RQ62_002 RQ65_028 RQ65_029
10	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)	
11	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
12	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
13	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_2_6_1_EX_BC_cA))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_026 RQ45_026 RQ45_026_1 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_030 RQ58_036_1 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029
14	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)	
15	PROC_TLS_	I INITIALIZATION_SERVER_AUTH		
16	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
17	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>,</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059

V1.4 Page 487 of 777

	#AUTH_SERVER_RESP_SMDS	RQ31_060
	_8_1_2_6_1_EX_BC_PLC))	RQ36_017
		RQ45_006
		RQ45_026
		RQ45_026_1
		RQ45_027
		RQ45_028
		RQ45_029
		RQ57_037
		RQ57_108
		RQ58_030
		RQ58_036_1
		RQ58_037
		RQ58_039
		RQ65_028
		RQ62_001
		RQ62_002
		RQ65_029

Test Sequence #10 Error: Expired EUM Certificate (Subject Code 8.1.2 Reason Code 6.3)

Initial Conditions				
Entity	Description of the initial condition			
SM-DS	 #EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1. 			

Ste p	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_2_6_3))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_2_6_3)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_026

V1.4 Page 488 of 777

		RQ45_028
		RQ45_029
		RQ57_037
		RQ57_108
		RQ58_030
		RQ58_036_1
		RQ58_037
		RQ58_039
		RQ62_001
		RQ62_002
		RQ65_028
		RQ65_029

Test Sequence #11 Error: Invalid eUICC Certificate (Subject Code 8.1.3 Reason Code 6.1)

Initial Conditions	
Entity	Description of the initial condition
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH				
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_3_6_1_SIG))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_039 RQ58_039 RQ65_028 RQ65_028 RQ65_028	

V1.4 Page 489 of 777

				RQ62_002 RQ65_029
2	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)	
3	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
4	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
5	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_030 RQ58_036_1 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029
6	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)	
7	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
8	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
9	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_3_6_1_EX_CP))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060

V1.4 Page 490 of 777

				RQ36_017 RQ45_006 RQ45_026 RQ45_026_1 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029
10	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)	
11	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
12	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
13	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029
14	S_LPAd → SM-DS	Close TLS session (unless SM-DS	has already closed TLS session)	
15	PROC_TLS_	C_TLS_INITIALIZATION_SERVER_AUTH		

V1.4 Page 491 of 777

16	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
17	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_ERROR_8_1_3_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026_1 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #12 Error: Expired eUICC Certificate (Subject Code 8.1.3 Reason Code 6.3)

Initial Conditions		
Entity	Description of the initial condition	
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS,	MTD_HTTP_RESP(#R_ERROR_8_1_3_6_3)	RQ26_005 RQ26_006

V1.4 Page 492 of 777

	#PATH_AUTH_CLIENT,	RQ26_012
	MTD_AUTHENTICATE_CLIENT(RQ26_014
	<s_transaction_id>,</s_transaction_id>	RQ31_058
	#AUTH_SERVER_RESP_SMDS	RQ31_059
	_8_1_3_6_3))	RQ31_060
		RQ36_017
		RQ45_006
		RQ45_026
		RQ45_026_1
		RQ45_027
		RQ45_028
		RQ45_029
		RQ57_037
		RQ57_108
		RQ58_030
		RQ58_036_1
		RQ58_037
		RQ58_039
		RQ62_001
		RQ62_002
		RQ65_028
		RQ65_029

Test Sequence #13 Error: Invalid eUICC Signature (Subject Code 8.1 Reason Code 6.1)

Initial Conditions		
Entity	Description of the initial condition	
SM-DS	 #EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1. 	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	NITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_6_1_SIG))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029

V1.4 Page 493 of 777

RQ57_037
RQ57_108
RQ58_030
RQ58_036_1
RQ58_037
RQ58_039
RQ62_001
RQ62_002
RQ65_028
RQ65_029

Test Sequence #14 Error: Invalid Server Challenge (Subject Code 8.1 Reason Code 6.1)

Initial Conditions	
Entity	Description of the initial condition
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	PROC_TLS_INITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_1_6_1_CHA))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_6_1)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029

V1.4 Page 494 of 777

Test Sequence #15 Error: Unknown Transaction ID in JSON transport layer (Subject Code 8.10.1 Reason Code 3.9)

Initial Conditions		
Entity	Description of the initial condition	
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	PROC_TLS_INITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<invalid_transaction_id>, #AUTH_SERVER_RESP_MATC HING_ID_EMPTY))</invalid_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #16 Error: Unknown Transaction ID in ASN.1 euiccSigned1 payload (Subject Code 8.10.1 Reason Code 3.9)

Initial Conditions	
Entity	Description of the initial condition
SM-DS	#EVENT_ID_1 has been registered in the SM-DS with #EID1 and #TEST_DP_ADDRESS1.

V1.4 Page 495 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	PROC_TLS_INITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_SMDS _8_10_1_3_9))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_10_1_3_9)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_028 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029

Test Sequence #17 Error: Matching ID containing EventID with no pending Event

Initial Conditions	
Entity	Description of the initial condition
SM-DS	No Events have been registered in the SM-DS for #EID1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_	INITIALIZATION_SERVER_AUTH		
IC2	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 496 of 777

1	S_LPAd → SM-DS	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_MATC HING_ID_EVENT_ID))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	RQ26_005 RQ26_006 RQ26_012 RQ26_014 RQ31_058 RQ31_059 RQ31_060 RQ36_017 RQ45_006 RQ45_026 RQ45_026 RQ45_027 RQ45_027 RQ45_029 RQ57_037 RQ57_108 RQ58_030 RQ58_036_1 RQ58_037 RQ58_037 RQ58_039 RQ62_001 RQ62_002 RQ65_028 RQ65_029
---	-------------------	--	---------------------------------------	--

4.5.6.2.2 TC_SM-DS_ES11.AuthenticateClientBRP

General Initial Conditions		
Entity Description of the general initial condition		
SM-DS	SM-DS is configured with the #CERT_SM_DSauth_ECDSA for BrainpoolP256r1	

Test Sequence #01 Nominal Matching ID Empty for one pending Event

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #02 Nominal Matching ID Empty for two pending Events

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #03 Nominal Matching ID Empty for no pending Events

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

V1.4 Page 497 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #04 Nominal Matching ID Omitted for one pending Event

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #05 Nominal Matching ID Omitted for two pending Events

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #06 Nominal Matching ID Omitted for no pending Events

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #07 Nominal Matching ID containing EventID with one pending Event

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

Test Sequence #08 Nominal Matching ID containing EventID with two pending Events

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.5.6.2.1 TC_SM-DS_ES11.AuthenticateClientNIST except that all keys and certificates SHALL be based on BrainpoolP256r1.

4.5.7 ES15 (SM-DS -- SM-DS): TLS, Mutual Authentication, Client, Session Establishment

4.5.7.1 TC_ALT_SMDS_ES15_Client_Mutual_Authentication_for_HTTPS_EstablishmentNIST

Perform all test sequences defined in section 4.6.1.2.1 with the following variables set as follows:

- CLIENT = Alternative SM-DS under test
 - CERT_CLIENT_TLS = #CERT_SM_DS_TLS for NIST
- SERVER = Root S_SM-DS
 - CERT_S_SERVER_TLS = #CERT_S_SM_DS_TLS for NIST

V1.4 Page 498 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

4.5.7.2 TC_ALT_SMDS_ES15_Client_Mutual_Authentication_for_HTTPS_EstablishmentBRP

Perform all test sequences defined in section 4.6.1.2.2 with the following variables set as follows:

- CLIENT = Alternative SM-DS under test
 - CERT CLIENT TLS = #CERT SM DS TLS for BRP
- SERVER = Root S_SM-DS
 - CERT S SERVER TLS = #CERT S SM DS TLS for BRP

4.5.8 ES12 (SM-DS -- SM-DP+): TLS, Mutual Authentication, Server, Session Establishment

4.5.8.1 TC_SM-

DS_ES12_Server_Mutual_Authentication_for_HTTPS_EstablishmentNIST

Perform all test sequences defined in section 4.6.2.2.1 with the following variables set as follows:

- CLIENT = S SM-DP+
 - CERT_S_CLIENT_TLS = CERT_S_SM_DP_TLS for NIST
- SERVER = Alternative or Root SM-DS under test.
 - CERT_SERVER_TLS = CERT_SM_DS_TLS for NIST
- 4.5.8.2 TC SM-

DS_ES12_Server_Mutual_Authentication_for_HTTPS_EstablishmentBRP

Perform all test sequences defined in section 4.6.2.2.2 with the following variables set as follows:

- CLIENT = S_SM-DP+
 - o CERT_S_CLIENT_TLS = CERT_S_SM_DP_TLS for BRP
- SERVER = Alternative or Root SM-DS under test.
 - CERT_SERVER_TLS = CERT_SM_DS_TLS for BRP
- 4.5.9 ES15 (SM-DS -- SM-DS): TLS, Mutual Authentication, Server, Session Establishment
- 4.5.9.1 TC_ROOT_SM-

DS_ES15_Server_Mutual_Authentication_for_HTTPS_EstablishmentNIST

Perform all test sequences defined in section 4.6.2.2.1 with the following variables set as follows:

V1.4 Page 499 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

- CLIENT = Alternative S_SM-DS
 - CERT_S_CLIENT_TLS = CERT_S_SM_DS_TLS for NIST
- SERVER = Root SM-DS under test.
 - CERT_SERVER_TLS = CERT_SM_DS_TLS for NIST

4.5.9.2 TC ROOT SM-

DS_ES15_Server_Mutual_Authentication_for_HTTPS_EstablishmentBRP

Perform all test sequences defined in section 4.6.2.2.2 with the following variables set as follows:

- CLIENT = Alternative S_SM-DS
 - o CERT_S_CLIENT_TLS = CERT_S_SM_DS_TLS for BRP
- SERVER = Root SM-DS under test.
 - CERT_SERVER_TLS = CERT_SM_DS_TLS for BRP

4.5.10 ES11 (LPA -- SM-DS): TLS, Server Authentication, Session Establishment

4.5.10.1 TC_SM-

DS_ES11_Server_Mutual_Authentication_for_HTTPS_EstablishmentNIST

Perform all test sequences defined in section 4.6.3.2.1 with the following variables set as follows:

- CLIENT = S_LPAd
- SERVER = Root SM-DS under test.
 - CERT SERVER TLS = #CERT SM DS TLS for NIST

4.5.10.2 TC SM-

DS ES11 Server Mutual Authentication for HTTPS EstablishmentBRP

Perform all test sequences defined in section 4.6.3.2.2 with the following variables set as follows:

- CLIENT = S LPAd
- SERVER = Root SM-DS under test.
 - CERT_SERVER_TLS = #CERT_SM_DS_TLS for BRP

4.6 TLS Interface

4.6.1 TLS, Mutual Authentication, Client, TLS Establishment

4.6.1.1 Conformance Requirements

References

V1.4 Page 500 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

GSMA RSP Technical Specification [2]

Requirements

- RQ26_023, RQ26_024, RQ26_025, RQ26_025_1, RQ26_026, RQ26_027, RQ26_028
- RQ31_032
- RQ45_006, RQ45_026, RQ45_026_1
- RQ56_001, RQ56_002, RQ56_003,
- RQ58_001, RQ58_002,
- RQ59_001
- RQ60_002, RQ60_003
- RQ61_001
- RQ63_006
- RQ510_001

4.6.1.2 Test Cases

4.6.1.2.1 TC_Client_Mutual_Authentication_for_HTTPS_EstablishmentNIST

General Initial Conditions for SM-DP+ as Client under test			
Entity	Entity Description of the initial condition		
SM-DP+	 PROFILE_OPERATIONAL1 is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> There is currently no TLS connection established to the S_SM-DS 		

General Initial Conditions for SM-DS as Client under test			
Entity	Description of the initial condition		
SM-DS	 EventID to be used by the S_SM-DP+ is not already used in the SM-DS There is currently no TLS connection established to the S_SM-DS 		

Test Sequence #01 Nominal: HTTPS Session Establishment

The purpose of this test is to verify that the Client correctly establishes an HTTPS Session with the Server using Mutual Authentication.

Step	Direction	Sequence / Description	Expected result	REQ	
	When the Client under test is the SM-DP+, initiate the download order procedure (see SGP.22 [2] section 3.1.1) for the SM-DS use case with smdsAddress #TEST_ROOT_DS_ADDRESS to be used for Event Registration.				
	When the Client under test is the SM-DS, the S_SM-DP+ calls ES12.RegisterEvent configured as follows:				
IC1					

V1.4 Page 501 of 777

	<event_i TRUE)</event_i 	D>,		
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>) Verify that: • <tls_cipher_suites> SHALL contain at least one of TLS_ECDHE_ECDSA_WITH_ AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_ AES_128_CBC_SHA256 • <ext_sha256_ecdsa> SHALL have at least the 'supported_signature_algorith ms' extension set with HashAlgorithm sha256 (04) and SignatureAlgorithm ecdsa (03).</ext_sha256_ecdsa></tls_cipher_suites></ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS, <\$ERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #\$_SAH_SHA256_ECDSA, #DIST_NAME_CI)	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_CLIENT_TLS, <client_tls_ephem_key>)</client_tls_ephem_key>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
3	S_SERVER → CLIENT	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	HTTPS connection established	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #02 Nominal: Non-reuse of session keys

The purpose of this test sequence is to verify that the Client is not reusing ephemeral keys from the previous session.

V1.4 Page 502 of 777

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	section 3.1.1) for Event Regi When the Clie follows: MTD_HTTP_F #IUT_SM_D #PATH_REG MTD_REGIS #EID1, #TEST_DF	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#EID1, #TEST_DP_ADDRESS1, <event_id>,</event_id>			
IC2		NITIALIZATION_MUTUAL_AUTH NT_TLS_EPHEM_KEY> from the Clie	entKeyExchange message		
IC3	S_SERVER → CLIENT	Close TLS session (unless CLIENT	has already closed TLS session)		
IC4	Repeat IC1				
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>		
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS, <\$ERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #\$_SAH_SHA256_ECDSA, #DIST_NAME_CI)	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_CLIENT_TLS, <client_tls_ephem_key>) Verify that in the ClientKeyExchange message: <client_tls_ephem_key> is different from the one used by the CLIENT in IC1</client_tls_ephem_key></client_tls_ephem_key>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001	
3	S_SERVER → CLIENT	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	HTTPS connection established	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001	

V1.4 Page 503 of 777

Test Sequence #03 Error: Invalid Server TLS Version

Step	Direction	Sequence / Description	Expected result	REQ		
IC1	When the Client under test is the SM-DP+, initiate the download order procedure (see SGP.22 [2] section 3.1.1) for the SM-DS use case with smdsAddress #TEST_ROOT_DS_ADDRESS to be used for Event Registration.					
	When the Client under test is the SM-DS, the S_SM-DP+ calls ES12.RegisterEvent configured as follows:					
	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#EID1, #TEST_DP_ADDRESS1, <event_id>, TRUE)</event_id>					
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001		
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_1, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS, <\$ERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #S_SAH_SHA256_ECDSA, #DIST_NAME_CI)	Client sends a TLS Fatal-alert during or after any of the messages sent by the S_SERVER in MTD_TLS_MUTUAL_AUTH_ SERVER_HELLO_ETC	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ510_001 RQ59_001 RQ61_001		

Test Sequence #04 Error: Invalid Server TLS Certificate Signature

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	When the Client under test is the SM-DP+, initiate the download order procedure (see SGP.22 [2] section 3.1.1) for the SM-DS use case with smdsAddress #TEST_ROOT_DS_ADDRESS to be used for Event Registration.				
	When the Client under test is the SM-DS, the S_SM-DP+ calls ES12.RegisterEvent configured as follows:				
	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#EID1, #TEST_DP_ADDRESS1,				

V1.4 Page 504 of 777

GSM Association Official Document SGP.23 - SGP.23 RSP Test Specification

	<event_i TRUE)</event_i 	D>,		
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS_INV_S IG, <\$_SERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #S_SAH_SHA256_ECDSA, #DIST_NAME_CI)	Client sends a TLS Fatal-alert during or after any of the messages sent by the S_SERVER in MTD_TLS_MUTUAL_AUTH_ SERVER_HELLO_ETC	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #05 Error: Expired Server TLS Certificate

Step	Direction	Sequence / Description	Expected result	REQ
		nt under test is the SM-DP+, initiate the SM-DS use case with smdsAd stration.	1	
	When the Clie follows:	nt under test is the SM-DS, the S_SM	I-DP+ calls ES12.RegisterEvent c	onfigured as
IC1	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#EID1, #TEST_DP_ADDRESS1, <event_id>, TRUE)</event_id>			
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

V1.4 Page 505 of 777

2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS_EXPIR ED, <\$SERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #S_SAH_SHA256_ECDSA, #DIST_NAME_CI)	Client sends a TLS Fatal-alert during or after any of the messages sent by the S_SERVER in MTD_TLS_MUTUAL_AUTH_ SERVER_HELLO_ETC	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
---	----------------------	---	---	---

Test Sequence #06 Error: Invalid Server TLS Certificate with critical extension not set

Step	Direction	Sequence / Description	Expected result	REQ	
	When the Client under test is the SM-DP+, initiate the download order procedure (see SGP.22 [2] section 3.1.1) for the SM-DS use case with smdsAddress #TEST_ROOT_DS_ADDRESS to be used for Event Registration.				
	When the Clie follows:	nt under test is the SM-DS, the S_SM	l-DP+ calls ES12.RegisterEvent c	onfigured as	
IC1	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#EID1, #TEST_DP_ADDRESS1, <event_id>, TRUE)</event_id>				
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001	
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS_INV_C RITICAL_EXT, <\$ERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #S_SAH_SHA256_ECDSA, #DIST_NAME_CI)	Client sends a TLS Fatal-alert during or after any of the messages sent by the S_SERVER in MTD_TLS_MUTUAL_AUTH_ SERVER_HELLO_ETC	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001	

V1.4 Page 506 of 777

Test Sequence #07 Error: Invalid Server TLS Certificate with invalid 'key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ	
	When the Client under test is the SM-DP+, initiate the download order procedure (see SGP.22 [2] section 3.1.1) for the SM-DS use case with smdsAddress #TEST_ROOT_DS_ADDRESS to be used for Event Registration.				
	When the Clie follows:	nt under test is the SM-DS, the S_SM	I-DP+ calls ES12.RegisterEvent co	onfigured as	
IC1 MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_REGISTER_EVENT, MTD_REGISTER_EVENT(#EID1, #TEST_DP_ADDRESS1, <event_id>, TRUE)</event_id>					
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001	
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS_INV_K EY_USAGE, <\$ERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #\$_SAH_SHA256_ECDSA, #DIST_NAME_CI)	Client sends a TLS Fatal-alert during or after any of the messages sent by the S_SERVER in MTD_TLS_MUTUAL_AUTH_ SERVER_HELLO_ETC	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001	

Test Sequence #08 Error: Invalid TLS Certificate with invalid 'extended key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	When the Client under test is the SM-DP+, initiate the download order procedure (see SGP.22 [2] section 3.1.1) for the SM-DS use case with smdsAddress #TEST_ROOT_DS_ADDRESS to be used for Event Registration. When the Client under test is the SM-DS, the S_SM-DP+ calls ES12.RegisterEvent configured as				
		REQ(S_ADDRESS, GISTER_EVENT,			

V1.4 Page 507 of 777

	#EID1,	P_ADDRESS1, D>,		
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS_INV_E XT_KEY_USAGE, <\$ERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #\$_SAH_SHA256_ECDSA, #DIST_NAME_CI)	Client sends a TLS Fatal-alert during or after any of the messages sent by the S_SERVER in MTD_TLS_MUTUAL_AUTH_ SERVER_HELLO_ETC	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #09 Error: Invalid Client TLS Certificate with invalid 'Certificate Policies' extensions

Step	Direction	Sequence / Description	Expected result	REQ
		nt under test is the SM-DP+, initiate the sm-DS use case with smdsAd stration.	·	
	When the Clie follows:	nt under test is the SM-DS, the S_SM	l-DP+ calls ES12.RegisterEvent c	onfigured as
IC1	#PATH_REC MTD_REGIS #EID1,	S_ADDRESS, GISTER_EVENT, GTER_EVENT(P_ADDRESS1,		
1	CLIENT → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_CLIENT_TLS_VER, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001

V1.4 Page 508 of 777

				RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_SERVER → CLIENT	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <\$_SEL_TLS_CIPHER_SUITE>, <\$ESSION_ID_RANDOM>, #CERT_S_SERVER_TLS_INV_C ERT_POL, <\$ERVER_TLS_EPHEM_KEY>, #CLIENT_CERT_TYPE, #S_SAH_SHA256_ECDSA, #DIST_NAME_CI)	Client sends a TLS Fatal-alert during or after any of the messages sent by the S_SERVER in MTD_TLS_MUTUAL_AUTH_SERVER_HELLO_ETC	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

4.6.1.2.2 TC_Client_Mutual_Authentication_for_HTTPS_EstablishmentBRP

Test Sequence #01 Nominal: HTTPS Session Establishment

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.6.1.2.1 TC_Client_Mutual_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

Test Sequence #02 Nominal: Non-reuse of session keys

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.6.1.2.1 TC_Client_Mutual_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

4.6.2 TLS, Mutual Authentication, Server, TLS Establishment

4.6.2.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26_023, RQ26_024, RQ26_025, RQ26_026, RQ26_027, RQ26_028
- RQ45_006, RQ45_026, RQ45_026_1
- RQ56_002
- RQ59_001
- RQ60_003
- RQ61_001

V1.4 Page 509 of 777

4.6.2.2 Test Cases

4.6.2.2.1 TC_Server_Mutual_Authentication_for_HTTPS_EstablishmentNIST

Test Sequence #01 Nominal: HTTPS Session Establishment

The purpose of this test is to verify that the Server correctly establishes an HTTPS Session with the Client using Mutual Authentication.

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_S_CLIENT_TLS, <client_tls_ephem_key>)</client_tls_ephem_key>	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	RQ26_023 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #02 Nominal: Non-reuse of session keys

The purpose of this test sequence is to verify that the Server is not reusing ephemeral keys from the previous session.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_MUTUAL_AUTH Extract <server_tls_ephem_key> from the ServerKeyExchange message</server_tls_ephem_key>			
IC2	Terminate the TLS session			
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(RQ26_025

V1.4 Page 510 of 777

		#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the ServerKeyExchange message: •<server_tls_ephem_key> is different from the <server_tls_ephem_key> value used in IC1.</server_tls_ephem_key></server_tls_ephem_key></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_CL IENT_EXCH(#CERT_S_CLIENT_TLS, <client_tls_ephem_key>)</client_tls_ephem_key>	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	RQ26_023 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #03 Nominal: HTTPS Session Establishment with supported and unsupported Cipher Suites

The purpose of this test is to verify that the Server correctly establishes an HTTPS Session with the Client when supported and unsupported Cipher Suites are offered by the Client.

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #PROP_TLS_CIPHER_SUITE S, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

V1.4 Page 511 of 777

2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_S_CLIENT_TLS, <client_tls_ephem_key>)</client_tls_ephem_key>	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	RQ26_023 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
---	----------------------	--	---	---

Test Sequence #04 Error: Invalid TLS Version

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_1, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ510_001 RQ59_001 RQ61_001

Test Sequence #05 Error: Unsupported Cipher Suites and Extensions

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #UNSUP_TLS_CIPHER_SUITES , #S_SESSION_ID_EMPTY, #EXT_SHA256_RSA)	Server sends a TLS Fatal-alert	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ510_001 RQ59_001 RQ61_001

Test Sequence #06 Error: Invalid Client TLS Certificate Signature

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

V1.4 Page 512 of 777

			S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256	
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_S_CLIENT_TLS_INV _SIG, <client_tls_ephem_key>)</client_tls_ephem_key>	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #07 Error: Expired Client TLS Certificate

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_S_CLIENT_TLS_EXP IRED, <client_tls_ephem_key>)</client_tls_ephem_key>	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

V1.4 Page 513 of 777

Test Sequence #08 Error: Invalid Client TLS Certificate with critical extension not set

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_S_CLIENT_TLS_INV _CRITICAL_EXT, <client_tls_ephem_key>)</client_tls_ephem_key>	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #09 Error: Invalid Client TLS Certificate with invalid 'key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

V1.4 Page 514 of 777

			TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256	
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_CL IENT_EXCH(#CERT_S_CLIENT_TLS_INV_ KEY_USAGE, <client_tls_ephem_key>)</client_tls_ephem_key>	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #10 Error: Invalid TLS Certificate with invalid 'extended key usage' extension

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_S_CLIENT_TLS_INV _EXT_KEY_USAGE, <client_tls_ephem_key>)</client_tls_ephem_key>	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

V1.4 Page 515 of 777

Test Sequence #11 Error: Invalid Client TLS Certificate with invalid 'Certificate Policies' extensions

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></sah_sha256_ecdsa></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_ CLIENT_EXCH(#CERT_S_CLIENT_TLS_INV _CERT_POL, <client_tls_ephem_key>)</client_tls_ephem_key>	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_006 RQ45_026 RQ45_026 RQ45_0261 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

Test Sequence #12 Error: No suitable Client certificate available

The purpose of this test is to verify that the Server does not establish an HTTPS Session with the Client using Mutual Authentication when the CERT.CLIENT.TLS certificate of the S_CLIENT certificate message contains no certificates (the certificate_list structure has a length of zero).

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SER VER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>, #CLIENT_CERT_TYPE,</server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001

V1.4 Page 516 of 777

			<sah_sha256_ecdsa>, #DIST_NAME_CI) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></sah_sha256_ecdsa>	RQ60_003 RQ61_001
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_CL IENT_EXCH(NO_PARAM, <client_tls_ephem_key>)</client_tls_ephem_key>	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ26_028 RQ45_026 RQ45_026_1 RQ510_001 RQ56_002 RQ59_001 RQ60_003 RQ61_001

4.6.2.2.2 TC_Server_Mutual_Authentication_for_HTTPS_EstablishmentBRP

Test Sequence #01 Nominal: HTTPS Session Establishment

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.6.2.2.1 TC_Server_Mutual_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

Test Sequence #02 Nominal: Non-reuse of session keys

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.6.2.2.1 TC_Server_Mutual_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

Test Sequence #03 Nominal: HTTPS Session Establishment with supported and unsupported Cipher Suites

This test sequence SHALL be the same as the Test Sequence #03 defined in section 4.6.2.2.1 TC_Server_Mutual_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

4.6.3 TLS, Server Authentication, TLS Establishment

4.6.3.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

V1.4 Page 517 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

- RQ26_023, RQ26_024, RQ26_025, RQ26_025_1, RQ26_026, RQ26_027, RQ26_028
- RQ31_032
- RQ45_026, RQ45_026_1
- RQ56_001, RQ56_002, RQ56_003,
- RQ58_001, RQ58_002,
- RQ60_002,
- RQ61_001
- RQ63_006

4.6.3.2 Test Cases

4.6.3.2.1 TC_Server_Authentication_for_HTTPS_EstablishmentNIST

Test Sequence #01 Nominal: HTTPS Session Establishment

The purpose of this test is to verify that the Server correctly establishes an HTTPS Session with the Client.

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_SERVER_HELLO_ET C(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_028 RQ31_032 RQ31_032_1 RQ45_026 RQ45_026_1 RQ56_001 RQ56_002 RQ56_003 RQ58_001 RQ58_001 RQ58_002 RQ60_002 RQ60_002 RQ61_001
2	S_LPAd → SERVER	MTD_TLS_CLIENT_KEY_EX CH_ETC(<client_tls_eph EM_KEY>)</client_tls_eph 	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	RQ26_023 RQ26_026 RQ26_027 RQ31_032 RQ45_026 RQ45_026_1 RQ56_001 RQ58_001 RQ60_002 RQ61_001

Test Sequence #02 Nominal: Non-reuse of session keys

The purpose of this test sequence is to verify that the Server is not reusing ephemeral keys from the previous session.

V1.4 Page 518 of 777

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH Extract <server_tls_ephem_key> from the ServerKeyExchange message</server_tls_ephem_key>				
IC2	Terminate the	TLS session			
1	S_LPAd → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_SERVER_HELLO_ET C(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>) Verify that in the ServerKeyExchange message: •<server_tls_ephem_key> is different from the <server_tls_ephem_key> value used in IC1.</server_tls_ephem_key></server_tls_ephem_key></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_025 RQ31_032	
2	S_LPAd → SERVER	MTD_TLS_CLIENT_KEY_EX CH_ETC(<client_tls_eph EM_KEY>)</client_tls_eph 	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	RQ26_023 RQ26_026 RQ26_027 RQ31_032 RQ45_026 RQ45_026_1 RQ56_001 RQ58_001 RQ60_001 RQ60_002 RQ61_001	

Test Sequence #03 Nominal: HTTPS Session Establishment with supported and unsupported Cipher Suites

The purpose of this test is to verify that the Server correctly establishes an HTTPS Session with the Client when supported and unsupported Cipher Suites are offered by the Client.

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #PROP_TLS_CIPHER_SUITE S, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_SERVER_HELLO_ET C(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, <server_tls_ephem_key>) Verify that in the Server Hello message: •<sel_tls_cipher_suite> SHALL contain either TLS_ECDHE_ECDSA_WITH_AE S_128_GCM_SHA256 OR TLS_ECDHE_ECDSA_WITH_AE S_128_CBC_SHA256</sel_tls_cipher_suite></server_tls_ephem_key></session_id_random></sel_tls_cipher_suite>	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_028 RQ31_032_1 RQ31_032_1 RQ45_026 RQ45_026_1 RQ56_001 RQ56_002 RQ56_003 RQ58_001 RQ58_001 RQ58_002 RQ60_002 RQ60_002 RQ61_001

V1.4 Page 519 of 777

12 1	S_LPAd → SERVER	MTD_TLS_CLIENT_KEY_EX CH_ETC(<client_tls_eph EM_KEY>)</client_tls_eph 	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	RQ26_023 RQ26_026 RQ26_027 RQ31_032 RQ45_026 RQ45_026_1 RQ56_001 RQ58_001 RQ60_002 RQ61_001
------	--------------------	---	---	--

Test Sequence #04 Error: Invalid TLS Version

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_1, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, NO_PARAM)	Server sends a TLS Fatal-alert	RQ26_023 RQ26_025 RQ26_026 RQ26_027 RQ31_032 RQ45_026 RQ45_026_1 RQ56_001 RQ58_001 RQ60_002 RQ61_001

Test Sequence #05 Error: Unsupported Cipher Suites and Extensions

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #UNSUP_TLS_CIPHER_SUITES , #S_SESSION_ID_EMPTY, #EXT_SHA256_RSA)	Server sends a TLS Fatal-alert	RQ26_023 RQ26_024 RQ26_025 RQ26_026 RQ26_027 RQ31_032 RQ45_026 RQ45_026_1 RQ56_001 RQ58_001 RQ60_002 RQ61_001

4.6.3.2.2 TC_Server_Authentication_for_HTTPS_EstablishmentBRP

Test Sequence #01 Nominal: HTTPS Session Establishment

This test sequence SHALL be the same as the Test Sequence #01 defined in section 4.6.3.2.1 TC_Server_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

V1.4 Page 520 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #02 Nominal: Non-reuse of session keys

This test sequence SHALL be the same as the Test Sequence #02 defined in section 4.6.3.2.1 TC_Server_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

Test Sequence #03 Nominal: HTTPS Session Establishment with supported and unsupported Cipher Suites

This test sequence SHALL be the same as the Test Sequence #03 defined in section 4.6.3.2.1 TC_Server_Authentication_for_HTTPS_EstablishmentNIST, except that the brainpoolP256r1 curve is used.

4.7 LPAe Interfaces

This section is defined as FFS.

V1.4 Page 521 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

5 Procedure - Behaviour Testing

5.1 General Overview

5.2 eUICC Behaviour

5.2.1 Retry mechanism

5.2.1.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ26 029, RQ26 030
- RQ31_130, RQ31_131, RQ31_132, RQ31_133, RQ31_134, RQ31_135, RQ31_137, RQ31_139, RQ31_140, RQ31_141
- RQ57_112
- RQ57_025, RQ57_026, RQ57_027, RQ57_028, RQ57_029, RQ57_030, RQ57_033, RQ57_034, RQ57_035, RQ57_036, RQ57_037, RQ57_038, RQ57_039, RQ57_047

5.2.1.2 Test Cases

5.2.1.2.1 TC_eUICC_PrepareDownload_Retry_ReuseOTKeys

General Initial Cond	General Initial Conditions		
Entity	Description of the general initial condition		
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC		
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.		
eUICC	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+		
	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 		

Test Sequence #01 Nominal: Confirmation Code retry mechanism by reusing previous One-Time key pair

The purpose of this test is to check the Confirmation Code retry mechanism. The S_LPAd simulates that an incorrect Confirmation Code has been filled by the End User. Then, the S_LPAd sends another ES10b.PrepareDownload function with a correct Confirmation Code value. In this case, the eUICC does not have to generate a new one-time key pair and uses the previous one given by the SM-DP+.

V1.4 Page 522 of 777

Step	Direction	Sequence / Description	Expected result	REQ
IC1	<s_hashed <s_transa< td=""><td>CC> = MTD_GENERATE_HASHE CTION_ID>)</td><td>D_CC(#CONFIRMATION_CODE1,</td><td></td></s_transa<></s_hashed 	CC> = MTD_GENERATE_HASHE CTION_ID>)	D_CC(#CONFIRMATION_CODE1,	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_WITH_C C)	#R_PREP_DOWNLOAD_WITH_C C SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Extract the <otpk_euicc_ecka> and reuse the same value in step 4</otpk_euicc_ecka></s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_035 RQ57_035 RQ57_036 RQ57_037 RQ57_038 RQ57_039 RQ57_039 RQ26_029 RQ26_030
2	Execute the Common Mutual Authentication procedure between the eUICC and the S_SM-DP+ • #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP are sent to the eUICC • the same GSMA CI as for the first attempt has been chosen for signing and for verification			RQ57_047
3	<s_hashed <s_transa< td=""><td>_CC> = MTD_GENERATE_HASHE CTION_ID>)</td><td>D_CC(#CONFIRMATION_CODE2,</td><td></td></s_transa<></s_hashed 	_CC> = MTD_GENERATE_HASHE CTION_ID>)	D_CC(#CONFIRMATION_CODE2,	
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_RETRY_C C)	#R_PREP_DOWNLOAD_WITH_CC SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_CC. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_CC. Verify that the <otpk_euicc_ecka> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_CC.</otpk_euicc_ecka></s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ31_147 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_036 RQ57_036 RQ57_037 RQ57_038 RQ57_038 RQ57_039

V1.4 Page 523 of 777

		RQ57_033
		RQ26_029
		RQ26_030

Test Sequence #02 Nominal: Retry after a CancelSession Reason "Postponed"

The purpose of this test is to check that the eUICC can reuse the one-time key pair generated during a previous attempt. In this case, the S_LPAd simulates that the End User has postponed the download of the Profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1		D_CC> = MTD_GENERATE_HASHED ACTION_ID>)	D_CC(#CONFIRMATION_CODE1,	
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_WITH_CC)	#R_PREP_DOWNLOAD_WITH_C C SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Extract the <otpk_euicc_ecka> and reuse the same value in step 4</otpk_euicc_ecka></s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_035 RQ57_035 RQ57_035 RQ57_036 RQ57_037 RQ57_038 RQ57_039 RQ57_039 RQ57_039 RQ26_029 RQ26_030
2	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_POSTPONE D)	#R_CANCEL_SESSION_POSTP ONED SW = 0x9000	RQ57_112
3	S_SM-DP+	Common Mutual Authentication proced ET_EUICC_INFO1, #GET_EUICC_CH UTHENTICATE_SMDP are sent to the same GSMA CI as for the first attempt verification	ALLENGE and eUICC	RQ57_047
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_RETRY_C)	#R_PREP_DOWNLOAD_WITH_C C SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA.</euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140

V1.4 Page 524 of 777

	Verify that the	RQ31_141
	<s_transaction_id> present</s_transaction_id>	RQ31_137
	in the euiccSigned2 is the same as	RQ57_025
	in #DDED DOWNHOAD DETDY C	RQ57_026
	#PREP_DOWNLOAD_RETRY_C C.	RQ57_027
		RQ57_028
	Verify that the <s_hashed_cc></s_hashed_cc>	RQ57_029
	present in the euiccSigned2 is the	RQ57_030
	same as in #PREP_DOWNLOAD_RETRY_C	RQ57_034
	C.	RQ57_035
	Marife dia at the	RQ57_036
	Verify that the	RQ57_037
	<otpk_euicc_ecka> present in</otpk_euicc_ecka>	RQ57_038
	the euiccSigned2 is the same as in	RQ57_039
	#PREP_DOWNLOAD_RETRY_C	RQ57_033
	C.	RQ26_029
		RQ26_030

Test Sequence #03 Nominal: Retry after a CancelSession Reason "Timeout"

The purpose of this test is to check that the eUICC can reuse the one-time key pair generated during a previous attempt. In this case, the S_LPAd simulates that the End User does not confirm the download of the Profile within the timeout interval.

Step	Direction	Sequence / Description	Expected result	REQ			
IC1		<s_hashed_cc> = MTD_GENERATE_HASHED_CC(#CONFIRMATION_CODE1, <s_transaction_id>)</s_transaction_id></s_hashed_cc>					
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_WITH_CC)	#R_PREP_DOWNLOAD_WITH_C C SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Extract the <otpk_euicc_ecka> and reuse the same value in step 4</otpk_euicc_ecka></s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_034 RQ57_035 RQ57_035 RQ57_036 RQ57_037 RQ57_037 RQ57_038 RQ57_039 RQ57_039 RQ26_029 RQ26_030			
2	S_LPAd → eUICC	MTD_STORE_DATA(#CANCEL_SESSION_TIMEOUT)	#R_CANCEL_SESSION_TIMEOU T SW = 0x9000	RQ57_112			

V1.4 Page 525 of 777

3	Execute the Common Mutual Authentication procedure between the eUICC and the S_SM-DP+ • #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP are sent to the eUICC • the same GSMA CI as for the first attempt has been chosen for signing and for verification			
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_RETRY_CC)	#R_PREP_DOWNLOAD_WITH_C C SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_C C. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_C C. Verify that the <otpk_euicc_ecka> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_C C.</otpk_euicc_ecka></s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ31_141 RQ31_147 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_034 RQ57_035 RQ57_036 RQ57_036 RQ57_037 RQ57_038 RQ57_038 RQ57_039 RQ57_033 RQ57_033 RQ57_033 RQ57_033 RQ57_033 RQ57_039 RQ57_033 RQ57_039 RQ57_033 RQ26_029 RQ26_030

5.2.1.2.2 TC_eUICC_PrepareDownload_Retry_NewOTKeys

General Initial Conditions				
Entity	Description of the general initial condition			
eUICC	The PROFILE_OPERATIONAL1 is not loaded on the eUICC			
	The communication between the S_Device and the eUICC has been initialized and the S_LPAd has selected the ISD-R.			
eUICC	Common Mutual Authentication procedure has been successfully executed between the eUICC and the S_SM-DP+			
	 #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP have been sent to the eUICC the same GSMA CI has been chosen for signing and for verification 			

Test Sequence #01 Nominal: Confirmation Code retry mechanism by not reusing previous One-Time key pair

The purpose of this test is to check the Confirmation Code retry mechanism. The S_LPAd simulates that an incorrect Confirmation Code has been filled by the End User. Then, the S_LPAd sends another ES10b.PrepareDownload function with a correct Confirmation Code

V1.4 Page 526 of 777

value. In this case, the eUICC does not support the storage of unused one-time key pair or the eUICC has discarded the previous one-time public key: we expect the eUICC to generate a new set of keys.

Step	Direction	Sequence / Description	Expected result	REQ		
IC1		<s_hashed_cc> = MTD_GENERATE_HASHED_CC(#CONFIRMATION_CODE1, <s_transaction_id>)</s_transaction_id></s_hashed_cc>				
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#PREP_DOWNLOAD_WITH_ CC)	#R_PREP_DOWNLOAD_WITH_C C SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_WITH_CC. Extract the <otpk_euicc_ecka> and reuse the same value in step 4</otpk_euicc_ecka></s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_030 RQ57_035 RQ57_036 RQ57_035 RQ57_036 RQ57_037 RQ57_037 RQ57_038 RQ57_039 RQ26_029 RQ26_030		
2	S_SM-DP+ • #GET_ #AUTH • the sai	_EUICC_INFO1, #GET_EUICC_C HENTICATE_SMDP are sent to the		RQ57_047		
3	<s_hashed_0 <s_transact< td=""><td></td><td>D_CC(#CONFIRMATION_CODE2,</td><td></td></s_transact<></s_hashed_0 		D_CC(#CONFIRMATION_CODE2,			
4	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT (#PREP_DOWNLOAD_RETRY _CC)	#R_PREP_DOWNLOAD_WITH_C C SW=0x9000 The <euicc_signature2> SHALL be verified with the #PK_EUICC_ECDSA. Verify that the <s_transaction_id> present in the euiccSigned2 is the same as in #PREP_DOWNLOAD_RETRY_CC . Verify that the <s_hashed_cc> present in the euiccSigned2 is the same as in</s_hashed_cc></s_transaction_id></euicc_signature2>	RQ31_130 RQ31_131 RQ31_132 RQ31_133 RQ31_134 RQ31_135 RQ31_139 RQ31_140 RQ31_141 RQ31_137 RQ57_025 RQ57_026 RQ57_027 RQ57_028 RQ57_029 RQ57_030 RQ57_034 RQ57_035		

V1.4 Page 527 of 777

		#PREP_DOWNLOAD_RETRY_CC	RQ57_036	
			RQ57_037	
		Verify that the	RQ57_038	
		<otpk_euicc_ecka> present in</otpk_euicc_ecka>	RQ57_039	
		the euiccSigned2 is NOT the same	RQ57_033	
		as in	RQ26_029	
		#PREP_DOWNLOAD_RETRY_CC	RQ26_030	
		•		

5.2.2 Forbidden PPRs

5.2.2.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ57_053, RQ57_054
- RQ57_056, RQ57_057
- RQ25_025, RQ25_023
- RQ55_032

5.2.2.2 Test Cases

5.2.2.2.1 TC_eUICC_ForbiddenPPRs

General Initial Conditions			
Entity Description of the general initial condition			
eUICC	There is no Profile installed in the eUICC		

Test Sequence #01 Nominal: PPR1 management and handling when Operational Profile is installed

The purpose of this test is to verify that the eUICC automatically sets PPR1 in the forbiddenProfilePolicyRules of EUICCInfo2 when an Operational Profile is installed. Any Operational Profile with PPR1 SHALL be rejected by the eUICC once an Operational Profile has been installed.

Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE				
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR				
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	forbiddenProfilePolicyRules in EUICCInfo2 does not contain ppr1	RQ57_053 RQ57_054 RQ57_056 RQ57_057	
2	Install PROFILE_OPERATIONAL1			RQ57_057	

V1.4 Page 528 of 777

3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	forbiddenProfilePolicyRules in EUICCInfo2 contains ppr1(1)	RQ57_053 RQ57_054 RQ57_056		
4	Execute the Common Mutual Authentication procedure between the eUICC and the S_SM-DP+ #GET_EUICC_INFO1, #GET_EUICC_CHALLENGE and #AUTHENTICATE_SMDP are sent to the eUICC the same GSMA CI is chosen for signing and for verification					
5	eUICC and the		d Installation – End User Confirmation be the eUICC	etween the		
6	Generate the <	OTPK_S_SM_DP+_ECKA> and <	<ot_sk_s_sm_dp+_ecka></ot_sk_s_sm_dp+_ecka>			
7	<pre><bpp> = MTD_GENERATE_BPP(#S_INIT_SC_PROF1, #CONF_ISDP_EMPTY, #METADATA_OP_PROF4, NO_PARAM, #UPP_OP_PROF4)</bpp></pre>					
8	Split the <bpp> into several segments arrays named: • <bpp_seg_init> • <bpp_seg_a0> • <bpp_seg_a1> • <bpp_seg_a3></bpp_seg_a3></bpp_seg_a1></bpp_seg_a0></bpp_seg_init></bpp>					
9	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_init>)</bpp_seg_init>	SW=0x9000 without response data for all STORE DATA commands			
10	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a0>)</bpp_seg_a0>	SW=0x9000 without response data for all STORE DATA commands			
11	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(<bpp_seg_a1>)</bpp_seg_a1>	SW=0x9000 with the response data #R_PIR_PPR_NOT_ALLOWED	RQ25_025 RQ25_023 RQ57_056 RQ55_032 RQ57_057		
12	S_LPAd → eUICC MTD_STORE_DATA(#GET_PROFILES_INFO_ALL) response ProfileInfoListResponse::= profileInfoListOk : { #PROFILE_INFO1_DISABLED } SW=0x9000					
13	Delete PROFIL	LE_OPERATIONAL1				
14	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	forbiddenProfilePolicyRules in EUICCInfo2 does not contain ppr1	RQ57_053 RQ57_054 RQ57_056		

V1.4 Page 529 of 777

5.2.3 eUICC's RAT

5.2.3.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_097, RQ31_097, RQ31_098, RQ31_130
- RQ32_057
- RQ57_117, RQ57_118, RQ57_119, RQ57_123, RQ57_179, RQ57_180, RQ57_181, RQ57_182, RQ57_184

5.2.3.2 Test Cases

5.2.3.2.1 TC_eUICC_GetProfilesInfo_GetRAT_RSPSession

Test Sequence #01 Nominal: GetProfilesInfo and GetRAT during RSP session

The purpose of this test is to ensure that the eUICC can be requested during a RSP session context to retrieve the list of installed Profiles and the Rules Authorization Table.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The eUICC's RAT is configured as detailed SGP.21 Annex H: one PPAR authorizing PPR1 and PPR2 for all MNOs with End User consent required (i.e. #PPRS_ALLOWED) no additional rules
eUICC	The PROFILE_OPERATIONAL1 is installed and Enabled on the eUICC

Ste p	Directio n	Sequence / Description	Expected result	REQ
IC1	PROC_EUI	CC_INITIALIZATION_SEQUENCE		
IC2	PROC_OPE	N_LOGICAL_CHANNEL_AND_SEL	ECT_ISDR	
IC3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO1)	#R_EUICC_INFO1 SW = 0x9000 Extract the <euicc_ci_pk_id_list_for_sig ning=""> and <euicc_ci_pk_id_list_for_ve rification=""> from response data and verify if they contain at least one same GSMA CI Key ID</euicc_ci_pk_id_list_for_ve></euicc_ci_pk_id_list_for_sig>	
IC4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_CHALLENGE)	#R_CHALLENGE SW = 0x9000	

V1.4 Page 530 of 777

			Extract the <euicc_challenge></euicc_challenge>		
IC5	The following inputs are required for Step IC6 as described in the InitiateAuthentication function: • <s_transaction_id> • <euicc_challenge> • <s_smdp_challenge> • <s_smdp_signature1> • Set the <euicc_ci_pk_id_to_be_used> to the CI Key ID in highest priority from the <euicc_ci_pk_id_list_for_signing> • Choose the #CERT_S_SM_DPauth_ECDSA leading to the same Root CI certificate</euicc_ci_pk_id_list_for_signing></euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id>				
IC6	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTHENTICATE_SMDP)	#R_AUTHENTICATE_SMDP SW = 0x9000		
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_RAT)	#R_DEFAULT_RAT with exact same structure and order SW = 0x9000	RQ57_179 RQ57_180 RQ57_181 RQ57_182 RQ57_184 RQ31_097	
2	S_LPAd → eUICC	MTD_STORE_DATA(#GET_PROFILES_INFO_ALL)	response ProfileInfoListResponse::= profileInfoListOk: { #PROFILE_INFO1 } SW = 0x9000	RQ32_057 RQ57_117 RQ57_118 RQ57_119 RQ57_123 RQ31_098	
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_NO_CC)	#R_PREP_DOWNLOAD_NO_CC SW=0x9000	RQ31_130	

5.2.4 eUICC File Structure

5.2.4.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

RQ34_003, RQ34_005_1, Q34_010, RQ34_011, RQ34_004_1

5.2.4.2 Test Cases

5.2.4.2.1 TC_eUICC_Default_FileSystem

General Initial Conditions		
Entity	Description of the general initial condition	
eUICC	There is no Profile installed in the eUICC	

Test Sequence #01 Nominal: Default file system available

The purpose of this test is to verify that if there is no Profile on the eUICC, the eUICC still ensures a file system to the Device.

V1.4 Page 531 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	S_Device → eUICC	RESET	ATR present	RQ34_003 RQ34_004_1
2	S_Device → eUICC	[SELECT_MF]	FCP Template present with tag 0xA5 (Proprietary Information) containing 0x87 01 01 (Supported system commands = TERMINAL CAPABILITY) SW=0x9000	RQ34_010, RQ34_011, RQ34_005_1, RQ34_003 RQ34_004_1
3	S_Device → eUICC	[TERMINAL_CAPABILITY_LPAd]	SW=0x9000	RQ34_005_1, RQ34_003 RQ34_004_1
4	S_Device → eUICC	[TERMINAL_PROFILE]	Toolkit initialization THEN SW=0x9000	RQ34_003 RQ34_004_1

5.2.5 eUICC Delete Profile Process

5.2.5.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ24_020
- RQ31_027, RQ31_028, RQ31_183
- RQ57_051, RQ57_052, RQ57_054

5.2.5.2 Test Cases

5.2.5.2.1 TC_eUICC_DeleteProfile_ISDP_And_Components

Test Sequence #01 Nominal: ISD-P and Profile Components Deletion

The purpose of this test is to verify that when a Profile is deleted, the eUICC removes the ISD-P and all Profile Components related to it. In order to do so, we are checking the eUICC Non-Volatile Memory variation.

Initial Conditions	
Entity	Description of the initial condition
eUICC	There is no Profile installed on the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			

V1.4 Page 532 of 777

IC3	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	Retrieve free non-volatile memory value (tag 0x82) from <ext_card_resource> in EUICCInfo2 as <free_memory_no_profile></free_memory_no_profile></ext_card_resource>	
IC4	Install PROFILE_OP	PERATIONAL1		
IC5	Remove all Install No	otifications from eUICC		
1	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	Retrieve free non-volatile memory value (tag 0x82) from <ext_card_resource> in EUICCInfo2 as <free_mem_op_prof1_insta LLED> Verify that <free_mem_op_prof1_insta LLED> is lower than <free_memory_no_profile ></free_memory_no_profile </free_mem_op_prof1_insta </free_mem_op_prof1_insta </ext_card_resource>	RQ31_027 RQ31_028 RQ57_051 RQ57_052 RQ57_054 RQ31_183
2	Delete PROFILE_OF	PERATIONAL1		
3	Remove the Delete I	Notification from eUICC		
4	S_LPAd → eUICC	MTD_STORE_DATA(#GET_EUICC_INFO2)	Retrieve free non-volatile memory value (tag 0x82) from <ext_card_resource> in EUICCInfo2 as <free_mem_op_prof1_dele TED> Verify that <free_mem_op_prof1_dele TED> is higher than <free_mem_op_prof1_insta LLED></free_mem_op_prof1_insta </free_mem_op_prof1_dele </free_mem_op_prof1_dele </ext_card_resource>	RQ31_027 RQ31_028 RQ57_051 RQ57_052 RQ57_054 RQ24_020

5.2.6 eUICC Enable Profile Process

5.2.6.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ35_001, RQ35_002, RQ35_007
- RQ55_048_1
- RQ57_135_5

V1.4 Page 533 of 777

5.2.6.2 Test Cases

5.2.6.2.1 TC_eUICC_EnableProfile_Twice_Notifications

General Initial Conditions	
Entity	Description of the general initial condition
eUICC	The PROFILE_OPERATIONAL1 is installed and Enabled on the eUICC
eUICC	No Notification is stored in the eUICC's Pending Notifications List

Test Sequence #01 Nominal: Notifications generation

The purpose of this test is to verify that when an Enable Profile operation is performed and the current Enabled Profile is implicitly Disabled, both Notifications are generated. The eUICC automatically increments its sequence number each time a Notification is generated across all Profiles.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN	N_LOGICAL_CHANNEL_AND_SE	ELECT_ISDR	
IC3	Install PROFILE_OPERATIONAL2 The default Profile downloading procedure defined in section 2.2.3.1 SHALL be used with the following exceptions: #CERT_S_SM_DP2auth_ECDSA SHALL be set in #AUTH_SMDP_MATCH_ID rather than #CERT_S_SM_DPauth_ECDSA #TEST_DP_ADDRESS2 SHALL be set in #AUTH_SMDP_MATCH_ID rather than #TEST_DP_ADDRESS1 #CERT_S_SM_DP2pb_ECDSA SHALL be set in #PREP_DOWNLOAD_NO_CC rather than #CERT_S_SM_DPpb_ECDSA			
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_IN2_PIR_IN2 SW = 0x9000 Verify that <notif_seq_no_in2_pir> and <notif_seq_no_in2> follow this order in an incremental sequence (see Note)</notif_seq_no_in2></notif_seq_no_in2_pir>	RQ35_001 RQ35_002 RQ55_048_1
2	Remove the ProfileInstallationResult and OtherSignedNotification for Install			•
3	Enable PROFILE_OPERATIONAL2			
4	PROC_EUICC_INITIALIZATION_SEQUENCE			
5	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1_EN2 SW = 0x9000 Verify that	RQ35_001 RQ35_002 RQ35_007 RQ57_135_5

V1.4 Page 534 of 777

<notif_seq_no_in2> is lower than <notif_seq_no_di1>.</notif_seq_no_di1></notif_seq_no_in2>
Verify that
<notif_seq_no_di1> and <notif_seq_no_en2> follow this order in an incremental sequence</notif_seq_no_en2></notif_seq_no_di1>

Note: In order to compare the sequence numbers, the test tool can retrieve the <NOTIF_SEQ_NO_IN2_PIR> value through the PIR returned at the end of the step IC3.

5.2.7 eUICC Disable Profile Process

5.2.7.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

• RQ24_026

5.2.7.2 Test Cases

5.2.7.2.1 TC_eUICC_DisableProfile_ApplicationManagement

General Initial Conditions		
Entity	Description of the general initial condition	
eUICC	PROFILE_OPERATIONAL1 is installed and Enabled	

Test Sequence #01 Nominal: Application Selection/Deletion not available on Disabled Profile

The purpose of this test is to verify that when a Profile is Disabled, the eUICC does not allow the selection or deletion of any application within the Profile.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	S_Device → eUICC	[SELECT_USIM]	FCP Template present SW=0x9000	
IC3	S_Device → eUICC	MTD_SELECT(#SSD_AID)	SSD is selected SW=0x9000	
IC4	Disable PROFILE_OPERATIONAL1			
1	S_Device → eUICC	[SELECT_USIM]	USIM is not found SW=0x6A82	RQ24_026

V1.4 Page 535 of 777

2	S_Device → eUICC	MTD_SELECT(#SSD_AID)	SSD is not found SW=0x6A82	RQ24_026
3	PROC_EUICC_	INITIALIZATION_SEQUENCE		
4	S_Device → eUICC	MTD_SEND_SMS_PP([DELETE_SSD])	SW=0x91XX or SW=0x9000 (i.e. envelope rejected, see Note) or any error SW (i.e. envelope rejected, see Note)	RQ24_026
5	S_Device →eUICC	FETCH 'XX'	SMS POR received SCP80 response status code equal to 0x06 (Unidentified security error) or 0x09 (TAR unknown)	RQ24_026
6	S_Device → eUICC	TERMINAL RESPONSE	SW=0x9000	
7	Enable PROFILE_OPERATIONAL1			
8	S_Device → eUICC	MTD_SELECT(#SSD_AID)	SSD is selected SW=0x9000	RQ24_026

NOTE: Depending on the implementation, the eUICC MAY decide to not send back a POR (e.g. SW=0x9000 on the ENVELOPE command). Therefore, the steps 5 and 6 SHALL only be executed in case SW=0x91XX.

5.2.8 eUICC Notifications

5.2.8.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

• RQ57_135_6, RQ57_142_17, RQ57_158_1

5.2.8.2 Test Cases

5.2.8.2.1 TC_eUICC_Enable_Disable_Delete_Notifications

General Initial Conditions	
Entity Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 with #METADATA_EN_DI_DE_NOTIFS is loaded on the eUICC
eUICC	The PROFILE_OPERATIONAL1 is Disabled
eUICC	No Notification is stored in the eUICC's Pending Notifications List

V1.4 Page 536 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #01 Nominal: Multiple Enable, Disable and Delete Notifications

The purpose of this test is to verify that when a Local Profile Management Operation (i.e. Enable, Disable and Delete Profile) is performed, all Notifications configured in the notificationConfigurationInfo are generated by the eUICC.

NOTE: In this sequence, the maximum number of Notifications simultaneously

tested has been set as to two as there is not minimum defined in SGP.21 or SGP.22 [2] for the number of Notifications that can be stored by the eUICC.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_EUICC_INITIALIZATION_SEQUENCE			
IC2	PROC_OPEN_	LOGICAL_CHANNEL_AND_SE	LECT_ISDR	
IC3	Enable PROFII	LE_OPERATIONAL1		
IC4	PROC_EUICC	_INITIALIZATION_SEQUENCE		
IC5	PROC_OPEN_	LOGICAL_CHANNEL_AND_SE	LECT_ISDR	
1	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_EN1_EN1 SW = 0x9000	RQ57_135_6
2	Remove all the pending notifications			
3	Disable PROFILE_OPERATIONAL1			
4	PROC_EUICC_INITIALIZATION_SEQUENCE			
5	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR			
6	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DI1_DI1 SW = 0x9000	RQ57_142_17
7	Remove all the pending notifications			
8	Delete PROFILE_OPERATIONAL1			
9	S_LPAd → eUICC	MTD_STORE_DATA(#LIST_NOTIF_ALL)	#R_LIST_NOTIF_DE1_DE1 SW = 0x9000	RQ57_158_1

5.3 Platform Procedures

5.3.1 Profile Download and Installation Procedure

This section is defined as FFS and not applicable for this version of test specification.

5.3.2 Common Mutual Authentication Process

This section is defined as FFS and not applicable for this version of test specification.

5.3.3 Profile Download and Installation Process

5.3.3.1 Conformance Requirements

References

V1.4 Page 537 of 777

GSMA RSP Technical Specification [2]

Requirements

- RQ44_002
- RQ55_033_1

5.3.3.2 Test Cases

5.3.3.2.1 TC_SM_DP+_ProfileMetadata

General Initial Conditions			
Entity	Description of the general initial condition		
SM-DP+	 SM-DP+ is configured with the #CERT_SM_DPauth_ECDSA for NIST. PROFILE_OPERATIONAL1 (configured with metadata as specified in each sequence) is securely loaded as a Protected Profile Package using <ppk_enc> and <ppk_mac>.</ppk_mac></ppk_enc> Pending Profile PROFILE_OPERATIONAL1 is in the 'Released' state with an empty MatchingID. EID #EID1 is known to the SM-DP+ and associated to PROFILE_OPERATIONAL1. Confirmation Code is not provided by the Operator to the SM-DP+. NOTE: the Profile Metadata for PROFILE_OPERATIONAL1 SHALL be specified in the Initial Conditions for each individual sequence. 		

Test Sequence #01 Nominal: all elements present

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	SM-DP+ is configured with #SMDP_METADATA_ALL for the pending Profile PROFILE_OPERATIONAL1.	

Run the sequence below with the following parameter assignments:

- PARAM_R_AUTH_CLIENT = #R_AUTH_CLIENT_META_ALL
- PARAM_METADATA = #SMDP_METADATA_ALL

The sequence below has the following parameters:

- PARAM_R_AUTH_CLIENT
- PARAM_METADATA

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_IN	TIALIZATION_SERVER_AUTH on ES9+		
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE _AUTH_OK)	

V1.4 Page 538 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC _OK))</s_transaction_id>	MTD_HTTP_RESP(PARAM_R_A UTH_CLIENT)	RQ44_002
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BP P_RESP_OP1_PPK) Construct the complete metadata element from the <smdp_metadata_seg_mac > segment(s) and verify that it matches PARAM_METADATA</smdp_metadata_seg_mac 	RQ44_002

Test Sequence #02 Nominal: optional elements missing

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	SM-DP+ is configured with #SMDP_METADATA_ABS for the pending Profile PROFILE_OPERATIONAL1.

This test sequence SHALL be the same as the Test Sequence #01 defined in the current section, with the following parameter assignments:

- PARAM_R_AUTH_CLIENT = #R_AUTH_CLIENT_META_ABS
- PARAM_METADATA = #SMDP_METADATA_ABS

Test Sequence #03 Nominal: large icon

Initial Conditions	
Entity Description of the initial condition	
SM-DP+	SM-DP+ is configured with #SMDP_METADATA_OP_PROF1_2_SEG for the pending Profile PROFILE_OPERATIONAL1.

This test sequence SHALL be the same as the Test Sequence #01 defined in the current section, with the following parameter assignments:

- PARAM_R_AUTH_CLIENT = #R_AUTH_CLIENT_META_LARGE_ICON
- PARAM_METADATA = #SMDP_METADATA_OP_PROF1_2_SEG

Test Sequence #04 Nominal: long Service Provider name

Initial Conditions			
Entity	Description of the initial condition		
SM-DP+	SM-DP+ is configured with #SMDP_METADATA_SPN_LONG for the pending Profile PROFILE_OPERATIONAL1.		

This test sequence SHALL be the same as the Test Sequence #01 defined in the current section, with the following parameter assignments:

V1.4 Page 539 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

- PARAM_R_AUTH_CLIENT = #R_AUTH_CLIENT_META_SPN_LONG
- PARAM_METADATA = #SMDP_METADATA_SPN_LONG

Test Sequence #05 Nominal: long Profile name

Initial Conditions	
Entity	Description of the initial condition
SM-DP+	SM-DP+ is configured with #SMDP_METADATA_PN_LONG for the pending Profile PROFILE_OPERATIONAL1.

This test sequence SHALL be the same as the Test Sequence #01 defined in the current section, with the following parameter assignments:

- PARAM_R_AUTH_CLIENT = #R_AUTH_CLIENT_META_PN_LONG
- PARAM_METADATA = #SMDP_METADATA_PN_LONG

Test Sequence #06 Nominal: non-ASCII characters

Initial Conditions		
Entity	Description of the initial condition	
SM-DP+	SM-DP+ is configured with #SMDP_METADATA_NON_ASCII for the pending Profile PROFILE_OPERATIONAL1.	

This test sequence SHALL be the same as the Test Sequence #01 defined in the current section, with the following parameter assignments:

- PARAM_R_AUTH_CLIENT = #R_AUTH_CLIENT_META_NON_ASCII
- PARAM_METADATA = #SMDP_METADATA_NON_ASCII

Test Sequence #07 Nominal: multiple notificationConfigurationInfo elements

Initial Conditions	
Entity Description of the initial condition	
SM-DP+	SM-DP+ is configured with #SMDP_METADATA_NOTIF_MULTI for the pending Profile PROFILE_OPERATIONAL1.

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE _AUTH_OK)	

V1.4 Page 540 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC _OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_C LIENT_META_NOTIF_MULTI)	RQ44_002 RQ55_033_1
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BP P_RESP_OP1_PPK) Construct the complete metadata element from the response and verify that it matches #SMDP_METADATA_NOTIF_M ULTI	RQ44_002 RQ55_033_1

5.4 Device Procedures

5.4.1 Local Profile Management - Add Profile

5.4.1.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ29_007_1, RQ29_008, RQ29_009, RQ29_011, RQ29_013, RQ29_015
- RQ31_062, RQ31_064, RQ31_072, RQ31_077, RQ31_079, RQ31_096, RQ31_100, RQ31_102, RQ31_106, RQ31_108, RQ31_112, RQ31_161
- RQ32_001, RQ32_002, RQ32_003, RQ32_004, RQ32_062, RQ32_065, RQ32_066, RQ32_068, RQ32_069, RQ32_070, RQ32_071
- RQ41_001, RQ41_005, RQ44_001
- RQC1_006, RQC1_008, RQC1_009, RQC3_014

5.4.1.2 Test Cases

5.4.1.2.1 TC_LPAd_AddProfile_Manual_Entry

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	

V1.4 Page 541 of 777

Test Sequence #01 Nominal: Add a new Operational Profile by using Activation Code (manual entry)

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Initiate Add Profile operation	LPAd requests the Activation Code from the End User	RQ32_062 RQ32_066 RQC1_009
2	S_EndUser→ LPAd	Provide #ACTIVATION_CODE_1 by manual entry	No error	RQ31_064 RQ31_077 RQ41_001
3	PROC_TLS_IN	IITIALIZATION_SERVER_AUTH on	ES9+	
4	PROC_ES9+_I	NIT_AUTH		
5	PROC_ES9+_/	AUTH_CLIENT with #MATCHING_I	D_1 as <matching_id></matching_id>	
6	PROC_ES9+_GET_BPP (see Note 1)			
7	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_062 RQ31_106 RQ32_001 RQ32_002 RQ32_065 RQC1_008 RQC1_014
8	PROC_ES9+_HANDLE_NOTIF			
9	S_EndUser → LPAd	List Profile operation is initiated	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071 RQ44_001
				RQC3_006

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

Test Sequence #02 Nominal: Add a new Operational Profile by using Activation Code (manual entry) with Confirmation Code

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state

V1.4 Page 542 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (PROFILE_OPERATIONAL1) associated with #CONFIRMATION_CODE1
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Initiate Add Profile operation	LPAd requests the Activation Code from the S_End User	RQ32_062 RQ32_066 RQC1_009
2	S_EndUser→ LPAd	Provide #ACTIVATION_CODE_3 by manual entry	No error	RQ31_064 RQ31_077 RQ41_001
3	PROC_TLS_INI	TIALIZATION_SERVER_AUT	ΓH on ES9+	
4	PROC_ES9+_I	NIT_AUTH		
5	PROC_ES9+_A	UTH_CLIENT_CC with #MAT	CHING_ID_3 as <matching_id></matching_id>	
6	LPAd → S_EndUser	LPAd requests the Confirmation Code from the S_End User.	CONFIRMATION_CODE1 is provided by manual entry.	RQ31_108 RQ31_112
7	PROC_ES9+_GET_BPP_CC (see Note 1)			
8	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_062 RQ31_106 RQ32_065 RQC1_008 RQC3_014
9	PROC_ES9+_HANDLE_NOTIF			
10	S_EndUser → LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071 RQ44_001 RQC1_006

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

5.4.1.2.2 TC_LPAd_AddProfile_QRcode_scanning

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	

V1.4 Page 543 of 777

Test Sequence #01 Nominal: Add a new Operational Profile by using Activation Code (QR code scanning)

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Initiate Add Profile operation	LPAd requests the Activation Code from the End User	RQ32_062 RQ32_066 RQC1_009
2	S_EndUser→ LPAd	Provide #ACTIVATION_CODE_1 by scanning the QR code	No error	RQ41_001 RQ41_005
3	PROC_TLS_IN	IITIALIZATION_SERVER_AUTH on ES	59+	
4	PROC_ES9+_I	NIT_AUTH		
5	PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_1 as <matching_id></matching_id>			
6	PROC_ES9+_GET_BPP (see Note 1)			
7	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_106 RQ32_065 RQC1_008 RQC3_014
8	PROC_ES9+_HANDLE_NOTIF			
9	S_EndUser→ LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071 RQ44_001 RQC1_006

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

5.4.1.2.3 TC_LPAd_AddProfile_ActivationCode_InvalidFormat_QRcode

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	
eUICC	The PROFILE_OPERATIONAL1 is not installed on the eUICC	

V1.4 Page 544 of 777

Test Sequence #01 Error: Add a new Operational Profile by using wrongly formatted Activation Code (QR code scanning)

Initial Conditions	
Entity	Description of the initial condition
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate Add Profile operation	Activation Code is requested from the End User by LPAd	RQ32_062 RQ32_066
2	S_EndUser → LPAd	Provide #ACTIVATION_CODE_INVALID_F ORMAT by scanning the QR code	LPAd provides an error message to the EndUser	RQ31_072
3	S_EndUser → LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is not displayed	RQ31_072

5.4.1.2.4 TC_LPAd_AddProfile_ActivationCode_InvalidFormat_ManualEntry

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Error: Add a new Operational Profile by using wrongly formatted Activation Code (Manual entry)

Initial Conditions	
Entity	Description of the initial condition
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate Add Profile operation	Activation Code is requested from the End User by LPAd	RQ32_062 RQ32_066
2	S_EndUser → LPAd	Provide #ACTIVATION_CODE_INVALID_FO RMAT by manual entry	LPAd provides an error message to the EndUser	RQ31_072
3	S_EndUser → LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is not displayed	RQ31_072

5.4.1.2.5 TC_LPAd_AddProfile_ConfirmationCode_smdpSigned2_QR

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	

V1.4 Page 545 of 777

Test Sequence #01 Nominal: Add a new Operational Profile by using Activation Code (QR code scanning) with confirmation code indicated only in smdpSigned2

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1) which requires confirmation code
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate Add Profile operation	Activation Code is requested from the End User by LPAd	RQ32_062 RQ32_066
2	S_EndUser → LPAd	Provide #ACTIVATION_CODE_1 by scanning the QR code	No error	RQ41_001 RQ41_005
3	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES	9+	
4	PROC_ES9+	_INIT_AUTH		
5	PROC_ES9+_AUTH_CLIENT_CC with #MATCHING_ID_1 as <matching_id></matching_id>			
6	LPAd → S_EndUser	Request the Confirmation Code from the S_End User.	#CONFIRMATION_CODE1 is provided by manual entry.	RQ31_108 RQ31_112
7	PROC_ES9+_GET_BPP_CC (see Note 1)			
8	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_106 RQ32_065
9	PROC_ES9+_HANDLE_NOTIF			
10	S_EndUser → LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071
Note 1:	Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to			

postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

5.4.1.2.6 TC_LPAd_AddProfile_ConfirmationCode_smdpSigned2_Manual_Entry

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	

V1.4 Page 546 of 777

Test Sequence #01 Nominal: Add a new Operational Profile by using Activation Code (manual entry) with confirmation code indicated only in smdpSigned2

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1) which requires confirmation code
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate Add Profile operation	Activation Code is requested from the End User by LPAd	RQ32_062 RQ32_066
2	S_EndUser → LPAd	Provide #ACTIVATION_CODE_1 by manual entry	No error	RQ41_001
3	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES9		
4	PROC_ES9+	_INIT_AUTH		
5	PROC_ES9+	_AUTH_CLIENT_CC with #MATCHING_II	D_1 as <matching_id></matching_id>	
6	LPAd → S_EndUser	Request the Confirmation Code from the S_End User.	#CONFIRMATION_CODE1 is provided by manual entry.	RQ31_108 RQ31_112
7	PROC_ES9+_GET_BPP_CC (see Note 1)			
8	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_106 RQ32_065
9	PROC_ES9+_HANDLE_NOTIF			
10	S_EndUser → LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

5.4.1.2.7 TC_LPAd_AddProfile_default_SM-DP+_address

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

V1.4 Page 547 of 777

Test Sequence #01 Nominal: Add a new Operational Profile by using the default SM-DP+ Address

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for PROFILE_OPERATIONAL1 linked to the EID of the eUICC

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate Add Profile operation See Note1	No error	RQ31_079 RQ32_062 RQ32_068
2	PROC_TLS_	INITIALIZATION_SERVER_AUTH on ES	9+	
3	PROC_ES9+	PROC_ES9+_INIT_AUTH		
4	PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_EMPTY as <matching_id> or missing MatchingID data object</matching_id>			
5	PROC_ES9+_GET_BPP (see Note 2)			
6	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_106 RQ32_065
7	PROC_ES9+_HANDLE_NOTIF			
8	S_EndUser → LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071

Note 1: The Profile download by default SM-DP+ address MAY be implemented in different ways (e.g. some Device MAY implement a separate LUI menu for this function, some Device MAY request first the activation code, etc.). In order to enforce that the default SM-DP+ address is used the user SHALL not enter the Activation Code in case it is requested.

Note 2: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

5.4.1.2.8 TC_LPAd_AddProfile_QRCode_with_ConfirmationCode

General Initial Conditions	
Entity Description of the general initial condition	
Device	The protection of access to the LUI is disabled

V1.4 Page 548 of 777

Test Sequence #01 Nominal: Add a new Operational Profile by using Activation Code (QR code scanning) with confirmation code

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (PROFILE_OPERATIONAL1)
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Initiate Add Profile operation	Activation Code is requested from the End User by LPAd	RQ32_06 2RQ32_0 66
2	S_EndUser→ LPAd	Provide#ACTIVATION_CODE_3 by scanning the QR code		RQ41_00 1RQ41_0 05
3	PROC_TLS_IN	IITIALIZATION_SERVER_AUTH on ES9+		
4	PROC_ES9+_I	NIT_AUTH		
5	PROC_ES9+_AUTH_CLIENT_CC with #MATCHING_ID_3 as <matching_id></matching_id>			
6	LPAd → S_EndUser	Request the Confirmation Code from the S_End User.	#CONFIRMATION_CODE1 is provided by manual entry.	RQ31_10 8
7	PROC_ES9+_GET_BPP_CC (see Note 1)			
8	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_106 RQ32_065
9	PROC_ES9+_HANDLE_NOTIF			
10	S_EndUser → LPAd	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071 RQ44_001

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

V1.4 Page 549 of 777

5.4.1.2.9 TC_LPAd_AddProfile_PPRs

Test Sequence #01 Nominal: End User Confirmation after PPR1 consent requested

Initial Conditions		
Entity Description of the initial condition		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_4.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_4 (associated with PROFILE_OPERATIONAL4)	

Step	Direction	Sequence / Description	Expected result	REQ
IC1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
IC2	PROC_ES9+_INIT_AUTH			
IC3		AUTH_CLIENT		
	Extract <s_tr< td=""><td>ANSACTION_ID></td><td></td><td></td></s_tr<>	ANSACTION_ID>		
IC4	PROC_ES9+_	GET_BPP with #METADATA_OP_	PROF4 used in #GET_BPP_OK	
1	LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation either at this point or at a previous point of the procedure If Authenticated Confirmation was requested at a previous point, simple End User Confirmation/Rejection is requested. Relevant information about PPRs is shown and the End User consent is requested either at this point or at a previous point of the procedure. (See Note)	RQ29_007 _1 RQ29_008 RQ29_009 RQ29_015 RQ31_096 RQ31_100 RQ31_102 RQ29_011 RQ29_013
2	S_EndUser → LPAd	End User Confirmation is performed within the period as defined in #IUT_EU_CONFIRMATION_TI MEOUT		
3	PROC_ES9+_HANDLE_NOTIF			
4	S_EndUser → LPAd	List Profile operation is initiated	PROFILE_OPERATIONAL4 is displayed in Disabled state	RQ31_161

V1.4 Page 550 of 777

Note: The request for this End User consent for the installation of Profile Policy Rules and Profile download MAY be combined into a single prompt.

Test Sequence #02 Nominal: End User Confirmation after PPR2 consent requested

Initial Conditions		
Entity Description of the initial condition		
LPAd	Add Profile operation is initiated by using #ACTIVATION_CODE_3_NO_CC.	
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_3 (associated with PROFILE_OPERATIONAL3)	

PROC_ES9+_IN PROC_ES9+_AL Extract <s_trai< th=""><th>JTH_CLIENT</th><th>ES9+</th><th></th></s_trai<>	JTH_CLIENT	ES9+	
PROC_ES9+_Al Extract <s_trai< td=""><td>JTH_CLIENT</td><td></td><td></td></s_trai<>	JTH_CLIENT		
Extract <s_traf< td=""><td></td><td></td><td></td></s_traf<>			
PROC ES9+ GI			
1 NOO_LOS1_O	ET_BPP with #METADATA_OP_P	ROF3 used in #GET_BPP_OK	
LPAd → S_EndUser	Request for Confirmation if not requested before.	The LPA provides means for the End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation either at this point or at a previous point of the procedure If Authenticated Confirmation was requested at a previous point, simple End User Confirmation/Rejection is requested. Relevant information about PPRs is shown and the End User consent is requested either at this point or at a previous point of the procedure. (See Note)	RQ29_007 _1 RQ29_008 RQ29_009 RQ29_015 RQ31_096 RQ31_100 RQ31_102 RQ29_011 RQ29_013
S_EndUser → LPAd	End User Confirmation is performed within the period as defined in #IUT_EU_CONFIRMATION_TI MEOUT		
PROC_ES9+_HANDLE_NOTIF			
S_EndUser → LPAd	List Profile operation is initiated	PROFILE_OPERATIONAL3 is displayed in Disabled state	RQ31_161
SL	S_EndUser → .PAd PROC_ES9+_H S_EndUser → .PAd	End User Confirmation is performed within the period as defined in #IUT_EU_CONFIRMATION_TI MEOUT PROC_ES9+_HANDLE_NOTIF S_EndUser → List Profile operation is initiated	End User Confirmation/Rejection of the Profile Download as defined in SGP.21 [3] for Authenticated Confirmation either at this point or at a previous point of the procedure Request for Confirmation if not requested before. Request for Confirmation if not requested before. Request for Confirmation if not requested before. If Authenticated Confirmation was requested at a previous point, simple End User Confirmation/Rejection is requested. Relevant information about PPRs is shown and the End User consent is requested either at this point or at a previous point of the procedure. SENDED SENDERS → List Profile expertion is initiated. PROFILE_OPERATIONAL3 is

Note: The request for this End User consent for the installation of Profile Policy Rules and Profile download MAY be combined into a single prompt

V1.4 Page 551 of 777

5.4.1.2.10TC_LPAd_LUI_access_protected

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is enabled	

Test Sequence #01 Nominal: Add a new Operational Profile

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Enter the LUI	End User Intent verification for Authenticated Confirmation is requested.	RQ32_003
2	S_EndUser→ LPAd	Initiate Add Profile operation	LPAd requests the Activation Code from the End User	RQ32_062 RQ32_066
3	S_EndUser→ LPAd	Provide #ACTIVATION_CODE_1 by manual entry		RQ31_064 RQ31_077 RQ41_001
4	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
5	PROC_ES9+_INIT_AUTH			
6	PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_1 as <matching_id></matching_id>			
7	PROC_ES9+_GET_BPP (see Note 1)			
8	LPAd → S_EndUser	Request for Authenticated or Simple Confirmation, if not requested before.	End User Intent successfully verified for Authenticated or Simple Confirmation as defined in SGP.21 [3], if not verified before.	RQ32_001 RQ32_003
9	PROC_ES9+_HANDLE_NOTIF			
10	S_EndUser → LPAd	List Profile operation is initiated	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ32_069 RQ32_070 RQ32_071

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

V1.4 Page 552 of 777

5.4.1.2.11 TC_LPAd_AddProfile_Security_Errors

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	
eUICC	The PROFILE_OPERATIONAL1 is not installed on the eUICC	

Test Sequence #01 Error: Stop Add Profile Operation if No Confirmation Provided

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for #MATCHING_ID_1 (PROFILE_OPERATIONAL1)
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
IC1	S_EndUser → LPAd	Initiate Add Profile operation	LPAd requests the Activation Code from the End User	
IC2	S_EndUser → LPAd	Provide #ACTIVATION_CODE_1	No error	
IC3	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+ (See Note 2)			
IC4	PROC_ES9+_INIT_AUTH			
IC5	PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_1 as <matching_id></matching_id>			
IC6	PROC_ES9+_GET_BPP (see Note 1)			
1	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before. The End User SHALL not provide Authenticated Confirmation.	The LPAd stops the Add Profile procedure	RQ32_001 RQ32_002 RQ32_004 RQ32_065
2	S_EndUser → LPAd	List Profile operation is initiated	PROFILE_OPERATIONAL1 is not displayed	RQ32_004

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

Note 2: Step IC6 is conditional - occurs only if Step 1 (Request for Confirmation) was not executed before

5.4.2 Local Profile Management - ListProfiles

5.4.2.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

V1.4 Page 553 of 777

GSM Association

Official Document SGP.23 - SGP.23 RSP Test Specification

Requirements

- RQ32_053, RQ32_054, RQ32_058, RQ32_059
- RQ44_001

5.4.2.2 Test Cases

5.4.2.2.1 TC_LPAd_ListProfiles

General Initial Conditions	
Entity Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is installed on the eUICC
Device	The protection of access to the LUI is disabled

Non-confidential

Test Sequence #01 Nominal: List the Profiles and their current state

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Enabled
eUICC	The PROFILE_OPERATIONAL2 is Disabled

Ste	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Request the list of Profiles	Display PROFILE_OPERATIONAL1 with Enabled state and the PROFILE_OPERATIONAL2 with Disabled state in human readable format.	RQ32_053 RQ32_054 RQ32_058 RQ32_059 RQ44_001

5.4.3 Local Profile Management - SetNickname

5.4.3.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

RQ32_0001, RQ32_002, RQ32_073, RQ32_074, RQ32_076, RQ32_078

V1.4 Page 554 of 777

5.4.3.2 Test Cases

5.4.3.2.1 TC_LPAd_SetNickname

General Initial Conditions		
Entity	ntity Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL2 is installed on the eUICC	
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Nominal: Add a Nickname on a Disabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is Disabled
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is not defined

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Select PROFILE_OPERATIONAL1. Indicates the intention to change the Profile Nickname of PROFILE_OPERATIONAL1.	LPA offers to the End User a way to enter the Nickname.	RQ32_074
2	S_EndUser→ LPAd	Set the Profile Nickname of the PROFILE_OPERATIONAL1 to #NICKNAME2	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation, if not verified before. LPAd sets the Profile Nickname (No Error)	RQ32_001 RQ32_002 RQ32_073 RQ32_076
3	Exit the UI mer	nu		
4	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName of PROFILE_OPERATIONAL1.	Profile Nickname of PROFILE_OPERATIONAL1 equals to #NICKNAME2	RQ32_078
5	Power off then power on the Device			
6	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName of PROFILE_OPERATIONAL1.	Profile Nickname of PROFILE_OPERATIONAL1 equals to #NICKNAME2	RQ32_078

Test Sequence #02 Nominal: Add a Nickname on an Enabled Operational Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL2 is Enabled

V1.4 Page 555 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Select PROFILE_OPERATIONAL2. Indicates the intention to change the Profile Nickname of PROFILE_OPERATIONAL2	LPA offers to the End User a way to enter the nickname.	RQ32_074
2	S_EndUser→ LPAd	Set the Profile Nickname of the PROFILE_OPERATIONAL2 to #NICKNAME3	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation, if not verified before. LPAd sets the Profile Nickname (No Error)	RQ32_073 RQ32_076
3	Exit the UI mer	nu		
4	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName ofPROFILE_OPERATIONAL2.	Profile Nickname of PROFILE_OPERATIONAL2 equals to #NICKNAME3	RQ32_078
5	Power off then power on the Device			
6	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName of PROFILE_OPERATIONAL2.	Profile Nickname of PROFILE_OPERATIONAL2 equals to #NICKNAME3	RQ32_078

5.4.3.2.2 TC_LPAd_EditNickname

General Initial Conditions	
Entity Description of the general initial condition	
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL2 is installed on the eUICC
Device	The protection of access to the LUI is disabled

Test Sequence #01 Nominal: Edit the Nickname on a Disabled Operational Profile

Initial Conditions		
Entity	ntity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is Disabled	
eUICC	The Nickname of the PROFILE_OPERATIONAL1 is equal to #NICKNAME1	

Ste	p Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Select PROFILE_OPERATIONAL1	Profile Nickname equals to #NICKNAME1	RQ32_075

V1.4 Page 556 of 777

Non-confidential

		Indicates the intention to change the Profile Nickname of PROFILE_OPERATIONAL1	LPA offers to the End User a way to enter a new Nickname.	
2	S_EndUser→ LPAd	Set the Profile Nickname of the PROFILE_OPERATIONAL1 to #NICKNAME2	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation, if not verified before. LPAd sets the Profile Nickname (No Error)	RQ32_073 RQ32_076
3	Exit the UI mer	nu		
4	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName ofPROFILE_OPERATIONAL1	Profile Nickname equals to #NICKNAME2	RQ32_078
5	Power off then power on the Device			
6	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName ofPROFILE_OPERATIONAL1	Profile Nickname equals to #NICKNAME2	RQ32_078

Test Sequence #02 Nominal: Edit the Nickname on an Enabled Operational Profile

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL2 is Enabled	
eUICC	The Nickname of the PROFILE_OPERATIONAL2 is equal to #NICKNAME3	

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Select PROFILE_OPERATIONAL2 Indicates the intention to change the Profile Nickname of PROFILE_OPERATIONAL2	Profile Nickname equals to #NICKNAME3 LPA offers to the End User a way to enter a new Nickname.	RQ32_075
2	S_EndUser→ LPAd	Set the Profile Nickname of the PROFILE_OPERATIONAL2 to #NICKNAME4	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation, if not verified before. LPAd sets the Profile Nickname (No Error)	RQ32_073 RQ32_076
3	Exit the UI mer	nu		
4	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName of PROFILE_OPERATIONAL2	Profile Nickname equals to #NICKNAME4	RQ32_078
5	Power off then power on the Device			

V1.4 Page 557 of 777 Non-confidential

	6	S_EndUser→ LPAd	Perform an LUI dependent action to display the NickName ofPROFILE_OPERATIONAL2	Profile Nickname equals to #NICKNAME4	RQ32_078	
--	---	--------------------	--	---------------------------------------	----------	--

Local Profile Management - Delete Profile 5.4.4

5.4.4.1 **Conformance Requirements**

References

GSMA RSP Technical Specification [2]

Requirements

- RQ32_001, RQ32_002, RQ32_004, RQ32_043, RQ32_044, RQ32_047, RQ32_050
- RQ35_008

5.4.4.2 **Test Cases**

5.4.4.2.1 TC_LPAd_DeleteProfile_Disabled_without_PPR

General Initial Conditions	
Entity Description of the general initial condition	
Device	The protection of access to the LUI is disabled

Test Sequence #01 Nominal: Deleting Disabled Profile, No PPRs

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_TEST_DP_ADDRESS1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL1 is in Disabled state
eUICC	The PROFILE_OPERATIONAL2 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Delete Profile procedure is initiated for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation.	RQ32_001 RQ32_002 RQ32_043 RQ32_044
2	LPAd → S_SM-DP+	Delete Notification containing #ICCID_OP_PROF1 is sent by the LPAd	The delete Notification as defined below is received by the S_SM-DP+ within the timeout	RQ35_015 RQ35_008

V1.4 Page 558 of 777

			#IUT_LPAd_NOTIFICATION_ TIMEOUT MTD_HANDLE_NOTIF(#PEN DING_NOTIF_DEL1) Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA</tbs_euicc_notif_sig>	
3	S_EndUser → LPAd	Request for List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format. PROFILE_OPERATIONAL1 is not shown.	RQ32_058

Note: The timeout in Step 2 SHALL start after the End User Intent verification.

5.4.4.2.2 TC_LPAd_DeleteProfile_Enabled_without_PPR

General Initial Conditions Entity Description of the general initial condition	

Test Sequence #01 Nominal: Deleting Enabled Profile, No PPRs

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL5 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL2 with #METADATA_OP_PROF2_TEST_DP_ADDRESS1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL5 is in Enabled state
eUICC	The PROFILE_OPERATIONAL2 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate Delete Profile procedure for PROFILE_OPERATIONAL5	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation.	RQ32_043 RQ32_044 RQ32_047
2	LPAd → S_SM-DP+	Send Disable Notification containing #ICCID_OP_PROF5	The disable Notification as defined below is received by the S_SM-DP+ within the timeout	RQ35_008 RQ35_015

V1.4 Page 559 of 777

			#IUT_LPAd_NOTIFICATION_ TIMEOUT MTD_HANDLE_NOTIF(#PEN DING_NOTIF_DIS5) Verify the	
			euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA See Note</tbs_euicc_notif_sig>	
3	LPAd → S_SM-DP+	Send Delete Notification containing #ICCID_OP_PROF5	The delete Notification as defined below is received by the S_SM-DP+ within the timeout #IUT_LPAd_NOTIFICATION_ TIMEOUT MTD_HANDLE_NOTIF(#PEN DING_NOTIF_DEL5) Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA See Note</tbs_euicc_notif_sig>	RQ35_008 RQ35_015 RQ35_018
4	S_EndUser → LPAd	Request for List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format. PROFILE_OPERATIONAL5 is not shown.	RQ32_058
5	S_EndUser → Device	Power off then power on the Device	During Device boot up no PIN entry is requested from the End User.	RQ32_051
Note:	. The timeout	SHALL start after the End User Intent ver	rification.	

Note: The timeout SHALL start after the End User Intent verification.

5.4.4.2.3 TC_LPAd_DeleteProfile_Error_with_PPR1

General Initial Conditions			
Entity Description of the general initial condition			
Device	evice The protection of access to the LUI is disabled		

V1.4 Page 560 of 777

Test Sequence #01 Error: Deleting Enabled Profile, PPR1 set

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL4 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL4 is in Enabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Delete Profile procedure is initiated for PROFILE_OPERATIONAL4	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation. See Note 1 and Note 2	RQ32_043 RQ32_044 RQ32_047 RQ32_050
2	S_EndUser→ LPAd	Request for List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format. PROFILE_OPERATIONAL4 is shown in Enabled state.	RQ32_058

Note 1: The LPAd MAY check the policy rules of the Profiles and give a warning to the End User. The procedure can be continued after the warning and the End User shall continue the procedure.

Note 2: The LPAd MAY display an error indicating that the deletion of the Profile is failed.

5.4.4.2.4 TC_LPAd_DeleteProfile_Error_Disabled_with_PPR2

General Initial Conditions			
Entity Description of the general initial condition			
Device	The protection of access to the LUI is disabled		

Test Sequence #01 Error: Deleting Disabled Profile, PPR2 set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL7 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL7 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Delete Profile procedure is initiated for PROFILE_OPERATIONAL7	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation. See Note 1 and Note 2	RQ32_043 RQ32_044 RQ32_047 RQ32_050

V1.4 Page 561 of 777

2	S_EndUser→ LPAd	Request for List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format. PROFILE_OPERATIONAL7 is shown in Disabled state.	RQ32_058
---	--------------------	---------------------------	---	----------

Note 1: The LPAd MAY check the policy rules of the Profiles and give a warning to the End User. The procedure can be continued after the warning and the End User shall continue the procedure.

Note 2: The LPAd MAY display an error indicating that the deletion of the Profile is failed.

5.4.4.2.5 TC_LPAd_DeleteProfile_Error_Enabled_with_PPR2

General Initial Conditions			
Entity Description of the general initial condition			
Device The protection of access to the LUI is disabled			

Test Sequence #01 Error: Deleting Enabled Profile, PPR2 set

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL8 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL8 is in Enabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate Delete Profile procedure for PROFILE_OPERATIONAL8	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation. See Note 2 and Note 3	RQ32_043 RQ32_044 RQ32_047 RQ32_050
2	LPAd → S_SM-DP+	Send Disable Notification containing #ICCID_OP_PROF8	The disable Notification as defined below is received by the S_SM-DP+ within the timeout #IUT_LPAd_NOTIFICATION_TI MEOUT MTD_HANDLE_NOTIF (#PENDING_NOTIF_DIS8) Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA See Note 1</tbs_euicc_notif_sig>	RQ35_008 RQ35_015
3	S_EndUser → LPAd	Request for List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format.	RQ32_058

V1.4 Page 562 of 777

Non-confidential

			PROFILE_OPERATIONAL8 is shown in Disabled state.	
4	S_EndUser → Device	Power off then power on the Device	During Device boot up no PIN entry is requested from the End User.	RQ32_051

Note 1: The timeout SHALL start after the End User Intent verification.

Note 2: The LPAd MAY check the policy rules of the Profiles and give a warning to the End User. The procedure can be continued after the warning and the End User shall continue the procedure.

Note 3: The LPAd MAY display an error indicating that the deletion of the Profile is failed.

5.4.4.2.6 TC_LPAd_DeleteProfile_Security_Errors

General Initial Conditions			
Entity Description of the general initial condition			
Device The protection of access to the LUI is disabled			

Test Sequence #01 Error: Stop Delete Profile Operation if No Confirmation Provided

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL1 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Delete Profile procedure is initiated for PROFILE_OPERATIONAL1. The End User SHALL not provide Authenticated Confirmation.	The LPAd stops the Delete Profile procedure.	RQ32_001 RQ32_002 RQ32_004 RQ32_043
2	S_EndUser → LPAd	Request for List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format. PROFILE_OPERATIONAL1 is shown.	RQ32_004

5.4.5 Local Profile Management - Enable Profile

5.4.5.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

V1.4 Page 563 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Requirements

- RQ32_001, RQ32_002, RQ32_004, RQ32_006, RQ32_007, RQ32_008, RQ32_011,
 RQ32_012, RQ32_014, RQ32_019_1, RQ32_053
- RQ35_008, RQ35_012, RQ35_014_1, RQ35_014_3, RQ35_018, RQ35_019

5.4.5.2 Test Cases

5.4.5.2.1 TC_LPAd_EnableProfile

General Initial Conditions			
Entity Description of the general initial condition			
Device	The protection of access to the LUI is disabled		
Device The End User gets presented a list of installed (operational) Profiles with the current state			

Test Sequence #01 Nominal: Enable a formerly disabled Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL5 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL5 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Enable Profile operation for PROFILE_OPERATIONAL5	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation. PROFILE_OPERATIONAL5 is enabled	RQ32_001 RQ32_002 RQ32_006 RQ32_007
2	LPAd → S_SM-DP+	Send the Enable Notification containing #ICCID_OP_PROF5	The Enable Notification MTD_HANDLE_NOTIF(#PEND ING_NOTIF_EN5) is received by the S_SM-DP+ within the timeout #IUT_LPAd_NOTIFICATION_TI MEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA S_SM-DP+ SHALL return #R_HTTP_204_OK</tbs_euicc_notif_sig>	RQ35_008
3	S_EndUser → Device	Enter #PO1_PIN1 to authenticate the user	Successful End User authentication for the selected application	RQ32_19_1

V1.4 Page 564 of 777

4	S_EndUser → LPAd	Request List Profiles	PROFILE_OPERATIONAL5 is shown in Enabled state.	RQ32_058	
NOTE: The timeout SHALL start after the End User Intent verification.					

5.4.5.2.2 TC_LPAd_EnableProfile_ImplicitDisable

General Initial Conditions			
Entity Description of the general initial condition			
Device The protection of access to the LUI is disabled			

Test Sequence #01 Nominal: Enable a Profile with implicit disabling of the formerly enabled Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL5 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL6 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL5 is in Enabled state
eUICC	The PROFILE_OPERATIONAL6 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Enable Profile operation for PROFILE_OPERATIONAL6	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation.	RQ32_006 RQ32_007
2	LPAd → S_SM-DP+(1)	Disable Notification containing #ICCID_OP_PROF5 is sent by the LPAd	The Disable Notification MTD_HANDLE_NOTIF(#PEND ING_NOTIF_DIS5) is received by the S_SM-DP+ (configured with #TEST_DP_ADDRESS1) within the timeout #IUT_LPAd_NOTIFICATION_T IMEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA S_SM-DP+ SHALL return #R_HTTP_204_OK</tbs_euicc_notif_sig>	RQ35_008
3	$\begin{array}{c} LPAd \to \\ S_SM\text{-DP\text{+}(2)} \end{array}$	Send the Enable Notification containing #ICCID_OP_PROF6	The Enable Notification MTD_HANDLE_NOTIF(#PEND ING_NOTIF_EN6) is received by the S_SM-DP+ (configured	RQ35_008

V1.4 Page 565 of 777

5	S_EndUser → LPAd	Request List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format. PROFILE_OPERATIONAL6 is shown in Enabled state.	RQ32_058
4	S_EndUser → Device	Enter #PO2_PIN1 to authenticate the user	Successful End User authentication for the selected application	RQ32_19_1
			with #TEST_DP_ADDRESS2) within the timeout #IUT_LPAd_NOTIFICATION_T IMEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA S_SM-DP+ SHALL return #R_HTTP_204_OK</tbs_euicc_notif_sig>	

Note 1: The Notifications (steps 2 and 3) MAY be sent sequentially in either order or in parallel.

Note 2: The timeout (steps 2 and 3) SHALL start after the End User Intent verification.

5.4.5.2.3 TC_LPAd_EnableProfile_Error_ProfileAlreadyEnabled

General Initial Conditions	
Entity Description of the general initial condition	
Device	The protection of access to the LUI is disabled

Test Sequence #01 Error: Enable an already enabled Profile

Initial Conditions	
Entity Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL1 is in Enabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Enable Profile operation for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation.	RQ32_006 RQ32_007
2	LPAd → S_EndUser	Result of the Profile enabling	Enable Profile procedure terminates indicating an error	RQ32_012

V1.4 Page 566 of 777

5.4.5.2.4 TC_LPAd_EnableProfile_Error_PPR1Set

General Initial Conditions	
Entity Description of the general initial condition	
Device	The protection of access to the LUI is disabled

Test Sequence #01 Error: Enabled Profile when a formerly enabled Profile has set PPR1

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL4 is installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL4 is in Enabled state	
eUICC	The PROFILE_OPERATIONAL1 is in Disabled state	

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Enable Profile operation for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation. See Note 1 and Note 2	RQ32_006 RQ32_007 RQ32_008 RQ32_014
2	S_EndUser → LPAd	Request List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format. PROFILE_OPERATIONAL4 is shown in Enabled state.	RQ32_058

Note 1: The LPAd MAY check the policy rules of the Profiles and give a warning to the End User. The procedure can be continued after the warning and the End User shall continue the procedure.

Note 2: The LPAd MAY display an error indicating that the enabling of the Profile is failed.

5.4.5.2.5 TC_LPAd_EnableProfile_Security_Errors

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Error: Stop Enable Profile Operation if No Confirmation Provided

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC

V1.4 Page 567 of 777

eUICC

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Enable Profile operation for PROFILE_OPERATIONAL1 The End User SHALL not provide Simple Confirmation.	The LPAd stops the Enable Profile procedure.	RQ32_001 RQ32_002 RQ32_004 RQ32_006
2	S_EndUser → LPAd	Request List Profiles	PROFILE_OPERATIONAL1 is shown in Disabled state.	RQ32_004

5.4.6 Local Profile Management - Disable Profile

5.4.6.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ32_001, RQ32_002, RQ32_004, RQ32_025, RQ32_026, RQ32_028, RQ32_032, RQ32_034, RQ32_038, RQ32_053
- RQ35_008, RQ35_018, RQ35_019

5.4.6.2 Test Cases

5.4.6.2.1 TC_LPAd_DisableProfile

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Nominal: Disable an Enabled Profile

Initial Conditions		
Entity	Description of the initial condition	
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC	
eUICC	The PROFILE_OPERATIONAL1 is in Enabled state	
eUICC	There is no default SM-DP+ address configured	

V1.4 Page 568 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Disable Profile operation for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation. PROFILE_OPERATIONAL1 is disabled	RQ32_001 RQ32_002 RQ32_025 RQ32_026
2	LPAd → S_SM-DP+	Send the Disable Notification containing #ICCID_OP_PROF1	The Disable Notification MTD_HANDLE_NOTIF(#PEND ING_NOTIF_DIS1) is received by the S_SM-DP+ within the timeout #IUT_LPAd_NOTIFICATION_TI MEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA S_SM-DP+ SHALL return #R_HTTP_204_OK</tbs_euicc_notif_sig>	RQ35_008 RQ35_018 RQ35_019
3	S_EndUser → LPAd	Request List Profiles	Installed Operational Profile(s) with their current states are displayed in a human readable format. PROFILE_OPERATIONAL1 is shown in Disabled state.	RQ32_038 RQ32_053
Note 2: The timeout SHALL start after the End User Intent verification.				

${\bf 5.4.6.2.2\ TC_LPAd_Disable Profile_Error_ProfileAlready Disabled}$

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Error: Disable an already disabled Profile

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL1 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser→ LPAd	Initiate the Disable Profile operation for PROFILE_OPERATIONAL1	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation	RQ32_025 RQ32_026

V1.4 Page 569 of 777

Non-confidential

2	LPAd → S_EndUser	Result of the Profile disabling	The Disable Profile procedure terminates indicating a failure	RQ32_034
---	---------------------	---------------------------------	---	----------

5.4.6.2.3 TC_LPAd_DisableProfile_Error_PPR1Set

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Error: Disable an Enabled Profile with PPR1 set

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL4 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL4 is in Enabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Disable Profile operation for PROFILE_OPERATIONAL4	Successful End User Intent verified as defined in SGP.21 [3] for Simple Confirmation. See Note 1 and Note 2	RQ32_025 RQ32_026 RQ32_028 RQ32_034
2	S_EndUser → LPAd	Request List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format PROFILE_OPERATIONAL4 is shown in Enabled state	RQ32_053

Note 1: The LPAd MAY check the policy rules of the Profiles and give a warning to the End User. The procedure can be continued after the warning and the End User shall continue the procedure.

Note 2: The LPAd MAY display an error indicating that the disabling of the Profile is failed.

5.4.6.2.4 TC_LPAd_DisableProfile_Security_Errors

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

V1.4 Page 570 of 777

Test Sequence #01 Nominal: Stop Disable Profile Operation if No Confirmation Provided

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL1 is in Enabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the Disable Profile operation for PROFILE_OPERATIONAL1. The End User SHALL not provide Simple Confirmation.	The LPAd stops the Disable Profile procedure.	RQ32_001 RQ32_002 RQ32_004 RQ32_025
2	S_EndUser → LPAd	Request List Profiles	Installed Operational Profile(s) with their current states are displayed in a human readable format. PROFILE_OPERATIONAL1 is shown in Enabled state.	RQ32_004

5.4.7 Local eUICC Management - Retrieve EID Process

5.4.7.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

RQ33_001, RQ33_002, RQ33_003, RQ33_004

5.4.7.2 Test Cases

5.4.7.2.1 TC_LPAd_RetrieveEID

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Nominal: Retrieve EID

The purpose of this test is to check if the Device is capable to display the stored EID in as QR code or in text string format.

V1.4 Page 571 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Request to display EID. (See Note)	EID is displayed.	RQ33_001 RQ33_002
			The LPA presents the #EID1 to the End User as a text string and/or as a QR code.	
2	LPAd → S_EndUser	Presentation of the EID	If the EID is represented as text string, the text SHALL be identical to #EID1	RQ33_003 RQ33_004 RQ33_005
			If the #EID1 is shown as a QR code it SHALL be either #EID1_QR_CODE1 or #EID1_QR_CODE2 with or without blank spaces.	RQ33_005_1
Note: LPAd may display the EID by default				

5.4.8 Local eUICC Management - eUICC Memory Reset Process

5.4.8.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ32_053,
- RQ33_006, RQ33_012, RQ33_021_1, RQ33_021_2,
- RQ35_008, RQ35_018, RQ35_019

5.4.8.2 Test Cases

5.4.8.2.1 TC_LPAd_eUICCMemoryReset

General Initial Conditions		
Entity Description of the general initial condition		
Device	No proactive session is ongoing. NOTE: these test cases MAY fail due to the fact that a proactive is ongoing but it is impossible to determine that this is the case. In this instance it is recommended to repeat the test.	
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Nominal: eUICC Memory Reset, Operational Profile installed, no Operational Profile enabled

The purpose of this test is to check the basic functions of the eUICC Memory Reset. An installed but not enabled Operational Profile SHALL be deleted.

V1.4 Page 572 of 777

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL1 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the eUICC Memory Reset for operational profiles	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation.	RQ33_006
2	LPAd → S_SM-DP+	Delete Notification containing #ICCID_OP_PROF1 is sent by the LPAd	The Delete Notification MTD_HANDLE_NOTIF(#PEND ING_NOTIF_DEL1) is received by the S_SM-DP+ within the timeout #IUT_LPAd_NOTIFICATION_TI MEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA The S_SM-DP+ SHALL return #R_HTTP_204_OK</tbs_euicc_notif_sig>	RQ35_008 RQ35_018 RQ35_019
3	S_EndUser → LPAd	Request List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format No Operational Profile is available	RQ32_053 RQ33_012
Note: The timeout (step 2) SHALL start after the End User Intent verification.				

Test Sequence #02 Nominal: eUICC Memory Reset, Operational Profile with PPR2 installed, no Operational Profile enabled

The purpose of this test is to check if an initiated eUICC Memory Reset deletes an installed but not enabled Operational Profile with PPR2 ('Deletion of this Profile is not allowed').

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL1 is installed on the eUICC with #METADATA_OP_PROF1_MEMRES1
eUICC	The PROFILE_OPERATIONAL1 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
------	-----------	---------------------------	-----------------	-----

V1.4 Page 573 of 777

1	S_EndUser → LPAd	Initiate the eUICC Memory Reset for operational profiles	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation.	RQ33_00 6
2	LPAd → S_SM-DP+	Delete Notification containing #ICCID_OP_PROF1 is sent by the LPAd	The Delete Notification MTD_HANDLE_NOTIF(#PENDI NG_NOTIF_DEL1) is received by the S_SM-DP+ within the timeout #IUT_LPAd_NOTIFICATION_TI MEOUT Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA The S_SM-DP+ SHALL return #R_HTTP_204_OK</tbs_euicc_notif_sig>	RQ35_00 8 RQ35_01 8 RQ35_01 9
3	S_EndUser → LPAd	Request List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format No Operational Profile is available	RQ32_05 3 RQ33_01 2

Note: The timeout (step 2) SHALL start after the End User Intent verification.

5.4.8.2.2 TC_LPAd_eUICCMemoryResetWithPINVerification

General Initial Conditions		
Entity	Entity Description of the general initial condition	
Device	No proactive session is ongoing. NOTE: these test cases may fail due to the fact that a proactive session is ongoing but it is impossible to determine that this is the case. In this instance it is recommended to repeat the test.	
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Nominal: eUICC Memory Reset, installed and enabled Operational Profile with PPR1 and PPR2

The purpose of this test is to check if an initiated eUICC Memory Reset deletes an installed and enabled Operational Profile with PPR1 ('Disabling of this Profile is not allowed') and PPR2 ('Deletion of this Profile is not allowed').

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL5 is installed on the eUICC with #METADATA_OP_PROF5_MEMRES2
eUICC	The PROFILE_OPERATIONAL5 is in Enabled state

Step	Direction	Sequence / Description	Expected result	REQ
------	-----------	---------------------------	-----------------	-----

V1.4 Page 574 of 777

1	S_EndUser → LPAd	Initiate the eUICC Memory Reset for operational profiles	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation.	RQ33_006
2	LPAd → S_SM- DP+	Delete Notification containing #ICCID_OP_PROF5 is sent by the LPAd	The Delete Notification MTD_HANDLE_NOTIF(#PEN DING_NOTIF_DEL5) is received by the S_SM-DP+ within the timeout (#IUT_LPAd_NOTIFICATION _TIMEOUT, + #IUT_LPAd_READY_AFTER _REBOOT_TIMEOUT) Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA The S_SM-DP+ SHALL return #R_HTTP_204_OK See Note 3</tbs_euicc_notif_sig>	RQ35_008 RQ35_018 RQ35_019
3	Device	Power off then power on the Device If the Device does not automatically power off and power on, the S_EndUser SHALL power off and power on the Device.	During Device boot up no PIN entry is requested from the End User.	RQ33_011 RQ33_012
4	S_EndUser → LPAd	Request List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format No Operational Profile is available	RQ32_053 RQ33_012

Note 1:The Delete Notification (step 2) can be sent at any step after having successfully initiated the eUICC Memory Reset.

Note 2:The timeout (step 2) SHALL start after the End User Intent verification.

Note 3: A Disable Notification for PROFILE_OPERATIONAL5 MAY be sent before the Delete Notification. This notification SHALL NOT be checked.

Test Sequence #02 Nominal: eUICC Memory Reset, multiple Operational Profiles are installed, an Operational Profile is enabled

The purpose of this test is to check if an initiated eUICC Memory Reset deletes all Operational Profiles installed and send the required Notifications to the appropriate SM-DP+.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The PROFILE_OPERATIONAL5 is installed on the eUICC
eUICC	The PROFILE_OPERATIONAL5 is in Enabled state
eUICC	The PROFILE_OPERATIONAL6 is installed on the eUICC

V1.4 Page 575 of 777

eUICC The PROFILE_OPERATIONAL6 is in Disabled state

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the eUICC Memory Reset for operational profiles	Successful End User Intent verified as defined in SGP.21 [3] for Authenticated Confirmation.	RQ33_006
2	LPAd → S_SM- DP+(1)	Delete Notifications containing #ICCID_OP_PROF5 is sent by the LPAd	The Delete Notification MTD_HANDLE_NOTIF(#PEN DING_NOTIF_DEL5) is received by the S_SM-DP+ (configured with #TEST_DP_ADDRESS1) within the timeout #IUT_LPAd_NOTIFICATION_TIMEOUT The S_SM-DP+ SHALL return #R_HTTP_204_OK	RQ35_008 RQ35_018 RQ35_019
3	LPAd → S_SM- DP+(2)	Delete Notification containing #ICCID_OP_PROF6 is sent by the LPAd	The Delete Notification MTD_HANDLE_NOTIF(#PEN DING_NOTIF_DEL6) is received by the S_SM-DP+ (configured with #TEST_DP_ADDRESS2) within the timeout (#IUT_LPAd_NOTIFICATION _TIMEOUT, + #IUT_LPAd_READY_AFTER _REBOOT_TIMEOUT) Verify the euiccNotificationSignature <tbs_euicc_notif_sig> using the #PK_EUICC_ECDSA The S_SM-DP+ SHALL return #R_HTTP_204_OK See Note 3</tbs_euicc_notif_sig>	RQ35_008 RQ35_018 RQ35_019
4	Device	Power off then power on the Device If the Device does not automatically power off and power on, the S_EndUser SHALL power off and power on the Device.	During Device boot up no PIN entry is requested from the End User.	RQ33_011 RQ33_012
5	S_EndUser → LPAd	Request List Profiles	Installed Operational Profiles with their current states are displayed in a human readable format No Operational Profile is available	RQ32_053 RQ33_012

Note 1:The Delete Notifications (steps 2 and 3) MAY be sent sequentially in either order or in parallel and can be sent at any step after having successfully initiated the eUICC Memory Reset.

V1.4 Page 576 of 777

Note 2: The timeout (steps 2 and 3) SHALL start after the End User Intent verification.

Note 3: A Disable Notification for PROFILE_OPERATIONAL5 MAY be sent before the Delete Notification. This notification SHALL NOT be checked.

5.4.9 Local eUICC Management - eUICC Test Memory Reset Process

This section is defined as FFS and not applicable for this version of test specification.

5.4.10 Local eUICC Management - Set/Edit Default SM-DP+ Address Process

5.4.10.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

RQ33_021_2, RQ33_021_3, RQ33_021_5

5.4.10.2 Test Cases

5.4.10.2.1TC_LPAd_Set/Edit Default SM-DP+ Address

General Initial Conditions		
Entity	Description of the general initial condition	
Device	The protection of access to the LUI is disabled	

Test Sequence #01 Nominal: Set Default SM-DP+ Address where no Default Address has been set before

The purpose of this test is to set a default SM-DP+ address on a eUICC where no SM-DP+ default address is stored.

Initial Conditions	
Entity	Description of the initial condition
eUICC	No value is assigned to the Default SM-DP+ field

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the function to retrieve the configured address	The LPAd retrieves the Default SM-DP+ Address and presents it to the EndUser The current Default SM-DP+ Address is empty respectively no Default SM-DP+ Address is shown	RQ33_021_2

V1.4 Page 577 of 777

2	2	S_EndUser → LPAd	If required, initiate the function to enter #TEST_DP_ADDRESS1 as the new Default SM-DP+ address or enter directly #TEST_DP_ADDRESS1 as the new Default SM-DP+.	Successful End User Intent verified as defined in SGP.21 [4] for Simple Confirmation, if not verified before. The newly entered SM-DP+ Address is stored on the eUICC as the Default SM-DP+ Address	RQ33_021_3
3	3	S_EndUser → LPAd	Initiate the function to retrieve the configured address	The LPAd retrieves the Default SM-DP+ Address and presents it to the EndUser The current Default SM-DP+ Address #TEST_DP_ADDRESS1 is shown	RQ33_021_5

Test Sequence #02 Nominal: Edit the Default SM-DP+ Address and store it on the eUICC

The purpose of this test is to edit an existing default SM-DP+ address on a eUICC and to ensure that the changes are stored.

Initial Conditions	
Entity	Description of the initial condition
eUICC	The Default SM-DP+ field is set to #TEST_DEFAULT_DP_ADDRESS_1

Step	Direction	Sequence / Description	Expected result	REQ
	C. Frallica		The LPAd retrieves the Default SM-DP+ Address and presents it to the EndUser	
1	S_EndUser → LPAd	Initiate the function to retrieve the configured address	The current Default SM-DP+ Address is #TEST_DEFAULT_DP_ADDR ESS_1	RQ33_021_2
2	S_EndUser → LPAd	If required, initiate the function to enter #TEST_DP_ADDRESS1 as the new Default SM-DP+ address or enter directly #TEST_DP_ADDRESS1 as the new Default SM-DP+.	Successful End User Intent verified as defined in SGP.21 [4] for Simple Confirmation, if not verified before. The newly entered SM-DP+ Address is stored on the eUICC as the Default SM-DP+ Address	RQ33_021_3
3	S_EndUser → LPAd	Initiate the function to retrieve the configured address	The LPAd retrieves the Default SM-DP+ Address and presents it to the EndUser The current Default SM-DP+ Address #TEST_DP_ADDRESS1 is shown	RQ33_021_5

V1.4 Page 578 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Test Sequence #03 Nominal: Edit the Default SM-DP+ Address and store a Default Address with an empty value

The purpose of this test is to edit an existing Default SM-DP+ address on a eUICC and to ensure that the changes are stored even if the new Default Address value is empty

Initial Conditions	
Entity	Description of the initial condition
eUICC	The Default SM-DP+ field is set to #TEST_DEFAULT_DP_ADDRESS_1

Step	Direction	Sequence / Description	Expected result	REQ
1	S_EndUser → LPAd	Initiate the function to retrieve the configured address	The LPAd retrieves the Default SM-DP+ Address and presents it to the EndUser The current Default SM-DP+ Address is #TEST_DEFAULT_DP_ADDR ESS_1	RQ33_021_2
2	S_EndUser → LPAd	If required, initiate the function to enter "" (empty value) as the new Default SM-DP+ address or enter directly "" as the new Default SM-DP+.	Successful End User Intent verified as defined in SGP.21 [4] for Simple Confirmation, if not verified before. The newly entered SM-DP+ Address is stored on the eUICC as the Default SM-DP+ Address	RQ33_021_3
3	S_EndUser → LPAd	Initiate the function to retrieve the configured address	The LPAd retrieves the Default SM-DP+ Address and presents it to the EndUser The current Default SM-DP+ Address is empty respectively no Default SM-DP+ Address is shown	RQ33_021_5

5.4.11 Device Power On - Profile Discovery

5.4.11.1 Conformance Requirements

References

GSMA RSP Technical Specification [2]

Requirements

- RQ31_106
- RQ34_18, RQ34_020, RQ34_021, RQ34_023, RQ34_024

V1.4 Page 579 of 777

5.4.11.2 Test Cases

5.4.11.2.1TC_LPAd_DevicePowerOnProfileDiscovery_SM-DP+_address

General Initial Conditions	
Entity Description of the general initial condition	
Device	The protection of access to the LUI is disabled
Device	The setting of the configuration parameter for Device Power-on Profile discovery is 'Enabled'
Device	The Device is powered off

Test Sequence #01 Nominal: Power-on Profile discovery by using the default SM-DP+ Address

Initial Conditions	
Entity	Description of the initial condition
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
S_SM-DP+	There is a pending Profile download order for PROFILE_OPERATIONAL1 linked to the EID of the eUICC

Direction	Sequence / Description	Expected result	REQ
Power on the Device			
PROC_TLS_INITI	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+		
PROC_ES9+_INIT	Γ_AUTH		
PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_EMPTY as <matching_id> or missing MatchingID data object</matching_id>			
PROC_ES9+_GET_BPP (see Note 1)			
LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_106 RQ34_023 RQ34_024
PROC_ES9+_HANDLE_NOTIF			
LPAd → S_EndUser	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ34_018 RQ34_020
	Power on the Dev PROC_TLS_INITI PROC_ES9+_INIT PROC_ES9+_AU MatchingID data of PROC_ES9+_GE (see Note 1) LPAd -> S_EndUser PROC_ES9+_HAI LPAd ->	Power on the Device PROC_TLS_INITIALIZATION_SERVER_AUTH on E PROC_ES9+_INIT_AUTH PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_ MatchingID data object PROC_ES9+_GET_BPP (see Note 1) LPAd → S_EndUser Request for Authenticated Confirmation, if not requested before. PROC_ES9+_HANDLE_NOTIF LPAd → Initiate List Profile operation	Power on the Device PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+ PROC_ES9+_INIT_AUTH PROC_ES9+_AUTH_CLIENT with #MATCHING_ID_EMPTY as <matching_id> or MatchingID data object PROC_ES9+_GET_BPP (see Note 1) LPAd → S_EndUser Request for Authenticated Confirmation, if not requested before. PROC_ES9+_HANDLE_NOTIF LPAd → Initiate List Profile operation PROFILE_OPERATIONAL1</matching_id>

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

V1.4 Page 580 of 777

5.4.11.2.2TC_LPAd_DevicePowerOnProfileDiscovery_SM-DS

General Initial Conditions		
Entity Description of the general initial condition		
Device	The protection of access to the LUI is disabled	
Device	The setting of the configuration parameter for Device Power-on Profile discovery is 'Enabled'	
Device	The Device is powered off	

Test Sequence #01 Nominal: Power-on Profile discovery by using the SM-DS

Initial Conditions	
Entity	Description of the initial condition
S_SM-DS	S_SM-DP+ (#TEST_DP_ADDRESS1) performed Profile download Event Registration to the S_SM-DS (#TEST_ROOT_DS_ADDRESS) with #EVENT_ID_1
S_SM-DP+	There is a pending Profile download order for #EVENT_ID_1 (PROFILE_OPERATIONAL1)
S_SM-DP+	The PROFILE_OPERATIONAL1 on the S_SM-DP+ is in "Released" state
eUICC	There is no default SM-DP+ address configured

Step	Direction	Sequence / Description	Expected result	REQ
IC1	1 Power-on the Device			
1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH or	n ES11	
2	PROC_ES11_IN	NIT_AUTH		
3	PROC_ES11_AUTH_CLIENT with #MATCHING_ID_EMPTY as <matching_id> or missing MatchingID data object</matching_id>			
4	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+			
5	PROC_ES9+_INIT_AUTH			
6	PROC_ES9+_AUTH_CLIENT with #EVENT_ID_1 as <matching_id></matching_id>			
7	PROC_ES9+_GET_BPP (see Note 1)			
8	LPAd → S_EndUser	Request for Authenticated Confirmation, if not requested before.	End User Intent successfully verified for Authenticated Confirmation as defined in SGP.21 [3], if not verified before.	RQ31_106 RQ34_023 RQ34_024
9	9 PROC_ES9+_HANDLE_NOTIF			
10	LPAd → S_EndUser	Initiate List Profile operation	PROFILE_OPERATIONAL1 is displayed in Disabled state	RQ34_018 RQ34_021
N	No. 4 THE PARKACLE IN THE STATE OF THE STATE			

Note 1: The LPAd MAY display any relevant part of the Profile Metadata and MAY offer the S_EndUser to postpone or reject the Profile installation. The S_EndUser SHALL not abort the transaction.

V1.4 Page 581 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

6 End-to-End Testing

This section is defined as FFS and not applicable for this version of test specification.

V1.4 Page 582 of 777

GSM Association
Official Document SGP.23 - SGP.23 RSP Test Specification

7 External Test Specifications

Some test specifications related to the RSP ecosystem have been developed by external organisations (e.g. SIMAlliance). These organisations defined their own requirements for test benches, test applicability and pass criteria.

This section lists the test specifications that relate to SGP.21 [3] and SGP.22 [2] requirements.

7.1 SIMAlliance eUICC Profile Package Test Specification

The SIMAlliance eUICC Profile Package: Interoperable Format Test Specification [23] SHALL be executed on the eUICC in order to check its compliance with the SIMAlliance eUICC Profile Package: Interoperable Format Technical Specification [4].

Test cases are applicable according to the applicability table of the referred Test Specification [23].

The table below describes the restrictions on the SIMalliance tests applicability depending on the SGP.22 version supported by the eUICC:

SGP.22 version	SIMalliance [4] version indicating which test cases are applicable for the given SGP.22 version
2.1	2.0 or 2.1
2.2.x	2.1

Moreover, eUICC Manufacturers SHALL declare that the following SIMAlliance options are supported by the eUICC:

- O MILENAGE
- O_TUAK_128
- O_JAVACARD

The successful execution of SIMAlliance test cases allows the following RSP requirements to be covered:

- RQ24_022
- RQ24_042
- RQ24_043

V1.4 Page 583 of 777

Annex A Constants

A.1 Generic Constants

Name	Content
ACTIVATION_CODE_1	1\$#TEST_DP_ADDRESS1\$#MATCHING_ID_1 ACTIVATION_CODE_1.png as defined in Annex H
ACTIVATION_CODE_2	1\$#TEST_DP_ADDRESS1\$#MATCHING_ID_2\$#S_SM_DP+_OID ACTIVATION_CODE_2.png as defined in Annex H
ACTIVATION_CODE_3	1\$#TEST_DP_ADDRESS1\$#MATCHING_ID_3\$\$1 ACTIVATION_CODE_3.png as defined in Annex H
ACTIVATION_CODE_3_NO_CC	1\$#TEST_DP_ADDRESS1\$#MATCHING_ID_3 ACTIVATION_CODE_3_NO_CC.png as defined in Annex H
ACTIVATION_CODE_4	1\$#TEST_DP_ADDRESS1\$#MATCHING_ID_4 ACTIVATION_CODE_4.png as defined in Annex H
ACTIVATION_CODE_INVALID_FORMAT	1#TEST_DP_ADDRESS1\$#MATCHING_ID_1 ACTIVATION_CODE_INVALID_FORMAT.png as defined in Annex H
ADDITIONAL_SMDP_DATA_MAX_LENG TH	0x01 02 0375 76 77 additional data objects defined by the S_SM-DP+ depending on the length of the SM-DP+ OID, to ensure that total length of dpProprietaryData is 128 bytes
ADDITIONAL_SMDP_DATA_EXCEEDE D_MAX	0x01 02 0376 77 78 additional data objects defined by the S_SM-DP+ depending on the length of the SM-DP+ OID, to ensure that total length of dpProprietaryData is 129 bytes
CHANGE_CIPHER_SPEC	1
CLIENT_CERT_TYPE	64. The Certificate Type requested from the client by the server in the Certificate Request message as ecdsa_sign(64).
CONFIRMATION_CODE1	0102030405
CONFIRMATION_CODE2	ABCDEFGHIJ
CTX_PARAMS1 (CtxParams1)	<pre>ctxParamsForCommonAuthentication : { #s_DEVICE_INFO }</pre>
CTX_PARAMS1_EVENT_ID (CtxParams1)	<pre>ctxParamsForCommonAuthentication : { matchingId #EVENT_ID_1, #S_DEVICE_INFO }</pre>

V1.4 Page 584 of 777

```
ctxParamsForCommonAuthentication : {
CTX_PARAMS1_EVENT_ID_IMEI
                                     matchingId #EVENT ID 1,
                                      #S DEVICE INFO IMEI
(CtxParams1)
                                   ctxParamsForCommonAuthentication : {
CTX_PARAMS1_IMEI
                                      #S_DEVICE_INFO_IMEI
(CtxParams1)
                                   ctxParamsForCommonAuthentication : {
CTX_PARAMS1_MATCH_ID
                                     matchingId #MATCHING ID 1,
                                      #S DEVICE INFO
(CtxParams1)
                                   ctxParamsForCommonAuthentication : {
CTX_PARAMS1_MATCH_ID_DEV_INFO
                                     matchingId <MATCHING ID>,
                                      #DEVICE INFO
(CtxParams1)
                                   deviceInfo {
                                     tac #IUT TAC,
                                     deviceCapabilities {
                                    },-- Check only that the field is present and
DEVICE INFO
                                   has a valid TLV asn.1 structure
                                     imei ... -- Optional
                                   Note: the content of deviceCapabilities is verified in individual
DIST_NAME_CI
                                   GSMA Test CI
                                   0x0A 2E 14 8C E7 32 04 00 00 00 00 00 00
EF_UST1
                                   -- NOTE: Service n°17 (GID1) and n°18 (GID2) not available
                                   0x0A 2E 17 8C E7 32 04 00 00 00 00 00 00
EF UST2
                                   -- NOTE: Service n°17 (GID1) and n°18 (GID2) available
                                   0x89 04 90 32 12 34 51 23 45 12 34 56 78 90 12
EID1
                                   3.5
                                   QR code which decodes as:
EID1_QR_CODE1
                                   EID:89049032123451234512345678901235
                                   QR code which decodes as:
                                   EID:89 04 90 32 12 34 51 23 45 12 34 56 78 90 12
EID1_QR_CODE2
                                   0x89 29 90 00 11 23 41 23 40 12 34 56 78 90 13
EID2
                                    53
                                    #CI PKI ID1,
EUICC_CI_PK_ID_LIST_FOR_SIGNING
                                   #CI_PKI_ID2
_1
EUICC_CI_PK_ID_LIST_FOR_SIGNING
                                    #CI_PKI_ID3,
                                    #CI PKI ID4
_2
```

V1.4 Page 585 of 777

EUICC_CI_PK_ID_LIST_FOR_VERIFICA TION_1	#CI_PKI_ID1, #CI_PKI_ID2
EUICC_CI_PK_ID_LIST_FOR_VERIFICA TION_2	#CI_PKI_ID3, #CI_PKI_ID4
EUICC_INFO1_8_8_2_3_1	<pre>euiccInfo1_8_8_2_3_1 EUICCInfo1 ::= { svn #RSP_SVN, euiccCiPKIdListForVerification { #EUICC_CI_PK_ID_LIST_FOR_VERIFICATION_1 }, euiccCiPKIdListForSigning { #EUICC_CI_PK_ID_LIST_FOR_SIGNING_2 } }</pre>
EUICC_INFO1_8_8_3_3_1_HIGHER	<pre>euiccInfo1_8_8_3_3_1 EUICCInfo1 ::= { svn #RSP_SVN_HIGHER, euiccCiPKIdListForVerification { #EUICC_CI_PK_ID_LIST_FOR_VERIFICATION_1 }, euiccCiPKIdListForSigning { #EUICC_CI_PK_ID_LIST_FOR_SIGNING_1 } }</pre>
EUICC_INFO1_8_8_3_3_1_LOWER	<pre>euiccInfo1_8_8_3_3_1 EUICCInfo1 ::= { svn #RSP_SVN_LOWER, euiccCiPKIdListForVerification { #EUICC_CI_PK_ID_LIST_FOR_VERIFICATION_1 }, euiccCiPKIdListForSigning { #EUICC_CI_PK_ID_LIST_FOR_SIGNING_1 } }</pre>
EUICC_INFO1_8_8_4_3_7	<pre>euiccInfo1_8_8_4_3_7 EUICCInfo1 ::= { svn #RSP_SVN, euiccCiPKIdListForVerification { #EUICC_CI_PK_ID_LIST_FOR_VERIFICATION_2 }, euiccCiPKIdListForSigning { #EUICC_CI_PK_ID_LIST_FOR_SIGNING_1 } }</pre>
EUICC_SIGNED1	<pre>{ transactionId <s_transaction_id>, serverAddress #TEST_DP_ADDRESS1, serverChallenge <s_smdp_challenge>, euiccInfo2 #R_EUICC_INFO2, check only that the field is present and has a valid TLV asn.1 structure ctxParams1 #CTX_PARAMS1 }</s_smdp_challenge></s_transaction_id></pre>
EVENT_ID_1	07399-BGH7E-T8779

V1.4 Page 586 of 777

EVENT_ID_2	07399-BGH7E-T8778
EXT_SHA256_RSA	TLS extension data for "supported_signature_algorithms" set as: o HashAlgorithm sha256 (04) and o SignatureAlgorithm rsa (01).
FUNCTION_CALL_ID_1	0000-0000-0001
FUNCTION_CALL_ID_2	0000-0000-00002
GID1	0x47 53 4D 41
GID2	0x52 53 50 FF
HOST_ID	0x47 53 4D 41 20 53 4D 2D 58 58 NOTE: 'GSMA SM-XX' in ASCII
ICCID_OP_PROF1	0x98 92 09 01 21 43 65 87 09 F5
ICCID_OP_PROF2	0x98 92 09 01 32 54 76 98 10 F9
ICCID_OP_PROF3	0x98 92 09 01 43 65 87 09 21 F5
ICCID_OP_PROF4	0x98 92 09 01 54 76 98 10 32 F9
ICCID_OP_PROF5	0x98 92 09 01 65 87 09 21 43 F5
ICCID_OP_PROF6	0x98 92 09 01 76 98 10 32 54 F9
ICCID_OP_PROF7	0x98 92 09 01 87 09 21 43 65 F5
ICCID_OP_PROF8	0x98 92 09 01 98 10 32 54 76 F9
ICCID_OP_PROF9	0x98 92 09 01 21 43 65 87 76 F5
ICCID_OP_PROFX	0x98 92 09 01 43 65 87 09 FF FF
ICCID_UNKNOWN	0x98 92 01 0A 21 43 65 87 09 F8
ICON_JPG	ICON_JPG.jpg as defined in Annex H
ICON_OP_PROF1	profile_O1.png as defined in Annex H
ICON_OP_PROF2	profile_O2.png as defined in Annex H
ICON_OP_PROF3	profile_O3.png as defined in Annex H
ICON_OP_PROF4	profile_O4.png as defined in Annex H
ICON_OP_PROF5	profile_O5.png as defined in Annex H
ICON_OP_PROF6	profile_O6.png as defined in Annex H
ICON_OP_PROF7	profile_O7.png as defined in Annex H
ICON_OP_PROF8	profile_O8.png as defined in Annex H
ICON_OP_PROF1_2_SEG	profile_O1_2_SEG.png as defined in Annex H
IMSI_OP_PROF1	0x08 29 99 18 11 32 54 76 98

V1.4 Page 587 of 777

IMSI_OP_PROF2	0x08 29 99 28 11 32 54 76 97
IMSI_OP_PROF3	0x08 29 99 28 11 32 54 76 96
IMSI_OP_PROF4	0x08 29 99 48 43 65 87 09 21
IMSI_OP_PROF5	0x08 29 99 18 11 32 54 76 98
IMSI_OP_PROF6	0x08 29 99 28 11 32 54 76 97
IMSI_OP_PROF7	0x08 29 99 88 43 65 87 09 21
IMSI_OP_PROF8	0x08 29 99 88 43 65 87 09 21
IMSI_OP_PROF9	0x08 29 99 98 43 65 87 09 21
INSTALLED_PROFILES	0x00
INVALID_KEY_TYPE	0x80
INVALID_REMOTE_OP_ID	8
ISD_R_AID	0xA0 00 00 05 59 10 10 FF FF FF FF 89 00 00 01 00
KEY_LENGTH	0x10
KEY_TYPE	0x88
MATCHING_ID_1	04386-AGYFT-A74Y8-3F815
MATCHING_ID_2	04386-AGYFT-A74Y8-3F816
MATCHING_ID_3	04386-AGYFT-A74Y8-3F817
MATCHING_ID_4	04386-AGYFT-A74Y8-3F818
MCC_MNC_WILDCARD	0x92 F9 EE
MCC_MNC1	0x92 F9 18
MCC_MNC2	0x92 F9 28
MCC_MNC4	0x92 F9 48
MCC_MNC8	0x92 F9 88
MCC_MNC9	0x92 F9 98
MIN_TLS_CIPHER_SUITES	The minimum TLS cipher suites proposed by the Client: o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
MNO_SCP80_AUTH_KEY	0x11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 10

V1.4 Page 588 of 777

MNO_SCP80_DATA_ENC_KEY	0x99 AA BB CC DD EE FF 10 11 22 33 44 55 66 77 88
MNO_SCP80_ENC_KEY	0x66 77 88 99 AA BB CC DD 11 22 33 44 55 EE FF 10
NAME_OP_PROF1	Operational Profile Name 1
NAME_OP_PROF2	Operational Profile Name 2
NAME_OP_PROF3	Operational Profile Name 3
NAME_OP_PROF4	Operational Profile Name 4
NAME_OP_PROF5	Operational Profile Name 5
NAME_OP_PROF6	Operational Profile Name 6
NAME_OP_PROF7	Operational Profile Name 7
NAME_OP_PROF8	Operational Profile Name 8
NAME_OP_PROF9	Operational Profile Name 9
NAME_OP_PROF_LONG	Operational Profile Name with long name of sixty four characters NOTE: the exact text above SHOULD be used, as it is exactly 64 characters long.
NAME_OP_PROF1_NON_ASCII	Operational Profile Name UTF-8 encoding: 0x4F 70 65 72 61 74 69 6F 6E 61 6C 20 50 72 6F 66 69 6C 65 20 4E 61 6D 65 20 E4 BD A0 E5 A5 BD
NICKNAME1	Nickname 1
NICKNAME2	Nickname 2
NICKNAME3	Nickname 3
NICKNAME4	Nickname 4
OWNER_OP_PROF1	{ mccMnc #MCC_MNC1 }
OWNER_OP_PROF2	{ mccMnc #MCC_MNC2 }
PATH_AUTH_CLIENT	/gsma/rsp2/es9plus/authenticateClient
PATH_CANCEL_SESSION	/gsma/rsp2/es9plus/cancelSession
PATH_DELETE_EVENT	/gsma/rsp2/es12/deleteEvent
PATH_GET_BPP	/gsma/rsp2/es9plus/getBoundProfilePackage
PATH_HANDLE_NOTIF	/gsma/rsp2/es9plus/handleNotification
PATH_INITIATE_AUTH	/gsma/rsp2/es9plus/initiateAuthentication
PATH_REGISTER_EVENT	/gsma/rsp2/es12/registerEvent
PO1_PIN1	0x32 34 36 38 FF FF FF FF
PO2_PIN1	0x33 35 37 39 FF FF FF FF
PPK_ENC_INV_SIZE	0x01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 0D 0E 0F 10

V1.4 Page 589 of 777

PPK_INIT_MAC_INV_SIZE	0x05 0A 04 0B 03 0C 02 0D 01 0E 00 0F 09 01 08 02 09 01 08 02 09 01 08 02
PPK_MAC_INV_SIZE	0x01 0E 00 0F 09 01 08 02 05 0A 04 0B 03 0C 02 0D 03 0C 02 0D 03 0C 02 0D
PROP_TLS_CIPHER_SUITES	The TLS cipher suites proposed by the Client: o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
REMOTE_OP_ID_INSTALL	1
RSP_SVN	This field is set to #IUT_RSP_VERSION (e.g. 2.1.0)
RSP_SVN_H	This field is set to #IUT_RSP_VERSION encoded as the value part of an ASN.1 VersionType (e.g. 0x02 01 00)
RSP_SVN_HIGHER	100.0.0
RSP_SVN_LOWER	0.0.0
S_DEVICE_INFO	<pre>deviceInfo { tac #S_TAC, deviceCapabilities { gsmSupportedRelease '050000'H, utranSupportedRelease '080000'H, cdma2000onexSupportedRelease '010000'H, cdma2000hrpdSupportedRelease '010000'H, cdma2000ehrpdSupportedRelease '020000'H, eutranSupportedRelease '020000'H, contactlessSupportedRelease '090000'H, rspCrlSupportedVersion #RSP_SVN_H } }</pre>
S_DEVICE_INFO_IMEI	<pre>deviceInfo { tac #S_TAC, deviceCapabilities { gsmSupportedRelease '050000'H, utranSupportedRelease '080000'H, cdma2000onexSupportedRelease '01000'H, eutranSupportedRelease '020000'H }, imei #S_IMEI }</pre>
S_EUICC_CHALLENGE	0x01 02 03 04 05 06 07 08 01 02 03 04 05 06 07 08
S_EUICC_CHALLENGE_2	0x21 22 23 24 25 26 27 28 21 22 23 24 25 26 27 28
S_EUICC_INFO1	<pre>euiccInfo1 EUICCInfo1 ::= { svn #RSP_SVN, euiccCiPKIdListForVerification { #EUICC_CI_PK_ID_LIST_FOR_VERIFICATION_1</pre>

V1.4 Page 590 of 777

	<pre>}, euiccCiPKIdListForSigning { #EUICC_CI_PK_ID_LIST_FOR_SIGNING_1 } </pre>
S_EUICC_INFO2	<pre>euiccInfo2 EUICCInfo2 ::= { profileVersion #PROFILE_VERSION, svn #RSP_SVN_H, euiccFirmwareVer #EUICC_FIRMWARE_VER, extCardResource #S_EXT_CARD_RESOURCE, uiccCapability #UICC_CAPABILITY, rspCapability #RSP_CAPABILITY, euiccCiPKIdListForVerification {#EUICC_CI_PK_ID_LIST_FOR_VERIFICATION_1}, euiccCiPKIdListForSigning {#EUICC_CI_PK_ID_LIST_FOR_SIGNING_1}, ppVersion #PP_VERSION, sasAcreditationNumber #SAS_ACREDITATION_NUMBER }</pre>
S_EXT_SHA256_ECDSA	TLS extension data for "supported_signature_algorithms" set as: o HashAlgorithm sha256 (04) and SignatureAlgorithm ecdsa (03).
S_IMEI	0x00 00 00 00 11 11 11 11
S_SAH_SHA256_ECDSA	Signature And Hash Algorithm extension sent in the CertificateRequest message set as: o HashAlgorithm sha256 (04) and o SignatureAlgorithm rsa (01).
S_SESSION_ID_EMPTY	Empty TLS session ID to identify a new session, with the Length set as `zero'.
S_SM_DP+_F_REQ_ID	"S_SM_DP_PLUS"
S_SM_DP+_OID	2.999.10
S_SM_DP+_OID2	2.999.12
S_SM_DP+_OID4	2.999.14
S_SM_DP+_OID8	2.999.18
S_SM_DS_F_REQ_ID	"S_SM_DS"
S_SM_DS_OID	2.999.15
S_TAC	0x00 00 00 00
S_TLS_CIPHER_SUITE	TLS cipher suite selected as follows: o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 if present in <tls_cipher_suites>, otherwise o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</tls_cipher_suites>

V1.4 Page 591 of 777

SERVER_ADDRESS	FQDN of the SERVER Under Test which can be one of the following depending on the entity under test: • #IUT_SM_DP_ADDRESS • #IUT_SM_DS_ADDRESS
SESSION_ID_0	Empty TLS session ID to identify a new session
SIMA_RESULT_OK	<pre>simaresp EUICCResponse ::= { peStatus { {status ok} } }</pre>
SP_NAME1	SP Name 1
SP_NAME2	SP Name 2
SP_NAME3	SP Name 3
SP_NAME4	SP Name 4
SP_NAME8	SP Name 8
SP_NAME9	SP Name 9
SP_NAME_LONG	SP Name as thirty two characters NOTE: the exact text above SHOULD be used, as it is exactly 32 characters long.
SP_NAME_NON_ASCII	SP Name UTF-8 encoding: 0x53 50 20 4E 61 6D 65 20 E3 83 AB
SSD_AID	0xA0 00 00 05 59 10 10 01 02 73 64 56 61 6C 75 65
TEST_ALT_DS_ADDRESS	testaltsmds.gsma.com
TEST_DEFAULT_DP_ADDRESS_1	testdefaultsmdpplus1.gsma.com
TEST_DP_ADDRESS1	testsmdpplus1.gsma.com
TEST_DP_ADDRESS2	testsmdpplus2.gsma.com
TEST_DP_ADDRESS3	testsmdpplus3.gsma.com
TEST_DP_ADDRESS4	testsmdpplus4.gsma.com
TEST_DP_ADDRESS8	testsmdpplus8.gsma.com
TEST_DS_ADDRESS1	testsmds1.gsma.com
TEST_ROOT_DS_ADDRESS	testrootsmds.gsma.com
TLS_VERSION_1_1	1.1.
TLS_VERSION_1_2	1.2 The minimum TLS Version supported by the Server
UNKNOWN_BPP_SEGMENT	0xC9 05 01 02 03 04 05
UNKNOWN_SERVER_ADDRESS	unknownserver.gsma.com

V1.4 Page 592 of 777

UNSUP_TLS_CIPHER_SUITES	The TLS cipher suites proposed by the Client: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA256
UPP_OP_PROF1	The Unprotected Profile Package related to the PROFILE_OPERATIONAL1 (see Annex E).
UPP_OP_PROF2	The Unprotected Profile Package related to the PROFILE_OPERATIONAL2 (see Annex E).
UPP_OP_PROF3	The Unprotected Profile Package related to the PROFILE_OPERATIONAL3 (see Annex E).
UPP_OP_PROF4	The Unprotected Profile Package related to the PROFILE_OPERATIONAL4 (see Annex E).
UPP_OP_PROF9	The Unprotected Profile Package related to the PROFILE_OPERATIONAL9 (see Annex E).
USIM_AID	0xA0 00 00 00 87 10 02 FF 33 FF 01 89 00 00 01 00

A.2 Test Certificates and Test Keys

All ECC certificates and keys described below are based on either:

- NIST P-256 curve, defined in Digital Signature Standard [11]
- brainpoolP256r1 curve, defined in RFC 5639 [8]
- FRP256V1 curve, defined in ANSSI ECC [9]

NOTE:

SGP.26 [25] contains test keys, valid test certificates and instructions for how to generate invalid certificates. All test keys and test certificates used in the present document are contained in SGP.23_Certificates.zip, which accompanies the present document.

Name	Description
CERT_CI_ECDSA	Certificate of the CI for its Public ECDSA Key
CERT_CLIENT_TLS	CERT.CLIENT.TLS certificate of the Client under test, based on NIST or Brainpool for this version of the specification, where the Certificate MAY be one of the following depending on the type of Server and whether it is a Client under test or a Client Simulator: • #CERT_SM_DP_TLS • #CERT_SM_DS_TLS • #CERT_S_SM_DP_TLS • #CERT_S_SM_DP_TLS
CERT_EUICC_ECDSA	Certificate of the eUICC for its Public ECDSA key CERT.EUICC.ECDSA in the X.509 format signed by the EUM with SK.EUM.ECDSA
CERT_EUICC_ECDSA_EID2	Certificate of the eUICC for its Public ECDSA key (CERT.EUICC.ECDSA) in the X509 format signed by the EUM with SK.EUM.ECDSA with the subject field value serialNumber set as #EID2.

V1.4 Page 593 of 777

	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUICC_ECDSA_EXPIRED	RSP Certificate of the eUICC (CERT.EUICC.ECDSA) set as a fixed test CERT with 13th January 2016 set in the validity field.
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUICC_ECDSA_INVALID_EX_CP	RSP Certificate of the eUICC (CERT.EUICC.ECDSA) set as a fixed test CERT with an invalid Certificate Policies extension field OID extnValue set as "id-rspRole-ci".
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUICC_ECDSA_INVALID_EX_KU	RSP Certificate of the eUICC (CERT.EUICC.ECDSA) set as a fixed test CERT with an invalid Key Usage extension field extnValue set as "dataEncipherment".
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUICC_ECDSA_INVALID_SIG	RSP Certificate of the eUICC (CERT.EUICC.ECDSA) set as a fixed test CERT with an invalid signature in the signatureValue field.
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUICC_ECDSA_INVALID_SUB_ORG	RSP Certificate of the eUICC (CERT.EUICC.ECDSA) set as a fixed test CERT with an invalid 'organization' attribute value in the subject field set as "ERRORNAME".
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUICC_ECDSA_INVALID_SUB_SN	RSP Certificate of the eUICC (CERT.EUICC.ECDSA) set as a fixed test CERT with an invalid 'serialNumber' attribute value in the subject field set as "89000000000000000000000000000000000000
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
	Certificate of the EUM for its Public ECDSA key
CERT_EUM_ECDSA	CERT.EUM.ECDSA in the X.509 format signed by the requested CI with SK.CI.ECDSA.
CERT_EUM_ECDSA_EXPIRED	RSP Certificate of the eUICC (CERT.EUM.ECDSA) set as a fixed test CERT with 13 th January 2016 set in the validity field.
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUM_ECDSA_INVALID_EX_BC_cA	RSP Certificate of the EUM (CERT.EUM.ECDSA) set as a fixed test CERT with an invalid Basic Constraints extension field set as "cA = false".
	Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.

V1.4 Page 594 of 777

CERT_EUM_ECDSA_INVALID_EX_BC_PLC	RSP Certificate of the EUM (CERT.EUM.ECDSA) set as a fixed test CERT with an invalid Basic Constraints extension field set as "pathLenConstraint = 1". Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUM_ECDSA_INVALID_EX_CP	RSP Certificate of the EUM (CERT.EUM.ECDSA) set as a fixed test CERT with an invalid Certificate Policies extension field OID extnValue set as "id-rspRole-ci". Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUM_ECDSA_INVALID_EX_KU	RSP Certificate of the EUM (CERT.EUM.ECDSA) set as a fixed test CERT with an invalid Key Usage extension field extnValue set as "dataEncipherment". Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUM_ECDSA_INVALID_SIG	RSP Certificate of the EUM (CERT.EUM.ECDSA) set as a fixed test CERT with an invalid signature in the signatureValue field. Depending on the eUICC configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_EUM_ECDSA_UNKNOWN	RSP Certificate of the EUM (CERT.EUM.ECDSA) set as a fixed test CERT with the Authority Key Identity not trusted by the SM-DP+ as it is not found in #EUICC_CI_PK_ID_LIST_FOR_VERIFICATION_1 or #EUICC_CI_PK_ID_LIST_FOR_SIGNING_1. Depending on the eUICC configuration, this certificate is
CERT_S_CLIENT_TLS	based on NIST P-256, brainpoolP256r1 or FRP256V1. CERT.CLIENT.TLS certificate of the S_CLIENT, based on NIST or Brainpool for this version of the specification, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS #CERT_S_SM_DS_TLS
CERT_S_CLIENT_TLS_EXPIRED	CERT.CLIENT.TLS certificate of the S_CLIENT, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_EXPIRED #CERT_S_SM_DS_TLS_EXPIRED
CERT_S_CLIENT_TLS_INV_CERT_POL	CERT.CLIENT.TLS certificate of the S_CLIENT, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_CERT_POL #CERT_S_SM_DS_TLS_INV_CERT_POL
CERT_S_CLIENT_TLS_INV_CRITICAL_EXT	CERT.CLIENT.TLS certificate of the S_CLIENT, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_CRITICAL_EXT #CERT_S_SM_DS_TLS_INV_CRITICAL_EXT

V1.4 Page 595 of 777

CERT_S_CLIENT_TLS_INV_EXT_KEY_USAGE	CERT.CLIENT.TLS certificate of the S_CLIENT, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_EXT_KEY_USAGE #CERT_S_SM_DS_TLS_INV_EXT_KEY_USAGE
CERT_S_CLIENT_TLS_INV_KEY_USAGE	CERT.CLIENT.TLS certificate of the S_CLIENT, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_KEY_USAGE #CERT_S_SM_DS_TLS_INV_KEY_USAGE
CERT_S_CLIENT_TLS_INV_OID	CERT.CLIENT.TLS certificate of the S_CLIENT, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_OID #CERT_S_SM_DS_TLS_INV_OID
CERT_S_CLIENT_TLS_INV_SIG	CERT.CLIENT.TLS certificate of the S_CLIENT, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_SIG #CERT_S_SM_DS_TLS_INV_SIG
CERT_S_SERVER_TLS	CERT.SERVER.TLS certificate of the S_SERVER, based on NIST or Brainpool for this version of the specification, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS on ES9+ #CERT_S_SM_DS_TLS on ES11 or ES12
CERT_S_SERVER_TLS_EXPIRED	CERT.SERVER.TLS certificate of the S_SERVER, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_EXPIRED #CERT_S_SM_DS_TLS_EXPIRED
CERT_S_SERVER_TLS_INV_CERT_POL	CERT.SERVER.TLS certificate of the S_SERVER, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_CERT_POL #CERT_S_SM_DS_TLS_INV_CERT_POL
CERT_S_SERVER_TLS_INV_CRITICAL_EXT	CERT.SERVER.TLS certificate of the S_SERVER, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_CRITICAL_EXT #CERT_S_SM_DS_TLS_INV_CRITICAL_EXT
CERT_S_SERVER_TLS_INV_EXT_KEY_USAG E	CERT.SERVER.TLS certificate of the S_SERVER, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_EXT_KEY_USAGE #CERT_S_SM_DS_TLS_INV_EXT_KEY_USAGE
CERT_S_SERVER_TLS_INV_KEY_USAGE	CERT.SERVER.TLS certificate of the S_SERVER, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_KEY_USAGE

V1.4 Page 596 of 777

	#CERT_S_SM_DS_TLS_INV_KEY_USAGE
CERT_S_SERVER_TLS_INV_SIG	CERT.SERVER.TLS certificate of the S_SERVER, where the Certificate MAY be one of the following depending on the role of the simulator: #CERT_S_SM_DP_TLS_INV_SIG #CERT_S_SM_DS_TLS_INV_SIG
CERT_S_SM_DP_TLS	CERT.DP.TLS certificate of the S_SM-DP+, based on the same CI as defined in #IUT_LPAd_CI based on NIST for this version of the specification
CERT_S_SM_DP2_TLS	CERT.DP.TLS certificate of the S_SM-DP+, based on the same CI as defined in #IUT_LPAd_CI based on NIST for this version of the specification. Contains different SM-DP+ hostname (FQDN) as #CERT_S_SM_DP2_TLS.
CERT_S_SM_DP4_TLS	CERT.DP.TLS certificate of the S_SM-DP+, based on the same CI as defined in #IUT_LPAd_CI based on NIST for this version of the specification. Contains the SM-DP+ hostname (FQDN) #TEST_DP_ADDRESS4 and OID value #S_SM_DP+_OID4.
CERT_S_SM_DP8_TLS	CERT.DP.TLS certificate of the S_SM-DP+, based on the same CI as defined in #IUT_LPAd_CI based on NIST for this version of the specification. Contains the SM-DP+ hostname (FQDN) #TEST_DP_ADDRESS8 and OID value #S_SM_DP+_OID8.
CERT_S_SM_DP_TLS_EXPIRED	Expired CERT.DP.TLS certificate of the S_SM-DP+ with a valid signature, correctly formatted as X.509 certificate.
CERT_S_SM_DP_TLS_INV_CERT_POL	CERT.DP.TLS certificate of the S_SM-DP+ with invalid 'Certificate Policies' extension (OID not set to 'id-rspRoledp-tls' or 'id-rspRole-ds-tls'), formatted as X.509 certificate.
CERT_S_SM_DP_TLS_INV_CRITICAL_EXT	CERT.DP.TLS certificate of the S_SM-DP+ with one of the critical extensions not present, formatted as X.509 certificate.
CERT_S_SM_DP_TLS_INV_CURVE	CERT.DP.TLS certificate of the S_SM-DP+, based on the different CI as defined in #IUT_LPAd_CI, not based on NIST P-256 curve, defined in Digital Signature Standard [11]
	 brainpoolP256r1 curve, defined in RFC 5639 [8] FRP256V1 curve, defined in ANSSI ECC [9]
CERT_S_SM_DP_TLS_INV_EXT_KEY_USAGE	CERT.DP.TLS certificate of the S_SM-DP+ with invalid 'extended key usage' extension (not set to any combination of 'id-kp-serverAuth' or 'id-kp-clientAuth'), formatted as X.509 certificate.
CERT_S_SM_DP_TLS_INV_KEY_USAGE	CERT.DP.TLS certificate of the S_SM-DP+ with invalid 'key usage' extension (not set to 'digitalSignature'), formatted as X.509 certificate.
CERT_S_SM_DP_TLS_INV_OID	CERT.DP.TLS certificate of the S_SM-DP+ containing an invalid SM-DP+OID, different to #S_SM_DP+_OID, correctly formatted as X.509 certificate.

V1.4 Page 597 of 777

CERT_S_SM_DP_TLS_INV_SIG	Invalid CERT.DP.TLS certificate of the S_SM-DP+ with an invalid signature with the same tag and length as a valid signature, correctly formatted as X.509 certificate.
CERT_S_SM_DPauth_ECDSA	Certificate of the S_SM-DP+ for its Public ECDSA key used for SM-DP+ authentication. This certificate contains the OID #S_SM_DP+_OID.
CERT_S_SM_DP2auth_ECDSA	Certificate of the S_SM-DP+ for its Public ECDSA key used for SM-DP+ authentication. This certificate contains the OID #S_SM_DP+_OID2.
CERT_S_SM_DPauth_INV_SIGN	Invalid certificate of the S_SM-DP+ for its Public ECDSA key used for authentication. This certificate contains the OID #S_SM_DP+_OID and contains an invalid signature (i.e. not generated with the #SK_CI_ECDSA but with the same tag and length as a valid signature)
CERT_S_SM_DPauth_INV_CURVE	Certificate of the S_SM-DP+ for its Public ECDSA key used for Authentication. This certificate contains the OID #S_SM_DP+_OID and a public key based on a curve different from the following ones: NIST P-256 curve, defined in Digital Signature Standard [11] brainpoolP256r1 curve, defined in RFC 5639 [8] FRP256V1 curve, defined in ANSSI ECC [9]
CERT_S_SM_DSauth_INV_CURVE	Certificate of the S_SM-DS for its Public ECDSA key used for Authentication. This certificate contains the OID #S_SM_DS_OID and a public key based on a curve different from the following ones: NIST P-256 curve, defined in Digital Signature Standard [11] brainpoolP256r1 curve, defined in RFC 5639 [8] FRP256V1 curve, defined in ANSSI ECC [9]
CERT_S_SM_DPpb_ECDSA	Certificate of the S_SM-DP+ for its Public ECDSA key used for Profile Package Binding. This certificate contains the OID #S_SM_DP+_OID.
CERT_S_SM_DPpb_INV_SIGN	Invalid certificate of the S_SM-DP+ for its Public ECDSA key used for Profile Package Binding. This certificate contains the OID #S_SM_DP+_OID and contains an invalid signature (i.e. not generated with the #SK_CI_ECDSA but with the same tag and length as a valid signature)
CERT_S_SM_DPpb_INV_CURVE	Certificate of the S_SM-DP+ for its Public ECDSA key used for Profile Package Binding. This certificate contains the OID #S_SM_DP+_OID and a public key based on a curve different from the following ones: NIST P-256 curve, defined in Digital Signature Standard [11] brainpoolP256r1 curve, defined in RFC 5639 [8] FRP256V1 curve, defined in ANSSI ECC [9]
CERT_S_SM_DP2pb_ECDSA	Certificate of the S_SM-DP+ for its Public ECDSA key used for Profile Package Binding. This certificate contains the OID #S_SM_DP+_OID2.

V1.4 Page 598 of 777

CERT_S_SM_DS_TLS	CERT.DS.TLS certificate of the S_SM-DS based on the same CI as defined in #IUT_LPAd_CI based on NIST or
	Brainpool for this version of the specification
CERT_S_SM_DS2_TLS	CERT.DS.TLS certificate of the S_SM-DS based on the same CI as defined in #IUT_LPAd_CI based on NIST or Brainpool for this version of the specification. Contains different SM-DS hostname (FQDN) as #CERT_S_SM_DS2_TLS.
CERT_S_SM_DS_TLS_EXPIRED	Expired CERT.DS.TLS certificate of the S_SM-DS with a valid signature, correctly formatted as X.509 certificate.
CERT_S_SM_DS_TLS_INV_CERT_POL	CERT.DS.TLS certificate of the S_SM-DS with invalid 'Certificate Policies' extension (OID not set to 'id-rspRoleds-tls'), formatted as X.509 certificate.
CERT_S_SM_DS_TLS_INV_CRITICAL_EXT	CERT.DS.TLS certificate of the S_SM-DS with one of the critical extensions not present, formatted as X.509 certificate.
	CERT.DP.TLS certificate of the S_SM-DP+, based on the different CI as defined in #IUT_LPAd_CI, not based on
CERT_S_SM_DS_TLS_INV_CURVE	 NIST P-256 curve, defined in Digital Signature Standard [11] brainpoolP256r1 curve, defined in RFC 5639 [8] FRP256V1 curve, defined in ANSSI ECC [9]
CERT_S_SM_DS_TLS_INV_EXT_KEY_USAGE	CERT.DS.TLS certificate of the S_SM-DS with invalid 'extended key usage' extension (not set to any combination of 'id-kp-serverAuth' or 'id-kp-clientAuth'), formatted as X.509 certificate.
CERT_S_SM_DS_TLS_INV_KEY_USAGE	CERT.DP.TLS certificate of the S_SM-DS with invalid 'key usage' extension (not set to 'digitalSignature'), formatted as X.509 certificate.
CERT_S_SM_DS_TLS_INV_OID	CERT.DS.TLS certificate of the S_SM-DS containing an invalid SM-DS OID, different to #S_SM_DS_OID, correctly formatted as X.509 certificate.
CERT_S_SM_DS_TLS_INV_SIG	Invalid CERT.DS.TLS certificate of the S_SM_DS with an invalid signature with the same tag and length as a valid signature, correctly formatted as X.509 certificate.
CERT_S_SM_DSauth_ECDSA	Certificate of the S_SM-DS for its Public ECDSA key used for SM-DS authentication. This certificate contains the OID #S_SM_DS_OID.
CERT_S_SM_DSauth_INV_SIGN	Invalid certificate of the S_SM-DS for its Public ECDSA key used for SM-DS authentication. This certificate contains an invalid signature, (i.e. not generated with the #SK_CI_ECDSA but with the same tag and length as a valid signature)
CERT_SERVER_TLS	CERT.SERVER.TLS certificate of the Server under test, based on NIST or Brainpool for this version of the specification, where the Certificate MAY be one of the following depending on the type of Server and whether it is a Server under test or a Server simulator: #CERT_SM_DP_TLS #CERT_SM_DS_TLS

V1.4 Page 599 of 777

GSM Aseociation Official Document SGP.23 - SGP.23 RSP Test	Public Key of the CI, contained within SpecifiqationECDSA
	#CERT_S_SM_DP_TLS#CERT_S_SM_DS_TLS
CERT_SM_DP_TLS	Certificate of the SM-DP+ for securing TLS, based on NIST or Brainpool for this version of the specification. CERT.DP.TLS in X.509 format.
CERT_SM_DPauth_ECDSA	Certificate of the S_SM-DP+ for its Public ECDSA key used for SM-DP+ authentication (CERT.DPauth.ECDSA) set as a fixed test CERT. Depending on the SM-DP+ configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1. The Authority Key Identifier is set as #CI_PKI_ID1
CERT_SM_DPpb_ECDSA	Certificate of the SM-DP+ for its Public ECDSA key used for Profile Package Binding (CERT.DPpb.ECDSA) set as a fixed test CERT. Depending on the SM-DP+ configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1.
CERT_SM_DS_TLS	Certificate of the SM-DS for securing TLS, based on NIST or Brainpool for this version of the specification. CERT.DS.TLS in X.509 format.
CERT_SM_DSauth_ECDSA	Certificate of the SM-DS for its Public ECDSA key used for SM-DS authentication (CERT.DSauth.ECDSA) set as a fixed test CERT. Depending on the SM-DS configuration, this certificate is based on NIST P-256, brainpoolP256r1 or FRP256V1. The Authority Key Identifier is set as #CI_PKI_ID1
CERT_SM_XXauth_ECDSA	CERT_SM_XXauth_ECDSA of the server under test, where XX = DP or XX = DS depending on the entity under test: #CERT_SM_DPauth_ECDSA #CERT_SM_DSauth_ECDSA
CI_PKI_ID1	The CI Subject Key Identifier as defined in SGP.26 [25].
CI_PKI_ID2	0x21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33
CI_PKI_ID3	0x31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43
CI_PKI_ID4	0x41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53
CI_PK_ID_INV	0x00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12
PK_EUICC_ECDSA	Public Key of the eUICC, contained within #CERT_EUICC_ECDSA

V1.4 Page 600 of 777

PK_S_CLIENT_TLS	Public key of CERT_S_CLIENT_TLS of the S_CLIENT, where the key MAY be one of the following depending on the role of the simulator: #PK_S_SM_DP_TLS #PK_S_SM_DS_TLS
PK_S_SERVER_TLS	Public key of CERT_S_SERVER_TLS of the S_SERVER, where the Certificate MAY be one of the following depending on the role of the simulator: #PK_S_SM_DP_TLS on ES9+ #PK_S_SM_DS_TLS on ES11
PK_S_SM_DP_TLS	Public key of CERT.DP.TLS of the S_SM-DP+.
PK_S_SM_DPauth_ECDSA	Public Key of the S_SM-DP+, contained within #CERT_S_SM_DPauth_ECDSA
PK_S_SM_DPpb_ECDSA	Public Key of the S_SM-DP+, contained within #CERT_S_SM_DPpb_ECDSA
PK_S_SM_DS_TLS	Public key of CERT_S_DS_TLS of the S_SM-DS.
PK_SM_DPauth_ECDSA	Public Key of the SM-DP+, contained within #CERT_SM_DPauth_ECDSA
PK_SM_DPpb_ECDSA	Public Key of the SM-DP+, contained within #CERT_SM_DPpb_ECDSA
PK_SM_DSauth_ECDSA	Public Key of the SM-DS, contained within #CERT_SM_DSauth_ECDSA
PK_SM_XXauth_ECDSA	PK_SM_XXauth_ECDSA of the server under test, where XX = DP or XX = DS depending on the entity under test: #PK_SM_DPauth_ECDSA #PK_SM_DSauth_ECDSA
SK_CI_ECDSA	Private Key of the CI
SK_EUICC_ECDSA	Private key of the eUICC for creating signatures
SK_S_SM_DPauth_ECDSA	Private Key of the of S_SM-DP+ for creating signatures for SM-DP+ authentication
SK_S_SM_DSauth_ECDSA	Private Key of the of S_SM-DS for creating signatures for SM-DS authentication
SK_S_SM_DPpb_ECDSA	Private key of the S_SM-DP+ used to provide signatures for Profile binding

V1.4 Page 601 of 777

Annex B Dynamic Content

Variable	Description
ANY_SW_IN_ERROR	Any Status Word in error (different from 0x9000)
BPP	Content of a Bound Profile Package to download within the eUICC.
BPP_OTPK_EUICC_ECKA	One-time Public Key of the eUICC for ECKA used for the BPP
BPP_SEG_A0	Bound Profile Package TLV segment containing the tag and length fields of the firstSequenceOf87 TLV plus the first 0x87 TLV containing the ConfigureISDP command
	Bound Profile Package following TLV segment array, as defined in SGP.22 [2] – section 2.5.5:
BPP_SEG_A1	array first element containing the Tag and length fields of the sequenceOf88 TLV
	array following elements containing each of the '88' TLVs containing the StoreMetadata command
BPP_SEG_A2	Bound Profile Package TLV segment containing the Tag and length fields of the secondSequenceOf87 TLV plus the first '87' TLV, containing the ReplaceSessionKeys command
	Bound Profile Package following TLV segment array, as defined in SGP.22 [2] – section 2.5.5:
BPP_SEG_A3	 array first element containing the tag and length fields of the sequenceOf86 TLV
	array following elements containing each of the '86' TLVs containing the Protected Profile Package (PPP)
BPP_SEG_INIT	Bound Profile Package TLV segment containing the tag and length fields of the BoundProfilePackage TLV plus the initialiseSecureChannelRequest command
C_APDUS_SCRIPT	List of Command APDUs formatted as an expanded structure with definite length coding as defined in ETSI TS 102 226 [14].
СС	SCP80 cryptographic checksum as defined in ETSI TS 102 225 [13] (8 bytes long).
CHANNEL_NUMBER	The logical channel number newly opened in the eUICC. If no logical channel is opened, the value is set to 0x00 (i.e. Basic Channel).
CLIENT_TLS_EPHEM_KEY	Client's ephemeral key and associated information.
CONF_ISDP_PROF1_ENC	An element of firstSequenceOf87, consisting of #CONF_ISDP_PROF1_SMDP protected with <s_enc> and <s_mac> and encapsulated in a TLV with tag 0x87, length <l> to a maximum size of 1020 bytes including the tag and length fields.</l></s_mac></s_enc>
EUICC_CANCEL_SESSION_SIGNA TURE	euiccCancelSessionSignature is created using the SK.EUICC.ECDSA signed over euiccCancelSessionSigned coded as ASN.1 OCTET STRING.
EUICC_CANCEL_SESSION_SIGNA TURE_INVALID	eUICC signature randomly generated and coded as an ASN.1 OCTET STRING not equal to <euicc_cancel_session_signature> but with the same length as a valid signature</euicc_cancel_session_signature>
EUICC_CHALLENGE	Random eUICC challenge, coded as asn.1 OCTET STRING, 16 bytes.

V1.4 Page 602 of 777

	List of CI Public Key Identifiers supported on the eUICC for signature
EUICC_CI_PK_ID_LIST_FOR_SIGNI NG	creation, coded as ASN.1 sequence of SubjectKeyIdentifier. The CI Public Key Identifier is from the list of possible CI Public Key Identifier. This possible CI Public Key Identifiers as supported by the eUICC will be defined later on.
EUICC_CI_PK_ID_LIST_FOR_VERI FICATION	List of CI Public Key Identifiers supported on the eUICC for signature verification, coded as ASN.1 sequence of SubjectKeyIdentifier. The CI Public Key Identifier is from the list of possible CI Public Key Identifier. This possible CI Public Key Identifiers as supported by the eUICC will be defined later on.
EUICC_CI_PK_ID_TO_BE_USED	CI Public Key Identifier to be used by the eUICC for signature, coded as ASN.1 sequence of SubjectKeyIdentifier.
EUICC_CS_SIGNATURE	The eUICC cancel session signature computed using the #SK_EUICC_ECDSA across the EuiccCancelSessionSigned present in the CancelSessionResponse structure
EUICC_RSP_CAPABILITY	RspCapability of the eUICC, coded as ASN.1 BIT STRING (4 bits) to be used for indication of additionalProfile, crlSupport, rpmSupport, testProfileSupport
EUICC_SIGN_PIR	The eUICC signature of the Profile Installation Result (PIR). The input data used to generate the <euicc_sign_pir> is the profileInstallationResultData TLV.</euicc_sign_pir>
EUICC_SIGNATURE1	The eUICC signature 1 (euiccSignature1) computed using #SK_EUICC_ECDSA across the euiccSigned1 present in the AuthenticateServerResponse structure, coded as ASN.1 OCTET STRING.
EUICC_SIGNATURE1_INVALID	eUICC signature randomly generated and coded as an ASN.1 OCTET STRING not equal to <euicc_signature1></euicc_signature1>
EUICC_SIGNATURE2	The eUICC signature 2 (euiccSignature2) computed using the #SK_EUICC_ECDSA across the following data objects: • euiccSigned2 • smdpSignature2 present in the PrepareDownloadRequest structure
EUICC_SIGNATURE2_INVALID	eUICC signature randomly generated and coded as an ASN.1 OCTET STRING not equal to <euicc_signature2></euicc_signature2>
EVENT_ID	An EventID value in String format, generated by the SM-DS during Event Record registration.
EVENT_ID_R	The EventID value in String format generated by the SM-DS during Event Record registration.
EXT_CARD_RESOURCE	Extended Card Resource Information according to ETSI TS 102 226 [14], coded as ASN.1 OCTET STRING. 'Number of installed application' value field is '00'.
EXT_SHA256_ECDSA	TLS extension data for "supported_signature_algorithms" set as a minimum of HashAlgorithm sha256 (04) and SignatureAlgorithm ecdsa (03).
FREE_MEMORY_NO_PROFILE	Non-volatile memory (tag 0x82) available in the eUICC when there is no Profile installed

V1.4 Page 603 of 777

FREE_MEM_OP_PROF_INSTALLE D	Non-volatile memory (tag 0x82) available in the eUICC when two or more PROFILE_OPERATIONAL are installed
FREE_MEM_OP_PROF1_DELETED	Non-volatile memory (tag 0x82) available in the eUICC after PROFILE_OPERATIONAL1 deletion
FREE_MEM_OP_PROF1_INSTALLE D	Non-volatile memory (tag 0x82) available in the eUICC when only PROFILE_OPERATIONAL1 is installed
FUNCTION_CALL_ID	The function call ID generated by the entity that calls the function
FUNCTION_REQ_ID	The function requester ID
INVALID_TRANSACTION_ID	A Transaction Identifier generated by the S_SM-DP+ or the S_SM-DS that SHALL be different from <s_transaction_id> if exists. Otherwise, a random value is generated.</s_transaction_id>
INVALID_SM_DP_OID	SM-DP+ OID (as defined in section 1.3) not equal to #IUT_SM_DP_OID
ISD_P_AIDX	An invalid ISD-P AID not present on the eUICC. This AID value is in the range from 0xA0 00 00 05 59 10 10 FF FF FF F8 90 00 00 10 00 to 0xA0 00 00 05 59 10 10 FF FF FF 89 00 FF FF 00.
ISD_P_AID	The ISD-P AID newly created in the eUICC. This AID value is in the range from 0xA0 00 00 05 59 10 10 FF FF FF F8 90 00 01 00 00 0xA0 00 00 05 59 10 10 FF FF FF FF 89 00 FF FF 00. Last byte is set to '00' as defined in SGP.02[1].
ISD_P_AID1	The ISD-P AID created in the eUICC for the PROFILE_OPERATIONAL1. This AID value belongs to the range from 0xA0 00 00 05 59 10 10 FF FF FF FF 89 00 00 10 00 to 0xA0 00 00 559 10 10 FF FF FF 89 00 FF FF 00. Last byte is set to '00' as defined in SGP.02[1].
ISD_P_AID2	The ISD-P AID created in the eUICC for the PROFILE_OPERATIONAL2. This AID value belongs to the range from 0xA0 00 00 05 59 10 10 FF FF FF FF 89 00 00 10 00 to 0xA0 00 00 559 10 10 FF FF FF 89 00 FF FF 00. Last byte is set to '00' as defined in SGP.02[1].
ISD_P_AID3	The ISD-P AID created in the eUICC for the PROFILE_OPERATIONAL3. This AID value belongs to the range from 0xA0 00 00 05 59 10 10 FF FF FF F8 9 00 00 10 00 to 0xA0 00 00 559 10 10 FF FF FF FF 89 00 FF FF 00. Last byte is set to '00' as defined in SGP.02[1].
ISD_P_AID4	The ISD-P AID created in the eUICC for the PROFILE_OPERATIONAL4. This AID value belongs to the range from 0xA0 00 00 05 59 10 10 FF FF FF FF 89 00 00 10 00 to 0xA0 00 00 559 10 10 FF FF FF 89 00 FF FF 00. Last byte is set to '00' as defined in SGP.02[1].
L	Exact length of the corresponding tag or of the remaining data.
MATCHING_ID	Unique identifier as defined in [2]. The content can be either empty, or the value of the EventID, or the value of the Activation Code token.

V1.4 Page 604 of 777

	1
MATCHING_ID_EVENT	A Unique identifier of an Event for a specific EID generated by the SM-DP+ / SM-DS.
METADATA_OP_PROF1_SEG	The #METADATA_OP_PROF1 is mac-ed with <s_mac> and split as necessary into segments of a maximum size of 1020 bytes (including the tag, length field, and MAC),</s_mac>
MNO_SCP80_COUNTER	SCP80 counter of the MNO-SD related to the KVN 0x01 (5 bytes long). Initial value is set to 0x00 00 00 01 and is incremented by one each time a secured packet is sent.
NB_EXECUTED_C_APDUS	Number of executed Command TLV objects as defined in ETSI TS 102 226 [14].
NOTIF_SEQ_NO_DE1	The Sequence Number of the Delete Notification related to the PROFILE_OPERATIONAL1.
NOTIF_SEQ_NO_DI1	The Sequence Number of the Disable Notification related to the PROFILE_OPERATIONAL1.
NOTIF_SEQ_NO_EN1	The Sequence Number of the Enable Notification related to the PROFILE_OPERATIONAL1.
NOTIF_SEQ_NO_EN2	The Sequence Number of the Enable Notification related to the PROFILE_OPERATIONAL2.
NOTIF_SEQ_NO_IN1	The Sequence Number of the Install Notification related to the PROFILE_OPERATIONAL1.
NOTIF_SEQ_NO_IN2	The Sequence Number of the Install Notification related to the PROFILE_OPERATIONAL2.
NOTIF_SEQ_NO_IN1_PIR	The Sequence Number of the Install Notification (PIR) related to the PROFILE_OPERATIONAL1.
NOTIF_SEQ_NO_IN2_PIR	The Sequence Number of the Install Notification (PIR) related to the PROFILE_OPERATIONAL2.
NOTIF_SEQ_NO2_DE1	The Sequence Number of the second Delete Notification related to the PROFILE_OPERATIONAL1.
NOTIF_SEQ_NO2_DI1	The Sequence Number of the second Disable Notification related to the PROFILE_OPERATIONAL1.
NOTIF_SEQ_NO2_EN1	The Sequence Number of the second Enable Notification related to the PROFILE_OPERATIONAL1.
OTPK_EUICC_ECKA	One-time Public Key generated by the eUICC for ECKA. Depending on the eUICC configuration, this key is based on NIST P-256, brainpoolP256r1 or FRP256V1.
OTPK_S_SM_DP+_ECKA	One-time Public Key generated by the S_SM-DP+ for ECKA. Depending on the eUICC configuration, this key is based on NIST P-256, brainpoolP256r1 or FRP256V1.

V1.4 Page 605 of 777

OT_SK_S_SM_DP+_ECKA	One-time Private Key generated by the S_SM-DP+ for ECKA. Depending on the eUICC configuration, this key is based on NIST P-256, brainpoolP256r1 or FRP256V1.
OTPK_EUICC_ECKA_NEW	One-time Public Key of the eUICC for ECKA used for the BPP which is a new generated value different from <otpk_euicc_ecka></otpk_euicc_ecka>
OTPK_SM_DP+_ECKA	One-time Public Key generated by the SM-DP+ for ECKA. Depending on the eUICC configuration, this key is based on NIST P-256, brainpoolP256r1 or FRP256V1.
PPK_ENC	Random PPK-ENC value (16 bytes key length). This value is different from <s_enc> value.</s_enc>
PPK_INIT_MAC	Random initial MAC chaining value (16 bytes). This value is different from the <s_mac_chain> value.</s_mac_chain>
PPK_MAC	Random PPK-MAC value (16 bytes key length). This value is different from <s_mac> value.</s_mac>
PPP_OP_PROF1_SEG_PPK	An element of sequenceOf86, consisting of a <upp_op_prof1_seg> protected with <ppk_enc> and <ppk_mac> and encapsulated in a TLV with tag 0x86 length <l>, up to a maximum size of 1020 bytes including the tag and length field.</l></ppk_mac></ppk_enc></upp_op_prof1_seg>
PPP_OP_PROF1_SEG_SK	An element of sequenceOf86, consisting of a <upp_op_prof1_seg> segment protected with <s_enc> and <s_mac> and encapsulated in a TLV with tag 0x86, length <l>, up to a maximum size of 1020 bytes including the tag and length field.</l></s_mac></s_enc></upp_op_prof1_seg>
PPP_OP_PROF1_SEG_SK_INV	<ppp_op_prof1_seg_sk> modified (wrong encryption)</ppp_op_prof1_seg_sk>
PPR_IDS	Forbidden Profile Policy Rules. This PPR list MAY be empty or MAY contain either PPR1 or PPR2 or both.
PROPRIETARY_DATA	Proprietary Data returned by the eUICC as part of FCI template
R_APDU_PARTx	Sub-part of a R-APDU (see Annex D.4.2)
RANDOM_SM_DP+_SIGN	Random SM-DP+ signature (i.e. content of the tag 0x5F37) with a size corresponding to a valid one.
RANDOM_SM_DS_SIGN	Random SM-DS signature (i.e. content of the tag 0x5F37) with a size corresponding to a valid one.
REPLACE_S_KEYS_REQ_ENC	An element of secondSequenceOf87, consisting of #REPLACE_S_KEYS_REQ protected with <s_enc> and <s_mac> and encapsulated in a TLV with tag 0x87, up to a maximum size of 1020 bytes including the tag and length field.</s_mac></s_enc>
RSP_SERVER_ADDRESS	RSP Server address in FQDN format where the operation corresponding to the Event can be processed.
S_ENC	SCP03T Encryption Session key (128 bits length) resulting from the key agreement with eUICC.

V1.4 Page 606 of 777

S_HASHED_CC	Hashed Confirmation Code generated by the LPA
S_HASHED_CC_ERROR	A random generated hash value of the Confirmation Code not equal to S_HASHED_CC.
S_INIT_MAC	SCP03T Initial MAC chaining value (128 bits length) resulting from the key agreement with eUICC.
S_MAC	SCP03T MACing Session key (128 bits length) resulting from the key agreement with eUICC.
S_MAC_CHAIN	Current MAC chaining value used for SCP03t BPP protection.
S_SEL_TLS_CIPHER_SUITE	TLS cipher suite selected by the Server set as follows: o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 if present in <tls_cipher_suites>, otherwise o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256.</tls_cipher_suites>
S_SM_DP+_SIGN	The S_SM-DP+ signature (smdpSign), computed using the #SK_S_SM_DPpb_ECDSA across the following data objects: • remoteOpId • transactionId • controlRefTemplate • smdpOtpk • euiccOtpk, as provided earlier in the prepareDownloadResponse data object
S_SM_DP+_SIGNATURE2	The ASN.1 OCTET STRING encoded SM-DP+ signature 2 (field smdpSignature2) computed using the private key related to the server certificate (field smdpCertificate) present in the PrepareDownloadRequest structure. This signature SHALL be generated across the following data objects: • smdpSignature2 • euiccSignature1 present in the AuthenticateServerResponse structure
S_SMDP_CHALLENGE	The SM-DP+ Challenge (serverChallenge) randomly chosen by the simulated SM-DP+ to be signed later by the eUICC for the eUICC authentication, coded as ASN.1 OCTET STRING of 16 bytes.
S_SMDP_SIGNATURE1	The ASN.1 OCTET STRING encoded SM-DP+ signature (field serverSignature1) computed using the private key related to the server certificate (field serverCertificate) present in the AuthenticateServerRequest structure.
S_SMDP_SIGNATURE_INV	<s_smdp_signature1> NOT computed with the #SK_S_SM_DPauth_ECDSA but with the same length as a valid signature</s_smdp_signature1>
S_SMDP_SIGNED1 (ServerSigned1)	<pre>{ transactionId <s_transaction_id>, euiccChallenge <euicc_challenge>, serverAddress #TEST_DP_ADDRESS1, serverChallenge <s_smdp_challenge> }</s_smdp_challenge></euicc_challenge></s_transaction_id></pre>

V1.4 Page 607 of 777

S_SMDP_SIGNED_INV_ADDR	<s_smdp_signed1> with a different SM-DP+ address (#TEST_DP_ADDRESS2 instead of #TEST_DP_ADDRESS1)</s_smdp_signed1>
S_SMDS_CHALLENGE	The SM-DS Challenge (serverChallenge) randomly chosen by the simulated SM-DS to be signed later by the eUICC for the eUICC authentication, coded as ASN.1 OCTET STRING of 16 bytes.
S_SMDS_SIGNATURE_INV	<s_smds_signature1> NOT computed with the #SK_S_SM_DSauth_ECDSA but with the same length as a valid signature</s_smds_signature1>
S_SMDS_SIGNED1 (ServerSigned1)	<pre>{ transactionId <s_transaction_id>, euiccChallenge <euicc_challenge>, serverAddress #TEST_ROOT_DS_ADDRESS, serverChallenge <s_smds_challenge> }</s_smds_challenge></euicc_challenge></s_transaction_id></pre>
S_SMDS_SIGNED_ADDR1 (ServerSigned1)	<pre>{ transactionId <s_transaction_id>, euiccChallenge <euicc_challenge>, serverAddress #TEST_DS_ADDRESS1, serverChallenge <s_smds_challenge> }</s_smds_challenge></euicc_challenge></s_transaction_id></pre>
S_SMDS_SIGNED_INV_ADDR	<s_smds_signed1> with a different SM-DS address (#TEST_DP_ADDRESS1 instead of #TEST_ROOT_DS_ADDRESS)</s_smds_signed1>
S_SMDS_SIGNATURE1	The SM-DS signature 1 (serverSignature1) computed using #SK_S_SM_DSauth_ECDSA across the serverSigned1 present in the AuthenticateServerRequest structure, coded as ASN.1 OCTET STRING
S_TRANSACTION_ID	The TransactionID (Unique Transaction Identifier) generated by the (S_)SM-DP+, or (S_)SM-DS which is used to uniquely identify the RSP session and to correlate the multiple ESXX request messages that belong to the same RSP session. This value (binary value) can start from 0x01 and can be increased by 1 each time a Profile is downloaded in the eUICC. 1-16 bytes (ASN.1 OCTET STRING).
SAH_SHA256_ECDSA	Signature And Hash Algorithm extension sent in the CertificateRequest message set as a minimum of: o HashAlgorithm sha256 (04) and o SignatureAlgorithm ecdsa (03).
SEL_TLS_CIPHER_SUITE	TLS cipher suite selected by the Server
SEQ_NUMBER	Sequence Number related to a Notification Metadata generated by the eUICC.
SERVER_CHALLENGE	Random value generated by the SM-XX server under test coded as ASN.1 OCTET STRING of 16 bytes which can be one of the following depending on the entity under test: • <smdp_challenge> • <smds_challenge></smds_challenge></smdp_challenge>

V1.4 Page 608 of 777

SERVER_CHALLENGE_2	Random value generated by the SM-XX server under test coded as ASN.1 OCTET STRING of 16 bytes which can be one of the following depending on the entity under test:
	<smdp_challenge_2></smdp_challenge_2><smds_challenge_2></smds_challenge_2>
SERVER_FINISHED	The first protected message with the negotiated algorithms, keys, and secrets. It is the Hash of the concatenation of all the data from all messages in this handshake up to, but not including, this message i.e. all handshake messages starting at ClientHello up to, but not including, this Finished message itself.
	NOTE: ChangeCipherSpec messages, alerts, and any other record type are not handshake messages and are not included in the hash computations. Also, HelloRequest messages are omitted from handshake hashes.
	Server signature (serverSignature1) which can be one of the following depending on the entity under test:
SERVER_SIGNATURE1	 SM-DP+ signature (serverSignature1) generated over #SERVER_SIGNED1 using SK.DPauth.ECDSA, coded as ASN.1 OCTET STRING SM-DS signature (serverSignature1) generated over #SERVER_SIGNED1 using SK.DSauth.ECDSA, coded as ASN.1 OCTET STRING
SERVER_SIGNATURE1_2	SERVER signature (serverSignature1) which can be one of the following depending on the entity under test: • SM-DP signature (serverSignature1) generated over #SERVER_SIGNED1_2 using SK.DPauth.ECDSA, coded as ASN.1 OCTET STRING • SM-DS signature (serverSignature1) generated over #SERVER_SIGNED1_2 using SK.DSauth.ECDSA, coded as ASN.1 OCTET STRING
SERVER_TLS_EPHEM_KEY	Server's ephemeral key and associated information.
SESSION_ID_RANDOM	Random value of the TLS session
SHS	Shared Secret resulting from the key agreement with eUICC.
SM_DP+_SIGN	The SM-DP+ signature in ES8+/InitialiseSecureChannelRequest/smdpSign.
SMDP_CHALLENGE	Random value generated by the SM-DP+ coded as ASN.1 OCTET STRING of 16 bytes.
SMDP_CHALLENGE_2	Random value generated by the SM-DP+ coded as ASN.1 OCTET STRING of 16 bytes.
SMDP_CHALLENGE_INVALID	SM-DP+ Challenge randomly generated by the simulated SM-DP+ coded as ASN.1 OCTET STRING of 16 bytes not equal to <smdp_challenge>.</smdp_challenge>
SMDP_METADATA_SEG_MAC	An element of sequenceOf88, consisting of a segment of maximum size 1008 bytes protected with <s_mac> and encapsulated in a TLV with</s_mac>

V1.4 Page 609 of 777

	tag 0x88, length <l>, up to a maximum size of 1020 bytes including the tag and length field.</l>
SMDP_SIGNATURE2	SM-DP+ signature (smdpSignature2) generated over smdpSigned2 using SK.DPauth.ECDSA, coded as ASN.1 OCTET STRING
SMDS_CHALLENGE	Random value generated by the SM-DS coded as ASN.1 OCTET STRING of 16 bytes.
SMDS_CHALLENGE_2	Random value generated by the SM-DS coded as ASN.1 OCTET STRING of 16 bytes.
SMDS_CHALLENGE_INVALID	SM-DS Challenge randomly generated by the simulated SM-DS coded as ASN.1 OCTET STRING of 16 bytes not equal to <smds_challenge>.</smds_challenge>
STORE_DATA_BLOCK_NUM	The STORE DATA block number coded sequentially from 0x00 to 0xFF. If the value 0xFF has been reached and more STORE DATA commands are needed to complete the transfer, the numbering restarts and the next STORE DATA block number is set to 0x00.
TBS_EUICC_NOTIF_SIG	The eUICC signature generated over tbsOtherNotification. NotificationMetadata, coded as ASN.1 OCTET STRING.
TLS_CIPHER_SUITES	TLS cipher suite list supported by LPAd or the Client (SM-DP+ or SM-DS) under test.
TRANSACTION_ID_2	A unique Transaction ID generated by an SM-DP+ or an SM-DS within the scope and lifetime of each SM-DP+ or SM-DS to uniquely identify the ongoing RSP session as OCTET STRING of up to 16 bytes.
TRANSACTION_ID_AC	A unique Transaction ID generated by an SM-DP+ or an SM-DS within the scope and lifetime of each SM-DP+ or SM-DS to uniquely identify the ongoing RSP session used by the AuthenticateClient function as OCTET STRING of up to 16 bytes.
TRANSACTION_ID_GBPP	A unique Transaction ID generated by an SM-DP+ within the scope and lifetime of each SM-DP+ to uniquely identify the ongoing RSP session used by the GetBoundProfilePackage function as OCTET STRING of up to 16 bytes.
TRANSACTION_ID_IA	A unique Transaction ID generated by an SM-DP+ or an SM-DS within the scope and lifetime of each SM-DP+ or an SM-DS to uniquely identify the ongoing RSP session used by the InitiateAuthentication function as OCTET STRING of up to 16 bytes.
TRANSACTION_ID_ISC	A unique Transaction ID generated by an SM-DP+ within the scope and lifetime of each SM-DP+ to uniquely identify the ongoing RSP session used by the InitialiseSecureChannelRequest function as OCTET STRING of up to 16 bytes.
TRANSACTION_ID_SIGNED	A unique Transaction ID generated by an SM-DP+ or an SM-DS within the scope and lifetime of each SM-DP+ or SM-DS to uniquely identify the ongoing RSP session as OCTET STRING of up to 16 bytes signed as part of #SERVER_SIGNED1
TRANSACTION_ID_SIGNED_2	A unique Transaction ID generated by an SM-DP+ or an SM-DS within the scope and lifetime of each SM-DP+ or SM-DS to uniquely identify

V1.4 Page 610 of 777

	the ongoing RSP session as OCTET STRING of up to 16 bytes signed as part of #SERVER_SIGNED1
TRANSACTION_ID_SIGNED_AC	A unique Transaction ID generated by an SM-DP+ or an SM-DS within the scope and lifetime of each SM-DP+ or SM-DS to uniquely identify the ongoing RSP session used by the AuthenticateClient function as OCTET STRING of up to 16 bytes.
TRANSACTION_ID_SIGNED_IA	A unique Transaction ID generated by an SM-DP+ or an SM-SD within the scope and lifetime of each SM-DP+ or SM-DS to uniquely identify the ongoing RSP session used by the InitiateAuthentication function as OCTET STRING of up to 16 bytes.
UPP_OP_PROF1_SEG	A segment of the #UPP_OP_PROF1, with a maximum size of 1007 bytes.
UPP_OP_PROF2_SEG	A segment of the #UPP_OP_PROF2, with a maximum size of 1007 bytes.

V1.4 Page 611 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Annex C Methods and Procedures

This section describes methods and procedures used in the interfaces compliance test cases. They are part of test cases and SHALL not be executed in standalone mode.

C.1 Methods

If the method is used in the "expected result" column, all parameters SHALL be verified by the simulated entity (test tool). If the method is used in the "Sequence / Description" column, the command SHALL be generated by the simulated entity.

Method	MTD_AUTHENTICATE_CLIENT
Description	Generates or verifies the JSON formatted AuthenticateClient request
Parameter(s)	 paramTransactionId: random 16 byte identifier encoded as String Hexadecimal. paramAuthenticateServerResponse: server authentication response
	structured as ASN.1 encoded as base 64. JSON body
Details	<pre>{ "transactionId" : paramTransactionId, "authenticateServerResponse" : paramAuthenticateServerResponse }</pre>

Method	MTD_CANCEL_SESSION
Description	Sends or verifies the JSON formatted CancelSession request
Parameter(s)	 paramTransactionId: random 16 byte identifier. paramCancelSessionResponse: eUICC information structured as ASN.1 encoded as base 64.
Details	<pre>JSON body { "transactionId" : paramTransactionId, "cancelSessionResponse" : paramCancelSessionResponse }</pre>

Method	MTD_CHECK_SMS_POR
Description	Check the content of the SMS POR containing the response of the ES6.UpdateMetadata request
Parameter(s)	paramExpectedSW: the expected Status Word of the last STORE DATA command
	Parse and retrieve the SCP80 response packet from the SMS.
Details	SCP80 response status code SHALL be equal to $0x00 - POR OK$.
	The additional data from the response packet SHALL be formatted as an expanded structure with definite length as defined in ETSI TS 102 226 [14] and contains the following TLV:

V1.4 Page 612 of 777

```
AB <L>
80 <L> <NB_EXECUTED_C_APDUS> -- Number of executed C-APDUS
23 <L> 00 90 00 -- R-APDU of the INSTALL FOR PERSONALIZATION
command
23 <L> paramexpectedsw -- Sw of the last STORE DATA command
executed

<NB_EXECUTED_C_APDUS> SHALL be equal to the number of executed C-APDUs (i.e. one INSTALL FOR PERSONALIZATION + n STORE DATA command(s))
```

Method	MTD_DELETE_EVENT	
Description	Sends and checks the JSON formatted DeleteEvent request	
Parameter(s)	 paramFunctionRequesterId: identification of the function requester. paramFunctionCallId: identification of the function call. paramEID: EID of the targeted eUICC paramEventId: unique Identification of the Event to be registered 	
Details	<pre>JSON requestHeader { "header" : { "functionRequesterIdentifier" : "paramFunctionRequesterId", "functionCallIdentifier" : "paramFunctionCallId" } JSON body { "eid" : paramEID, "eventId" : paramEventId } }</pre>	

Method	MTD_DISABLE_PROFILE
Description	Generate the ASN.1 DisableProfileRequest structure according to the input parameters.
Parameter(s)	 paramIccidValue: The ICCID of the Profile to Disable (optional) paramIsdpAidValue: The ISD-P AID of the Profile to Disable (optional) paramRefreshFlag: Boolean, TRUE if refreshFlag SHALL be set, FALSE otherwise Either paramIccidValue or paramIsdpAidValue is passed as a parameter.
Details	<pre>IF paramlccidValue is provided Then req DisableProfileRequest::= { profileIdentifier iccid : paramIccidValue, refreshFlag paramRefreshFlag } Else</pre>

V1.4 Page 613 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

```
req DisableProfileRequest::= {
   profileIdentifier isdpAid : paramIsdpAidValue,
   refreshFlag paramRefreshFlag
}
End if
```

Method	MTD_ENABLE_PROFILE
Description	Generate the ASN.1 EnableProfileRequest structure according to the input parameters.
Parameter(s)	 paramIccidValue: The ICCID of the Profile to Disable (optional) paramIsdpAidValue: The ISD-P AID of the Profile to Disable (optional) paramRefreshFlag: Boolean, TRUE if refreshFlag SHALL be set, FALSE otherwise
	Either paramIccidValue or paramIsdpAidValue is passed as a parameter.
	<pre>IF paramlccidValue is provided Then req EnableProfileRequest ::= { profileIdentifier iccid : paramIccidValue, refreshFlag paramRefreshFlag }</pre>
Details	<pre>req EnableProfileRequest ::= { profileIdentifier isdpAid : paramIsdpAidValue, refreshFlag paramRefreshFlag } Fnd if</pre>
	End if

Method	MTD_DELETE_PROFILE
Description	Generate the ASN.1 DeleteProfileRequest structure according to the input parameters.
Parameter(s)	 paramIccidValue: The ICCID of the Profile to Delete (optional) paramIsdpAidValue: The ISD-P AID of the Profile to Delete (optional) Either paramIccidValue or paramIsdpAidValue is passed as a parameter.
Details	<pre>IF paramIccidValue is provided Then req DeleteProfileRequest ::= iccid : paramIccidValue Else req DeleteProfileRequest ::= isdpAid : paramIsdpAidValue End if</pre>

Method	MTD_GET_PROFILE_INFO
Description	Generate the ASN.1 ProfileInfoListRequest according to the input parameters.

V1.4 Page 614 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

Parameter(s)	paramIccidValue: The ICCID of the Profile paramIsdpAidValue: The ISD-P AID of the Profile
	Either paramlccidValue or paramlsdpAidValue is passed as a parameter.
	<pre>IF paramlccidValue is provided Then req ProfileInfoListRequest::= {</pre>
Details	<pre>searchCriteria iccid: paramIccidValue } Else</pre>
	<pre>req ProfileInfoListRequest::= { searchCriteria isdpAid: paramIsdpAidValue }</pre>
	End If

Method	MTD_GENERATE_BPP	
Description	Generate a BPP according to the input parameters.	
Parameter(s)	 paramInitSC: The InitialiseSecureChannel request paramConfISDP: The ConfigureISDP request (plain) paramStoreMetadata: The StoreMetadata request (plain) paramReplaceSessionKeys: The ReplaceSessionKeys request (plain) – Optional parameter paramUPP: The Unprotected Profile Package to download 	
Details	Split the paramStoreMetadata in several segments of maximum 1008 bytes. Each Metadata segment is named <metadata_segment 1007="" <upp_seg="" bytes.="" each="" eafter.="" in="" maximum="" named="" of="" paramupp="" segment="" segments="" several="" split="" the="" upp=""> here after. Create the following structure of data:</metadata_segment>	

V1.4 Page 615 of 777

```
req BoundProfilePackage ::= {
  paramInitSC,
  firstSequenceOf87 {
    0x87 <L> paramConfISDP
  sequenceOf88 {
    0x88 <L> <METADATA SEG>,
    0x88 <L> <METADATA SEG>
  },
  -- secondSequenceOf87 SHALL be set only if paramReplaceSessionKeys is
  -- provided
  secondSequenceOf87 {
    0x87 <L> paramReplaceSessionKeys
  },
  sequenceOf86 {
    0x86 <L> <UPP_SEG>,
    0x86 <L> <UPP SEG>
Use <OT SK S SM DP+ ECKA> and <OTPK EUICC ECKA> in order to generate the
<SHS>.
Concatenate #KEY_TYPE, #KEY_LENGTH, <L> #HOST_ID and <L> #EID1 as SharedInfo.
Retrieve <S_ENC>, <S_MAC> and <S_INIT_MAC> across SHA-256 calculated from <SHS>
and SharedInfo.
Encrypt paramConfISDP with <S_ENC>.
Calculate and add a MAC to the tag 0x87 of firstSequenceOf87 by using <S MAC>.
Calculate and add a MAC to all tags 0x88 of sequenceOf88 by using <S MAC>.
If paramReplaceSessionKeys is provided Then
 Encrypt paramReplaceSessionKeys with <S ENC>
 Calculate and add a MAC to the tag 0x87 of secondSequenceOf87 by using <S MAC>.
End If
Encrypt all <UPP SEG> with <S ENC>, or <PPK ENC> if paramReplaceSessionKeys is
provided.
Calculate and add a MAC to all tags 0x86 of sequenceOf86 by using <S MAC>, or
<PPK MAC> (and <PPK INIT MAC> for the first tag) if paramReplaceSessionKeys is
provided.
```

Method	MTD_GENERATE_HASHED_CC
Description	Generate an Hashed Confirmation Code based on the Confirmation Code and the Transaction ID given in parameter.
Parameter(s)	 paramConfirmationCode: The Confirmation Code (plain) paramTransactionId: The Transaction ID (plain)

V1.4 Page 616 of 777

Details	Generate a SHA-256 of the paramConfirmationCode. Concatenate the obtained hash value with the paramTransactionId.
	Generate and return a SHA-256 of these two concatenated elements.

Method	MTD_GET_BPP
Description	Generates or verifies the JSON formatted GetBoundProfilePackage request
Parameter(s)	 paramTransactionId: random 16 byte identifier. paramPrepareDownloadResponse structured as ASN.1 encoded as base 64.
Details	<pre>JSON body { "transactionId" : paramTransactionId, "prepareDownloadResponse" : paramPrepareDownloadResponse }</pre>

Method	MTD_HANDLE_NOTIF
Description	Generates or verifies the JSON formatted HandleNotification request
Parameter(s)	paramPendingNotification: PendingNotification data object
Details	<pre>JSON body { "pendingNotification" : paramPendingNotification }</pre>

Method	MTD_HTTP_REQ
Description	Sends or verifies a secured HTTP request message delivering a JSON object payload using a network to an off-card entity.
Parameter(s)	 paramServerAddress: Target Server address paramFunctionPath: Function path paramRequestMessage: JSON Request message
Details	HTTP POST paramFunctionPath HTTP/1.1 Host: paramServerAddress User-Agent: See Note X-Admin-Protocol:gsma/rsp/v#RSP_SVN Content-Type:application/json Content-Length: <l> paramRequestMessage NOTE: If the request is sent by the LPAd, the User-Agent SHALL be gsma-rsp-load. The "User-Agent" field may contain additional information after a semicolon</l>
25.55	

V1.4 Page 617 of 777

The HTTP POST request may contain additional header fields. These shall not be checked.

Method	MTD_HTTP_RESP
Description	Sends or verifies a secured HTTP response message delivering a JSON object payload using a network to an off-card entity.
Parameter(s)	paramResponseMessage: JSON Response message
Details	HTTP/1.1 200 (OK) X-Admin-Protocol: gsma/rsp/v#RSP_SVN Content-Type: application/json Content-Length: <l></l>
	paramResponseMessage The HTTP response may contain additional header fields. These shall not be checked.

Method	MTD_INITIATE_AUTHENTICATION
Description	Generates or verifies the JSON formatted Initiate Authentication request on ES9+ or ES11 as applicable.
Parameter(s)	 paramEUICCChallenge: random 16 byte challenge coded as base 64 paramEUICCInfo1: eUICC information structured coded as base 64 paramServerAddress: FQDN of the Server.
Details	<pre>JSON body { "euiccChallenge" : paramEUICCChallenge, "euiccInfol" : paramEUICCInfol, "smdpAddress" : paramServerAddress }</pre>

Method	MTD_REGISTER_EVENT
Description	Send or checks the JSON formatted RegisterEvent request
Parameter(s)	 paramFunctionRequesterId: identification of the function requester. paramFunctionCallId: identification of the function call. paramEID: EID of the targeted eUICC paramRspServerAddress: Address of the Server sending the RegisterEvent formatted as FQDN paramEventId: unique Identification of the Event to be registered paramForwardingIndicator: TRUE if registration has to be made to the Root SM-DS; FALSE if this is not to be made to the Root SM-DS
Details	JSON requestHeader

V1.4 Page 618 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

```
"header" : {
    "functionRequesterIdentifier" :
"paramFunctionRequesterId",
    "functionCallIdentifier" : "paramFunctionCallId"
    }

JSON body

{
    "eid" : paramEID,
    "rspServerAddress" : paramRspServerAddress,
    "eventId" : paramEventId,
    "forwardingIndicator" : paramForwardingIndicator
    }
}
```

Method	MTD_REMOVE_NOTIF
Description	Constructs the command data for RemoveNotificationFromList
Parameter(s)	paramSeqNumber: the sequence number to be removed
Details	request NotificationSentRequest ::= { seqNumber paramSeqNumber }

Method	MTD_RETRIEVE_NOTIF_SEQ_NUM
Description	Constructs the command data for RetrieveNotificationsList filtered by sequence number
Parameter(s)	paramSeqNumber: the sequence number to be retrieved
Details	request RetrieveNotificationsListRequest ::= { searchCriteria seqNumber paramSeqNumber }

Method	MTD_SELECT
Description	Generates the SELECT command as defined in GlobalPlatform Card Specification [6].
Parameter(s)	paramAID: the AID to select
Details	- CLA = 0x or 4x (x = <channel_number>) - INS = A4 - P1 = 04 - P2 = 00 - LC = <l> - paramAID - LE = 00</l></channel_number>

V1.4 Page 619 of 777

Method	MTD_SEND_SMS_PP
Description	Generate and send an envelope SMS-PP download to the MNO-SD
Parameter(s)	paramApdusList: the list of APDUs (plain) to send
Details	Generate and send the following envelope: 80 C2 00 00 <l> D1 CL> D1 CL> C2 02 83 81 Device identity Tag 06 07 91 33 86 09 40 00 F0 Address Tag (TON/NPI/) 08 <l> SMS TPDU 44 SMS-DELIVER 05 85 02 13 F2 TP-Originating-Address 7F TP-Protocol-Identifier F6 TP-Data-Coding-Scheme 71 30 12 41 55 74 40 TP-Service-Centre-Time-Stamp <l> TP-User-Data-Header-Length 02 User-Data-Header-Length 02 User-Data-Header-Length 10 IEIJA CL> Command Packet Length (2 bytes) <l> Command Header Length (1 byte) 12 21 SPI 00 KIC 15 KID (SCP80 Keyset version 0x01 in Triple DES) B2 01 00 MNO-SD TAR <mno_scp80_counter> 00 Padding Counter <cc> Cryptographic checksum <c_apdus_script> Command APDUs script <c_apdus_script> SHALL contain the paramApdusList (i.e. each APDU is named <apdu1>; <apdu2>;; <apdud> here after) formatted as an expanded structure with definite length as defined in ETSLTS 102 226 [14]: AA CL> 22 <l> <apdud> The Cryptographic checksum <cc> SHALL be generated in Triple DES (outer-CBC mode using two different keys) with the #MNO_SCP80_AUTH_KEY as defined in ETSLTS 102 225 [13]. If the command packet length is higher than 140 bytes, it SHALL be sent over several envelopes: SMS concatenation as defined in 3GPP TS 23.040 [22] SHALL be used.</cc></apdud></l></apdud></apdu2></apdu1></c_apdus_script></c_apdus_script></cc></mno_scp80_counter></l></l></l></l>

Method	MTD_STORE_DATA
Description	Generates the STORE DATA command (Case 4) as defined in GlobalPlatform Card Specification [6].

V1.4 Page 620 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

Parameter(s)	paramCommandData: the command data
Details	- CLA = 8x or Cx (x = <channel_number>) - INS = E2 - P1 = 91 - P2 = 00 - LC = <l> - paramCommandData - LE = 00</l></channel_number>

Method	MTD_STORE_DATA_Case3
Description	Generates the STORE DATA command (Case3) as defined in GlobalPlatform Card Specification [6].
Parameter(s)	paramCommandData: the command data
Details	- CLA = 8x or Cx (x = <channel_number>) - INS = E2 - P1 = 90 - P2 = 00 - LC = <l> - paramCommandData</l></channel_number>

Method	MTD_STORE_DATA_SCRIPT
Description	Generate (multiple) STORE DATA command(s) by breaking the data into smaller components (if needed) for transmission.
Parameter(s)	 paramTLVDataToTransmit: TLVs array or single TLV to transfer to the eUICC paramCase4Command (optional parameter, default value = TRUE): TRUE if the APDU is a Case 4 command, FALSE if the APDU is a Case 3 command
Details	For each element of paramTLVDataToTransmit If the size of the element is greater than 255 bytes, split the element in several blocks of 255 bytes. The last block MAY be shorter. Each block is named <data_sub_part> here after. If the element is up to 255 bytes, <data_sub_part> contains the value of the element. The bit b1 of P1 in the STORE DATA commands is named <b1_p1> here after and is defined as below: If paramCase4Command = TRUE Then</b1_p1></data_sub_part></data_sub_part>

V1.4 Page 621 of 777

```
If \mbox{\tt CDATA\_SUB\_PART}> is an intermediate part, generate the following STORE DATA:
         - CLA = 8x or Cx (x = <CHANNEL_NUMBER>)
         - INS = E2
         - P1 = 1x (x = <B1_P1>)
         - P2 = <STORE_DATA_BLOCK_NUM>
         - LC = \langle L \rangle
         - <DATA_SUB_PART>
         - LE = \overline{0}0 -- present only if paramCase4Command = TRUE
    If <DATA SUB PART> is the last part, generate the following STORE DATA:
         - CLA = 8x or Cx (x = <CHANNEL_NUMBER>)
- INS = E2
         - P1 = 9x (x = <B1 P1>)
         - P2 = <STORE DATA BLOCK NUM>
         - LC = <L>
         - <DATA_SUB_PART>
         - LE = \overline{00} -- present only if paramCase4Command = TRUE
    Increase the <STORE_DATA_BLOCK_NUM> by 1
  End
End
```

Method	MTD_TEST_ES8+_GET_BPP_PPK			
Description	Tests the received boundProfilePackage element according to #R_GET_BPP_RESP_OP1_PPK			
 paramResponse the response to GetBoundProfilePackage paramS_MAC the 128 bit SCP03t MACing Session key paramS_ENC the 128 bit SCP03t Encryption Session key paramPPK_MAC the 128 bit Profile Protection MACing Key paramPPK_ENC the 128 bit Profile Protection Encryption Key paramMetaData the ASN.1 StoreMetadataRequest element to a RSP profile 				
Details	Parse paramResponse into #R_GET_BPP_RESP_OP1_PPK and perform the following tests: Verify that each element in firstSequenceOf87, sequenceOf88, secondSequenceOf87 and sequenceOf86 has a total length (including tag and length fields) of 1020 or less Verify the integrity of each element in firstSequenceOf87, sequenceOf88 and secondSequenceOf87 using paramS_MAC Verify that <transaction_id_isc> in #INIT_SC_PROF1 matches <s_transaction_id> Verify the validity of smdpSign <sm_dp+_sign> in #INIT_SC_PROF1 using #PK_SM_DPpb_ECDSA Retrieve #CONF_ISDP_PROF1_SMDP from <conf_isdp_prof1_enc> using paramS_ENC and validate the content of #CONF_ISDP_PROF1_SMDP Construct the complete metadata element from the <smdp_metadata_seg_mac> segment(s) and verify that it matches paramMetaData Retrieve #REPLACE_S_KEYS_REQ from <replace_s_keys_req_enc> using paramS_ENC and validate the content of #REPLACE_S_KEYS_REQ_ENC> using paramS_ENC and validate the content of #REPLACE_S_KEYS_REQ</replace_s_keys_req_enc></smdp_metadata_seg_mac></conf_isdp_prof1_enc></sm_dp+_sign></s_transaction_id></transaction_id_isc>			

V1.4 Page 622 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

 Verify that the lengths of paramPPK_ENC and paramPPK_MAC in
#REPLACE_S_KEYS_REQ are each 16 bytes
 Verify the integrity of each <ppp_op_prof1_seg_ppk> element using paramPPK_MAC</ppp_op_prof1_seg_ppk>
 Retrieve the <upp_op_prof1_seg> segment(s) from the <ppp_op_prof1_seg_ppk> segment(s) using paramPPK_ENC, construct the complete Profile from the <upp_op_prof1_seg> segment(s), then verify that the complete Profile matches #UPP_OP_PROF1</upp_op_prof1_seg></ppp_op_prof1_seg_ppk></upp_op_prof1_seg>

Method	MTD_TEST_ES8+_GET_BPP_SK			
Description	ests the received boundProfilePackage element according to R_GET_BPP_RESP_OP1_SK			
Parameter(s)	 paramResponse the response to GetBoundProfilePackage paramS_MAC the 128 bit SCP03t MACing Session key paramS_ENC the 128 bit SCP03t Encryption Session key paramMetaData the ASN.1 StoreMetadataRequest element associated to a RSP profile 			
Details	Parse paramResponse into #R_GET_BPP_RESP_OP1_SK and perform the following tests: Verify that each element in firstSequenceOf87, sequenceOf88 and sequenceOf86 has a total length (including tag and length fields) of 1020 or less Verify the integrity of each element in firstSequenceOf87, sequenceOf88 and sequenceOf86 using paramSMAC Verify that <transaction_id_isc> in #INIT_SC_PROF1 matches <s_transaction_id> Verify the validity of smdpSign <sm_dp+_sign> in #INIT_SC_PROF1 using #PK_SM_DPpb_ECDSA Retrieve #CONF_ISDP_PROF1_SMDP from <conf_isdp_prof1_enc> using paramS_ENC and validate the content of #CONF_ISDP_PROF1_SMDP Construct the complete metadata element from the <smdp_metadata_seg_mac> segment(s) and verify that it matches paramMetaData Retrieve the <upp_op_prof1_seg> segment(s) from the <ppp_op_prof1_seg_sk> segment(s) using paramS_ENC, then construct the complete Profile from the <upp_op_prof1_seg> segment(s), then verify that the complete Profile matches #UPP_OP_PROF1</upp_op_prof1_seg></ppp_op_prof1_seg_sk></upp_op_prof1_seg></smdp_metadata_seg_mac></conf_isdp_prof1_enc></sm_dp+_sign></s_transaction_id></transaction_id_isc>			

Method	MTD_TLS_CLIENT_KEY_EXCH_ETC			
Description	Finalizes the Transport Layer Security (TLS) handshake in Server authentication mode on ES9+, or ES11 (Client side).			
Parameter(s)	paramClientKeyExchange: ClientKeyExchange message			
Details	Sends the session key information in TLS ClientKeyExchange message, ChangeCipherSpec and Finished message.			

V1.4 Page 623 of 777

Method	MTD_TLS_CLIENT_HELLO		
Description	Sends or checks the Client Hello message used to initiate the Transport Layer Security (TLS) handshake in Server authentication or Mutual authentication mode on ES9+, ES11, ES12 or ES15.		
Parameter(s)	 paramTLSversion: TLS protocol version paramAlgs: cipher suite types supported paramSessionID: Session ID paramExts: Extensions data for "supported_signature_algorithms", "trusted_ca_keys" or other (optional) 		
Details	Sends or receives a TLS ClientHello message according to the parameters defined above. In addition the following parameters will be set: The list of compression algorithms supported by the client is not explicitly defined, but by default it will be set to NULL. The random of 4 bytes representing time since epoch on client host and 28 random bytes is not explicitly defined but it SHALL be generated by the test tool TLS implementation		

NOTE: The Supported Elliptic Curves Extension and the Supported Point Formats Extension extensions MAY be sent by the Client.

Non-confidential

Method	MTD_TLS_MUTUAL_AUTH_CLIENT_EXCH			
Description	Sends or checks the messages to finalize the Transport Layer Security (TLS) handshake in Mutual authentication mode on ES12 or ES15 (Client side).			
paramClientCertificate: TLS Client certificate for authentication used in the Certificate Message paramClientKeyExchange: The Client TLS Ephemeral Key used in the ClientKeyExchange message				
	Sends the TLS Client Certificate, ClientKeyExchange, Certificate Verify, ChangeCipherSpec and Finished message in this order according to the parameters defined above.			
Details	NOTE: The CertificateVerify Message is not explicitly defined in this method but the CLIENT or test tool implementation SHALL be responsible for generating this message. It is the signature of the concatenation of all the data from all messages in this handshake up to, but not including, this message i.e. all handshake messages starting at ClientHello up to, but not including, this message itself using the specified Signature and Hash Algorithm.			
	NOTE: ChangeCipherSpec messages, alerts, and any other record type are not handshake messages and are not included in the signature computations.			

Method	MTD_TLS_MUTUAL_AUTH_SERVER_HELLO_ETC		
Description	Sends or checks the replies to the Client Hello in the Transport Layer Security (TLS) handshake in Mutual authentication mode on ES12 or ES15.		
Parameter(s)	 paramTLSVersion: TLS protocol version used in the Server Hello Message paramAlgs: cipher suite selected used in the Server Hello Message paramSessionID: Session ID used in the Server Hello Message paramServerCertificate: TLS Server certificate for authentication used in the Server Certificate Message 		

V1.4 Page 624 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

	 paramServerTLSEphemeralKey: TLS Server ephemeral key used in the Server Key Exchange Message paramClientCertificateType: type of certificate requested used in the Client Certificate Request Message paramSignatureAndHashAlgorithm: Signature and Hash Algorithm to be verified used in the Client Certificate Request Message paramDistinguishedName: DN of the CI that signed and issued the certificate used in the Client Certificate Request Message 		
Details	Sends or receives a TLS ServerHello, Server Certificate, ServerKeyExchange, Client Certificate Request and ServerHelloDone message in this order according to the parameters defined above. In addition the following parameter will be received: • ServerHello • The random of 4 bytes representing time since epoch on client host and 28 random bytes is not explicitly defined but it SHALL be generated by the Server under test. • ServerKeyExchange • The ECParameters are not explicitly defined in the ServerKeyExchange message but it SHALL be generated by the Server under test or the test tool implementation.		
	NOTE: The Supported Elliptic Curves Extension and the Supported Point Formats Extension extensions MAY be sent by the CLIENT therefore this method SHALL respond appropriately when used by the SERVER or the S_SERVER.		

Method	MTD_TLS_SERVER_END			
Description	Send or checks the finalization of the Transport Layer Security (TLS) handshake in Server or Mutual authentication mode on ES9+,ES11, ES12 or ES15 (Server side).			
Parameter(s)	paramChangeCipherSpec: ChangeCipherSpec messageparamFinish: Finished message			
Details	Sends a ChangeCipherSpec and Finished message in this order according to the parameters defined above.			

Method	MTD_TLS_SERVER_HELLO_ETC			
Description	Send or Receives to the Client Hello in the Transport Layer Security (TLS) handshake in Server authentication mode on ES9+, or ES11.			
 paramTLSversion: TLS protocol version paramAlgs: cipher suite selected paramSessionID: Session ID paramCertificate: TLS server certificate for authentication paramServerTLSEphemeralKey: TLS Server ephemeral key. 				
Details	Sends or Receives a TLS ServerHello, Server Certificate, ServerKeyExchange and ServerHelloDone message in this order according to the parameters defined above. Note1: The random of 4 bytes representing time since epoch on client host and 28 random bytes is not explicitly defined in the Server Hello message but it SHALL be generated by the Server under test. Note2: If no parameter mentioned paramServerTLSEphemeralKey, the value SHALL be set as defined in [24] for ServerKeyExchange. No verification required.			

V1.4 Page 625 of 777

C.2 Procedures

	Procedure	PROC_ES11_AUTH_CLIENT			
	Description	Authenticate Server procedure and E	vent Retrieval from SM-SD.		
For LPA	For LPAd testing, execute the following steps:				
Step	Direction	Sequence / Description	Expected result	REQ	
1	LPAd → S_SM-DS	Send ES11.AuthenticateClient method	MTD_HTTP_REQ(#TEST_R OOT_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIE NT(<s_transaction_id>, #R_AUTH_SERVER_DS_MA TCH_ID_DEV_INFO))</s_transaction_id>		
2	S_SM-DS → LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_DS_OK)	No error		

	Procedure	PROC_ES11_VERIFY_EVENT_RETRIEVAL			
	Description	Performs Common Mutual Authentication on ES11 from S_LPAd to SM-DS under test and verifies that the pending Event #EVENT_ENTRY_1 is retrieved.			
Step	Direction	Sequence / Description	Expected result	REQ	
1	$S_LPAd \to SM\text{-}DS$	PROC_TLS_INITIALIZATION_SERVER_AUTH			
2	$S_LPAd \to SM-DS$	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)		
3	$S_LPAd \to SM-DS$	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_MATCHI NG_ID_EVENT_ID))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_DS_EVE NT_ENTRY_1_OK)		

	Procedure	PROC_ES11_VERIFY_EVENT_RETRIEVAL_ERROR		
	Description	Performs Common Mutual Authentication on ES11 from S_LPAd to SM-DS under test and verifies that the pending Event #EVENT_ENTRY_1 is not available.		
Step	Direction	Sequence / Description	Expected result	REQ
1	$S_LPAd \to SM-DS$	PROC_TLS_INITIALIZATION_SERVER_AUTH		

V1.4 Page 626 of 777

2	$S_LPAd \to SM-DS$	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DS_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	$S_LPAd \to SM-DS$	MTD_HTTP_REQ(#IUT_SM_DS_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_ERROR_8_9_5_3_9)	

Procedure	PROC_ES11_INIT_AUTH
Description	Initiate Authentication procedure with SM-DS.

For LPAd testing, execute the following steps:

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DS	Send ES11.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_ROOT_DS_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICAT ION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_ROOT_DS_ADDRESS))</euicc_challenge>	
2	S_SM-DS → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_DS_OK)	No error	

	Procedure	PROC_EUICC_INITIALIZATION_SEQUENCE		
	Description	Initialize communication between the S_Device and the eUICC.		
Step	Direction	Sequence / Description	Expected result	REQ
1	$S_Device \to eUICC$	RESET	ATR present	
2	S_Device → eUICC	[SELECT_MF]	FCP Template present SW=0x9000	
3	$S_Device \to eUICC$	[TERMINAL_CAPABILITY_LPAd]	SW=0x9000	
4	S_Device → eUICC	[TERMINAL_PROFILE]	Toolkit initialization THEN SW=0x9000	

V1.4 Page 627 of 777

	Procedure	PROC_EUICC_INITIALIZATION_SEQUENCE_eUICCProfileSt ateChanged		
	Description	Initialize communication between the S_Device and the eUICC.		
Ste p	Direction	Sequence / Description	Expected result	REQ
1	$S_Device \to eUICC$	RESET	ATR returned by eUICC	
2	S_Device → eUICC	[SELECT_MF]	FCP Template present SW=0x9000	
3	S_Device → eUICC	[TERMINAL_CAPABILITY_LPAd]	SW=0x9000	
4	S_Device → eUICC	[TERMINAL_PROFILE_eUICCProfileStateChanged]	Toolkit initialization THEN SW=0x9000	

	Procedure	PROC_OPEN_LOGICAL_CHANNEL_AND_SELECT_ISDR		
	Description	The LPAd opens a logical channel and selects the ISD-R.		
Step	Direction	Sequence / Description Expected result RE		
1	$S_LPAd \to eUICC$	[MANAGE_CHANNEL_OPEN]	Extract the <channel_number> from response data SW=0x9000</channel_number>	
2	$S_LPAd \to eUICC$	MTD_SELECT(#ISD_R_AID)	SW=0x9000	

	Procedure	PROC_ES9+_AUTH_CLIENT	PROC_ES9+_AUTH_CLIENT		
	Description	Authenticate Server procedure without Confirmation Code. #R_AUTH_SERVER_MATCH_ID_DEV_INFO and #AUTH_SERVER_RESP_ACT_CODE_UC_OK are used with the correct MatchingID defined by the Add Profile initiation procedure (Activation Code content or Empty MatchingID)			
Step	Direction	Sequence / Description	Expected result	REQ	
For LP	For LPAd testing, execute the following steps:				
1	$LPAd \to S_{-}SM-DP+$	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIE NT(<s_transaction_id>, #R_AUTH_SERVER_MATCH _ID_DEV_INFO))</s_transaction_id>		
2	S_SM-DP+ \rightarrow LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_OK)	No error		
For SM	-DP+ testing, execute the	ne following steps:			

V1.4 Page 628 of 777

1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_CO DE_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUT H_CLIENT_OK)	
---	-----------------	--	--------------------------------------	--

	Procedure	PROC_ES9+_AUTH_CLIENT	_cc	
	Description	Authenticate Server procedure (via Activation Code) with Confirmation Code. #R_AUTH_SERVER_MATCH_ID_DEV_INFO and #AUTH_SERVER_RESP_ACT_CODE_UC_OK are used with the correct MatchingID defined by the Add Profile initiation procedure (Activation Code content or Empty MatchingID).		
Step	Direction	Sequence / Description	Expected result	REQ
For LP	Ad testing, execute the	following steps:		
1	LPAd → S_SM-DP+	Send ES9+.AuthenticateClient method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIE NT(<s_transaction_id>, #R_AUTH_SERVER_MATCH _ID_DEV_INFO))</s_transaction_id>	
2	S_SM-DP+ \rightarrow LPAd	MTD_HTTP_RESP (#AUTH_CLIENT_OK_CC)	No error	
For SM	-DP+ testing, execute the	he following steps:		
1	$S_LPAd \to SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_CO DE_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUT H_CLIENT_OK_CC)	

	Procedure	PROC_ES9+_GET_BPP		
	Description	Get BPP procedure without Confirmation Code.		
Step	Direction	Sequence / Description	Expected result	REQ
For LP	Ad testing, execute	e the following steps:		
1	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_trans action="" id="">.</s_trans>	

V1.4 Page 629 of 777

			#R_PREP_DOWNLOAD_NO _CC))	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_BPP_OK)	No error	
For SM	-DP+ testing, exe	cute the following steps:		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET _BPP_RESP_OP1_SK)	

	Procedure	PROC_ES9+_GET_BPP_CC	PROC_ES9+_GET_BPP_CC	
	Description Get BPP procedure with Confirmation Code.			
Step	Direction	Sequence / Description	Expected result	REQ
For LP	Ad testing, execute	e the following steps:		
1	LPAd → S_SM-DP+	Send ES9+.GetBoundProfilePackage method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_GET_BPP, MTD_GET_BPP(<s_transa ction_id="">, #R_PREP_DOWNLOAD_WIT H_CC))</s_transa>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#GET_BPP_OK)	No error	
For SM	I-DP+ testing, exe	cute the following steps:		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_ BPP_RESP_OP1_SK)	

	Procedure	PROC_ES9+_HANDLE_NOTIF		
	Description	Handle Notification procedure		
Step	Direction	Sequence / Description	Expected result	REQ
For LP	Ad testing, execute	e the following steps:		
1	LPAd → S_SM-DP+	Send ES9+.HandleNotification method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_HANDLE_NOTIF, MTD_HANDLE_NOTIF(#R_PI R_OK)) See Note2	

V1.4 Page 630 of 777

2	S_SM-DP+ → LPAd	#R_HTTP_204_OK	No error	
Note1:	Other Notification	s MAY be sent within the same HTTPS se	ession	
	Note2: The values of notificationAddress, iccid and smdpOid used in #R_PIR_OK MAY vary depending on the context (ICCID of the downloaded profile, used SM-DP+ address and certificate)			
For SM	For SM-DP+ testing: Not Used (FFS)			

	Procedure PROC_ES9+_AUTH_CLIENT_FAIL_DEF_DP_USE_CASE_VALID_MATCHING_ID		SE_IN	
	Description	AuthenticateClient fails due to an Inva	alid Matching ID.	
Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INITIALIZ	ZATION_SERVER_AUTH on ES9+		
2	$S_LPAd \to SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_ERROR_8_2_6_3_8)	

Procedure		PROC_ES9+_PROF_DOWNL NCEL_SESSION_SK	OAD_DEF_DP_USE_CAS	E_CA
	Description	End User cancels ongoing Profile Dov time ECKA key pair, session keys and Package.	9	
Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INITIALIZ	ZATION_SERVER_AUTH		
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

V1.4 Page 631 of 777

3	$S_LPAd \rightarrow SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_AUTH_CLIENT_OK)	
4	$S_LPAd \to SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_ SK)	
5	$S_LPAd \rightarrow SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS) Cancel Session request accepted by SM-DP+ and ongoing RSP session SHALL enter retry mode.	

	Procedure	PROC_ES9+_PROF_DOWNL NCEL_SESSION_PPK	OAD_DEF_DP_USE_CASI	E_CA
	Description	End User cancels ongoing Profile Doo time ECKA key pair, session keys, pro of the Bound Profile Package.		
Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INITIALIZ	ZATION_SERVER_AUTH		
2	$S_LPAd \to SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP _UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK)	
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_ PPK)	

V1.4 Page 632 of 777

		MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS,	MTD_HTTP_RESP(#R_SUCCESS)	
5	S_LPAd → SM-DP+	#PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(Cancel Session request	
		<s_transaction_id>,</s_transaction_id>	accepted by SM-DP+ and ongoing RSP session SHALL	
		#CS_RESP_OK_POSTPONED))	enter retry mode.	

	Procedure	PROC_ES9+_PROF_DOWNLOAD_DE NCEL_SESSION_PPK	F_DP_USE_CASE_CC_	_CA
	Description	End User cancels ongoing Profile Download afte ECKA key pair, session keys, profile protection k Profile Package when a Confirmation Code is recommended.	eys and the generation of the	
Step	Direction	Sequence / Description	Expected result	RE Q
1	PROC_TLS_IN	IITIALIZATION_SERVER_AUTH on ES9+		
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK_ CC)	
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP 1_PPK)	
5	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS) Cancel Session request accepted by SM-DP+ and ongoing RSP session SHALL enter retry mode.	

Procedure	PROC_ES9+_PROFILE_DOWNLOAD_DEF_SMDP_ADDRE SS_UC_NO_CC_EN
Description	Performs Common Mutual Authentication and then delivers the Bound Profile Package to the LPAd for enable metadata notifications.

V1.4 Page 633 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+		59+	
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_AUTH_CLIENT_OK_EN)	
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_P PK)	

	Procedure	PROC_ES9+_PROF_DOWNLO _CANCEL_SESSION	AD_ACT_CODE_USE_C	CASE
Description		End User cancels ongoing Profile Download after the generation of the one- time ECKA key pair, session keys and the generation of the Bound Profile Package.		
Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INITIALIZ	ZATION_SERVER_AUTH on ES9+		
2	$S_LPAd \to SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	$S_LPAd \to SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_ACT_COD E_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK)	
4	$S_LPAd \to SM-DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1 _PPK)	

V1.4 Page 634 of 777

		<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>		
5	$S_LPAd \to SM\text{-}DP+$	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS) Cancel Session request accepted by SM-DP+ and ongoing RSP session SHALL enter retry mode.	

Procedure	PROC_ES9+_PROF_DOWNLOAD_SM_DS_USE_CASE_CANCEL _SESSION
Description	End User cancels ongoing Profile Download after the generation of the one-time ECKA key pair, session keys and the generation of the bound profile package.

Step	Direction	Sequence / Description	Expected result	REQ	
1	PROC_ES9+_T	PROC_ES9+_TLS_INITIALIZATION_SERVER_AUTH			
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICA TION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUT H_OK)		
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIE NT(<s_transaction_id>, #AUTH_SERVER_RESP_SMD S_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK)		
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_PPK)		
5	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPON ED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS) Cancel Session request accepted by SM-DP+ and ongoing RSP session shall enter retry mode.		

Procedure	PROC ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_NO_CC
Description	Performs Common Mutual Authentication for the Profile Download Default SM_DP+ use case without a confirmation code.

V1.4 Page 635 of 777

Step	Direction	Sequence / Description	Expected result	REQ		
1	PROC_TLS_INIT	PROC_TLS_INITIALIZATION_SERVER_AUTH on ES9+				
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)			
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT,MTD_AUTH ENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_ UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK)			

	Procedure	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_CC		
	Description	Performs Common Mutual Authentication for the Profile Download Default SM_DP-use case with a confirmation code.		
Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_IN	ITIALIZATION_SERVER_AUTH on ES	S9+	
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_AUTH_CLIENT_OK_CC)	

	Procedure	PROC_ES9+_INIT_AUTH	
	Description	Initiate Authentication procedure.	
For LPAd testing, execute the following steps:			

V1.4 Page 636 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SM-DP+	Send ES9+.InitiateAuthentication method	MTD_HTTP_REQ(#TEST_DP_ADDRESS1, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICAT ION(<euicc_challenge>, #R_EUICC_INFO1, #TEST_DP_ADDRESS1))</euicc_challenge>	
2	S_SM-DP+ → LPAd	MTD_HTTP_RESP(#INITIATE_AUTH_OK)	No error	
For SM	-DP+ testing, exe	cute the following steps:		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	

Procedure	PROC_ES9+_VERIFY_CMA_PD_DEF_SMDP_ADDRESS_N O_CC_FAIL
Description	Verifies that Common Mutual Authentication for the Profile Download Default SM_DP+ use case without a confirmation code fails due to the profile being in the 'Installed' or 'Error' state.

Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH on ES9+		
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE _AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC _OK))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_1_1_3_8)	

V1.4 Page 637 of 777

	Procedure	PROC_VERIFY_SESSION_IS_CANCELLED			
	Description	Verify that the RSP session identified by the TransactionID <s_transaction_id> has been cancelled by the eUICC (i.e. Common Mutual Authentication and Profile Download procedures SHALL be rejected as long as no GetEUICCChallenge has been requested).</s_transaction_id>			
Step	Direction	Sequence / Description	Sequence / Description Expected result REQ		
1	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#PREP_DOWNLOAD_NO_CC)	#R_PREP_DOWN_NO_SESSION SW=0x9000 The transactionId returned in the response SHALL not be checked (any value SHALL be accepted)		
3	S_LPAd → eUICC	MTD_STORE_DATA_SCRIPT(#AUTHENTICATE_SMDP)	#R_AUTH_SERVER_NO_SESSION SW = 0x9000 The transactionId returned in the response SHALL not be checked (any value SHALL be accepted)		

	Procedure	PROC_ES9+_PROF_DOWNLOAD_DEF_DP_USE_CASE_CC_CA NCEL_SESSION_SK		
	Description	ption End User cancels ongoing Profile Download after the generation of the one-time ECKA key pair, session keys and the generation of the Bound Profile Package who a Confirmation Code is required.		
Step	Direction	Sequence / Description	Expected result RE Q	
1	PROC_TLS_IN	IITIALIZATION_SERVER_AUTH on ES9+		
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATION(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_DP_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK_ CC)	
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_CC))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP 1_SK)	

V1.4 Page 638 of 777

5	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_CANCEL_SESSION, MTD_CANCEL_SESSION(<s_transaction_id>, #CS_RESP_OK_POSTPONED))</s_transaction_id>	MTD_HTTP_RESP(#R_SUCCESS) Cancel Session request accepted by SM-DP+ and ongoing RSP session SHALL enter retry mode.	
---	--------------------	--	---	--

	Procedure	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_CC_RETRY		
	Description	Performs Common Mutual Authentication for the Profile Download Default SM_DP+ use case with a confirmation code.		
Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_IN	IITIALIZATION_SERVER_AUTH on E	S9 +	
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<\$_TRANSACTION_ID>, #AUTH_SERVER_RESP_DEF_D P_UC_OK))	MTD_HTTP_RESP(#R_AUTH_CLIENT_RETRY_ OK_CC)	

	Procedure	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_INVALID_CC			
	Description	Performs Common Mutual Authentication for the Profile Download Default SM_DP+ use case with an invalid confirmation code provided in the GetBoundProfilePackage.			
Step	Direction	Sequence / Description	Expected result	REQ	
IC1	PROC_ES9+_0	CMA_PD_DEF_SMDP_ADDRESS_UC	MA_PD_DEF_SMDP_ADDRESS_UC_CC		
1	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP_8_2 _7_3_8))</s_transaction_id>	MTD_HTTP_RESP(#R_ERROR_8_2_7_3_8)		

V1.4 Page 639 of 777

	Procedure	PROC_ES9+_CMA_PD_DEF_SMDP_ADDRESS_UC_NO_CC_RET RY		
	Description	Performs Common Mutual Authentic use case without a confirmation code	cation for the Profile Download Default SI e.	M_DP+
Step	Direction	Sequence / Description	Expected result	RE Q
1	PROC_TLS_IN	ITIALIZATION_SERVER_AUTH on E	S9+	
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATIO N(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_AUTH_CLIENT_RETRY_OK)	

	Procedure	PROC_TLS_INITIALIZATION_S	ERVER_AUTH	
	Description Establishes the Transport Layer Security (TLS) v1.2 connection between the Client (S_)LPAd and (S_)SERVER using Server authentication mode on ES9+ or ES11.			
For LP	Ad testing, execute	e the following steps:		
Step	Direction	Sequence / Description	Expected result	REQ
1	LPAd → S_SERVER	Send TLS Client Hello	MTD_TLS_CLIENT_HELLO(#IUT_TLS_VERSION, <tls_cipher_suites>, #SESSION_ID_0, <ext_sha256_ecdsa>)</ext_sha256_ecdsa></tls_cipher_suites>	
2	S_SERVER → LPAd	MTD_TLS_SERVER_HELLO_ETC(# TLS_VERSION_1_2, #S_TLS_CIPHER_SUITE, <session_id_random>, #CERT_S_SERVER_TLS)</session_id_random>	MTD_TLS_CLIENT_KEY_EXCH _ETC(<client_tls_ephem_ KEY>)</client_tls_ephem_ 	
3	S_SERVER → LPAd	Finalize TLS Handshake (send Server ChangeCipherSpec and Finished messages)	HTTPS connection established	
For Ser	ver (SM-DP+ or S	M-DS) testing, execute the following step	os:	

V1.4 Page 640 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	S_LPAd → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_SERVER_HELLO _ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite> , <session_id_random>, #CERT_SERVER_TLS)</session_id_random></sel_tls_cipher_suite>	>
2	S_LPAd → SERVER	MTD_TLS_CLIENT_KEY_EXCH_ETC(<client_tls_ephem_key>)</client_tls_ephem_key>	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC <server_finished>)</server_finished>	,

	Procedure	PROC_ES9+_PROFILE_DO'C_NO_CC	WNLOAD_DEF_SMDP_AD	DRESS_U
	Description	Performs Common Mutual Authentic Package to the LPAd.	cation and then delivers the Bound	d Profile
Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH on ES	S9+	
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(<s_transaction_id>, #AUTH_SERVER_RESP_DEF_D P_UC_OK))</s_transaction_id>	MTD_HTTP_RESP(#R_AUTH_CLIENT_OK)	
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_P PK)	

Procedure	PROC_ES9+_VERIFY_PROFILE_DOWNLOAD_DEF_SMDP_AD DRESS_UC
Description	Verifies that Common Mutual Authentication occurs successfully and that the Bound Profile Package is generated and successfully delivered to the LPAd.

V1.4 Page 641 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	PROC_TLS_INI	TIALIZATION_SERVER_AUTH on ES	59+	
2	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_INITIATE_AUTH, MTD_INITIATE_AUTHENTICATI ON(#S_EUICC_CHALLENGE, #S_EUICC_INFO1, #IUT_SM_DP_ADDRESS))	MTD_HTTP_RESP(#R_INITIATE_AUTH_OK)	
3	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_AUTH_CLIENT, MTD_AUTHENTICATE_CLIENT(MTD_HTTP_RESP(#R_AUTH_CLIENT_OK) OR MTD_HTTP_RESP(#R_AUTH_CLIENT_RETRY_ OK)	
4	S_LPAd → SM-DP+	MTD_HTTP_REQ(#IUT_SM_DP_ADDRESS, #PATH_GET_BPP, MTD_GET_BPP(<s_transaction_id>, #PREP_DOWNLOAD_RESP))</s_transaction_id>	MTD_HTTP_RESP(#R_GET_BPP_RESP_OP1_P PK)	

	Procedure	PROC_TLS_INITIALIZATION_MUTUAL_AUTH		
	Description	Establishes the Transport Layer Security (TLS) v1.2 connection between the Client and Server using Mutual authentication mode on ES12 or ES15. For Client and Server testing the Server MAY be the SM-DS or the SM-DP+.		
Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SE RVER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI)</sah_sha256_ecdsa></session_id_random></sel_tls_cipher_suite>	
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_CLIENT _EXCH(#CERT_CLIENT_TLS, <client_tls ephem="" key="">)</client_tls>	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	

Procedure	PROC_TLS_INITIALIZATION_MUTUAL_AUTH_INV_OID
Description	Establishes the Transport Layer Security (TLS) v1.2 connection between the Client and Server using Mutual authentication mode on ES12 or ES15 with a Client Certificate that has an invalid OID. For Client and Server testing the Server MAY be the SM-DS or the SM-DP+.

V1.4 Page 642 of 777

Step	Direction	Sequence / Description	Expected result	REQ
1	S_CLIENT → SERVER	MTD_TLS_CLIENT_HELLO(#TLS_VERSION_1_2, #MIN_TLS_CIPHER_SUITES, #S_SESSION_ID_EMPTY, #S_EXT_SHA256_ECDSA)	MTD_TLS_MUTUAL_AUTH_SE RVER_HELLO_ETC(#TLS_VERSION_1_2, <sel_tls_cipher_suite>, <session_id_random>, #CERT_SERVER_TLS, #CLIENT_CERT_TYPE, <sah_sha256_ecdsa>, #DIST_NAME_CI)</sah_sha256_ecdsa></session_id_random></sel_tls_cipher_suite>	
2	S_CLIENT → SERVER	MTD_TLS_MUTUAL_AUTH_CLIENT _EXCH(#CERT_S_CLIENT_TLS_INV_OID, <client_tls_ephem_key>)</client_tls_ephem_key>	MTD_TLS_SERVER_END(#CHANGE_CIPHER_SPEC, <server_finished>)</server_finished>	

Annex D Commands And Responses

D.1 ES8+ Requests And Responses

D.1.1 ES8+ Requests

Name	Content
CONF_ISDP_EMPTY	<pre>req ConfigureISDPRequest ::={}</pre>
CONF_ISDP_MAX_LENGTH	<pre>req ConfigureISDPRequest ::={ dpProprietaryData { size=128 bytes dpOid #S_SM_DP+_OID, additionalSmdpData #ADDITIONAL_SMDP_DATA_MAX_LENGTH } } NOTE: Instead of DpProprietaryData ::= SEQUENCE { dpOid OBJECT IDENTIFIER additional data objects defined by the SM-DP+ MAY follow } the following structure is used to test the DpProprietaryData size: DpProprietaryData ::= SEQUENCE { dpOid OBJECT IDENTIFIER, additionalSmdpData OCTET STRING OPTIONAL }</pre>

V1.4 Page 643 of 777

```
req ConfigureISDPRequest ::={
                                           dpProprietaryData {
                                             dpOid #S_SM_DP+_OID
CONF_ISDP_PROF1
                                         }
                                         req ConfigureISDPRequest ::={
                                          dpProprietaryData {
CONF_ISDP_PROF1_SMDP
                                            dpOid #IUT SM DP OID
                                          }-- optional
                                         req ConfigureISDPRequest ::={
                                           dpProprietaryData { -- size=129 bytes
                                            dpOid #S_SM_DP+_OID,
                                            additionalSmdpData
                                             #ADDITIONAL SMDP DATA EXCEEDED MAX
                                         }
                                         -- NOTE: Instead of
                                         DpProprietaryData ::= SEQUENCE {
                                          dpOid OBJECT IDENTIFIER
                                          -- additional data objects defined by
CONF_ISDP_SIZE_EXCEEDED
                                         the
                                          -- SM-DP+ MAY follow
                                         -- the following structure is used to
                                         test the
                                         -- DpProprietaryData size:
                                         DpProprietaryData ::= SEQUENCE {
                                          dpOid OBJECT IDENTIFIER,
                                          additionalSmdpData OCTET STRING
                                         OPTIONAL
```

V1.4 Page 644 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           iconType png,
                                           icon #ICON OP PROF1,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                 notificationInstall,
                                                 notificationEnable,
FULL_METADATA
                                                 notificationDisable,
                                                 notificationDelete
                                             },
                                             notificationAddress
                                          #TEST DP ADDRESS1
                                            }
                                           },
                                           profileOwner {
                                             mccMnc #MCC_MNC1
                                           profilePolicyRules {ppr1}
                                         req InitialiseSecureChannelRequest ::={
                                           remoteOpId #REMOTE OP ID INSTALL,
                                           transactionId <S TRANSACTION ID>,
                                           controlRefTemplate {
                                             keyType #INVALID KEY TYPE,
                                             keyLen #KEY_LENGTH,
INIT_SC_INVALID_CRT
                                             hostId #HOST ID
                                           smdpOtpk <OTPK_S_SM_DP+_ECKA>,
                                           smdpSign <S SM DP+ SIGN>
                                         req InitialiseSecureChannelRequest ::={
                                           remoteOpId #INVALID REMOTE OP ID,
                                           transactionId <S TRANSACTION ID>,
                                           controlRefTemplate {
                                             keyType #KEY TYPE,
INIT_SC_INVALID_OP_ID
                                             keyLen #KEY LENGTH,
                                             hostId #HOST ID
                                           },
                                           smdpOtpk <OTPK S SM DP+ ECKA>,
                                           smdpSign <S SM DP+ SIGN>
```

V1.4 Page 645 of 777

```
req InitialiseSecureChannelRequest ::={
                                           remoteOpId #REMOTE OP ID INSTALL,
                                           transactionId <S TRANSACTION ID>,
                                           controlRefTemplate {
                                             keyType #KEY_TYPE,
                                             keyLen #KEY LENGTH,
                                            hostId #HOST ID
INIT_SC_INVALID_SIGN
                                           },
                                           smdpOtpk <OTPK_S_SM_DP+_ECKA>,
                                           smdpSign <S_SM_DP+_SIGN>
                                         The <S SM DP+ SIGN> SHALL NOT be
                                         computed using the #SK_S_SM_DPpb_ECDSA
                                         but SHALL have the same length as for a
                                         valid signature
                                         req InitialiseSecureChannelRequest ::={
                                           remoteOpId #REMOTE OP ID INSTALL,
                                           transactionId
                                         <INVALID TRANSACTION ID>,
                                           controlRefTemplate {
                                             keyType #KEY TYPE,
INIT_SC_INVALID_TRANS_ID
                                             keyLen #KEY LENGTH,
                                             hostId #HOST_ID
                                           },
                                           smdpOtpk <OTPK S SM DP+ ECKA>,
                                           smdpSign <S SM DP+ SIGN>
                                         req InitialiseSecureChannelRequest ::={
                                           remoteOpId #REMOTE_OP_ID_INSTALL,
                                           transactionId <TRANSACTION ID ISC>,
                                           controlRefTemplate {
                                            keyType #KEY TYPE,
INIT_SC_PROF1
                                            keyLen #KEY LENGTH,
                                             hostId #IUT_SM_DP_HOST_ID
                                           },
                                           smdpOtpk <OTPK SM DP+ ECKA>,
                                           smdpSign <SM DP+ SIGN>
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF2,
METADATA_ICCID_MISMATCH
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
METADATA_MCCMNC_MISMATCH
                                           profileOwner {
                                             mccMnc #MCC MNC2
                                           profilePolicyRules {ppr2}
```

V1.4 Page 646 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                 notificationInstall,
                                                 notificationEnable,
METADATA_NO_CLASS
                                                notificationDisable,
                                                notificationDelete
                                               notificationAddress
                                         #TEST DP ADDRESS1
                                            }
                                           }
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID_OP_PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           iconType png,
                                           icon #ICON_OP_PROF1,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                 notificationInstall,
                                                notificationEnable,
METADATA_OP_PROF1
                                                notificationDisable,
                                                notificationDelete
                                               notificationAddress
                                         #TEST_DP_ADDRESS1
                                             }
                                           },
                                           profileOwner {
                                            mccMnc #MCC MNC1
                                         }
```

V1.4 Page 647 of 777

```
metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF1,
                                          serviceProviderName #SP NAME1,
                                          profileName #NAME OP PROF1,
                                          iconType png,
                                          icon #ICON OP PROF1,
                                          profileClass operational,
                                          notificationConfigurationInfo {
                                             { profileManagementOperation {
METADATA_OP_PROF1_EN
                                                notificationEnable
                                              notificationAddress
                                         #TEST DP ADDRESS1
                                            }
                                           },
                                          profileOwner {
                                            mccMnc #MCC MNC1
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID_OP_PROF1,
                                          serviceProviderName #SP NAME1,
                                          profileName #NAME_OP_PROF1,
                                          iconType png,
                                          icon #ICON OP PROF1,
                                          profileClass operational,
                                          notificationConfigurationInfo {
                                            { profileManagementOperation {
                                                notificationInstall
METADATA_OP_PROF1_INST_DIFF
                                              notificationAddress
                                         #TEST_DP_ADDRESS2
                                            }
                                           },
                                          profileOwner {
                                            mccMnc #MCC MNC1
                                         }
```

V1.4 Page 648 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           iconType png,
                                           icon #ICON OP PROF1,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                notificationDelete
METADATA_OP_PROF1_MEMRES1
                                               notificationAddress
                                         #TEST DP ADDRESS1
                                            }
                                           },
                                           profileOwner {
                                            mccMnc #MCC MNC1
                                           profilePolicyRules { ppr2 }
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID_OP_PROF5,
                                          serviceProviderName #SP_NAME1,
                                           profileName #NAME OP PROF5,
                                          iconType png,
                                           icon #ICON OP PROF5,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                notificationDisable,
METADATA_OP_PROF5_MEMRES2
                                                notificationDelete
                                              },
                                              notificationAddress
                                         #TEST_DP_ADDRESS1
                                            }
                                           },
                                           profileOwner {
                                            mccMnc #MCC MNC1
                                           profilePolicyRules { ppr1,ppr2 }
```

V1.4 Page 649 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF2,
                                           serviceProviderName #SP NAME2,
                                           profileName #NAME OP PROF2,
                                           iconType png,
                                           icon #ICON OP PROF2,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                notificationInstall,
                                                 notificationEnable,
METADATA_OP_PROF2
                                                 notificationDisable,
                                                notificationDelete
                                               },
                                               notificationAddress
                                         #TEST DP ADDRESS2
                                            }
                                           },
                                           profileOwner {
                                             mccMnc #MCC_MNC2
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF2,
                                           serviceProviderName #SP NAME2,
                                           profileName #NAME OP PROF2,
                                          iconType png,
                                           icon #ICON OP PROF2,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                               profileManagementOperation {
                                                notificationEnable,
METADATA_OP_PROF2_NO_INSTALL
                                                notificationDisable,
                                                notificationDelete
                                               notificationAddress
                                         #TEST DP ADDRESS2
                                            }
                                           } ,
                                           profileOwner {
                                             mccMnc #MCC MNC2
```

V1.4 Page 650 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           iconType png,
                                           icon #ICON OP PROF1,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                               profileManagementOperation {
                                                 notificationEnable,
METADATA_OP_PROF1_NO_INSTALL
                                                 notificationDisable,
                                                 notificationDelete
                                               },
                                               notificationAddress
                                         #TEST DP ADDRESS1
                                            }
                                           },
                                           profileOwner {
                                             mccMnc #MCC MNC1
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF2,
                                           serviceProviderName #SP NAME2,
                                           profileName #NAME OP PROF2,
                                           iconType png,
                                           icon #ICON OP PROF2,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                 notificationInstall,
                                                 notificationEnable,
METADATA_OP_PROF2_TEST_DP_ADDRESS1
                                                 notificationDisable,
                                                 notificationDelete
                                               notificationAddress
                                         #TEST DP ADDRESS1
                                           },
                                           profileOwner {
                                             mccMnc #MCC MNC2
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF3,
                                           serviceProviderName #SP NAME3,
                                           profileName #NAME OP PROF3,
                                           iconType png,
                                           icon #ICON OP PROF3,
METADATA_OP_PROF3
                                           profileClass operational,
                                           profileOwner {
                                             mccMnc #MCC MNC2
                                           profilePolicyRules { ppr2 }
```

V1.4 Page 651 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF4,
                                           serviceProviderName #SP NAME4,
                                           profileName #NAME OP PROF4,
                                           iconType png,
                                           icon #ICON OP PROF4,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                              { profileManagementOperation {
                                                 notificationInstall,
                                                notificationEnable,
                                                notificationDisable,
METADATA_OP_PROF4
                                                notificationDelete
                                               },
                                               notificationAddress
                                         #TEST DP_ADDRESS4
                                             }
                                             },
                                           profileOwner {
                                             mccMnc #MCC_MNC4
                                           profilePolicyRules {
                                           ppr1
                                         }
                                         metadataReg StoreMetadataReguest ::= {
                                          iccid #ICCID OP PROF5,
                                          serviceProviderName #SP NAME1,
                                           profileName #NAME_OP_PROF5,
                                           iconType png,
                                           icon #ICON OP PROF5,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                notificationInstall,
                                                notificationEnable,
METADATA_OP_PROF5
                                                notificationDisable,
                                                notificationDelete
                                               notificationAddress
                                         #TEST_DP_ADDRESS1
                                            }
                                           },
                                           profileOwner {
                                            mccMnc #MCC MNC1
                                         }
```

V1.4 Page 652 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF6,
                                           serviceProviderName #SP NAME2,
                                           profileName #NAME OP PROF6,
                                           iconType png,
                                           icon #ICON OP PROF6,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                notificationInstall,
                                                notificationEnable,
METADATA_OP_PROF6
                                                notificationDisable,
                                                notificationDelete
                                               },
                                              notificationAddress
                                         #TEST DP_ADDRESS2
                                            }
                                           },
                                           profileOwner {
                                             mccMnc #MCC_MNC2
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF7,
                                           serviceProviderName #SP NAME2,
                                           profileName #NAME OP PROF7,
                                          iconType png,
                                          icon #ICON OP PROF7,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                 notificationInstall,
                                                 notificationEnable,
                                                notificationDisable,
                                                notificationDelete
METADATA_OP_PROF7
                                              notificationAddress
                                         #TEST DP ADDRESS8
                                            }
                                           profileOwner {
                                            mccMnc #MCC MNC8
                                           profilePolicyRules {
                                            ppr2
                                           }
                                         }
```

V1.4 Page 653 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF8,
                                           serviceProviderName #SP NAME8,
                                           profileName #NAME OP PROF8,
                                           iconType png,
                                           icon #ICON OP PROF8,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                            { profileManagementOperation {
                                                notificationInstall,
                                                 notificationEnable,
                                                 notificationDisable,
METADATA_OP_PROF8
                                                notificationDelete
                                               },
                                               notificationAddress
                                         #TEST DP ADDRESS8
                                             }
                                             },
                                           profileOwner {
                                             mccMnc #MCC_MNC8
                                           profilePolicyRules {
                                            ppr2
                                         }
                                         metadataReg StoreMetadataReguest ::= {
                                          iccid #ICCID OP PROF9,
                                           serviceProviderName #SP NAME9,
                                           profileName #NAME OP PROF9,
                                           profileOwner {
                                            mccMnc #MCC MNC9,
METADATA_OP_PROF9
                                            gid1 #GID1,
                                             gid2 #GID2
                                           },
                                           profilePolicyRules {
                                             ppr2
                                           }
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           profileOwner {
METADATA_OP1_GID1GID2_PRESENT
                                            mccMnc #MCC MNC1,
                                            gid1 #GID1,
                                            gid2 #GID2
                                           profilePolicyRules {ppr2}
```

V1.4 Page 654 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF9,
                                           serviceProviderName #SP NAME9,
                                           profileName #NAME OP PROF9,
METADATA_OP9_GID1GID2_MISSING
                                           profileOwner {
                                            mccMnc #MCC MNC9
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
METADATA_PPR_NO_OWNER
                                          profileName #NAME OP PROF1,
                                           profilePolicyRules {ppr2}
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME_OP_PROF1,
                                           profileOwner {
METADATA_WILDCARD
                                            mccMnc #MCC_MNC_WILDCARD
                                           profilePolicyRules {ppr2}
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
METADATA_WITH_JPG
                                           iconType jpg,
                                           icon #ICON JPG
```

V1.4 Page 655 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           notificationConfigurationInfo {
                                             { profileManagementOperation {
                                                 notificationInstall
                                               notificationAddress
                                         #TEST_DP_ADDRESS3
                                             { profileManagementOperation {
                                                notificationInstall
                                              notificationAddress
                                         #TEST DP ADDRESS2
                                             },
                                             { profileManagementOperation {
                                                notificationEnable
                                               notificationAddress
                                         #TEST_DP_ADDRESS2
                                             },
                                             { profileManagementOperation {
                                                notificationEnable
                                               notificationAddress
METADATA WITH NOTIFS
                                         #TEST DP ADDRESS3
                                             },
                                             { profileManagementOperation {
                                                notificationDisable
                                               notificationAddress
                                         #TEST DP ADDRESS3
                                             },
                                             { profileManagementOperation {
                                                 notificationDisable
                                               notificationAddress
                                         #TEST DP ADDRESS4
                                             },
                                             { profileManagementOperation {
                                                  notificationDelete
                                               notificationAddress
                                         #TEST DP ADDRESS1
                                             },
                                             { profileManagementOperation {
                                                  notificationDelete
                                              notificationAddress
                                         #TEST_DP_ADDRESS3
                                             }
                                           }
                                         }
```

V1.4 Page 656 of 777

```
metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           profileOwner {
METADATA_WITH_PPR1_PPR2
                                            mccMnc #MCC MNC1
                                           },
                                           profilePolicyRules {ppr1,ppr2}
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                          profileName #NAME OP PROF1,
METADATA_WITH_PPR2
                                           profileOwner {
                                            mccMnc #MCC MNC1
                                           profilePolicyRules {ppr2}
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF1,
                                           serviceProviderName #SP_NAME1,
                                           profileName #NAME OP PROF1,
                                          iconType png,
                                          icon #ICON OP PROF1,
METADATA_WITH_PPRS_AND_ICON
                                           profileOwner {
                                            mccMnc #MCC MNC1
                                           profilePolicyRules {ppr1,ppr2}
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF1,
                                          serviceProviderName #SP NAME1,
METADATA_WITHOUT_ICON
                                          profileName #NAME OP PROF1,
                                           iconType jpg
                                         req ReplaceSessionKeysRequest ::={
                                          initialMacChainingValue
                                         <PPK INIT MAC>,
REPLACE_S_KEYS_REQ
                                          ppkEnc <PPK ENC>,
                                           ppkCmac <PPK_MAC>
                                         req ReplaceSessionKeysRequest ::={
                                           initialMacChainingValue
                                         #PPK INIT MAC INV SIZE,
REPLACE_S_KEYS_REQ_INV_SIZE
                                          ppkEnc #PPK ENC INV SIZE,
                                           ppkCmac #PPK MAC INV SIZE
```

V1.4 Page 657 of 777

```
req InitialiseSecureChannelRequest ::={
                                           remoteOpId #REMOTE OP ID INSTALL,
                                           transactionId <S TRANSACTION ID>,
                                           controlRefTemplate {
                                             keyType #KEY TYPE,
S_INIT_SC_PROF1
                                             keyLen #KEY LENGTH,
                                            hostId #HOST ID
                                           },
                                           smdpOtpk <OTPK_S_SM_DP+_ECKA>,
                                           smdpSign <S SM DP+ SIGN>
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
SMDP_METADATA_ABS
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           iconType png,
                                           icon #ICON OP PROF1,
                                           profileClass operational,
                                           notificationConfigurationInfo {
                                               profileManagementOperation {
                                                  notificationInstall,
                                                  notificationEnable,
SMDP_METADATA_ALL
                                                  notificationDisable,
                                                  notificationDelete
                                               },
                                               notificationAddress
                                         #IUT SM DP ADDRESS
                                             }
                                           },
                                           profileOwner {
                                                 mccMnc #MCC MNC1
                                           profilePolicyRules { ppr1, ppr2 }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName
SMDP_METADATA_NON_ASCII
                                         #SP NAME NON ASCII,
                                           profileName #NAME_OP_PROF1_NON_ASCII
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
SMDP_METADATA_NOTIF_MULTI
                                           notificationConfigurationInfo {
                                               profileManagementOperation {
                                                  notificationInstall,
```

V1.4 Page 658 of 777

```
notificationEnable,
                                                  notificationDisable,
                                                  notificationDelete
                                               notificationAddress
                                         #IUT SM DP ADDRESS
                                            },
                                               profileManagementOperation {
                                                  notificationInstall,
                                                  notificationEnable,
                                                  notificationDisable,
                                                  notificationDelete
                                               },
                                               notificationAddress
                                         #TEST_DP_ADDRESS1
                                             }
                                           }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                         profileClass operational,
                                          notificationConfigurationInfo {
                                             { profileManagementOperation {
SMDP_METADATA_OP_PROF1_EN
                                                 notificationEnable
                                               notificationAddress
                                         #IUT SM DP ADDRESS
                                           }
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
                                           profileName #NAME OP PROF1,
                                           profileClass operational,
SMDP_METADATA_OP_PROF1_PPR2
                                           profileOwner {
                                                  mccMnc #MCC MNC1
                                           },
                                           profilePolicyRules { ppr2 }
                                         }
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
SMDP_METADATA_PN_LONG
                                           profileName #NAME OP PROF LONG
                                         metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME LONG,
SMDP_METADATA_SPN_LONG
                                           profileName #NAME OP PROF1
```

V1.4 Page 659 of 777

D.2 ES9+ Requests And Responses

D.2.1 ES9+ Requests

```
Name
                                       Content
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
                                               <SMDP CHALLENGE>,
AUTH SERVER RESP ACT CODE UC OK
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX PARAMS1 ACT CODE
                                           },
                                           euiccSignature1
                                           <EUICC SIGNATURE1>,
                                           euiccCertificate
                                           #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       }
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION_ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
                                               <SMDP CHALLENGE>,
AUTH SERVER RESP_ACT_CODE 2 UC_O
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX_PARAMS1_ACT_CODE_2
                                           },
                                           euiccSignature1
                                           <EUICC_SIGNATURE1>,
                                           euiccCertificate
                                           #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
AUTH_SERVER_RESP_DEF_DP_UC_8_1_1_
                                               serverAddress
3_8
                                               #IUT_SM_DP_ADDRESS,
                                               serverChallenge
                                               <SMDP_CHALLENGE>,
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
```

V1.4 Page 660 of 777

Non-confidential

```
euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate
                                           #CERT EUICC ECDSA EID2,
                                           eumCertificate #CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT_SM_DP_ADDRESS,
                                               serverChallenge
                                               <SMDP CHALLENGE>,
AUTH_SERVER_RESP_DEF_DP_UC_8_1_4_
                                               euiccInfo2
                                               #S_EUICC_INFO2_INSUF_MEM_ERROR,
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
                                               <SMDP CHALLENGE>,
AUTH_SERVER_RESP_DEF_DP_UC_8_1_2_
6_1_EX_BC_cA
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX_PARAMS1_MATCHING_ID_EMPTY
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate
                                           #CERT_EUM_ECDSA_INVALID_EX_BC_cA
                                       }
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
AUTH_SERVER_RESP_DEF_DP_UC_8_1_2_
                                               #IUT SM DP ADDRESS,
6_1_EX_BC_PLC
                                               serverChallenge
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
```

V1.4 Page 661 of 777

```
euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate
                                           #CERT_EUM_ECDSA_INVALID_EX_BC_PLC
                                       }
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_2_
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S EUICC INFO2,
6_1_EX_CP
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate
                                           #CERT EUM ECDSA INVALID EX CP
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH SERVER RESP_DEF_DP_UC_8_1_2_
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S EUICC INFO2,
6_1_EX_KU
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate
                                           #CERT EUM ECDSA INVALID EX KU
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
AUTH_SERVER_RESP_DEF_DP_UC_8_1_2_
                                               serverChallenge
6_1_SIG
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S_EUICC_INFO2,
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT_EUICC_ECDSA,
                                           eumCertificate
```

V1.4 Page 662 of 777

```
#CERT EUM ECDSA INVALID SIG
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION_ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_2_
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S_EUICC_INFO2,
6_3
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate
                                           #CERT EUM ECDSA EXPIRED
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT_SM_DP_ADDRESS,
                                               serverChallenge
                                               <SMDP CHALLENGE>,
AUTH_SERVER_RESP_DEF_DP_UC_8_1_3_
                                               euiccInfo2 #S EUICC INFO2,
6_1_EX_CP
                                               ctxParams1
                                               #CTX_PARAMS1_MATCHING_ID_EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate
                                           #CERT_EUICC_ECDSA_INVALID_EX_CP,
                                           eumCertificate
                                           #CERT_EUM_ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_3_
                                               <SMDP CHALLENGE>,
6_1_EX_KU
                                               euiccInfo2 #S_EUICC_INFO2,
                                               ctxParams1
                                               #CTX PARAMS1_MATCHING_ID_EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate
                                           #CERT EUICC ECDSA INVALID EX KU,
                                           eumCertificate
```

V1.4 Page 663 of 777

```
#CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION_ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_3_
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S_EUICC_INFO2,
6_1_SIG
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate
                                           #CERT EUICC ECDSA INVALID SIG,
                                           eumCertificate #CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT_SM_DP_ADDRESS,
                                               serverChallenge
                                               <SMDP CHALLENGE>,
AUTH_SERVER_RESP_DEF_DP_UC_8_1_3_
                                               euiccInfo2 #S EUICC INFO2,
6_1_SUB_ORG
                                               ctxParams1
                                               #CTX_PARAMS1_MATCHING_ID_EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate
                                           #CERT_EUICC_ECDSA_INVALID_SUB_ORG,
                                           eumCertificate
                                           #CERT_EUM_ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_3_
                                               <SMDP CHALLENGE>,
6_1_SUB_SN
                                               euiccInfo2 #S_EUICC_INFO2,
                                               ctxParams1
                                               #CTX PARAMS1_MATCHING_ID_EMPTY
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate
                                           #CERT EUICC ECDSA INVALID SUB SN,
                                           eumCertificate
```

V1.4 Page 664 of 777

```
#CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION_ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_3_
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S_EUICC_INFO2,
6_3
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate
                                       #CERT EUICC ECDSA EXPIRED,
                                           eumCertificate #CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT_SM_DP_ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_6_
                                               <SMDP CHALLENGE INVALID>,
1_CHA
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX_PARAMS1_MATCHING_ID_EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT_EUM_ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT_SM_DP_ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_1_6_
                                               <SMDP CHALLENGE>,
1_SIG
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX_PARAMS1_MATCHING_ID_EMPTY
                                           },
                                           euiccSignature1
                                           <EUICC SIGNATURE1 INVALID>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
```

V1.4 Page 665 of 777

```
resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_2_5_
                                               <SMDP CHALLENGE>,
4_3
                                               euiccInfo2 #S_EUICC_INFO2_PPR2,
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           },
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <INVALID TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_10_1
                                               <SMDP CHALLENGE>,
_3_9
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       resp AuthenticateServerResponse ::=
                                       authenticateResponseOk : {
                                           euiccSigned1 {
                                               transactionId
                                               <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_DEF_DP_UC_8_11_1
                                               <SMDP CHALLENGE>,
3 9
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1
                                               #CTX_PARAMS1_MATCHING_ID_EMPTY
                                           euiccSignature1 <EUICC SIGNATURE1>,
                                           euiccCertificate #CERT_EUICC_ECDSA,
                                           eumCertificate
                                           #CERT EUM ECDSA UNKNOWN
```

V1.4 Page 666 of 777

```
resp AuthenticateServerResponse ::=
                                      authenticateResponseOk : {
                                          euiccSigned1 {
                                              transactionId
                                              <S TRANSACTION ID>,
                                               serverAddress
                                               #IUT SM DP ADDRESS,
                                              serverChallenge
                                              <SMDP CHALLENGE>,
AUTH_SERVER_RESP_DEF_DP_UC_OK
                                               euiccInfo2 #S EUICC INFO2
                                               ctxParams1
                                               #CTX PARAMS1 MATCHING ID EMPTY
                                          },
                                          euiccSignature1 <EUICC SIGNATURE1>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT EUM ECDSA
                                      resp AuthenticateServerResponse ::=
                                      authenticateResponseOk : {
                                          euiccSigned1 {
                                              transactionId
                                              <S TRANSACTION_ID>,
                                              serverAddress
                                              #IUT SM DP ADDRESS,
                                               serverChallenge
AUTH_SERVER_RESP_SMDS_UC_OK
                                               <SMDP CHALLENGE>,
                                               euiccInfo2 #S EUICC INFO2,
                                               ctxParams1 #CTX PARAMS1 SMDS
                                          euiccSignature1 <EUICC SIGNATURE1>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT EUM ECDSA
                                      }
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId <S TRANSACTION ID>,
                                          smdpOid #IUT SM DP OID,
CS_RESP_ERROR_8_1_6_1
                                          reason postponed
                                        },
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE INVALID>
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId <S TRANSACTION ID>,
                                          smdpOid <INVALID SM DP OID>,
CS_RESP_ERROR_8_8_3_10
                                          reason postponed
                                        },
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE>
```

V1.4 Page 667 of 777

```
resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId
                                      <INVALID TRANSACTION ID>,
CS_RESP_ERROR_8_10_1_3_9
                                          smdpOid #IUT SM DP OID,
                                          reason postponed
                                        },
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE>
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId <S TRANSACTION ID>,
                                          smdpOid #IUT SM DP OID,
CS_RESP_OK_EU_REJ
                                          reason endUserRejection
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE>
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId <S TRANSACTION ID>,
                                          smdpOid #IUT SM DP OID,
CS_RESP_OK_L_BPP_EXE_ERROR
                                          reason loadBppExecutionError
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE>
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId <S TRANSACTION ID>,
                                          smdpOid #IUT SM DP OID,
CS_RESP_OK_M_DATA_MISMATCH
                                          reason metadataMismatch
                                        },
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE>
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId <S TRANSACTION ID>,
                                          smdpOid #IUT SM DP OID,
CS_RESP_OK_POSTPONED
                                          reason postponed
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE>
                                      resp CancelSessionResponse ::=
CS_RESP_OK_PPR_NOT_ALLOWED
                                      cancelSessionResponseOk : {
```

V1.4 Page 668 of 777

```
euiccCancelSessionSigned {
                                          transactionId <S TRANSACTION ID>,
                                          smdpOid #IUT_SM_DP_OID,
                                          reason pprNotAllowed
                                        },
                                        euiccCancelSessionSignature
                                        <EUICC CANCEL SESSION SIGNATURE>
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                          transactionId <S_TRANSACTION_ID>,
                                          smdpOid #IUT SM DP OID,
CS_RESP_OK_TIMEOUT
                                         reason timeout
                                        },
                                        euiccCancelSessionSignature
                                        <EUICC_CANCEL_SESSION_SIGNATURE>
                                      resp CancelSessionResponse ::=
                                      cancelSessionResponseOk : {
                                        euiccCancelSessionSigned {
                                         transactionId <S TRANSACTION ID>,
                                         smdpOid #IUT SM DP OID,
CS_RESP_OK_UNDEFINED
                                         reason undefinedReason
                                        },
                                        euiccCancelSessionSignature
                                        <EUICC_CANCEL_SESSION_SIGNATURE>
                                      ctx CtxParams1 ::=
                                      ctxParamsForCommonAuthentication : {
                                          matchingId #MATCHING ID 1,
CTX_PARAMS1_ACT_CODE
                                          deviceInfo #S DEVICE INFO
                                      ctx CtxParams1 ::=
                                      ctxParamsForCommonAuthentication : {
CTX_PARAMS1_ACT_CODE_2
                                         matchingId #MATCHING ID 2,
                                          deviceInfo #S_DEVICE_INFO
                                      ctx CtxParams1 ::=
                                      ctxParamsForCommonAuthentication : {
                                          matchingId #MATCHING ID EMPTY,
CTX_PARAMS1_MATCHING_ID_EMPTY
                                          deviceInfo #S_DEVICE_INFO
                                      }
                                      ctx CtxParams1 ::=
                                      ctxParamsForCommonAuthentication : {
                                        matchingId <MATCHING ID EVENT>,
CTX_PARAMS1_SMDS
                                        deviceInfo #S DEVICE INFO
                                      0x01 00 00
EUICC_FIRMWARE_VER
```

V1.4 Page 669 of 777

```
The Extended Card Resource Information
                                       according to ETSI TS 102 226 and set as:
                                       0x81 <L> #INSTALLED PROFILES
EXT_CARD_RESOURCE_LIMITED_SPACE
                                       0x82 <L> #NON VOLATILE MEM LIMITED SPACE
                                       0x83 <L> #S VOLATILE MEM
                                         "header" : {
                                            "functionExecutionStatus" : {
                                              "status" : "Executed-Success"
                                         },
                                         "transactionId" : <S TRANSACTION ID>,
                                         "serverSigned1" : <S SMDS SIGNED1>,
INITIATE_AUTH_DS_OK
                                         "serverSignature1":
                                        <S SMDS SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" :
                                         <EUICC CI PK ID TO BE USED>,
                                         "serverCertificate" :
                                         #CERT S SM DSauth ECDSA
                                       -- NOTE: select the CI as defined in the
                                       note in the chapter 2.1.4 of SGP.23
                                         "header"
                                            "functionExecutionStatus"
                                               "status" : "Executed-Success"
                                         },
                                         "transactionId" : <S_TRANSACTION_ID>,
"serverSigned1" : <S_SMDS_SIGNED_ADDR1>,
                                         "serverSignature1":
INITIATE_AUTH_DS_OK_1
                                        <S SMDS SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" :
                                         <EUICC CI PK ID TO BE USED>,
                                         "serverCertificate" :
                                         #CERT S SM DSauth ECDSA
                                       -- NOTE: select the CI as defined in the
                                       note in the chapter 2.1.4 of SGP.23
                                         "header" : {
                                            "functionExecutionStatus" : {
                                               "status" : "Executed-Success"
                                         "transactionId" : <S_TRANSACTION_ID>,
                                         "serverSigned1" : <S_SMDS_SIGNED1>,
INITIATE_AUTH_INV_CERT_DS
                                         "serverSignature1":
                                       <S SMDS SIGNATURE1>,
                                         "euiccCiPKIdTobeUsed" :
                                       <EUICC CI PK ID TO BE USED>,
                                       -- NOTE: select the CI Key ID in highest
                                       priority from the
                                       <EUICC CI PK ID LIST FOR SIGNING>
                                       "serverCertificate" :
```

V1.4 Page 670 of 777

```
#CERT S SM DSauth INV SIGN
                                        "header" : {
                                           "functionExecutionStatus" : {
                                               "status" : "Executed-Success"
                                        "transactionId" : <S TRANSACTION ID>,
                                        "serverSigned1" : <S SMDS SIGNED1>,
                                        "serverSignature1":
INITIATE_AUTH_INV_CI_DS
                                      <S SMDS SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" : #CI PK ID INV,
                                        "serverCertificate" :
                                      #CERT S SM DSauth ECDSA
                                      -- NOTE: select and choose the
                                      #CERT S SM DSauth ECDSA leading to the CI
                                      Key ID in highest priority from the
                                      <EUICC CI PK ID LIST FOR SIGNING>
                                        "header" : {
                                           "functionExecutionStatus" : {
                                              "status" : "Executed-Success"
                                        "transactionId" : <S_TRANSACTION_ID>,
                                        "serverSigned1" : <S SMDS SIGNED1>,
                                        "serverSignature1":
                                      <S SMDS SIGNATURE INV>,
INITIATE_AUTH_INV_SIGN_DS
                                        "euiccCiPKIdTobeUsed" :
                                      <EUICC CI PK ID TO BE USED>,
                                        "serverCertificate":
                                      #CERT S SM DSauth ECDSA
                                      -- NOTE: select the CI Key ID in highest
                                      priority from the
                                      <EUICC_CI_PK_ID_LIST_FOR_SIGNING> and
                                      choose the #CERT S SM DSauth ECDSA
                                      leading to the same Root CI certificate
                                        "header" : {
                                           "functionExecutionStatus" : {
                                               "status" : "Executed-Success"
                                        "transactionId" : <S TRANSACTION ID>,
INITIATE_AUTH_INV_SMDS_ADDRESS
                                        "serverSigned1" :
                                      <S_SMDS_SIGNED_INV_ADDR>,
                                        "serverSignature1" :
                                      <S SMDS SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" :
                                      <EUICC CI PK ID TO BE USED>,
                                        "serverCertificate" :
```

V1.4 Page 671 of 777

Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

```
#CERT S SM DSauth ECDSA
                                      -- NOTE: select the CI Key ID in highest
                                      priority from the
                                      <EUICC_CI_PK_ID_LIST_FOR_SIGNING> and
                                      choose the #CERT_S_SM_DSauth_ECDSA
                                      leading to the same Root CI certificate
                                        "header" : {
                                           "functionExecutionStatus" : {
                                              "status" : "Executed-Success"
                                        },
                                        "transactionId" : <S_TRANSACTION_ID>,
                                        "serverSigned1" : <S_SMDP_SIGNED1>,
INITIATE_AUTH_OK
                                        "serverSignature1":
                                        <S SMDP SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" :
                                        <EUICC CI PK ID TO BE USED>,
                                        "serverCertificate" :
                                        #CERT S SM DPauth ECDSA
                                      -- NOTE: select the CI as defined in the
                                      note in the chapter 2.1.4 of SGP.23
                                        "header" : {
                                           "functionExecutionStatus" : {
                                              "status" : "Executed-Success"
                                        },
                                        "transactionId" : <S_TRANSACTION_ID>,
                                        "serverSigned1" : <S SMDP SIGNED1>,
                                        "serverSignature1":
INITIATE_AUTH_INV_CERT
                                        <S SMDP SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" :
                                        <EUICC_CI_PK_ID_TO_BE_USED>,-- NOTE:
                                         select the CI Key ID in highest
                                         priority from the
                                         <EUICC CI PK ID LIST FOR SIGNING>
                                         "serverCertificate" :
                                         #CERT_S_SM_DPauth_INV_SIGN
                                      }
```

V1.4 Page 672 of 777

```
"header" : {
                                            "functionExecutionStatus" : {
                                              "status" : "Executed-Success"
                                        },
                                        "transactionId" : <S TRANSACTION ID>,
                                        "serverSigned1" : <S_SMDP_SIGNED1>,
                                        "serverSignature1" :
INITIATE_AUTH_INV_CI
                                        <S SMDP SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" : #CI_PKI_ID2,
                                        "serverCertificate" :
                                        #CERT S SM DPauth_ECDSA -- NOTE:
                                        select and choose the
                                        #CERT S SM DPauth ECDSA leading to
                                        the CI Key ID in highest priority from
                                        the <EUICC CI PK ID LIST FOR SIGNING>
                                        "header" : {
                                            "functionExecutionStatus" : {
                                              "status" : "Executed-Success"
                                        },
                                        "transactionId" : <S TRANSACTION ID>,
                                        "serverSigned1" : <S SMDP SIGNED1>,
                                        "serverSignature1":
                                        <S SMDP SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" :
INITIATE_AUTH_INV_OID
                                        <EUICC CI PK ID TO BE USED>,
                                        "serverCertificate" :
                                        #CERT S SM DP2auth ECDSA
                                      -- NOTE: select the CI Key ID in highest
                                      priority from the
                                      <EUICC CI PK ID LIST FOR SIGNING>
                                      -- NOTE: serverSignature1 SHALL be
                                      calculated correctly, using the secret key
                                      related to CERT S SM DP2auth ECDSA.
                                         "header" : {
                                           "functionExecutionStatus" : {
                                              "status" : "Executed-Success"
                                        },
                                        "transactionId" : <S_TRANSACTION_ID>,
                                        "serverSigned1" : <S_SMDP_SIGNED1>,
INITIATE_AUTH_INV_SIGN
                                        "serverSignature1" :
                                        <S_SMDP_SIGNATURE_INV>,
                                        "euiccCiPKIdTobeUsed"
                                        <EUICC CI PK_ID_TO_BE_USED>,
                                        "serverCertificate" :
                                        #CERT S SM DPauth ECDSA
                                       -- NOTE: select the CI Key ID in highest
                                      priority from the
```

V1.4 Page 673 of 777

```
<EUICC CI PK ID LIST FOR SIGNING> and
                                      choose the #CERT S SM DPauth ECDSA
                                      leading to the same Root CI certificate
                                        "header" : {
                                           "functionExecutionStatus" : {
                                               "status" : "Executed-Success"
                                        },
                                        "transactionId" : <S TRANSACTION ID>,
                                        "serverSigned1" :
                                        <S_SMDP_SIGNED_INV_ADDR>,
                                        "serverSignature1":
                                        <S SMDP SIGNATURE1>,
                                        "euiccCiPKIdTobeUsed" :
INITIATE_AUTH_INV_SMDP+_ADDRESS
                                        <EUICC CI PK ID TO BE USED>,
                                        "serverCertificate" :
                                        #CERT S SM DPauth ECDSA
                                      -- NOTE: select the CI Key ID in highest
                                      priority from the
                                      <EUICC CI PK ID LIST FOR SIGNING> and
                                      choose the #CERT_S_SM_DPauth_ECDSA
                                      leading to the same Root CI certificate
                                      -- NOTE: serverSignature1 SHALL be
                                      calculated correctly, using the secret key
                                      related to CERT S SM DP2auth ECDSA.
MATCHING_ID_EMPTY
                                      '0x00 01'
NON_VOLATILE_MEM_LIMITED_SPACE
                                      response PendingNotification ::=
                                      otherSignedNotification :{
                                      tbsOtherNotification {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationDelete
                                            },
                                            notificationAddress
PENDING_NOTIF_DEL1
                                            #TEST DP ADDRESS1,
                                            iccid #ICCID OP PROF1
                                          },
                                          euiccNotificationSignature
                                      <TBS EUICC NOTIF SIG>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT EUM ECDSA
                                      }
```

V1.4 Page 674 of 777

```
response PendingNotification ::=
                                      otherSignedNotification :
                                         tbsOtherNotification {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation
                                               notificationDelete
                                            },
PENDING_NOTIF_DEL2
                                            notificationAddress
                                            #TEST_DP_ADDRESS2,
                                            iccid #ICCID OP PROF2
                                         },
                                         euiccNotificationSignature
                                      <TBS EUICC NOTIF SIG>,
                                         euiccCertificate #CERT EUICC ECDSA,
                                         eumCertificate #CERT EUM ECDSA
                                      response PendingNotification ::=
                                      otherSignedNotification :{
                                      tbsOtherNotification {
                                            seqNumber <SEQ_NUMBER>,
                                            profileManagementOperation {
                                              notificationDelete
                                            notificationAddress
PENDING_NOTIF_DEL5
                                            #TEST DP ADDRESS1,
                                            iccid #ICCID OP PROF5
                                          euiccNotificationSignature
                                      <TBS_EUICC_NOTIF_SIG>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT EUM ECDSA
                                      response PendingNotification ::=
                                      otherSignedNotification :{
                                      tbsOtherNotification {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationDelete
                                            },
                                            notificationAddress
PENDING_NOTIF_DEL6
                                            #TEST DP ADDRESS2,
                                            iccid #ICCID_OP_PROF6
                                          },
                                          euiccNotificationSignature
                                      <TBS_EUICC_NOTIF_SIG>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT_EUM_ECDSA
```

V1.4 Page 675 of 777

```
response PendingNotification ::=
                                       otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                              notificationDisable
                                             },
PENDING_NOTIF_DIS1
                                             notificationAddress
                                             #TEST DP ADDRESS1,
                                             iccid #ICCID_OP_PROF1
                                           euiccNotificationSignature
                                       <TBS_EUICC_NOTIF_SIG>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       response PendingNotification ::=
                                       otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                              notificationDisable
                                             notificationAddress
PENDING_NOTIF_DIS5
                                             #TEST DP ADDRESS1,
                                            iccid #ICCID OP PROF5
                                           euiccNotificationSignature
                                       <TBS_EUICC_NOTIF_SIG>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       response PendingNotification ::=
                                       otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                               notificationDisable
                                             },
PENDING_NOTIF_DIS8
                                             notificationAddress
                                             #TEST DP ADDRESS8,
                                             iccid #ICCID OP PROF8
                                           },
                                           euiccNotificationSignature
                                       <TBS_EUICC_NOTIF_SIG>,
                                           euiccCertificate #CERT_EUICC_ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                       }
```

V1.4 Page 676 of 777

```
response PendingNotification ::=
                                      otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                               notificationEnable
                                            notificationAddress
PENDING_NOTIF_EN1
                                            #TEST DP ADDRESS1,
                                            iccid #ICCID OP PROF1
                                           euiccNotificationSignature
                                       <TBS EUICC NOTIF SIG>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT_EUM_ECDSA
                                      response PendingNotification ::=
                                      otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                              notificationEnable
                                             },
                                            notificationAddress
PENDING_NOTIF_EN2
                                            #TEST DP ADDRESS2,
                                            iccid #ICCID OP PROF2
                                           },
                                           euiccNotificationSignature
                                      <TBS EUICC NOTIF SIG>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                      response PendingNotification ::=
                                      otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                               notificationEnable
                                            notificationAddress
PENDING_NOTIF_EN5
                                            #TEST DP ADDRESS1,
                                            iccid #ICCID OP PROF5
                                           },
                                           euiccNotificationSignature
                                      <TBS EUICC NOTIF SIG>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT_EUM_ECDSA
```

V1.4 Page 677 of 777

```
response PendingNotification ::=
                                      otherSignedNotification : {
                                           tbsOtherNotification {
                                            seqNumber <SEQ_NUMBER>,
                                            profileManagementOperation {
                                              notificationEnable
                                            notificationAddress
PENDING_NOTIF_EN6
                                            #TEST DP ADDRESS2,
                                            iccid #ICCID OP PROF6
                                          euiccNotificationSignature
                                      <TBS EUICC NOTIF SIG>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT EUM ECDSA
PP_VERSION
                                      0x01 00 00
                                      resp PrepareDownloadResponse ::=
                                        downloadResponseOk : {
                                          euiccSigned2 {
                                            transactionId <S_TRANSACTION_ID>,
                                            euiccOtpk <BPP OTPK EUICC ECKA>
PREP_DOWNLOAD_RESP_8_1_6_1
                                          },
                                          euiccSignature2
                                      <EUICC SIGNATURE2 INVALID>
                                      resp PrepareDownloadResponse ::=
                                        downloadResponseOk : {
                                          euiccSigned2 {
                                            transactionId <S TRANSACTION ID>,
                                            euiccOtpk <BPP OTPK EUICC ECKA>,
PREP_DOWNLOAD_RESP_8_2_7_3_8
                                            hashCc <S HASHED CC ERROR>
                                          },
                                          euiccSignature2 <EUICC SIGNATURE2>
                                      resp PrepareDownloadResponse ::=
                                        downloadResponseOk : {
                                          euiccSigned2 {
                                            transactionId
                                      <INVALID TRANSACTION ID>,
PREP_DOWNLOAD_RESP_8_10_1_3_9
                                            euiccOtpk <BPP OTPK EUICC ECKA>
                                          euiccSignature2 <EUICC SIGNATURE2>
                                      resp PrepareDownloadResponse ::=
                                        downloadResponseOk : {
                                          euiccSigned2 {
                                            transactionId <S TRANSACTION ID>,
PREP_DOWNLOAD_RESP
                                            euiccOtpk <BPP OTPK EUICC ECKA>
                                          euiccSignature2 <EUICC SIGNATURE2>
```

V1.4 Page 678 of 777

```
resp PrepareDownloadResponse ::=
                                        downloadResponseOk : {
                                          euiccSigned2 {
                                            transactionId <S TRANSACTION ID>,
PREP_DOWNLOAD_RESP_CC
                                            euiccOtpk <BPP OTPK EUICC ECKA>,
                                            hashCc <S HASHED CC>
                                          euiccSignature2 <EUICC SIGNATURE2>
                                      resp PrepareDownloadResponse ::=
                                        downloadResponseOk : {
                                          euiccSigned2 {
                                            transactionId <S TRANSACTION ID>,
PREP_DOWNLOAD_RESP_NEW_OTPK
                                            euiccOtpk <OTPK EUICC ECKA NEW>
                                          euiccSignature2 <EUICC SIGNATURE2>
                                      resp PrepareDownloadResponse ::=
                                        downloadResponseOk : {
                                          euiccSigned2 {
                                            transactionId <S TRANSACTION ID>,
PREP DOWNLOAD RESP NEW OTPK CC
                                            euiccOtpk <OTPK EUICC ECKA NEW>,
                                            hashCc <S HASHED CC>
                                          euiccSignature2 <EUICC SIGNATURE2>
                                      0x02 01 00
PROFILE_VERSION
                                      rspCapability RspCapability ::= {
                                          additionalProfile, rpmSupport,
RSP_CAPABILITY
                                          testProfileSupport
                                      euiccInfo2 EUICCInfo2 ::= {
                                          profileVersion #PROFILE VERSION,
                                          svn #RSP SVN H,
                                          euiccFirmwareVer #EUICC FIRMWARE VER,
                                          {\tt extCardResource}
                                          #EXT_CARD_RESOURCE_LIMITED_SPACE,
                                          uiccCapability #UICC CAPABILITY,
                                          rspCapability #RSP CAPABILITY,
                                          euiccCiPKIdListForVerification
S_EUICC_INFO2_INSUF_MEM_ERROR
                                       {#EUICC CI PK ID LIST FOR VERIFICATION 1},
                                          euiccCiPKIdListForSigning
                                          {#EUICC CI PK ID LIST FOR SIGNING 1},
                                          ppVersion #PP VERSION,
                                          sasAcreditationNumber
                                          #SAS ACREDITATION NUMBER
                                      euiccInfo2 EUICCInfo2 ::= {
                                          profileVersion #PROFILE VERSION,
S_EUICC_INFO2_PPR2
                                          svn #RSP SVN H,
                                          euiccFirmwareVer
```

V1.4 Page 679 of 777

```
#EUICC FIRMWARE VER,
                                           extCardResource
                                           #S_EXT_CARD_RESOURCE,
                                           uiccCapability #UICC_CAPABILITY,
                                           rspCapability #RSP_CAPABILITY,
                                           euiccCiPKIdListForVerification
                                       {#EUICC CI PK ID LIST FOR VERIFICATION 1},
                                           euiccCiPKIdListForSigning
                                           {#EUICC CI PK ID LIST FOR SIGNING 1},
                                           forbiddenProfilePolicyRules { ppr2 },
                                           ppVersion #PP VERSION,
                                           sasAcreditationNumber
                                           #SAS_ACREDITATION_NUMBER
                                       The Extended Card Resource Information according to
                                       ETSI TS 102 226:
S_EXT_CARD_RESOURCE
                                       0x81 <L> #INSTALLED PROFILES
                                       0x82 <L> #S NON VOLATILE MEM
                                       0x83 <L> #S VOLATILE MEM
                                       0xA0 00
S_NON_VOLATILE_MEM
                                       response PendingNotification ::=
                                       profileInstallationResult : {
                                         profileInstallationResultData {
                                           transactionId <S TRANSACTION ID>,
                                           notificationMetadata {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                               notificationInstall
                                             },
                                             notificationAddress
S_PN_PIR_OK1
                                       #IUT_SM_DP_ADDRESS,
                                             iccid #ICCID_OP_PROF1
                                           smdpOid #IUT_SM_DP_OID,
                                           finalResult successResult : {
                                             aid <ISD P AID>,
                                             simaResponse #SIMA_RESULT_OK
                                         euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 680 of 777

```
response PendingNotification ::=
                                       profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId
                                       <INVALID TRANSACTION ID>,
                                          notificationMetadata {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                              notificationInstall
                                             },
                                            notificationAddress
S_PN_PIR_INVALID_TRANS_ID
                                             #IUT SM DP ADDRESS,
                                            iccid #ICCID OP PROF1
                                           },
                                           smdpOid #IUT SM DP OID,
                                           finalResult successResult : {
                                            aid <ISD P AID>,
                                             simaResponse #SIMA RESULT OK
                                         },
                                        euiccSignPIR <EUICC SIGN PIR>
                                       response PendingNotification ::=
                                       profileInstallationResult :
                                       profileInstallationResultData {
                                           transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                              notificationInstall
                                             },
                                            notificationAddress
S_PN_PIR_INCORRECT_INPUT_VALUES
                                       #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID_OP_PROF1
                                          },
                                           smdpOid #IUT SM DP OID,
                                           finalResult errorResult : {
                                            bppCommandId configureISDP,
                                             errorReason incorrectInputValues
                                         },
                                        euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 681 of 777

```
response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                             notificationInstall
S_PN_PIR_INVALID_SIGN
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          },
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId
                                      initialiseSecureChannel,
                                            errorReason invalidSignature }
                                        },
                                        euiccSignPIR <EUICC_SIGN_PIR>
                                      response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_UNSUPPORTED_CRT
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          smdpOid #IUT_SM_DP_OID,
                                          finalResult errorResult : {
                                           bppCommandId
                                      initialiseSecureChannel,
                                            errorReason unsupportedCrtValues
                                        euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 682 of 777

```
response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_UNSUP_REMOTE_OP_TYPE
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          },
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId
                                      initialiseSecureChannel,
                                            errorReason
                                            unsupportedRemoteOperationType
                                        },
                                        euiccSignPIR <EUICC_SIGN_PIR>
                                      response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ_NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
                                            },
S_PN_PIR_UNSUP_PROFILE_CLASS
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID_OP_PROF1
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId storeMetadata,
                                            errorReason unsupportedProfileClass
                                        },
                                        euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 683 of 777

```
response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_SCP03T_STRUCTURE_ERROR
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          },
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId storeMetadata,
                                            errorReason scp03tStructureError
                                         },
                                        euiccSignPIR <EUICC_SIGN_PIR>
                                      response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_SCP03T_SECURITY_ERROR
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          smdpOid #IUT_SM_DP_OID,
                                          finalResult errorResult : {
                                            bppCommandId replaceSessionKeys,
                                            errorReason scp03tSecurityError
                                          }
                                        },
                                        euiccSignPIR <EUICC_SIGN_PIR>
```

V1.4 Page 684 of 777

```
response PendingNotification ::=
                                       profileInstallationResult : {
                                         profileInstallationResultData {
                                           transactionId <S TRANSACTION ID>,
                                           notificationMetadata {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                              notificationInstall
S_PN_PIR_ICCID_ALREADY_EXISTS
                                             notificationAddress
                                       #IUT_SM_DP_ADDRESS,
                                             iccid #ICCID OP PROF1
                                           },
                                           smdpOid #IUT SM DP OID,
                                           finalResult errorResult : {
                                            bppCommandId storeMetadata,
                                             errorReason
                                       installFailedDueToIccidAlreadyExistsOnEuic
                                         },
                                         euiccSignPIR <EUICC SIGN PIR>
                                       response PendingNotification ::=
                                       profileInstallationResult : {
                                         profileInstallationResultData {
                                           transactionId <S TRANSACTION ID>,
                                           notificationMetadata {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                               notificationInstall
                                             },
                                             notificationAddress
                                       #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
S_PN_PIR_INSUFFICIENT_MEMORY
                                           },
                                           smdpOid #IUT SM DP OID,
                                           finalResult errorResult : {
                                             bppCommandId storeMetadata,
                                             errorReason
                                       in stall \verb|FailedDueToInsufficientMemoryForPro|\\
                                       file
                                         },
                                         euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 685 of 777

```
response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_INSTALL_INTERRUPTION
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          },
                                          smdpOid #IUT_SM_DP_OID,
                                          finalResult errorResult : {
                                            bppCommandId storeMetadata,
                                            errorReason
                                            installFailedDueToInterruption
                                        },
                                        euiccSignPIR <EUICC SIGN PIR>
                                      response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
                                            },
S_PN_PIR_PE_PROCESSING_ERROR
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID_OP_PROF1
                                          },
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId loadProfileElements,
                                            errorReason
                                            installFailedDueToPEProcessingError
                                        },
                                        euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 686 of 777

```
response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_DATA_MISMATCH
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          },
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId loadProfileElements,
                                            errorReason
                                            installFailedDueToDataMismatch
                                        },
                                        euiccSignPIR <EUICC SIGN PIR>
                                      response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
                                            },
                                            notificationAddress
S_PN_PIR_TEST_PROFILE_INVALID_NAA_K
                                      #IUT_SM_DP_ADDRESS,
ΕY
                                            iccid #ICCID OP PROF1
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId loadProfileElements,
                                            errorReason
                                      testProfileInstallFailedDueToInvalidNaaKey
                                        },
                                        euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 687 of 777

```
response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_PPR_NOT_ALLOWED
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          },
                                          smdpOid #IUT SM DP OID,
                                          finalResult errorResult : {
                                            bppCommandId storeMetadata,
                                            errorReason pprNotAllowed
                                        },
                                        euiccSignPIR <EUICC_SIGN_PIR>
                                      response PendingNotification ::=
                                      profileInstallationResult : {
                                        profileInstallationResultData {
                                          transactionId <S TRANSACTION ID>,
                                          notificationMetadata {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationInstall
S_PN_PIR_UNKNOWN_ERROR
                                            notificationAddress
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          smdpOid #IUT_SM_DP_OID,
                                          finalResult errorResult : {
                                            bppCommandId storeMetadata,
                                            errorReason
                                            installFailedDueToUnknownError
                                         },
                                        euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 688 of 777

```
response PendingNotification ::=
                                      otherSignedNotification :
                                          tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation
                                                notificationInstall
                                             },
S_PENDING_NOTIF_OTHER_INST1
                                             notificationAddress
                                             #IUT_SM_DP_ADDRESS,
                                             iccid #ICCID OP PROF1
                                         },
                                         euiccNotificationSignature
                                         <TBS EUICC NOTIF SIG>,
                                         euiccCertificate #CERT EUICC ECDSA,
                                         eumCertificate #CERT EUM ECDSA
                                       response PendingNotification ::=
                                      otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                              notificationEnable
                                            notificationAddress
S_PENDING_NOTIF_EN1
                                      #IUT SM DP ADDRESS,
                                            iccid #ICCID OP PROF1
                                           euiccNotificationSignature
                                           <TBS EUICC NOTIF SIG>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT EUM ECDSA
                                      response PendingNotification ::=
                                      otherSignedNotification : {
                                            tbsOtherNotification {
                                             seqNumber <SEQ NUMBER>,
                                             profileManagementOperation {
                                               notificationDisable
                                             },
                                            notificationAddress
S_PENDING_NOTIF_DIS1
                                       #IUT SM DP ADDRESS,
                                            iccid #ICCID OP PROF1
                                           },
                                           euiccNotificationSignature
                                           <TBS_EUICC_NOTIF_SIG>,
                                           euiccCertificate #CERT EUICC ECDSA,
                                           eumCertificate #CERT_EUM_ECDSA
```

V1.4 Page 689 of 777

```
response PendingNotification ::=
                                      otherSignedNotification :{
                                      tbsOtherNotification {
                                            seqNumber <SEQ NUMBER>,
                                            profileManagementOperation {
                                              notificationDelete
                                            notificationAddress
S_PENDING_NOTIF_DE1
                                      #IUT_SM_DP_ADDRESS,
                                            iccid #ICCID OP PROF1
                                          euiccNotificationSignature
                                          <TBS EUICC NOTIF SIG>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT EUM ECDSA
                                      req SmdpSigned2 ::= {
                                        transactionId <S TRANSACTION ID>,
S_SMDP_SIGNED2
                                        ccRequiredFlag FALSE
                                      req SmdpSigned2 ::= {
                                        transactionId <S TRANSACTION ID>,
S_SMDP_SIGNED2_CC
                                        ccRequiredFlag TRUE
                                      req SmdpSigned2 ::= {
                                        transactionId <INVALID TRANSACTION ID>,
S_SMDP_SIGNED2_INV_TRANSACTION_ID
                                        ccRequiredFlag FALSE
                                       '0x01 00'
S_VOLATILE_MEM
                                      GSMA_SAS_123456789
SAS_ACREDITATION_NUMBER
                                      uiccCapability UICCCapability ::= {
                                          contactlessSupport, usimSupport,
                                          isimSupport,
                                          akaMilenage, akaTuak128,
UICC CAPABILITY
                                          gbaAuthenUsim, eapClient,
                                          javacard, multipleUsimSupport
                                      }
```

V1.4 Page 690 of 777

D.2.2 ES9+ Responses

Name	Content
AUTH_CLIENT_OK	<pre>"header" : { "functionExecutionStatus" : { "status" : "Executed-Success" } }, "transactionId" : <s_transaction_id>, "profileMetadata" : #METADATA_OP_PROF1, "smdpSigned2" : #S_SMDP_SIGNED2, "smdpSignature2" : <s_sm_dp+_signature2>, "smdpCertificate" : #CERT_S_SM_DPpb_ECDSA }</s_sm_dp+_signature2></s_transaction_id></pre>
AUTH_CLIENT_OK_CC	<pre>"header" : { "functionExecutionStatus" : { "status" : "Executed-Success" } }, "transactionId" : <s_transaction_id>, "profileMetadata" : #METADATA_OP_PROF1, "smdpSigned2" : #S_SMDP_SIGNED2_CC, "smdpSignature2" : <s_sm_dp+_signature2>, "smdpCertificate" : #CERT_S_SM_DPpb_ECDSA }</s_sm_dp+_signature2></s_transaction_id></pre>
AUTH_CLIENT_INV_PB_CERT	<pre>"header" : { "functionExecutionStatus" : { "status" : "Executed-Success" } }, "transactionId" : <s_transaction_id>, "profileMetadata" : #METADATA_OP_PROF1, "smdpSigned2" : #S_SMDP_SIGNED2, "smdpSignature2" : <s_sm_dp+_signature2>, "smdpCertificate" : #CERT_S_SM_DPpb_INV_SIGN }</s_sm_dp+_signature2></s_transaction_id></pre>
AUTH_CLIENT_INV_CI	{ "header" : {

V1.4 Page 691 of 777

```
"functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            "transactionId" : <S_TRANSACTION_ID>,
                                            "profileMetadata" :
                                            #METADATA OP PROF1,
                                            "smdpSigned2" : #S SMDP SIGNED2,
                                            "smdpSignature2" :
                                            <S SM DP+ SIGNATURE2>,
                                            "smdpCertificate" :
                                            #CERT S SM DP2pb ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            "transactionId" : <S TRANSACTION ID>,
                                            "profileMetadata" :
                                            #METADATA OP PROF1,
                                            "smdpSigned2" : #S_SMDP_SIGNED2,
AUTH_CLIENT_INV_SIGN
                                            "smdpSignature2":
                                            <S SM DP+ SIGNATURE2>,
                                            "smdpCertificate" :
                                            #CERT_S_SM_DPpb_ECDSA
                                         }
                                         The <S_SM_DP+_SIGNATURE2> SHALL NOT be
                                         computed using the #SK_S_SM_DPpb_ECDSA
                                         but SHALL have the same length as for a
                                         valid signature
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            },
                                            "transactionId" :
                                            <S TRANSACTION ID>,
AUTH_CLIENT_INV_TRANSACTION_ID
                                            "profileMetadata" :
                                            #METADATA OP PROF1,
                                            "smdpSigned2" :
                                         #S SMDP SIGNED2 INV TRANSACTION ID,
                                            "smdpSignature2" :
                                            <S SM DP+ SIGNATURE2>,
                                            "smdpCertificate" :
                                            #CERT_S_SM_DPpb_ECDSA
                                         resp CancelSessionResponse ::=
                                         cancelSessionResponseOk : {
                                           euiccCancelSessionSigned {
CS_OK_EU_LOAD_BPP_ERROR
                                            transactionId <S TRANSACTION ID>,
                                             smdpOid #S SM DP+ OID,
                                             reason loadBppExecutionError
```

V1.4 Page 692 of 777

```
euiccCancelSessionSignature
                                          <EUICC CANCEL SESSION SIGNATURE>
                                         resp CancelSessionResponse ::=
                                         cancelSessionResponseOk : {
                                          euiccCancelSessionSigned {
                                            transactionId <S TRANSACTION ID>,
                                            smdpOid #S SM DP+ OID,
CS_OK_EU_POSTPONED
                                            reason postponed
                                          },
                                          euiccCancelSessionSignature
                                          <EUICC_CANCEL_SESSION_SIGNATURE>
                                         resp CancelSessionResponse ::=
                                         cancelSessionResponseOk : {
                                          euiccCancelSessionSigned {
                                            transactionId <S TRANSACTION ID>,
                                            smdpOid #S SM DP+ OID,
CS_OK_EU_REJ
                                            reason endUserRejection
                                          },
                                          euiccCancelSessionSignature
                                          <EUICC CANCEL SESSION SIGNATURE>
                                         resp CancelSessionResponse ::=
                                         cancelSessionResponseOk : {
                                          euiccCancelSessionSigned {
                                            transactionId <S TRANSACTION ID>,
                                            smdpOid #S SM DP+ OID,
CS_OK_PPR_NOT_ALLOWED
                                            reason pprNotAllowed
                                          euiccCancelSessionSignature
                                          <EUICC_CANCEL_SESSION_SIGNATURE>
                                         resp CancelSessionResponse ::=
                                         cancelSessionResponseOk : {
                                          euiccCancelSessionSigned {
                                            transactionId <S TRANSACTION ID>,
                                            smdpOid #S SM DP+ OID,
CS_OK_TIMEOUT
                                            reason timeout
                                          euiccCancelSessionSignature
                                          <EUICC CANCEL SESSION SIGNATURE>
                                           "header" : {
                                             "functionExecutionStatus" : {
                                                 "status" : "Executed-Success"
GET_BPP_LOAD_ERROR
                                          },
                                           "transactionId" : <S TRANSACTION ID>,
                                           "boundProfilePackage" :
                                         BoundProfilePackage {
```

V1.4 Page 693 of 777

Non-confidential

```
#S INIT SC PROF1,
                                              firstSequenceOf87 {
                                                #CONF_ISDP_PROF1
                                              },
                                              sequenceOf88 {
                                                <METADATA_OP_PROF1_SEG>
                                                <METADATA OP PROF1 SEG>
                                            }
                                          NOTE 1: boundProfilePackage is enconded as base64
                                          therefore the test tool SHALL decode
                                          boundProfilePackage to access the ASN.1.
                                         NOTE 2: For sequenceOf88 there will be only one or
                                         two '88' TLV segments depending on the size of
                                          StoreMetadata.
                                            "header"
                                               "functionExecutionStatus"
                                                  "status" : "Executed-Success"
                                            },
                                            "transactionId" : <S_TRANSACTION_ID>,
                                            "boundProfilePackage" {
                                              #S INIT SC PROF1,
                                              #UNKNOWN BPP SEGMENT,
                                              firstSequenceOf87 {
                                                #CONF_ISDP_PROF1
                                              sequenceOf88 {
                                                <METADATA OP PROF1 SEG>
GET_BPP_LOAD_ERROR_UNKNOWN_TAG
                                                <METADATA_OP_PROF1_SEG>
                                              },
                                              sequenceOf86 {
                                                <PPP OP PROF1 SEG SK>
                                                <PPP_OP_PROF1 SEG SK>
                                         NOTE 1: boundProfilePackage is encoded as
                                         base64 therefore the test tool shall
                                          decode boundProfilePackage to access the
                                         ASN.1.
                                         NOTE 2: For sequenceOf88 there will be
                                         only one or two '88' TLV segments
                                          depending on the size of StoreMetadata.
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
GET_BPP_OK
                                            "transactionId" : <S TRANSACTION ID>,
                                            "boundProfilePackage":
                                         BoundProfilePackage {
```

V1.4 Page 694 of 777

```
#S INIT SC PROF1,
                                                firstSequenceOf87
                                                 #CONF_ISDP_PROF1
                                               sequenceOf88 {
                                                  <METADATA OP PROF1 SEG>
                                                 <METADATA OP PROF1 SEG>
                                               sequenceOf86 {
                                                  <PPP_OP_PROF1_SEG_SK>
                                                  <PPP_OP_PROF1_SEG_SK>
                                                }
                                           NOTE 1: boundProfilePackage is enconded as base64
                                           therefore the test tool SHALL decode
                                           boundProfilePackage to access the ASN.1.
                                           NOTE 2: For sequenceOf88 there will be only one or
                                           two '88' TLV segments depending on the size of
                                           StoreMetadata.
                                             "header" : {
                                                "functionExecutionStatus" : {
                                                    "status" : "Executed-Success"
                                             },
                                             "transactionId" : <S TRANSACTION ID>,
                                             "boundProfilePackage" :
                                           BoundProfilePackage {
                                               #S INIT SC PROF1,
                                               firstSequenceOf87 {
                                                 0x87 <L> #CONF ISDP PROF1
                                               sequenceOf88 {
GET_BPP_OK_PPK
                                                  <METADATA_OP_PROF1_SEG>
                                                 <METADATA_OP_PROF1_SEG>
                                               },
                                               secondSequenceOf87 {
                                                 0x87 <L> #REPLACE S KEYS REQ
                                               },
                                               sequenceOf86 {
                                                  <PPP OP PROF1 SEG SK>
                                                  <PPP_OP_PROF1_SEG_SK>
                                             }
                                           }
                                             "header" : {
                                                "functionExecutionStatus" : {
GET_BPP_INV
                                                    "status" : "Executed-Success"
                                             },
                                             "transactionId" : <S_TRANSACTION_ID>,
```

V1.4 Page 695 of 777

```
"boundProfilePackage" :
                                         BoundProfilePackage {
                                             #S_INIT_SC_PROF1,
                                             firstSequenceOf87 {
                                              0x87 <L> #CONF_ISDP_PROF1
                                             sequenceOf88 {
                                               <METADATA OP PROF1 SEG>
                                               <metadata op prof1 seg>
                                             },
                                             sequenceOf86 {
                                               <PPP OP PROF1 SEG SK INV>
                                               <PPP_OP_PROF1_SEG_SK_INV>
                                             }
                                           }
                                         response PendingNotification ::=
                                         otherSignedNotification :
                                            tbsOtherNotification {
                                               seqNumber <SEQ NUMBER>,
                                               profileManagementOperation
                                                  notificationInstall
                                               },
PENDING_NOTIF_INST_ADDRESS2
                                              notificationAddress
                                         #TEST_DP_ADDRESS2,
                                               iccid #ICCID OP PROF1
                                            euiccNotificationSignature
                                         <TBS EUICC NOTIF SIG>,
                                            euiccCertificate #CERT EUICC ECDSA,
                                            eumCertificate #CERT EUM ECDSA
                                         response PendingNotification ::=
                                         otherSignedNotification :
                                            tbsOtherNotification {
                                               seqNumber <SEQ NUMBER>,
                                               profileManagementOperation
                                                  notificationInstall
PENDING_NOTIF_INST1
                                               notificationAddress
                                         #TEST DP ADDRESS1,
                                               iccid #ICCID OP PROF1
                                            euiccNotificationSignature
                                         <TBS EUICC NOTIF SIG>,
                                            euiccCertificate #CERT EUICC ECDSA,
                                            eumCertificate #CERT_EUM_ECDSA
                                         {
R_AUTH_CLIENT_META_ABS
                                            "header" : {
```

V1.4 Page 696 of 777

```
"functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            "transactionId" : <TRANSACTION_ID_AC>,
                                            "profileMetadata" :
                                         #SMDP METADATA ABS,
                                            "smdpSigned2" : #SMDP SIGNED2,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT_SM_DPpb_ECDSA
                                         {
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            "transactionId" : <TRANSACTION ID AC>,
R_AUTH_CLIENT_META_ALL
                                            "profileMetadata" :
                                         #SMDP METADATA ALL,
                                            "smdpSigned2" : #SMDP_SIGNED2,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT SM DPpb ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            },
                                            "transactionId" : <TRANSACTION ID AC>,
R_AUTH_CLIENT_META_LARGE_ICON
                                            "profileMetadata" :
                                         #SMDP METADATA OP PROF1 2 SEG,
                                            "smdpSigned2" : #SMDP_SIGNED2,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT SM DPpb ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            "transactionId" : <TRANSACTION ID AC>,
R_AUTH_CLIENT_META_NON_ASCII
                                            "profileMetadata" :
                                         #SMDP_METADATA_NON_ASCII,
                                            "smdpSigned2" : #SMDP_SIGNED2,
                                            "smdpSignature2" : <SMDP_SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT_SM_DPpb_ECDSA
```

V1.4 Page 697 of 777

```
"header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            },
                                            "transactionId" : <TRANSACTION ID AC>,
R_AUTH_CLIENT_META_NOTIF_MULTI
                                            "profileMetadata" :
                                         #SMDP_METADATA_NOTIF_MULTI,
                                            "smdpSigned2" : #SMDP SIGNED2,
                                            "smdpSignature2" : <SMDP_SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT SM_DPpb_ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                            },
                                            "transactionId" : <TRANSACTION_ID_AC>,
R_AUTH_CLIENT_META_PN_LONG
                                            "profileMetadata" :
                                         #SMDP METADATA PN_LONG,
                                            "smdpSigned2" : #SMDP_SIGNED2,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT SM DPpb ECDSA
                                            "header" : {
                                              "functionExecutionStatus" : {
                                                 "status" : "Executed-Success"
                                            "transactionId" : <TRANSACTION ID AC>,
R_AUTH_CLIENT_META_SPN_LONG
                                            "profileMetadata" :
                                         #SMDP METADATA_SPN_LONG,
                                            "smdpSigned2" : #SMDP SIGNED2,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate":
                                         #CERT SM DPpb ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                 "status" : "Executed-Success"
                                            },
R_AUTH_CLIENT_OK
                                            "transactionId" : <TRANSACTION ID AC>,
                                            "profileMetadata" :
                                            #SMDP METADATA OP PROF1,
                                            "smdpSigned2" : #SMDP SIGNED2,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
```

V1.4 Page 698 of 777

```
#CERT SM DPpb ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                           "transactionId" : <TRANSACTION ID AC>,
R_AUTH_CLIENT_OK_CC
                                            "profileMetadata" :
                                            #SMDP_METADATA_OP_PROF1,
                                            "smdpSigned2" : #SMDP_SIGNED2_CC,
                                            "smdpSignature2" : <SMDP_SIGNATURE2>,
                                            "smdpCertificate":
                                         #CERT_SM_DPpb_ECDSA
                                            "header" : {
                                              "functionExecutionStatus" : {
                                                 "status" : "Executed-Success"
                                           "transactionId" : <TRANSACTION ID AC>,
R_AUTH_CLIENT_OK_EN
                                            "profileMetadata" :
                                            #SMDP_METADATA_OP_PROF1_EN,
                                            "smdpSigned2" : #SMDP SIGNED2,
                                            "smdpSignature2" : <SMDP_SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT SM DPpb ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                 "status" : "Executed-Success"
                                           },
                                            "transactionId" : <TRANSACTION_ID_AC>,
R_AUTH_CLIENT_OK_PPR2
                                           "profileMetadata" :
                                            #SMDP_METADATA_OP_PROF1_PPR2,
                                            "smdpSigned2" : #SMDP SIGNED2,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT SM_DPpb_ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                 "status" : "Executed-Success"
R_AUTH_CLIENT_RETRY_OK
                                            },
                                            "transactionId" : <TRANSACTION_ID_AC>,
                                            "profileMetadata" :
                                            #SMDP METADATA OP PROF1,
                                            "smdpSigned2" : #SMDP SIGNED2 RETRY,
```

V1.4 Page 699 of 777

Non-confidential

```
"smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT_SM_DPpb_ECDSA
                                            "header" : {
                                               "functionExecutionStatus" : {
                                                  "status" : "Executed-Success"
                                           },
                                            "transactionId" : <TRANSACTION_ID_AC>,
                                            "profileMetadata" :
R_AUTH_CLIENT_RETRY_OK_CC
                                         #SMDP METADATA OP PROF1,
                                           "smdpSigned2":
                                         #SMDP SIGNED2 CC RETRY,
                                            "smdpSignature2" : <SMDP SIGNATURE2>,
                                            "smdpCertificate" :
                                         #CERT SM DPpb ECDSA
                                         resp AuthenticateServerResponse
                                         ::authenticateResponseOk : {
                                          euiccSigned1 {
                                            transactionId <S TRANSACTION ID>,
                                            serverAddress #TEST ROOT DS ADDRESS,
                                            serverChallenge <S_SMDS_CHALLENGE>,
                                            euiccInfo2 #R EUICC INFO2, -- check
                                         only that the field is present but not
R_AUTH_SERVER_DS_MATCH_ID_DEV_INFO
                                         the values
                                            ctxParams1
                                         #CTX PARAMS1 MATCH ID DEV INFO
                                          euiccSignature1 <EUICC SIGNATURE1>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT EUM ECDSA
                                         resp AuthenticateServerResponse ::=
                                        authenticateResponseOk : {
                                          euiccSigned1 {
                                            transactionId <S_TRANSACTION_ID>,
                                            serverAddress #TEST DS ADDRESS1,
                                            serverChallenge <S SMDS CHALLENGE>,
                                            euiccInfo2 #R EUICC INFO2, -- check
                                         only that the field is present but not
R_AUTH_SERVER_DS_MATCH_ID_DEV_INFO_1
                                         the values
                                            ctxParams1
                                         #CTX PARAMS1 MATCH ID DEV INFO
                                          },
                                          euiccSignature1 <EUICC SIGNATURE1>,
                                          euiccCertificate #CERT EUICC ECDSA,
                                          eumCertificate #CERT_EUM_ECDSA
```

V1.4 Page 700 of 777

```
resp AuthenticateServerResponse ::=
                                          authenticateResponseOk {
                                            euiccSigned1 {
                                              transactionId <S TRANSACTION ID>,
                                              serverAddress #TEST DP ADDRESS1,
                                              serverChallenge <S SMDP CHALLENGE>,
                                              euiccInfo2 #R EUICC INFO2, -- check
                                          only that the field is present but not
R_AUTH_SERVER_MATCH_ID_DEV_INFO
                                          the values
                                              ctxParams1
                                          #CTX_PARAMS1_MATCH_ID_DEV_INFO
                                            euiccSignature1 <EUICC SIGNATURE1>,
                                            euiccCertificate #CERT EUICC ECDSA,
                                            eumCertificate #CERT EUM ECDSA
                                             "header" : {
                                                "functionExecutionStatus" : {
                                                    "status" : "Executed-Success"
                                            "transactionId": <TRANSACTION ID GBPP>,
                                            "boundProfilePackage" :
                                          BoundProfilePackage {
                                              #INIT SC PROF1,
                                              firstSequenceOf87 {
                                                <CONF ISDP PROF1 ENC>
                                              },
                                              sequenceOf88 {
                                                <SMDP METADATA SEG MAC>
R_GET_BPP_RESP_OP1_PPK
                                                <SMDP METADATA SEG MAC>
(Pre-generated PPP for Profiles)
                                              },
                                              secondSequenceOf87 {
                                                <REPLACE S KEYS REQ ENC>
                                              },
                                              sequenceOf86 {
                                                <PPP OP PROF1 SEG PPK>
                                                <PPP OP PROF1 SEG PPK>
                                          NOTE 1: boundProfilePackage is enconded as base64
                                          therefore the test tool SHALL decode
                                          boundProfilePackage to access the ASN.1.
```

V1.4 Page 701 of 777

	NOTE 2: For sequenceOf88 there will be only one or two '88' TLV segments depending on the size of StoreMetadata.
R_GET_BPP_RESP_OP1_SK (Dynamically-generated PPP for Profiles)	<pre>"header" : { "functionExecutionStatus" : { "status" : "Executed-Success" } }, "transactionId": <transaction_id_gbpp>, "boundProfilePackage" : BoundProfilePackage { #INIT_SC_PROF1, firstSequenceOf87 { <conf_isdp_prof1_enc> }, sequenceOf88 { <smdp_metadata_seg_mac> <smdp_metadata_seg_mac> }, sequenceOf86 { <ppp_op_prof1_seg_sk> <pppp_op_prof1_seg_sk> } } NOTE 1: boundProfilePackage is enconded as base64 therefore the test tool SHALL decode boundProfilePackage to access the ASN.1. NOTE 2: For sequenceOf88 there will be only one or two '88' TLV segments depending on the size of StoreMetadata.</pppp_op_prof1_seg_sk></ppp_op_prof1_seg_sk></smdp_metadata_seg_mac></smdp_metadata_seg_mac></conf_isdp_prof1_enc></transaction_id_gbpp></pre>
R_HTTP_204_OK	HTTP/1.1 204 No Content X-Admin-Protocol: gsma/rsp/v#RSP_SVN NOTE: if the HTTP response is being received from the server under test, then the "Content-type" header MAY be present.
R_INITIATE_AUTH_OK	<pre>"header" : { "functionExecutionStatus" : { "status" : "Executed-Success" } }, "transactionId" : <transaction_id_ia>, "serverSigned1" : #SERVER_SIGNED1, "serverSignature1" : <server_signature1>, "euiccCipKIdTobeUsed" : #CI_PKI_ID1, "serverCertificate" : #CERT_SM_XXauth_ECDSA }</server_signature1></transaction_id_ia></pre>

V1.4 Page 702 of 777

```
"header" : {
                                              "functionExecutionStatus" : {
                                                 "status" : "Executed-Success"
                                           },
                                           "transactionId" : <TRANSACTION ID 2>,
R_INITIATE_AUTH_OK_2
                                           "serverSigned1" : #SERVER SIGNED1 2,
                                           "serverSignature1" :
                                         <SERVER SIGNATURE1 2>,
                                           "euiccCiPKIdTobeUsed" : #CI_PKI_ID1,
                                           "serverCertificate" :
                                         #CERT SM XXauth ECDSA
                                         For InitiateAuthentication testing XX = IA, and for
                                         AuthenticateClient testing XX = AC:
                                         ss1 ServerSigned1 ::= {
                                            transactionId
                                            <TRANSACTION ID SIGNED IA>,
SERVER_SIGNED1
                                            euiccChallenge #S_EUICC_CHALLENGE,
                                            serverAddress
                                            #SERVER ADDRESS,
                                            serverChallenge <SERVER CHALLENGE>
                                         ss1 2 ServerSigned1 ::= {
                                            transactionId
                                         <TRANSACTION ID SIGNED 2>,
                                            euiccChallenge #S EUICC CHALLENGE 2,
SERVER_SIGNED1_2
                                            serverAddress #SERVER ADDRESS,
                                            serverChallenge <SERVER_CHALLENGE 2>
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID OP PROF1,
                                           serviceProviderName #SP NAME1,
SMDP_METADATA_OP_PROF1
                                           profileName #NAME OP PROF1,
                                           profileClass operational
                                         metadataReq StoreMetadataRequest ::= {
                                           iccid #ICCID_OP_PROF1,
                                           serviceProviderName #SP_NAME1,
                                           profileName #NAME OP PROF1,
                                           iconType png,
                                           icon #ICON OP PROF1 2 SEG,
                                           profileClass operational,
SMDP_METADATA_OP_PROF1_2_SEG
                                           notificationConfigurationInfo {
                                               profileManagementOperation {
                                                  notificationInstall,
                                                  notificationEnable,
                                                  notificationDisable,
                                                  notificationDelete
                                               },
```

V1.4 Page 703 of 777

Non-confidential

```
notificationAddress
                                        #IUT_SM_DP_ADDRESS
                                           }
                                          },
                                          profileOwner {
                                               mccMnc #MCC_MNC1
                                        metadataReq StoreMetadataRequest ::= {
                                          iccid #ICCID OP PROF3,
                                          serviceProviderName #SP NAME3,
                                          profileName #NAME_OP_PROF3,
                                          profileClass operational,
SMDP_METADATA_OP_PROF3
                                          profileOwner {
                                           mccMnc #MCC MNC2
                                          profilePolicyRules { ppr2 }
                                        smdpSigned2 SmdpSigned2 ::= {
                                          transactionId
                                        <TRANSACTION_ID_SIGNED_AC>,
SMDP_SIGNED2
                                          ccRequiredFlag FALSE
                                        smdpSigned2 SmdpSigned2 ::= {
                                          transactionId
SMDP_SIGNED2_CC
                                        <TRANSACTION_ID_SIGNED_AC>,
                                          ccRequiredFlag TRUE
                                        smdpSigned2 SmdpSigned2 ::= {
                                          transactionId
                                        <TRANSACTION ID SIGNED AC>,
SMDP SIGNED2 CC RETRY
                                          ccRequiredFlag TRUE,
                                          bppEuiccOtpk <BPP OTPK EUICC ECKA>
                                        smdpSigned2 SmdpSigned2 ::= {
                                          transactionId
                                        <TRANSACTION ID SIGNED AC>,
SMDP_SIGNED2_RETRY
                                          ccRequiredFlag FALSE,
                                          bppEuiccOtpk <BPP OTPK EUICC ECKA>
```

V1.4 Page 704 of 777

D.3 ES10x Requests And Responses

D.3.1 ES10x Requests

Name	Content
AUTH_SMDP_MATCH_ID	<pre>req AuthenticateServerRequest ::= { serverSigned1 { transactionId <s_transaction_id>, euiccChallenge <euicc_challenge>, serverAddress #TEST_DP_ADDRESS1, serverChallenge <s_smdp_challenge> }, serverSignature1 <s_smdp_signature1>, euiccCiPKIdToBeUsed <euicc_ci_pk_id_to_be_used>, serverCertificate #CERT_S_SM_DPauth_ECDSA, ctxParams1 #CTX_PARAMS1_MATCH_ID }</euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id></pre>
AUTH_SMDP_IMEI	<pre>req AuthenticateServerRequest ::= { serverSigned1 { transactionId <s_transaction_id>, euiccChallenge <euicc_challenge>, serverAddress #TEST_DP_ADDRESS1, serverChallenge <s_smdp_challenge> }, serverSignature1 <s_smdp_signature1>, euiccCiPKIdToBeUsed <euicc_ci_pk_id_to_be_used>, serverCertificate #CERT_S_SM_DPauth_ECDSA, ctxParams1 #CTX_PARAMS1_IMEI }</euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id></pre>
AUTH_SMDP_INV_CERT	<pre>req AuthenticateServerRequest ::= { serverSigned1 { transactionId <s_transaction_id>, euiccChallenge <euicc_challenge>, serverAddress #TEST_DP_ADDRESS1, serverChallenge <s_smdp_challenge> }, serverSignature1 <s_smdp_signature1>, euiccCiPKIdToBeUsed <euicc_ci_pk_id_to_be_used>, serverCertificate #CERT_S_SM_DPauth_INV_SIGN, ctxParams1 #CTX_PARAMS1 }</euicc_ci_pk_id_to_be_used></s_smdp_signature1></s_smdp_challenge></euicc_challenge></s_transaction_id></pre>

V1.4 Page 705 of 777

```
req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge <EUICC CHALLENGE>,
                                    serverAddress #TEST DP ADDRESS1,
                                    serverChallenge <S SMDP CHALLENGE>
AUTH_SMDP_INV_CURV
                                  serverSignature1 <RANDOM SM DP+ SIGN>,
                                  euiccCiPKIdToBeUsed
                                  <EUICC CI PK ID TO BE USED>,
                                  serverCertificate #CERT_S_SM_DPauth_INV_CURVE,
                                  ctxParams1 #CTX PARAMS1
                                req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge #S EUICC CHALLENGE,
                                    serverAddress #TEST DP ADDRESS1,
                                    serverChallenge <S SMDP CHALLENGE>
AUTH_SMDP_INV_CHALLENGE
                                  },
                                  serverSignature1 <S_SMDP_SIGNATURE1>,
                                  euiccCiPKIdToBeUsed
                                  <EUICC_CI_PK_ID_TO_BE_USED>,
                                  serverCertificate #CERT S SM DPauth ECDSA,
                                  ctxParams1 #CTX PARAMS1
                                req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge <EUICC_CHALLENGE>,
                                    serverAddress #TEST DP ADDRESS1,
                                    serverChallenge <S_SMDP_CHALLENGE>
AUTH_SMDP_INV_OID
                                  },
                                  serverSignature1 <S SMDP SIGNATURE1>,
                                  euiccCiPKIdToBeUsed
                                  <EUICC CI PK ID TO BE USED>,
                                  serverCertificate #CERT S SM DPpb ECDSA,
                                  ctxParams1 #CTX PARAMS1
                                req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge <EUICC CHALLENGE>,
                                    serverAddress #TEST ROOT DS ADDRESS,
                                    serverChallenge <S_SMDS_CHALLENGE>
AUTH_SMDS_IMEI
                                  serverSignature1 <S SMDS SIGNATURE1>,
                                  euiccCiPKIdToBeUsed
                                  <EUICC CI PK ID TO BE USED>,
                                  serverCertificate #CERT S SM DSauth ECDSA,
                                  ctxParams1 #CTX PARAMS1 EVENT ID IMEI
```

V1.4 Page 706 of 777

```
req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge <EUICC_CHALLENGE>,
                                    serverAddress #TEST ROOT DS ADDRESS,
                                    serverChallenge <S SMDS CHALLENGE>
AUTH_SMDS_INV_CERT
                                  serverSignature1 <S SMDS SIGNATURE1>,
                                  euiccCiPKIdToBeUsed
                                <EUICC CI PK ID TO BE USED>,
                                  serverCertificate #CERT S SM DSauth INV SIGN,
                                  ctxParams1 #CTX PARAMS1 EVENT ID
                                req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge #S EUICC CHALLENGE,
                                    serverAddress #TEST ROOT DS ADDRESS,
                                    serverChallenge <S SMDS CHALLENGE>
AUTH_SMDS_INV_CHALLENGE
                                  },
                                  serverSignature1 <S_SMDS_SIGNATURE1>,
                                  euiccCiPKIdToBeUsed
                                  <EUICC_CI_PK_ID_TO_BE_USED>,
                                  serverCertificate #CERT S SM DSauth ECDSA,
                                  ctxParams1 #CTX PARAMS1 EVENT ID
                                req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge <EUICC_CHALLENGE>,
                                    serverAddress #TEST ROOT DS ADDRESS,
                                    serverChallenge <S_SMDS_CHALLENGE>
AUTH_SMDS_INV_CURV
                                  serverSignature1 <RANDOM SM DS SIGN>,
                                  euiccCiPKIdToBeUsed
                                <EUICC CI PK ID TO BE USED>,
                                  serverCertificate #CERT S SM DSauth INV CURVE,
                                  ctxParams1 #CTX PARAMS1 EVENT ID
                                req AuthenticateServerRequest ::= {
                                  serverSigned1 {
                                    transactionId <S TRANSACTION ID>,
                                    euiccChallenge <EUICC CHALLENGE>,
                                    serverAddress #TEST DP ADDRESS1,
                                    serverChallenge <S_SMDP_CHALLENGE>
AUTHENTICATE_SMDP
                                  serverSignature1 <S SMDP SIGNATURE1>,
                                  euiccCiPKIdToBeUsed
                                  <EUICC CI PK ID TO BE USED>,
                                  serverCertificate #CERT S SM DPauth ECDSA,
                                  ctxParams1 #CTX PARAMS1
```

V1.4 Page 707 of 777

AUTHENTICATE_SMDS	<pre>req AuthenticateServerRequest ::= { serverSigned1 { transactionId <s_transaction_id>, euiccChallenge <euicc_challenge>, serverAddress #TEST_ROOT_DS_ADDRESS, serverChallenge <s_smds_challenge> }, serverSignature1 <s_smds_signature1>, euiccCiPKIdToBeUsed <euicc_ci_pk_id_to_be_used>, serverCertificate #CERT_S_SM_DSauth_ECDSA, ctxParams1 #CTX_PARAMS1_EVENT_ID }</euicc_ci_pk_id_to_be_used></s_smds_signature1></s_smds_challenge></euicc_challenge></s_transaction_id></pre>
CANCEL_SESSION_INV_TRANS_ID	<pre>req CancelSessionRequest ::={ transactionId <invalid_transaction_id>, reason endUserRejection }</invalid_transaction_id></pre>
CANCEL_SESSION_REJECT	<pre>req CancelSessionRequest ::={ transactionId <s_transaction_id>, reason endUserRejection }</s_transaction_id></pre>
CANCEL_SESSION_POSTPONED	<pre>req CancelSessionRequest ::={ transactionId <s_transaction_id>, reason postponed }</s_transaction_id></pre>
CANCEL_SESSION_TIMEOUT	<pre>req CancelSessionRequest ::={ transactionId <s_transaction_id>, reason timeout }</s_transaction_id></pre>
CANCEL_SESSION_PPR	<pre>req CancelSessionRequest ::={ transactionId <s_transaction_id>, reason pprNotAllowed }</s_transaction_id></pre>
CANCEL_SESSION_METADATA	<pre>req CancelSessionRequest ::={ transactionId <s_transaction_id>, reason metadataMismatch }</s_transaction_id></pre>
CANCEL_SESSION_LOAD_BPP	<pre>req CancelSessionRequest ::={ transactionId <s_transaction_id>, reason loadBppExecutionError }</s_transaction_id></pre>
CANCEL_SESSION_UNDEF	<pre>req CancelSessionRequest ::={ transactionId <s_transaction_id>, reason undefinedReason }</s_transaction_id></pre>

V1.4 Page 708 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

```
req EuiccMemoryResetRequest ::= {
                                  resetOptions {
                                    deleteOperationalProfiles,
EUICC_MEMORY_RESET
                                    resetDefaultSmdpAddress
                                  }
                                }
                                req EuiccMemoryResetRequest ::= {
EUICC_MEMORY_RESET_DEF_SMD
                                  resetOptions { resetDefaultSmdpAddress }
PADDRESS
                                req EuiccMemoryResetRequest ::= {
EUICC_MEMORY_RESET_OP_PRO
                                  resetOptions { deleteOperationalProfiles }
                                opConfProf1Req ProfileInfoListRequest ::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_CONF_OP_PROF1
                                  tagList '4FB8'H
                                getEIDReq GetEuiccDataRequest ::= {
                                  tagList '5A'H
GET_EID
                                getEIDReq GetEuiccDataRequest ::= {
                                 tagList '6B'H
GET_EID_INVALID
GET_EUICC_CHALLENGE
                                request GetEuiccChallengeRequest ::= {}
GET_EUICC_CONFIGURED_ADDRES
                                request EuiccConfiguredAddressesRequest ::={}
SES
GET_EUICC_INFO1
                                request GetEuiccInfolRequest::= { }
GET_EUICC_INFO2
                                request GetEuiccInfo2Request::= { }
                                opConfProf1Req ProfileInfoListRequest ::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_METADATA_OP_PROF1
                                  tagList '5A9192939495B6B799'H
                                getupdate1Req ProfileInfoListRequest ::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_NEW_METADATA
                                  tagList '9192939499'H -- names, icon and PPRs
                                opConfProf1Req ProfileInfoListRequest ::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_NOTIF_CONF_OP_PROF1
                                  tagList '5AB6'H
                                opConfProf1Req ProfileInfoListRequest ::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_PPR_OP_PROF1
                                  tagList '5A99'H
```

V1.4 Page 709 of 777

```
GET_PROFILES_INFO_ALL
                                request ProfileInfoListRequest::= { }
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_ICCID_TAGLIS
                                  searchCriteria iccid: #ICCID OP PROF1,
                                  tagList '9F70'H --state
                                request ProfileInfoListRequest::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_PROFILES_INFO_ICCID_TAGLIS
                                  tagList '93'H --icon type
                                request ProfileInfoListRequest::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_PROFILES_INFO_ICCID_TAGLIS
                                  tagList '95'H --Profile Class
T3
                                request ProfileInfoListRequest::= {
                                  searchCriteria iccid: #ICCID OP PROF1,
GET_PROFILES_INFO_ICCID_TAGLIS
                                  tagList 'B6'H --Notification configuration
                                request ProfileInfoListRequest::= {
                                  searchCriteria iccid: #ICCID OP PROF3,
GET_PROFILES_INFO_ICCID_TAGLIS
                                  tagList '99'H --ppr
                                request ProfileInfoListRequest::= {
                                  searchCriteria profileClass: operational,
GET_PROFILES_INFO_OPTAGLIST1
                                  tagList '5A9F70'H -- ICCID and State
                                request ProfileInfoListRequest::= {
                                  searchCriteria profileClass: operational,
GET_PROFILES_INFO_OPTAGLIST2
                                  tagList '909F70'H --Nickname and State
                                request ProfileInfoListRequest::= {
                                  searchCriteria profileClass: operational,
GET_PROFILES_INFO_OPTAGLIST3
                                  tagList '9493'H --Icon, Icon type
                                request ProfileInfoListRequest::= {
                                  searchCriteria profileClass: operational,
GET_PROFILES_INFO_OPTAGLIST4
                                  tagList '949F70'H --Icon, state
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_PROFCLASS
                                  searchCriteria profileClass: operational
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_ICCI
                                  tagList '5A'H
```

V1.4 Page 710 of 777

```
request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_ICO
                                  tagList '94'H
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_ISD
                                  tagList '4F'H
PAID
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_PR
                                  tagList '92'H
OFILE_NAME
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_PR
                                  tagList '90'H
OFILE_NICKNAME
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_PR
                                  tagList 'B7'H
OFILE_OWNER
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_SM
                                  tagList 'B8'H
DP_PROP_DATA
                                request ProfileInfoListRequest::= {
GET_PROFILES_INFO_TAGLIST_SP_
                                  tagList '91'H
NAME
                                request ProfileInfoListRequest::= {
                                  tagList '5A9F70'H -- ICCID and State
GET_PROFILES_INFO_TAGLIST1
                                request ProfileInfoListRequest::= {
                                  tagList '909F70'H --Nickname and State
GET_PROFILES_INFO_TAGLIST2
                                request ProfileInfoListRequest::= {
                                  tagList '9493'H --Icon, Icon type
GET_PROFILES_INFO_TAGLIST3
                                request ProfileInfoListRequest::= {
                                  tagList '949F70'H --Icon, state
GET_PROFILES_INFO_TAGLIST4
                                request ProfileInfoListRequest::= {
                                  tagList 'B7'H
GET_PROFILES_OWNERS
                                request GetRatRequest ::={}
GET RAT
```

V1.4 Page 711 of 777

```
request ListNotificationRequest ::= {
                                  profileManagementOperation {
                                     notificationInstall,
                                    notificationEnable,
LIST_NOTIF_ALL
                                    notificationDisable,
                                    notificationDelete
                                  }
LIST_NOTIF_OMITTED
                                 request ListNotificationRequest ::= {}
                                 request ListNotificationRequest ::= {
LIST_NOTIF_NONE
                                  profileManagementOperation {}
                                 request ListNotificationRequest ::= {
                                   profileManagementOperation {
LIST_NOTIF_INSTALL
                                    notificationInstall
                                 request ListNotificationRequest ::= {
                                  profileManagementOperation {
                                    notificationEnable
LIST NOTIF ENABLE
                                 request ListNotificationRequest ::= {
                                  profileManagementOperation {
LIST_NOTIF_DISABLE
                                    notificationDisable
                                 request ListNotificationRequest ::= {
                                   profileManagementOperation {
LIST_NOTIF_DELETE
                                    notificationDelete
                                   }
                                 }
                                 request ListNotificationRequest ::= {
                                  profileManagementOperation {
                                    notificationInstall,
LIST_NOTIF_INSTALL_ENABLE
                                    notificationEnable
                                  }
                                 request ListNotificationRequest ::= {
                                  profileManagementOperation {
                                    notificationDisable,
LIST_NOTIF_DISABLE_DELETE
                                    notificationDelete
                                   }
```

V1.4 Page 712 of 777

```
request ListNotificationRequest ::= {
                                  profileManagementOperation {
                                    notificationDisable,
LIST_NOTIF_DISABLE_ENABLE
                                    notificationEnable
                                   }
                                }
                                request ListNotificationRequest ::= {
                                  profileManagementOperation {
                                    notificationInstall,
LIST_NOTIF_INSTALL_ENABLE_DISA
                                    notificationEnable,
BLE
                                    notificationDisable
                                  }
                                }
                                request ListNotificationRequest ::= {
                                  profileManagementOperation {
                                    notificationEnable,
LIST NOTIF ENABLE DISABLE DEL
                                    notificationDisable,
ETE
                                    notificationDelete
                                  }
                                }
                                metadataReq StoreMetadataRequest ::= {
                                  iccid #ICCID OP PROF1,
                                  serviceProviderName #SP NAME1,
                                  profileName #NAME OP PROF1,
                                  notificationConfigurationInfo {
                                     { profileManagementOperation {
                                        notificationEnable,
                                        notificationDisable,
                                        notificationDelete
                                      },
                                      notificationAddress #TEST DP ADDRESS1
METADATA_EN_DI_DE_NOTIFS
                                     { profileManagementOperation {
                                        notificationEnable,
                                        notificationDisable,
                                        notificationDelete
                                      },
                                      notificationAddress #TEST DP ADDRESS2
                                  }
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag TRUE
PREP_DOWNLOAD_INVALID_CC
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
                                   smdpCertificate #CERT_S_SM_DPpb_ECDSA
                                request RetrieveNotificationsListRequest ::= {
RETRIEVE_NOTIF_ALL
                                  searchCriteria profileManagementOperation {
                                    notificationInstall,
```

V1.4 Page 713 of 777

```
notificationEnable,
                                    notificationDisable,
                                    notificationDelete
                                  }
                                }
                                request RetrieveNotificationsListRequest ::= {
RETRIEVE_NOTIF_OMITTED
                                request RetrieveNotificationsListRequest ::= {
RETRIEVE_NOTIF_NONE
                                  searchCriteria profileManagementOperation {}
                                request RetrieveNotificationsListRequest::= {
                                  searchCriteria profileManagementOperation {
RETRIEVE_NOTIF_INSTALL
                                    notificationInstall
                                request RetrieveNotificationsListRequest::= {
                                  searchCriteria profileManagementOperation {
                                    notificationEnable
RETRIEVE_NOTIF_ENABLE
                                  }
                                request RetrieveNotificationsListRequest::= {
                                  searchCriteria profileManagementOperation {
RETRIEVE_NOTIF_DISABLE
                                    notificationDisable
                                request RetrieveNotificationsListRequest::= {
                                  searchCriteria profileManagementOperation {
                                    notificationDelete
RETRIEVE_NOTIF_DELETE
                                  }
                                }
                                request RetrieveNotificationsListRequest ::= {
                                  searchCriteria profileManagementOperation {
                                    notificationInstall,
RETRIEVE_NOTIF_INSTALL_ENABLE
                                    notificationEnable
                                  }
                                request RetrieveNotificationsListRequest ::= {
                                  searchCriteria profileManagementOperation {
                                    notificationDisable,
RETRIEVE_NOTIF_DISABLE_DELETE
                                    notificationDelete
                                  }
                                request RetrieveNotificationsListRequest ::= {
                                  searchCriteria profileManagementOperation {
                                    notificationDisable,
RETRIEVE_NOTIF_DISABLE_ENABLE
                                    notificationEnable
                                  }
```

V1.4 Page 714 of 777

```
request RetrieveNotificationsListRequest ::= {
                                  searchCriteria profileManagementOperation {
                                    notificationInstall.
RETRIEVE_NOTIF_INSTALL_ENABLE
                                    notificationEnable,
_DISABLE
                                    notificationDisable
                                  }
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag FALSE
PREP_DOWN_INV_CURVE
                                  },
                                  smdpSignature2 <RANDOM SM DP+ SIGN>,
                                  smdpCertificate #CERT S SM DPpb INV CURVE
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag FALSE
PREP_DOWNLOAD_CERT_SMDP2
                                  },
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
                                   smdpCertificate #CERT S SM DP2pb ECDSA
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag FALSE
PREP_DOWNLOAD_INV_CERT
                                  },
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
                                  smdpCertificate #CERT S SM DPpb INV SIGN
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag FALSE
PREP_DOWNLOAD_INV_OID
                                  },
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
                                  smdpCertificate #CERT S SM DPauth ECDSA
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag FALSE
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
PREP_DOWNLOAD_INV_SIGN
                                  smdpCertificate #CERT S SM DPpb ECDSA
                                NOTE: The <S SM DP+ SIGNATURE2> SHALL NOT be
                                computed using the #SK S SM DPpb ECDSA but SHALL have
                                the same length as for a valid signature
```

V1.4 Page 715 of 777

```
req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <INVALID TRANSACTION ID>,
                                    ccRequiredFlag FALSE
PREP_DOWNLOAD_INV_TRANS_ID
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
                                  smdpCertificate #CERT S SM DPpb ECDSA
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag FALSE
PREP_DOWNLOAD_NO_AUTH
                                  },
                                  smdpSignature2 <RANDOM SM DP+ SIGN>,
                                  smdpCertificate #CERT S SM DPpb ECDSA
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S_TRANSACTION_ID>,
                                    ccRequiredFlag FALSE
PREP_DOWNLOAD_NO_CC
                                  },
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
                                  smdpCertificate #CERT S SM DPpb ECDSA
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                   transactionId <S TRANSACTION ID>,
                                   ccRequiredFlag TRUE,
                                   bppEuiccOtpk <OTPK EUICC ECKA>
PREP_DOWNLOAD_RETRY_CC
                                  smdpSignature2 <S SM DP+ SIGNATURE2>,
                                  hashCc <S HASHED CC>,
                                  smdpCertificate #CERT S SM DPpb ECDSA
                                req PrepareDownloadRequest ::= {
                                  smdpSigned2 {
                                    transactionId <S TRANSACTION ID>,
                                    ccRequiredFlag TRUE
PREP_DOWNLOAD_WITH_CC
                                  smdpSignature2 <S_SM_DP+_SIGNATURE2>,
                                  hashCc <S HASHED CC>,
                                  smdpCertificate #CERT S SM DPpb ECDSA
                                request SetDefaultDpAddressRequest::={
SET_EUICC_CONFIGURED_ADDRES
                                  defaultDpAddress #TEST DP ADDRESS1
S_1
                                request SetDefaultDpAddressRequest::={
SET EUICC CONFIGURED ADDRES
                                  defaultDpAddress #TEST DP ADDRESS2
S 2
```

V1.4 Page 716 of 777

```
request SetDefaultDpAddressRequest::={
SET_EUICC_CONFIGURED_ADDRES
                                 defaultDpAddress ""
S_EMPTY
                               setNicknameReq SetNicknameRequest ::= {
                                 iccid #ICCID_OP_PROF1,
SET_NICKNAME_EMPTY_OP_PROF1
                                 profileNickname ""
                               setNicknameReq SetNicknameRequest ::= {
                                 iccid #ICCID UNKNOWN,
SET_NICKNAME_ICCID_UNKNOWN
                                 profileNickname #NICKNAME2
                               setNicknameReq SetNicknameRequest ::= {
                                 iccid #ICCID_OP_PROF1,
SET_NICKNAME_OP_PROF1
                                 profileNickname #NICKNAME2
```

D.3.2 ES10x Responses

Name	Content
NOTIF_METADATA_DELETE1 (NotificationMetadata)	<pre>{ seqNumber <notif_seq_no_de1>, profileManagementOperation { notificationDelete }, notificationAddress #TEST_DP_ADDRESS1, iccid #ICCID_OP_PROF1 }</notif_seq_no_de1></pre>
NOTIF_METADATA2_DELETE1 (NotificationMetadata)	<pre>{ seqNumber <notif_seq_no2_de1>, profileManagementOperation { notificationDelete }, notificationAddress #TEST_DP_ADDRESS2, iccid #ICCID_OP_PROF1 }</notif_seq_no2_de1></pre>
NOTIF_METADATA_DISABLE1 (NotificationMetadata)	<pre>{ seqNumber <notif_seq_no_di1>, profileManagementOperation { notificationDisable }, notificationAddress #TEST_DP_ADDRESS1, iccid #ICCID_OP_PROF1 }</notif_seq_no_di1></pre>
NOTIF_METADATA2_DISABLE1 (NotificationMetadata)	<pre>{ seqNumber <notif_seq_no2_di1>, profileManagementOperation { notificationDisable }, notificationAddress #TEST_DP_ADDRESS2, iccid #ICCID_OP_PROF1 }</notif_seq_no2_di1></pre>

V1.4 Page 717 of 777

```
seqNumber <NOTIF SEQ NO EN1>,
NOTIF_METADATA_ENABLE1
                                profileManagementOperation { notificationEnable },
                                notificationAddress #TEST DP ADDRESS1,
(NotificationMetadata)
                                iccid #ICCID OP PROF1
                                 seqNumber <NOTIF_SEQ_NO2_EN1>,
NOTIF_METADATA2_ENABLE1
                                profileManagementOperation { notificationEnable },
                                notificationAddress #TEST DP ADDRESS2,
(NotificationMetadata)
                                 iccid #ICCID_OP_PROF1
                              }
                                seqNumber <NOTIF SEQ NO EN2>,
NOTIF_METADATA_ENABLE2
                                profileManagementOperation { notificationEnable },
                                notificationAddress #TEST DP ADDRESS2,
(NotificationMetadata)
                                iccid #ICCID OP PROF2
                                seqNumber <NOTIF_SEQ_NO_IN1>,
                                profileManagementOperation { notificationInstall
NOTIF_METADATA_INSTALL1
(NotificationMetadata)
                                notificationAddress #TEST DP ADDRESS1,
                                iccid #ICCID OP PROF1
                                seqNumber <NOTIF_SEQ_NO_IN1_PIR>,
                                profileManagementOperation {
NOTIF_METADATA_INSTALL1_PI
                                  notificationInstall
(NotificationMetadata)
                                notificationAddress #TEST DP ADDRESS1,
                                iccid #ICCID OP PROF1
                                seqNumber <NOTIF SEQ NO IN2>,
                                profileManagementOperation {
NOTIF METADATA INSTALL2
                                  notificationInstall
(NotificationMetadata)
                                notificationAddress #TEST DP ADDRESS2,
                                iccid #ICCID OP PROF2
                                 seqNumber <NOTIF SEQ NO IN2 PIR>,
                                profileManagementOperation {
NOTIF_METADATA_INSTALL2_PI
                                  notificationInstall
(NotificationMetadata)
                                notificationAddress #TEST DP ADDRESS2,
                                iccid #ICCID OP PROF2
```

V1.4 Page 718 of 777

```
pprIds { ppr1 },
                                 allowedOperators {
                                  { mccMnc #MCC MNC2,
PPR1 WITH OWNER GID
                                     gid1 #GID1,
                                     gid2 #GID2
(ProfilePolicyAuthorisationRule)
                                   }
                                 },
                                 pprFlags {consentRequired}
                                 pprIds { ppr1 },
                                 allowedOperators {
PPR1_WITHOUT_GID
                                 { mccMnc #MCC MNC4 }
(ProfilePolicyAuthorisationRule)
                                 },
                                 pprFlags {consentRequired}
                                 pprIds { ppr2 },
                                 allowedOperators {
PPR2_WITHOUT_CONSENT
                                   { mccMnc '92EEEE'H, gid1 ''H, gid2 ''H}
(ProfilePolicyAuthorisationRule)
                                 },
                                 pprFlags { }
                                 pprIds { ppr1, ppr2 },
                                 allowedOperators {
PPRS_ALLOWED
                                   { mccMnc 'EEEEEEE'H, gid1 ''H, gid2 ''H}
(ProfilePolicyAuthorisationRule)
                                 pprFlags {consentRequired}
                               }
                                 iccid #ICCID OP PROF1,
                                isdpAid <ISD P AID1>,
                                profileState enabled,
PROFILE_INFO1
                                serviceProviderName #SP NAME1,
                                profileName #NAME OP PROF1,
(ProfileInfo)
                                iconType png,
                                 icon #ICON OP PROF1,
                                 profileClass operational
                                 iccid #ICCID OP PROF1,
                                 isdpAid <ISD P AID1>,
                                 profileState disabled,
PROFILE_INFO1_DISABLED
                                 serviceProviderName #SP NAME1,
                                profileName #NAME OP PROF1,
(ProfileInfo)
                                iconType png,
                                icon #ICON OP PROF1,
                                 profileClass operational
```

V1.4 Page 719 of 777

PROFILE_INFO2 (ProfileInfo)	<pre>iccid #ICCID_OP_PROF2, isdpAid <isd_p_aid2>, profileState disabled, serviceProviderName #SP_NAME2, profileName #NAME_OP_PROF2, iconType png, icon #ICON_OP_PROF2, profileClass operational }</isd_p_aid2></pre>
PROFILE_INFO2_ENABLED (ProfileInfo)	<pre>iccid #ICCID_OP_PROF2, isdpAid <isd_p_aid2>, profileState enabled, serviceProviderName #SP_NAME2, profileName #NAME_OP_PROF2, iconType png, icon #ICON_OP_PROF2, profileClass operational }</isd_p_aid2></pre>
PROFILE_INFO3 (ProfileInfo)	<pre>iccid #ICCID_OP_PROF3, isdpAid <isd_p_aid3>, profileState disabled, profileNickname #NICKNAME3, serviceProviderName #SP_NAME3, profileName #NAME_OP_PROF3, iconType png, icon #ICON_OP_PROF3, profileClass operational }</isd_p_aid3></pre>
PROFILE_INFO4 (ProfileInfo)	<pre>{ iccid #ICCID_OP_PROF4, isdpAid <isd_p_aid4>, profileState disabled, serviceProviderName #SP_NAME4, profileName #NAME_OP_PROF4, iconType png, icon #ICON_OP_PROF4, profileClass operational }</isd_p_aid4></pre>
PROFILE_INFO4_ENABLED (ProfileInfo)	<pre>{ iccid #ICCID_OP_PROF4, isdpAid <isd_p_aid4>, profileState enabled, serviceProviderName #SP_NAME4, profileName #NAME_OP_PROF4, iconType png, icon #ICON_OP_PROF4, profileClass operational }</isd_p_aid4></pre>
PROFILES_INFO_ICCID_TAGLIST 1	{profileState enabled}

V1.4 Page 720 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

(ProfileInfo)	
PROFILES_INFO_ICCID_TAGLIST 2 (ProfileInfo)	{iconType png}
PROFILES_INFO_ICCID_TAGLIST 3 (ProfileInfo)	{profileClass operational }
PROFILES_INFO_ICCID_TAGLIST 4 (ProfileInfo)	notificationConfigurationInfo from #METADATA_OP_PROF1
PROFILES_INFO_ICCID_TAGLIST 5 (ProfileInfo)	profilePolicyRules from #METADATA_OP_PROF3
PROFILES_INFO_TAGLIST_ICCID (ProfileInfo)	{iccid #ICCID_OP_PROF1}, {iccid #ICCID_OP_PROF2}, {iccid #ICCID_OP_PROF3}
PROFILES_INFO_TAGLIST_ICON (ProfileInfo)	<pre>{icon #ICON_OP_PROF1}, {icon #ICON_OP_PROF2}, {icon #ICON_OP_PROF3}</pre>
PROFILES_INFO_TAGLIST_ISDPA ID (ProfileInfo)	<pre>{isdpAid <isd_p_aid1>}, {isdpAid <isd_p_aid2>}, {isdpAid <isd_p_aid3>}</isd_p_aid3></isd_p_aid2></isd_p_aid1></pre>
PROFILES_INFO_TAGLIST_PROFI LE_NAME (ProfileInfo)	{profileName #NAME_OP_PROF1}, {profileName #NAME_OP_PROF2}, {profileName #NAME_OP_PROF3}
PROFILES_INFO_TAGLIST_PROFI LE_NICKNAME (ProfileInfo)	{profileNickname #NICKNAME3}
PROFILES_INFO_TAGLIST_PROFI LE_OWNER (ProfileInfo)	<pre>{profileOwner #OWNER_OP_PROF1}, {profileOwner #OWNER_OP_PROF2}, {profileOwner #OWNER_OP_PROF2}</pre>
PROFILES_INFO_TAGLIST_SMDP _PROP_DATA (ProfileInfo)	{dpProprietaryData #SMDP_PROP_DATA1}
PROFILES_INFO_TAGLIST_SP_N AME (ProfileInfo)	{serviceProviderName #SP_NAME1}, {serviceProviderName #SP_NAME2}, {serviceProviderName #SP_NAME3}

V1.4 Page 721 of 777

Non-confidential

```
iccid #ICCID_OP_PROF1,
                                profileState enabled
                               },
PROFILES_INFO_TAGLIST1
                                iccid #ICCID OP PROF2,
                                profileState disabled
(ProfileInfo)
                                 iccid #ICCID_OP_PROF3,
                                profileState disabled
                                profileState enabled
                              {
PROFILES_INFO_TAGLIST2
                                profileState disabled
(ProfileInfo)
                              {
                                  profileState disabled,
                                  profileNickname #NICKNAME3
                                iconType png,
                                icon #ICON_OP_PROF1
PROFILES_INFO_TAGLIST3
                                iconType png,
                                icon #ICON_OP_PROF2
(ProfileInfo)
                               },
                                iconType png,
                                icon #ICON_OP_PROF3
                                  profileState enabled,
                                  icon #ICON_OP_PROF1
                              },
PROFILES_INFO_TAGLIST4
                                 profileState disabled,
                                  icon #ICON_OP_PROF2
(ProfileInfo)
                              },
                              {
                                  profileState disabled,
                                  icon #ICON_OP_PROF3
```

V1.4 Page 722 of 777

```
resp AuthenticateServerResponse ::=
                             authenticateResponseOk : {
                               euiccSigned1 {
                                 transactionId <S TRANSACTION ID>,
                                 serverAddress #TEST DP ADDRESS1,
                                 serverChallenge <S SMDP CHALLENGE>,
                                 euiccInfo2 #R EUICC INFO2, -- check only that
                             the field is present and has a valid TLV asn.1
R_AUTH_SMDP_MATCH_ID
                             structure
                                 ctxParams1 #CTX PARAMS1 MATCH ID
                               euiccSignature1 <EUICC SIGNATURE1>,
                               euiccCertificate #CERT EUICC ECDSA,
                               eumCertificate #CERT EUM ECDSA
                             resp AuthenticateServerResponse ::=
                             authenticateResponseOk : {
                               euiccSigned1 {
                                 transactionId <S TRANSACTION ID>,
                                 serverAddress #TEST DP ADDRESS1,
                                 serverChallenge <S SMDP CHALLENGE>,
                                 euiccInfo2 #R_EUICC_INFO2, -- check only that
                             the field is present and has a valid TLV asn.1
R_AUTH_SMDP_IMEI
                             structure
                                 ctxParams1 #CTX PARAMS1 IMEI
                               },
                               euiccSignature1 <EUICC SIGNATURE1>,
                               euiccCertificate #CERT EUICC ECDSA,
                               eumCertificate #CERT EUM ECDSA
                             resp AuthenticateServerResponse ::=
                             authenticateResponseError : {
                               transactionId <S TRANSACTION ID>,
R_AUTH_SERVER_INV_CERT
                               authenticateErrorCode invalidCertificate
                             resp AuthenticateServerResponse ::=
                             authenticateResponseError : {
                               transactionId <S TRANSACTION ID>,
R_AUTH_SERVER_INV_SIGN
                               authenticateErrorCode invalidSignature
                             resp AuthenticateServerResponse ::=
                             authenticateResponseError : {
                               transactionId <S TRANSACTION ID>,
R_AUTH_SERVER_INV_CURV
                               authenticateErrorCode unsupportedCurve
                             resp AuthenticateServerResponse ::=
                             authenticateResponseError : {
R_AUTH_SERVER_INV_CHALLEN
                               transactionId <S TRANSACTION ID>,
                               authenticateErrorCode euiccChallengeMismatch
```

V1.4 Page 723 of 777

```
resp AuthenticateServerResponse ::=
                             authenticateResponseError : {
                               transactionId <S TRANSACTION ID>,
R_AUTH_SERVER_INV_CI
                               authenticateErrorCode ciPKUnknown
                             resp AuthenticateServerResponse ::=
                             authenticateResponseError : {
                               transactionId <S TRANSACTION ID>,
R_AUTH_SERVER_INV_OID
                               authenticateErrorCode invalidOid
                             resp AuthenticateServerResponse ::=
                             authenticateResponseError : {
                               transactionId <S TRANSACTION ID>,
R_AUTH_SERVER_NO_SESSION
                               authenticateErrorCode noSessionContext
                             resp AuthenticateServerResponse ::=
                             authenticateResponseOk : {
                               euiccSigned1 {
                                 transactionId <S TRANSACTION ID>,
                                 serverAddress #TEST ROOT DS ADDRESS,
                                 serverChallenge <S SMDS CHALLENGE>,
                                 euiccInfo2 #R EUICC INFO2, -- check only that
                             the field is present and has a valid TLV asn.1
R_AUTH_SMDS_IMEI
                             structure
                                 ctxParams1 #CTX PARAMS1 EVENT ID IMEI
                               euiccSignature1 <EUICC SIGNATURE1>,
                               euiccCertificate #CERT EUICC ECDSA,
                               eumCertificate #CERT EUM ECDSA
                             resp AuthenticateServerResponse ::=
                             authenticateResponseOk: {
                               euiccSigned1 #EUICC SIGNED1,
                               euiccSignature1 <EUICC SIGNATURE1>,
R_AUTHENTICATE_SMDP
                               euiccCertificate #CERT EUICC ECDSA,
                               eumCertificate #CERT EUM ECDSA
                             resp AuthenticateServerResponse ::=
                             authenticateResponseOk: {
                               euiccSigned1 {
                                 transactionId <S_TRANSACTION_ID>,
                                 serverAddress #TEST ROOT DS ADDRESS,
                                 serverChallenge <S SMDS CHALLENGE>,
                                 euiccInfo2 #R EUICC INFO2, -- check only that
R_AUTHENTICATE_SMDS
                             the field is present and has a valid TLV asn.1
                                 ctxParams1 #CTX_PARAMS1_EVENT_ID
                               },
                               euiccSignature1 <EUICC SIGNATURE1>,
                               euiccCertificate #CERT EUICC ECDSA,
                               eumCertificate #CERT EUM ECDSA
```

V1.4 Page 724 of 777

```
R_CANCEL_SESSION_INV_TRAN
                             resp CancelSessionResponse ::=
SID
                             cancelSessionResponseError : invalidTransactionId
                             resp CancelSessionResponse ::=
                             cancelSessionResponseOk : {
                               euiccCancelSessionSigned {
                                 transactionId <S_TRANSACTION_ID>,
                                 smdpOid #S_SM_DP+_OID,
R_CANCEL_SESSION_METADATA
                                 reason metadataMismatch
                               euiccCancelSessionSignature <EUICC CS SIGNATURE>
                             resp CancelSessionResponse ::=
                             cancelSessionResponseOk : {
                               euiccCancelSessionSigned {
                                 transactionId <S TRANSACTION ID>,
R_CANCEL_SESSION_REJ
                                 smdpOid #S SM DP+ OID,
                                 reason endUserRejection
                               },
                               euiccCancelSessionSignature <EUICC_CS_SIGNATURE>
                             resp CancelSessionResponse ::=
                             cancelSessionResponseOk : {
                               euiccCancelSessionSigned {
                                 transactionId <S TRANSACTION ID>,
R_CANCEL_SESSION_POSTPON
                                 smdpOid #S_SM_DP+_OID,
ED
                                 reason postponed
                               },
                               euiccCancelSessionSignature <EUICC CS SIGNATURE>
                             resp CancelSessionResponse ::=
                             cancelSessionResponseOk {
                               euiccCancelSessionSigned {
                                 transactionId <S TRANSACTION ID>,
                                 smdpOid #S SM DP+ OID,
R_CANCEL_SESSION_TIMEOUT
                                 reason timeout
                               },
                               euiccCancelSessionSignature <EUICC CS SIGNATURE>
                             resp CancelSessionResponse ::=
                             cancelSessionResponseOk : {
                               euiccCancelSessionSigned {
                                 transactionId <S TRANSACTION ID>,
                                 smdpOid #S SM DP+ OID,
R_CANCEL_SESSION_PPR
                                 reason pprNotAllowed
                               },
                               euiccCancelSessionSignature <EUICC CS SIGNATURE>
```

V1.4 Page 725 of 777

```
resp CancelSessionResponse ::=
                             cancelSessionResponseOk : {
                               euiccCancelSessionSigned {
                                 transactionId <S TRANSACTION ID>,
R_CANCEL_SESSION_LOAD_BPP
                                 smdpOid #S_SM_DP+_OID,
                                 reason loadBppExecutionError
                               },
                               euiccCancelSessionSignature <EUICC CS SIGNATURE>
                             resp CancelSessionResponse ::=
                             cancelSessionResponseOk : {
                               euiccCancelSessionSigned {
                                 transactionId <S TRANSACTION ID>,
R_CANCEL_SESSION_UNDEF
                                 smdpOid #S SM DP+ OID,
                                 reason undefinedReason
                               },
                               euiccCancelSessionSignature <EUICC CS SIGNATURE>
                             response GetEuiccChallengeResponse ::=
R_CHALLENGE
                               euiccChallenge <EUICC_CHALLENGE>
                             resp ProfileInfoListResponse ::=
                               profileInfoListOk :{
                                   isdpAid <ISD P AID>,
                                   dpProprietaryData {
                                     dpOid #S_SM_DP+_OID,
                                     additionalSmdpData
                                     #ADDITIONAL SMDP DATA MAX LENGTH
                                 }
                             }
R_CONF_OP_PROF1
                             -- NOTE: Instead of
                             DpProprietaryData ::= SEQUENCE {
                               dpOid OBJECT IDENTIFIER
                               -- additional data objects defined by the
                               -- SM-DP+ MAY follow
                             -- the following structure is used to test the
                             -- DpProprietaryData size:
                             DpProprietaryData ::= SEQUENCE {
                               dpOid OBJECT IDENTIFIER,
                               additionalSmdpData OCTET STRING OPTIONAL
                             response GetRatResponse ::= {
                               rat {
R_DEFAULT_RAT
                                 #PPRS ALLOWED
                               }
                             }
```

V1.4 Page 726 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

```
respDelProf DeleteProfileResponse ::= {
R_DELETE_PROFILE_DISALLOW
                               deleteResult disallowedByPolicy
EDBYPOLICY
                             respDelProf DeleteProfileResponse ::= {
R_DELETE_PROFILE_NOTDISABL
                               deleteResult profileNotInDisabledState
ESTATE
                             respDelProf DeleteProfileResponse ::= {
                               deleteResult ok
R_DELETE_PROFILE_OK
                             resp DeleteProfileResponse ::= {
R_DELETE_PROFILE_ICCID_ISDP
                               deleteResult iccidOrAidNotFound
NOTFOUND
                             resp DisableProfileResponse ::= {
R_DISABLE_PROFILE_DISALLOW
                               disableResult disallowedByPolicy
EDbyPOLICY
                             resp DisableProfileResponse ::= {
R_DISABLE_PROFILE_ICCID_ISD
                               disableResult iccidOrAidNotFound
P NOTFOUND
                             resp DisableProfileResponse ::= {
R_DISABLE_PROFILE_NOT_ENAB
                               disableResult profileNotInEnabledState
LE STATE
                             resp DisableProfileResponse ::= {
                               disableResult ok
R_DISABLE_PROFILE_OK
                             respEnaPro EnableProfileResponse ::= {
R_ENABLE_PROFILE_ICCID_ISDP
                               enableResult iccidOrAidNotFound
NOTFOUND
                             respEnaPro EnableProfileResponse ::= {
R_ENABLE_PROFILE_NOT_DISAB
                               enableResult profileNotInDisabledState
LE STATE
                             respEnaPro EnableProfileResponse ::= {
R_ENABLE_PROFILE_DISALLOW
                               enableResult disallowedByPolicy
EDbyPOLICY
                             resp EnableProfileResponse ::= {
                               enableResult ok
R_ENABLE_PROFILE_OK
                             response EuiccConfiguredAddressesResponse ::= {
                               -- defaultDpAddress SHALL not be present
R_ES10a_GECA_DS
                               rootDsAddress #TEST ROOT DS ADDRESS
```

V1.4 Page 727 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

```
response EuiccConfiguredAddressesResponse ::= {
                               defaultDpAddress #TEST DP ADDRESS1,
R_ES10a_GECA_DS_DP_1
                               rootDsAddress #TEST_ROOT_DS ADDRESS
                             response EuiccConfiguredAddressesResponse ::= {
                               defaultDpAddress #TEST DP ADDRESS2,
R_ES10a_GECA_DS_DP_2
                               rootDsAddress #TEST ROOT DS ADDRESS
                             response SetDefaultDpAddressResponse::= {
                               setDefaultDpAddressResult ok
R_ES10a_SD_DP_A_OK
                             response EUICCInfo1::=
                               svn #RSP SVN H, -- for device testing, check only
                             that the field is present and has a valid TLV asn.1
                             structure
R_EUICC_INFO1
                               euiccCiPKIdListForVerification
                                 <EUICC CI PK ID LIST FOR VERIFICATION>,
                               euiccCiPKIdListForSigning
                                 <EUICC CI PK ID LIST FOR SIGNING>
                             response EUICCInfo2::=
                               profileVersion #IUT SIMA VERSION,
                               svn #RSP SVN H,
                               euiccFirmwareVer #IUT EUICC FIRMWARE VER,
                               extCardResource <EXT CARD RESOURCE>,
                               uiccCapability #IUT UICC CAPABILITY,
                               ts102241Version #IUT_TS102241_VERSION,
                               globalplatformVersion
                               #IUT GLOBALPLATFORM VERSION,
                               rspCapability <EUICC RSP CAPABILITY>,
                               euiccCiPKIdListForVerification
                               <EUICC_CI_PK_ID_LIST_FOR_VERIFICATION>,
R_EUICC_INFO2
                               euiccCiPKIdListForSigning
                               <EUICC CI PK ID LIST FOR SIGNING>,
                               euiccCategory #IUT EUICC CATEGORY, -- OPTIONAL
                               forbiddenProfilePolicyRules <PPR IDS>, --
                             OPTIONAL
                               ppVersion #IUT_PP_VERSION,
                               sasAcreditationNumber
                             #IUT SAS ACCREDITATION NUMBER,
                               certificationDataObject {
                                 platformLabel #IUT PLATFORM LABEL,
                                 discoveryBaseURL #IUT DLOA URL
                               }-- OPTIONAL
                             resp EuiccMemoryResetResponse ::= {
                               resetResult ok
R_EUICC_MEMORY_RESET_OK
```

V1.4 Page 728 of 777

```
resp ProfileInfoListResponse ::=
                               profileInfoListOk :{
                                     serviceProviderName #SP NAME1,
                                    profileName #NAME OP PROF1,
R_GET_UPDATE_N1
                                    iconType png,
                                     icon #ICON OP PROF1,
                                     profilePolicyRules { ppr2 }
                              }
                              resp ProfileInfoListResponse ::=
                               profileInfoListOk :{
                                    serviceProviderName #SP NAME1,
                                    profileName #NAME OP PROF1,
R_GET_UPDATE_N2
                                    iconType jpg,
                                     icon #ICON JPG,
                                     profilePolicyRules { ppr1 }
                              }
                              resp ProfileInfoListResponse ::=
                               profileInfoListOk :{
                                 {
                                     serviceProviderName #SP NAME2,
                                    profileName #NAME OP PROF2,
R_GET_UPDATE_N3
                                     iconType png,
                                     icon #ICON OP PROF1
                                     -- profilePolicyRules SHALL not be present
                                  }
                              }
                              resp ProfileInfoListResponse ::=
                                profileInfoListOk :{
                                     -- serviceProviderName SHALL not be present
                                     -- profileName SHALL not be present
R_GET_UPDATE_N4
                                     iconType png,
                                     icon #ICON OP PROF1
                                     -- profilePolicyRules SHALL not be present
                              resp ProfileInfoListResponse ::=
                               profileInfoListOk :{
                                    serviceProviderName #SP NAME2,
                                    profileName #NAME OP PROF2,
R_GET_UPDATE_N6
                                    iconType png,
                                    icon #ICON OP PROF1
                                     -- profilePolicyRules SHALL not be present
                              }
```

V1.4 Page 729 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

```
response ListNotificationResponse ::=
                              notificationMetadataList : {
                                #NOTIF METADATA DISABLE1,
R_LIST_NOTIF_DI1_EN2
                                #NOTIF METADATA ENABLE2
                              resp ProfileInfoListResponse ::=
                               profileInfoListOk :{
                                     serviceProviderName #SP NAME1,
                                    profileName #NAME OP PROF1,
R_METADATA_UNCHANGED
                                    iconType png,
                                    icon #ICON OP PROF1,
                                    profilePolicyRules {ppr1,ppr2}
                              }
                              resp ProfileInstallationResult ::= {
                               profileInstallationResultData {
                                 transactionId <S TRANSACTION ID>,
                                 notificationMetadata {
                                   seqNumber <SEQ NUMBER>,
                                   profileManagementOperation {
                                     notificationInstall
                                   notificationAddress #TEST DP ADDRESS1,
R_PIR_DATA_MISMATCH
                                  },
                                  smdpOid #S SM DP+ OID,
                                  finalResult errorResult : {
                                   bppCommandId loadProfileElements,
                                   errorReason installFailedDueToDataMismatch,
                                 }
                               },
                               euiccSignPIR <EUICC SIGN PIR>
                              response ProfileInstallationResult ::= {
                               profileInstallationResultData {
                                 transactionId <S TRANSACTION ID>,
                                 notificationMetadata {
                                   seqNumber <SEQ NUMBER>,
                                   profileManagementOperation {
                                     notificationInstall
                                   notificationAddress #TEST DP ADDRESS1,
                                   iccid #ICCID_OP_PROF9
R_PIR_OK_PROF9
                                  },
                                  smdpOid #S SM DP+ OID,
                                  finalResult successResult : {
                                   aid <ISD P AID>,
                                   simaResponse #SIMA RESULT OK
                               },
                               euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 730 of 777

```
resp ProfileInstallationResult ::= {
                               profileInstallationResultData {
                                 transactionId <S TRANSACTION ID>,
                                 notificationMetadata {
                                   seqNumber <SEQ_NUMBER>,
                                   profileManagementOperation {
                                     notificationInstall
                                   },
                                   notificationAddress #TEST_DP_ADDRESS1,
R_PIR_PPR_NOT_ALLOWED
                                  },
                                  smdpOid #S SM DP+ OID,
                                  finalResult errorResult : {
                                   bppCommandId storeMetadata,
                                   errorReason pprNotAllowed
                                 }
                               },
                               euiccSignPIR <EUICC SIGN PIR>
                              resp ProfileInfoListResponse ::=
                               profileInfoListOk :{
                                 {
                                     iccid #ICCID_OP_PROF1,
                                    serviceProviderName #SP NAME1,
                                    profileName #NAME OP PROF1,
                                    iconType png,
                                    icon #ICON OP PROF1,
                                    profileClass operational,
                                    notificationConfigurationInfo {
                                       { profileManagementOperation {
                                           notificationInstall,
R_GET_METADATA_OP_PROF1
                                          notificationEnable,
                                          notificationDisable,
                                          notificationDelete
                                         notificationAddress #TEST DP ADDRESS1
                                       }
                                     },
                                     profileOwner {
                                      mccMnc #MCC MNC1
                                    profilePolicyRules {ppr1}
                                  }
                             }
```

V1.4 Page 731 of 777

```
resp ProfileInfoListResponse ::=
                                profileInfoListOk :{
                                    iccid #ICCID OP PROF1,
                                    notificationConfigurationInfo {
                                      { profileManagementOperation {
                                          notificationInstall
                                        },
                                        notificationAddress #TEST_DP_ADDRESS3
                                      },
                                      { profileManagementOperation {
                                          notificationInstall
                                       notificationAddress #TEST_DP ADDRESS2
                                      },
                                      { profileManagementOperation {
                                          notificationEnable
                                       notificationAddress #TEST DP ADDRESS2
                                      } ,
                                      { profileManagementOperation {
                                          notificationEnable
                                        notificationAddress #TEST DP ADDRESS3
R_GET_PROF_NOTIF_CONF
                                      },
                                      { profileManagementOperation {
                                         notificationDisable
                                       notificationAddress #TEST DP ADDRESS3
                                      { profileManagementOperation {
                                          notificationDisable
                                        notificationAddress #TEST DP ADDRESS4
                                      },
                                      { profileManagementOperation {
                                          notificationDelete
                                       notificationAddress #TEST_DP_ADDRESS1
                                      { profileManagementOperation {
                                          notificationDelete
                                      notificationAddress #TEST DP ADDRESS3
                                  }
                                }
                              resp ISDRProprietaryApplicationTemplate::= {
                               svn #RSP_SVN_H
R_ISDR_SELECTION
                              response ListNotificationResponse ::=
                             notificationMetadataList : {
R_LIST_NOTIF_DE1
                               #NOTIF METADATA DELETE1
```

V1.4 Page 732 of 777

```
response ListNotificationResponse ::=
                              notificationMetadataList : {
                                #NOTIF METADATA DELETE1,
R_LIST_NOTIF_DE1_DE1
                                #NOTIF METADATA2 DELETE1
                              response ListNotificationResponse ::=
                              notificationMetadataList : {
R_LIST_NOTIF_DI1
                                #NOTIF_METADATA_DISABLE1
                              response ListNotificationResponse ::=
                              notificationMetadataList : {
                                #NOTIF METADATA DISABLE1,
R_LIST_NOTIF_DI1_DE1
                                #NOTIF METADATA DELETE1
                              response ListNotificationResponse ::=
                              notificationMetadataList : {
                                #NOTIF METADATA DISABLE1,
R_LIST_NOTIF_DI1_DI1
                                #NOTIF METADATA2 DISABLE1
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
R_LIST_NOTIF_EN1
                                #NOTIF METADATA ENABLE1
                              response ListNotificationResponse ::=
                              notificationMetadataList : {
                                #NOTIF METADATA ENABLE1,
R_LIST_NOTIF_EN1_EN1
                                #NOTIF METADATA2 ENABLE1
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
R_LIST_NOTIF_IN1
                                #NOTIF METADATA INSTALL1
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
                                #NOTIF METADATA INSTALL1,
R_LIST_NOTIF_IN1_IN1_PIR
                                #NOTIF METADATA INSTALL1 PIR
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
R_LIST_NOTIF_IN1_PIR
                                #NOTIF METADATA INSTALL1 PIR
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
R_LIST_NOTIF_IN1_EN1
                                #NOTIF METADATA INSTALL1,
                                #NOTIF METADATA ENABLE1
```

V1.4 Page 733 of 777

```
response ListNotificationResponse ::=
                              notificationMetadataList: {
                                #NOTIF METADATA INSTALL1 PIR,
R_LIST_NOTIF_IN1_PIR_EN1
                                #NOTIF METADATA ENABLE1
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
R_LIST_NOTIF_IN2_PIR
                                #NOTIF_METADATA_INSTALL2_PIR
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
                                #NOTIF METADATA INSTALL2 PIR,
R_LIST_NOTIF_IN2_PIR_IN2
                                #NOTIF METADATA INSTALL2
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
                                #NOTIF_METADATA_INSTALL1_PIR,
R_LIST_NOTIF_IN1_PIR_IN2_PIR
                                #NOTIF_METADATA_INSTALL2_PIR
                              response ListNotificationResponse ::=
R_LIST_NOTIF_NONE
                                notificationMetadataList: {}
R_LIST_NOTIF_UNDEFINED_ERR
                              response ListNotificationResponse ::=
                              listNotificationsResultError : undefinedError
                              response ListNotificationResponse ::=
                              notificationMetadataList: {
R_LIST_NOTIF_EN1_IN2_PIR
                                #NOTIF METADATA ENABLE1,
                                #NOTIF METADATA INSTALL2 PIR
                              }
                              resp ProfileInstallationResult ::= {
                                profileInstallationResultData {
                                  transactionId <S TRANSACTION ID>,
                                  notificationMetadata {
                                    seqNumber <SEQ NUMBER>,
                                    profileManagementOperation {
                                      notificationInstall
                                    notificationAddress #TEST_DP_ADDRESS1,
                                    iccid #ICCID OP PROF1
R_PIR_ICCID_ALREADY_EXIST
                                  smdpOid #S SM DP+ OID,
                                  finalResult errorResult : {
                                    bppCommandId storeMetadata,
                                    errorReason
                                     installFailedDueToIccidAlreadyExistsOnEuicc
                                },
                                euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 734 of 777

```
resp ProfileInstallationResult ::= {
                                profileInstallationResultData {
                                  transactionId <S TRANSACTION ID>,
                                  notificationMetadata {
                                    seqNumber <SEQ NUMBER>,
                                    profileManagementOperation {
                                      notificationInstall
                                    },
                                    notificationAddress #TEST DP ADDRESS1
R_PIR_INVALID_CRT
                                  smdpOid #S_SM_DP+_OID,
                                  finalResult errorResult : {
                                    bppCommandId initialiseSecureChannel,
                                    errorReason unsupportedCrtValues
                                  }
                                },
                                euiccSignPIR <EUICC SIGN PIR>
                              resp ProfileInstallationResult ::= {
                                profileInstallationResultData {
                                  transactionId <S TRANSACTION ID>,
                                  notificationMetadata {
                                    seqNumber <SEQ_NUMBER>,
                                    profileManagementOperation {
                                      notificationInstall
                                    },
                                    notificationAddress #TEST DP ADDRESS1
R_PIR_INVALID_DATA
                                  },
                                  smdpOid #S SM DP+ OID,
                                  finalResult errorResult : {
                                    bppCommandId configureISDP,
                                    errorReason incorrectInputValues
                                  }
                                },
                                euiccSignPIR <EUICC SIGN PIR>
                              resp ProfileInstallationResult ::= {
                                profileInstallationResultData {
                                  transactionId <S TRANSACTION ID>,
                                  notificationMetadata {
                                    seqNumber <SEQ NUMBER>,
                                    profileManagementOperation {
                                      notificationInstall
                                    },
                                    notificationAddress #TEST DP ADDRESS1
R_PIR_INVALID_OP_ID
                                  },
                                  smdpOid #S SM DP+ OID,
                                  finalResult errorResult : {
                                    bppCommandId initialiseSecureChannel,
                                    \verb|errorReason| unsupportedRemoteOperationType|
                                  }
                                euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 735 of 777

```
resp ProfileInstallationResult ::= {
                               profileInstallationResultData {
                                 transactionId <S TRANSACTION ID>,
                                 notificationMetadata {
                                    seqNumber <SEQ NUMBER>,
                                    profileManagementOperation {
                                     notificationInstall
                                   },
                                   notificationAddress #TEST DP ADDRESS1
R_PIR_INVALID_SIGN
                                  },
                                  smdpOid #S_SM_DP+_OID,
                                  finalResult errorResult : {
                                   bppCommandId initialiseSecureChannel,
                                    errorReason invalidSignature
                                },
                                euiccSignPIR <EUICC SIGN PIR>
                              resp ProfileInstallationResult ::= {
                               profileInstallationResultData {
                                  transactionId <INVALID_TRANSACTION_ID>,
                                  notificationMetadata {
                                    seqNumber <SEQ NUMBER>,
                                    profileManagementOperation {
                                     notificationInstall
                                    },
                                   notificationAddress #TEST_DP_ADDRESS1
R_PIR_INVALID_TRANS_ID
                                  },
                                  smdpOid #S SM DP+ OID,
                                  finalResult errorResult : {
                                    bppCommandId initialiseSecureChannel,
                                    errorReason invalidTransactionId
                                  }
                                euiccSignPIR <EUICC_SIGN_PIR>
```

V1.4 Page 736 of 777

```
resp ProfileInstallationResult ::= {
                                profileInstallationResultData {
                                  transactionId <S TRANSACTION ID>,
                                  notificationMetadata {
                                    seqNumber <SEQ NUMBER>,
                                    profileManagementOperation {
                                      notificationInstall
                                    },
                                    notificationAddress #TEST DP ADDRESS1,
R_PIR_METADATA_INVALID
                                  smdpOid #S_SM_DP+_OID,
                                  finalResult errorResult : {
                                    bppCommandId storeMetadata,
                                    errorReason
                                      scp03tStructureError
                                      OR
                                      incorrectInputValues
                                  }
                                },
                                euiccSignPIR <EUICC SIGN PIR>
                              response ProfileInstallationResult ::= {
                                profileInstallationResultData {
                                  transactionId <S_TRANSACTION_ID>,
                                  notificationMetadata {
                                    seqNumber <SEQ NUMBER>,
                                    profileManagementOperation {
                                      notificationInstall
                                    notificationAddress #TEST DP ADDRESS1,
                                    iccid #ICCID OP PROF1
R_PIR_OK
                                  },
                                  smdpOid #S_SM_DP+_OID,
                                  finalResult successResult : {
                                    aid <ISD_P_AID>,
                                    simaResponse #SIMA_RESULT_OK
                                  }
                                },
                                euiccSignPIR <EUICC SIGN PIR>
                              resp ProfileInstallationResult ::= {
                                profileInstallationResultData {
                                  finalResult errorResult : {
                                    bppCommandId replaceSessionKeys,
                                    errorReason
                                      incorrectInputValues
R_PIR_PPK_INV
                                      scp03tStructureError
                                      scp03tSecurityError
                                  }
                                },
                                euiccSignPIR <EUICC SIGN PIR>
```

V1.4 Page 737 of 777

```
resp ProfileInstallationResult ::= {
                               profileInstallationResultData {
                                 transactionId <S TRANSACTION ID>,
                                 smdpOid #S SM DP+ OID,
                                 finalResult errorResult : {
                                   bppCommandId loadProfileElements,
                                   errorReason incorrectInputValues
R_PIR_SECU_INVALID
                                     scp03tStructureError
                                     scp03tSecurityError
                                 }
                               },
                               euiccSignPIR <EUICC SIGN PIR>
                             resp PrepareDownloadResponse ::=
                             downloadResponseError : {
                               transactionId <S TRANSACTION ID>,
R_PREP_DOWN_INV_CURVE
                               downloadErrorCode unsupportedCurve
                             }
                             resp PrepareDownloadResponse ::=
                             downloadResponseError : {
                               transactionId <INVALID TRANSACTION ID>,
R_PREP_DOWN_INV_TRANS_ID
                               downloadErrorCode invalidTransactionId
                             resp PrepareDownloadResponse ::=
                             downloadResponseError : {
R_PREP_DOWN_NO_SESSION
                               transactionId <S TRANSACTION ID>,
                               downloadErrorCode noSessionContext
                             resp PrepareDownloadResponse ::=
                             downloadResponseError : {
                               transactionId <S TRANSACTION ID>,
R_PREP_DOWNLOAD_INV_CERT
                               downloadErrorCode invalidCertificate
                             resp PrepareDownloadResponse ::=
                             downloadResponseError : {
                               transactionId <S TRANSACTION ID>,
R_PREP_DOWNLOAD_INV_SIGN
                               downloadErrorCode invalidSignature
                             resp PrepareDownloadResponse ::= downloadResponseOk
                             : {
                               euiccSigned2 {
                                 transactionId <S TRANSACTION ID>,
R PREP DOWNLOAD NO CC
                                 euiccOtpk <OTPK EUICC ECKA>
                               },
                               euiccSignature2 <EUICC SIGNATURE2>
```

V1.4 Page 738 of 777

```
resp PrepareDownloadResponse ::= downloadResponseOk
                             : {
                               euiccSigned2 {
                                 transactionId <S TRANSACTION ID>,
R_PREP_DOWNLOAD_WITH_CC
                                 euiccOtpk <OTPK EUICC ECKA>,
                                 hashCc <S HASHED CC>
                               },
                               euiccSignature2 <EUICC SIGNATURE2>
                             response GetRatResponse ::= {
                               rat {
                                 #PPR1 WITH OWNER GID,
                                  #PPR1 WITHOUT GID,
R_RAT_WITH_OTHER_RULES
                                  #PPR2 WITHOUT CONSENT,
                                  #PPRS ALLOWED
                               }
                             }
                              response NotificationSentResponse ::= {
R_REMOVE_NOTIF_NOTHING_TO
                               deleteNotificationStatus nothingToDelete
_DELETE
                             response NotificationSentResponse ::= {
R_REMOVE_NOTIF_OK
                               deleteNotificationStatus ok
                             resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               profileInstallationResult : {
                                 profileInstallationResultData {
                                   transactionId <S TRANSACTION ID>,
                                   notificationMetadata
                              #NOTIF METADATA INSTALL1 PIR,
                                   smdpOid #S_SM_DP+_OID,
                                    finalResult successResult : {
                                     aid <ISD P AID>,
                                     simaResponse #SIMA RESULT OK
R_RETRIEVE_NOTIF_IN1_IN1_PIR
                                 },
                                 euiccSignPIR <EUICC SIGN PIR>
                               },
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF METADATA INSTALL1,
                                 euiccNotificationSignature
                             <TBS_EUICC_NOTIF_SIG>,
                                 euiccCertificate #CERT_EUICC_ECDSA,
                                  eumCertificate #CERT EUM ECDSA
                              }
                             }
```

V1.4 Page 739 of 777

```
resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               profileInstallationResult : {
                                  profileInstallationResultData {
                                    transactionId <S TRANSACTION ID>,
                                    notificationMetadata
                              #NOTIF METADATA INSTALL1 PIR,
                                    smdpOid #S SM DP+ OID,
R_RETRIEVE_NOTIF_IN1_PIR
                                    finalResult successResult : {
                                      aid <ISD_P_AID>,
                                      simaResponse #SIMA_RESULT_OK
                                  euiccSignPIR <EUICC SIGN PIR>
                                }
                              }
                             resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               otherSignedNotification : {
                                  tbsOtherNotification #NOTIF_METADATA_INSTALL1,
                                 euiccNotificationSignature
R RETRIEVE NOTIF IN1
                              <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                  eumCertificate #CERT EUM ECDSA
                                }
                              }
                             resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               otherSignedNotification : {
                                  tbsOtherNotification #NOTIF METADATA ENABLE1,
                                 euiccNotificationSignature
R RETRIEVE NOTIF EN1
                              <TBS_EUICC_NOTIF_SIG>,
                                 euiccCertificate #CERT_EUICC_ECDSA,
                                 eumCertificate #CERT EUM ECDSA
                              }
                              resp RetrieveNotificationsListResponse ::=
                                notificationList : {
                               profileInstallationResult : {
                                 profileInstallationResultData {
                                    transactionId <S TRANSACTION ID>,
                                    notificationMetadata
                              #NOTIF METADATA INSTALL2 PIR,
                                    smdpOid #S SM DP+ OID2,
R_RETRIEVE_NOTIF_IN2_PIR
                                    finalResult successResult : {
                                      aid <ISD P AID>,
                                      simaResponse #SIMA_RESULT_OK
                                  },
                                  euiccSignPIR <EUICC SIGN PIR>
                                }
                              }
```

V1.4 Page 740 of 777

```
resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF METADATA DISABLE1,
                                 euiccNotificationSignature
R_RETRIEVE_NOTIF_DI1
                             <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                 eumCertificate #CERT_EUM_ECDSA
                               }
                             }
                             resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF METADATA DELETE1,
                                 euiccNotificationSignature
R_RETRIEVE_NOTIF_DE1
                             <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                 eumCertificate #CERT_EUM_ECDSA
                              }
                             resp RetrieveNotificationsListResponse ::=
R_RETRIEVE_NOTIF_NONE
                               notificationList : {}
                             resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               profileInstallationResult : {
                                 profileInstallationResultData {
                                   transactionId <S TRANSACTION ID>,
                                   notificationMetadata
                              #NOTIF METADATA INSTALL1 PIR,
                                   smdpOid #S SM DP+ OID,
                                    finalResult successResult : {
                                     aid <ISD_P_AID>,
                                     simaResponse #SIMA RESULT OK
R_RETRIEVE_NOTIF_IN1_PIR_EN
                                  },
                                 euiccSignPIR <EUICC SIGN PIR>
                               },
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF METADATA ENABLE1,
                                 euiccNotificationSignature
                             <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                 eumCertificate #CERT EUM ECDSA
                               }
```

V1.4 Page 741 of 777

```
resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               profileInstallationResult : {
                                 profileInstallationResultData {
                                    transactionId <S TRANSACTION ID>,
                                    notificationMetadata
                              #NOTIF METADATA INSTALL1 PIR,
                                    smdpOid #S SM DP+ OID,
                                    finalResult successResult : {
                                      aid <ISD P AID>,
                                      simaResponse #SIMA_RESULT_OK
                                  },
                                 euiccSignPIR <EUICC SIGN PIR>
R_RETRIEVE_NOTIF_IN1_PIR_IN2
_PIR
                               profileInstallationResult : {
                                 profileInstallationResultData {
                                    transactionId <S TRANSACTION ID>,
                                    notificationMetadata
                              #NOTIF_METADATA_INSTALL2_PIR,
                                    smdpOid #S SM DP+ OID2,
                                    finalResult successResult : {
                                      aid <ISD P AID>,
                                      simaResponse #SIMA RESULT OK
                                  },
                                  euiccSignPIR <EUICC SIGN PIR>
                                }
                              resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF_METADATA_DISABLE1,
                                 euiccNotificationSignature
                              <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                 eumCertificate #CERT EUM ECDSA
R_RETRIEVE_NOTIF_DI1_DE1
                               },
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF METADATA DELETE1,
                                 euiccNotificationSignature
                              <TBS EUICC NOTIF SIG>,
                                  euiccCertificate #CERT EUICC ECDSA,
                                  eumCertificate #CERT EUM ECDSA
                                }
```

V1.4 Page 742 of 777

```
resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF METADATA INSTALL1,
                                 euiccNotificationSignature
                             <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                 eumCertificate #CERT_EUM_ECDSA
R_RETRIEVE_NOTIF_IN1_EN1
                               otherSignedNotification : {
                                 tbsOtherNotification #NOTIF_METADATA_ENABLE1,
                                 euiccNotificationSignature
                              <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                 eumCertificate #CERT EUM ECDSA
                             resp RetrieveNotificationsListResponse ::=
                               notificationList : {
                               profileInstallationResult : {
                                 profileInstallationResultData {
                                   transactionId <S TRANSACTION ID>,
                                   notificationMetadata
                              #NOTIF METADATA INSTALL2 PIR,
                                   smdpOid #S SM DP+ OID2,
                                   finalResult successResult : {
                                     aid <ISD P AID>,
                                      simaResponse #SIMA RESULT OK
R_RETRIEVE_NOTIF_EN1_IN2_PI
                                 euiccSignPIR <EUICC SIGN PIR>
                               otherSignedNotification : {
                                 tbsOtherNotification#NOTIF_METADATA_ENABLE1,
                                 euiccNotificationSignature
                             <TBS EUICC NOTIF SIG>,
                                 euiccCertificate #CERT EUICC ECDSA,
                                 eumCertificate #CERT EUM ECDSA
                             }
SMDP_PROP_DATA1
                               dpOid #S_SM_DP+_OID
(DpProprietaryData)
```

D.4 APDU

D.4.1 APDU Commands

Name	Content
DELETE_SSD	- CLA = 80, INS = E4, P1 = 00, P2 = 80, LC = <l> - Data = 4F <l> #SSD_AID - LE = 00</l></l>

V1.4 Page 743 of 777

GET_RESPONSE	- CLA = 0x (x = <channel_number>), INS = C0, P1 = 00, P2 = 00, LE = <l></l></channel_number>
GET_MNO_SD	- CLA = 80, INS = F2, P1 = 80, P2 = 02, LC = <l> - Data = 4F 00 - LE = 00</l>
INSTALL_PERSO_RES_ISDP	- CLA = 80, INS = E6, P1 = 20, P2 = 00, LC = 16 - Data = 00 00 10 A0 00 00 05 59 10 10 FF FF FF FF 89 00 00 0F 00 00 00 00 - LE = 00
MANAGE_CHANNEL_OPEN	- CLA = 00, INS = 70, P1 = 00, P2 = 00, LE = 01
READ_BINARY	- CLA = 00, INS = B0, P1 = 00, P2 = 00, LE = <l></l>
SELECT_MF	- CLA = 00, INS = A4, P1 = 00, P2 = 04, LC = <l> - Data = 3F 00 - LE = 00</l>
SELECT_ICCID	- CLA = 00, INS = A4, P1 = 00, P2 = 0C, LC = 02 - Data = 2F E2
SELECT_USIM	- CLA = 00, INS = A4, P1 = 04, P2 = 04, LC = <l> - Data = #USIM_AID - LE = 00</l>
TERMINAL_CAPABILITY_LPAd	- CLA = 80, INS = AA, P1 = 00, P2 = 00, LC = <l> - Data = A9 05 81 00 83 01 07</l>
TERMINAL_PROFILE	- CLA = 80, INS = 10, P1 = 00, P2 = 00, LC = <l> - Data = FF FF FF FF 7F 9D 00 DF BF 00 00 1F E2 00 00 00 C7 EB 00 00 00 01 68 00 50 00 00 00 00 02 00</l>
TERMINAL_PROFILE_eUICCProfileStat eChanged	- CLA = 80, INS = 10, P1 = 00, P2 = 00, LC = <l> - Data = FF FF FF FF FF FF FF FF FF 03 02 FF FF 9F FF EF DF FF 0F FF 0F FF 0F FF 03 00 3F 7F FF 03 FF FF 20</l>

D.4.2 R-APDU Chaining

During the execution of all sequences related to the eUICC testing (i.e. section 4.2), for commands where the response exceeds 256 bytes, the chaining mechanism defined in ISO/IEC 7816-4 [7], using the 61XX status word and multiple GET RESPONSE commands, SHALL be used.

As an example, the following generic sequence, which describes this mechanism, SHALL apply.

Step	Direction	Sequence / Description	Result
1	OCE → eUICC	Send APDU command on logical channel x	<r_apdu_part1></r_apdu_part1>

V1.4 Page 744 of 777

			SW=0x61XX
2	OCE → eUICC	Send [GET_RESPONSE] on logical channel x with LE='XX'	<r_apdu_part2> SW=0x61XX</r_apdu_part2>
3	OCE → eUICC	Send [GET_RESPONSE] on logical channel x with LE='XX'	<r_apdu_part3> SW=0x61XX</r_apdu_part3>
4	OCE → eUICC	Send [GET_RESPONSE] on logical channel x with LE='XX'	<r_apdu_part4> SW=0x9000 The complete response is the result of the concatenation of all R-APDUs from <r_apdu_part1> to <r_apdu_part4></r_apdu_part4></r_apdu_part1></r_apdu_part4>

D.5 ES6 Requests And Responses

D.5.1 ES6 Requests

Name	Content
REMOVE_PPR1	<pre>metadataReq UpdateMetadataRequest ::= { profilePolicyRules {ppr2} }</pre>
UPD_ICON_REM_PPR2	<pre>metadataReq UpdateMetadataRequest ::= { iconType jpg, icon #ICON_JPG, profilePolicyRules {ppr1} }</pre>
UPD_NAMES_REM_PPRS	<pre>metadataReq UpdateMetadataRequest ::= { serviceProviderName #SP_NAME2, profileName #NAME_OP_PROF2, profilePolicyRules {} }</pre>
REMOVE_NAMES_PPRS	<pre>metadataReq UpdateMetadataRequest ::= { serviceProviderName "", profileName "", profilePolicyRules {} }</pre>
UPD_PPR_CONTROL	<pre>metadataReq UpdateMetadataRequest ::= { serviceProviderName #SP_NAME2, profileName #NAME_OP_PROF2, iconType jpg, icon #ICON_JPG, profilePolicyRules {pprUpdateControl, ppr1} }</pre>
UPD_NO_METADATA	<pre>metadataReq UpdateMetadataRequest ::= { }</pre>

V1.4 Page 745 of 777

```
metadataReq UpdateMetadataRequest ::= {
    serviceProviderName #SP_NAME2,
    profileName #NAME_OP_PROF2,
    icon #ICON_JPG,
    profilePolicyRules {}
}

metadataReq UpdateMetadataRequest ::= {
    serviceProviderName #SP_NAME2,
    profileName #NAME_OP_PROF2,
    iconType jpg,
    profilePolicyRules {}
}
```

D.6 ES11 Requests And Responses

D.6.1 ES11 Requests

Name	Content	
AUTH_SERVER_RESP_MATCHING_ID_EMPTY	resp authenticateServerResponse ::= authenticateResponseOk : { euiccSigned1 { transactionId <s_transaction_id>, serverAddress #IUT_SM_DS_ADDRESS, serverChallenge <smds_challenge>, euiccInfo2 #S_EUICC_INFO2, ctxParams1 #CTX_PARAMS1_MATCHING_ID_EMPTY }, euiccSignature1 <euicc_signature1>, euiccCertificate #CERT_EUICC_ECDSA,</euicc_signature1></smds_challenge></s_transaction_id>	
	eumCertificate #CERT_EUM_ECDSA }	
AUTH_SERVER_RESP_MATCHING_ID_ EVENT_ID	<pre>resp authenticateServerResponse ::= authenticateResponseOk : { euiccSigned1 { transactionId <s_transaction_id>, serverAddress #IUT_SM_DS_ADDRESS, serverChallenge <smds_challenge>, euiccInfo2 #S_EUICC_INFO2, ctxParams1</smds_challenge></s_transaction_id></pre>	

V1.4 Page 746 of 777

```
#CTX PARAMS1 MATCHING ID EVENT ID
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S_TRANSACTION_ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_MATCHING_ID_
                                          euiccInfo2 #S EUICC INFO2,
OMITTED
                                          ctxParams1
                                        #CTX PARAMS1 MATCHING ID OMITTED
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_2_6
                                          euiccInfo2 #S EUICC INFO2,
_1_EX_BC_cA
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC_SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate
                                      #CERT EUM ECDSA INVALID EX BC cA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
AUTH SERVER RESP SMDS 8 1 2 6
                                          <S TRANSACTION ID>,
_1_EX_BC_PLC
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
```

V1.4 Page 747 of 777

```
euiccInfo2 #S EUICC INFO2,
                                          ctxParams1
                                          #CTX_PARAMS1_MATCHING_ID_EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate
                                      #CERT EUM ECDSA INVALID EX BC PLC
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
                                          euiccInfo2 #S EUICC_INFO2,
AUTH_SERVER_RESP_SMDS_8_1_2_6
_1_EX_CP
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate
                                      #CERT_EUM_ECDSA_INVALID_EX_CP
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S_TRANSACTION_ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_2_6
                                          euiccInfo2 #S_EUICC_INFO2,
_1_EX_KU
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate
                                      #CERT EUM ECDSA INVALID EX KU
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
AUTH_SERVER_RESP_SMDS_8_1_2_6
                                      euiccSigned1 {
_1_SIG
                                          transactionId
                                          <S TRANSACTION ID>,
```

V1.4 Page 748 of 777

```
serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
                                          euiccInfo2 #S_EUICC_INFO2,
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate
                                      #CERT_EUM_ECDSA_INVALID_SIG
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION_ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_2_6
                                          euiccInfo2 #S EUICC INFO2,
                                          ctxParams1
_3
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate
                                      #CERT_EUM_ECDSA_EXPIRED
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION_ID>,
                                          serverAddress
                                          #IUT_SM_DS_ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_3_6
                                          euiccInfo2 #S EUICC INFO2,
_1_EX_CP
                                          ctxParams1
                                          #CTX_PARAMS1_MATCHING_ID_EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT_EUICC_ECDSA_INVALID_EX_CP,
                                      eumCertificate #CERT_EUM_ECDSA
```

V1.4 Page 749 of 777

```
resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS_CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_3_6
                                          euiccInfo2 #S_EUICC_INFO2,
_1_EX_KU
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA INVALID EX KU,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS_CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_3_6
                                          euiccInfo2 #S EUICC INFO2,
_1_SIG
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC_SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA INVALID SIG,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
AUTH_SERVER_RESP_SMDS_8_1_3_6
                                          <SMDS_CHALLENGE>,
_1_SUB_ORG
                                          euiccInfo2 #S_EUICC_INFO2,
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA INVALID SUB ORG,
```

V1.4 Page 750 of 777

```
eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION_ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_3_6
                                          euiccInfo2 #S_EUICC_INFO2,
1 SUB SN
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA INVALID SUB SN,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_3_6
                                          euiccInfo2 #S EUICC INFO2,
_3
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA EXPIRED,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
AUTH_SERVER_RESP_SMDS_8_1_6_1
                                          serverChallenge
_CHA
                                          <SMDS_CHALLENGE_INVALID>,
                                          euiccInfo2 #S_EUICC_INFO2,
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
```

V1.4 Page 751 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

```
#CERT EUICC ECDSA,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <S TRANSACTION ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_1_6_1
                                          euiccInfo2 #S_EUICC_INFO2,
_SIG
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1 INVALID>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate #CERT EUM ECDSA
                                  resp authenticateServerResponse ::=
                                  authenticateResponseOk : {
                                      euiccSigned1 {
                                          transactionId
                                          <INVALID_TRANSACTION_ID>,
                                          serverAddress
                                          #IUT SM DS ADDRESS,
                                          serverChallenge
                                          <SMDS CHALLENGE>,
AUTH_SERVER_RESP_SMDS_8_10_1_
                                          euiccInfo2 #S EUICC INFO2,
3_9
                                          ctxParams1
                                          #CTX PARAMS1 MATCHING ID EMPTY
                                      },
                                      euiccSignature1
                                      <EUICC SIGNATURE1>,
                                      euiccCertificate
                                      #CERT EUICC ECDSA,
                                      eumCertificate #CERT_EUM_ECDSA
                                  ctxParamsForCommonAuthentication : {
CTX_PARAMS1_MATCHING_ID_EVENT
                                    matchingId #EVENT ID 1,
                                    deviceInfo #S DEVICE INFO
(CtxParams1)
                                  ctxParamsForCommonAuthentication : {
CTX_PARAMS1_MATCHING_ID_OMITT
                                      deviceInfo #S_DEVICE_INFO
ED
(CtxParams1)
```

V1.4 Page 752 of 777

D.6.2 ES11 Responses

Name	Content
AUTH_CLIENT_DS_OK	<pre>"header" : { "functionExecutionStatus" : { "status" : "Executed-Success" } }, "transactionId" : <s_transaction_id>, "eventEntries" : #EVENT_ENTRY }</s_transaction_id></pre>
AUTH_CLIENT_DS_OK1	<pre>"header" :{ "functionExecutionStatus":{ "status" : "Executed-Success" } }, "transactionId" : <s_transaction_id>, "eventEntries" : [#EVENT_ENTRY_1] }</s_transaction_id></pre>
AUTH_CLIENT_DS_OK2	<pre>"header" :{ "functionExecutionStatus":{ "status" : "Executed-Success" } }, "transactionId" : <s_transaction_id>, "eventEntries" : [#EVENT_ENTRY_2] }</s_transaction_id></pre>
AUTH_CLIENT_DS_OK_DSADDR1	<pre>"header" :{ "functionExecutionStatus":{ "status" : "Executed-Success" } }, "transactionId" : <s_transaction_id>, "eventEntries" : [#EVENT_ENTRY_DSADDR1] }</s_transaction_id></pre>
EVENT_ENTRY	<pre>{ "eventid" : <event_id>, "rspServerAddress" : <rsp_server_address> }</rsp_server_address></event_id></pre>
EVENT_ENTRY_1	<pre>{ "eventId" : #EVENT_ID_1, "rspServerAddress" : #TEST_DP_ADDRESS1 }</pre>
EVENT_ENTRY_2	{ "eventId" : #EVENT_ID_2, "rspServerAddress" : #TEST_DP_ADDRESS1 }
EVENT_ENTRY_DSADDR1	{ "eventId" : #EVENT_ID_1,

V1.4 Page 753 of 777

```
"rspServerAddress" : #TEST DS ADDRESS1
                                  {
                                    "eventId" : #EVENT ID 1,
                                    "rspServerAddress": #TEST DP ADDRESS1
EVENT ENTRY MULTI
                                  {
                                    "eventId" : #EVENT_ID_2,
                                    "rspServerAddress": #TEST DP ADDRESS2
                                  {
                                     "header" : {
                                        "functionExecutionStatus" : {
                                           "status" : "Executed-Success"
R_AUTH_CLIENT_DS_EVENT_ENTRY_
                                     },
1_OK
                                     "transactionId" : <S_TRANSACTION_ID>,
                                     "eventEntries" : [#EVENT ENTRY 1]
                                     "header" : {
                                        "functionExecutionStatus" : {
                                            "status" : "Executed-Success"
R_AUTH_CLIENT_DS_EVENT_ENTRY_
EMPTY_OK
                                     "transactionId" : <S_TRANSACTION_ID>,
"eventEntries" : []
                                     "header" : {
                                        "functionExecutionStatus" : {
                                            "status" : "Executed-Success"
R_AUTH_CLIENT_DS_EVENT_ENTRY_
MULTI_OK
                                     "transactionId" : <S_TRANSACTION_ID>,
                                     "eventEntries" : [#EVENT ENTRY MULTI]
```

D.7 ES12 Requests And Responses

There are no specific ES12 requests or responses defined in the present document.

D.8 ES15 Requests And Responses

There are no specific ES15 requests or responses defined in the present document.

D.9 Common Server Responses

For all responses with a JSON component the "subjectIdentifier" and "message" are optional and may or may not be present in the response received from the RSP server.

Name	Content
R_ERROR_1_2_4_2	<pre>"header" : { "functionExecutionStatus" : { "status" : "Failed", "statusCodeData" : { "subjectCode" : "1.2", "reasonCode" : "4.2" }</pre>

V1.4 Page 754 of 777

```
}
                                    "header" : {
                                      "functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.1.1",
R_ERROR_8_1_1_3_8
                                        "reasonCode" : "3.8"
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                           "subjectCode" : "8.1.2",
R_ERROR_8_1_2_6_1
                                           "reasonCode" : "6.1"
                                      }
                                    }
                                 }
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                        "status" : "Expired",
                                        "statusCodeData" : {
R_ERROR_8_1_2_6_3
                                        "subjectCode" : "8.1.2",
                                        "reasonCode" : "6.3"
                                    "header" : {
                                      "functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.1.3",
R_ERROR_8_1_3_6_1
                                        "reasonCode" : "6.1"
                                      }
                                    }
                                 }
                                    "header" : {
                                      "functionExecutionStatus" : {
R_ERROR_8_1_3_6_3
                                        "status" : "Expired",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.1.3",
```

V1.4 Page 755 of 777

```
"reasonCode" : "6.3"
                                      }
                                    }
                                 }
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.1",
R_ERROR_8_1_4_8
                                        "reasonCode" : "4.8"
                                        }
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.1",
R_ERROR_8_1_6_1
                                        "reasonCode" : "6.1"
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.2",
R_ERROR_8_2_1_2
                                        "reasonCode" : "1.2"
                                    }
                                 }
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
R_ERROR_8_2_3_7
                                        "subjectCode" : "8.2",
                                        "reasonCode" : "3.7"
                                        }
                                      }
                                    }
                                    "header" : {
R_ERROR_8_2_5_4_3
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
```

V1.4 Page 756 of 777

```
"statusCodeData" : {
                                         "subjectCode" : "8.2.5",
                                         "reasonCode" : "4.3"
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
R_ERROR_8_2_6_3_8
                                        "subjectCode" : "8.2.6",
                                        "reasonCode" : "3.8"
                                        }
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.2.7",
R_ERROR_8_2_7_2_2
                                        "reasonCode" : "2.2"
                                 }
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.2.7",
R_ERROR_8_2_7_3_8
                                        "reasonCode" : "3.8"
                                      }
                                    }
                                 }
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
R_ERROR_8_2_7_6_4
                                        "subjectCode" : "8.2.7",
                                        "reasonCode" : "6.4"
                                        }
                                      }
                                    }
                                 {
R_ERROR_8_8_1_3_8
                                   "header" : {
```

V1.4 Page 757 of 777

```
"functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                           "subjectCode" : "8.8.1",
                                           "reasonCode" : "3.8"
                                     }
                                    }
                                  {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
R_ERROR_8_8_2_3_1
                                          "subjectCode" : "8.8.2",
                                          "reasonCode" : "3.1"
                                        }
                                      }
                                    }
                                    "header" : {
                                     "functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                          "subjectCode" : "8.8.3",
R_ERROR_8_8_3_3_1
                                          "reasonCode" : "3.1"
                                      }
                                    }
                                  }
                                    "header" : {
                                     "functionExecutionStatus" : {
                                       "status" : "Failed",
                                        "statusCodeData" : {
R_ERROR_8_8_3_10
                                          "subjectCode" : "8.8",
                                          "reasonCode" : "3.10"
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                          "subjectCode" : "8.8.4",
R_ERROR_8_8_4_3_7
                                          "reasonCode" : "3.7"
                                        }
                                      }
                                   }
```

V1.4 Page 758 of 777

```
"header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Expired",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.8.5",
R_ERROR_8_8_5_4_10
                                        "reasonCode" : "4.10"
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.8.5",
R_ERROR_8_8_5_6_4
                                        "reasonCode" : "6.4"
                                    }
                                 }
                                   "header" : {
                                     "functionExecutionStatus" : {
                                       "status" : "Failed",
                                       "statusCodeData" : {
                                          "subjectCode" : "8.9.1",
R_ERROR_8_9_1_3_8
                                          "reasonCode" : "3.8"
                                       }
                                     }
                                   }
                                   "header" : {
                                     "functionExecutionStatus" : {
                                       "status" : "Failed",
                                       "statusCodeData" : {
                                         "subjectCode" : "8.9.2",
R_ERROR_8_9_2_3_1
                                         "reasonCode" : "3.1"
                                     }
                                   }
                                   "header" : {
                                     "functionExecutionStatus" : {
                                       "status" : "Failed",
R ERROR 8 9 3 3 1
                                       "statusCodeData" : {
                                         "subjectCode" : "8.9.3",
                                         "reasonCode" : "3.1"
```

V1.4 Page 759 of 777

```
}
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
                                       "subjectCode" : "8.9",
R ERROR 8 9 4 2
                                       "reasonCode" : "4.2"
                                      }
                                    }
                                 }
                                   "header" : {
                                     "functionExecutionStatus" : {
                                       "status" : "Failed",
                                       "statusCodeData" : {
R_ERROR_8_9_4_3_7
                                         "subjectCode" : "8.9.4",
                                         "reasonCode" : "3.7"
                                     }
                                   }
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
                                         "status" : "Failed",
                                        "statusCodeData" : {
R_ERROR_8_9_5_1
                                        "subjectCode" : "8.9",
                                        "reasonCode" : "5.1"
                                        }
                                      }
                                    }
                                    "header" : {
                                      "functionExecutionStatus" : {
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.9.5",
R_ERROR_8_9_5_3_3
                                        "reasonCode" : "3.3"
                                      }
                                    }
                                 }
                                 {
                                    "header" : {
                                      "functionExecutionStatus" : {
R_ERROR_8_9_5_3_9
                                        "status" : "Failed",
                                        "statusCodeData" : {
                                        "subjectCode" : "8.9.5",
                                        "reasonCode" : "3.9"
```

V1.4 Page 760 of 777

```
}
                                         }
                                     }
                                     {
                                         "header" : {
                                           "functionExecutionStatus" : {
                                             "status" : "Failed",
                                             "statusCodeData" : {
                                             "subjectCode" : "8.10.1",
R_ERROR_8_10_1_3_9
                                             "reasonCode" : "3.9"
                                           }
                                        }
                                         "header" : {
                                           "functionExecutionStatus" : {
                                              "status" : "Failed",
                                             "statusCodeData" : {
                                             "subjectCode" : "8.11.1",
R_ERROR_8_11_1_3_9
                                             "reasonCode" : "3.9"
                                          }
                                         }
                                     The error response will be as follows dependent on the entity
                                     under test:
                                         • for SM-DP+ testing on ES9+ SHALL be
R_ERROR_SMXX_1_3_8
                                            #R ERROR 8 8 1 3 8
                                         • for SM-DS testing on ES11 SHALL be
                                            #R_ERROR_8_9_1_3_8
                                     The error response will be as follows dependent on the entity
                                     under test:
                                         • for SM-DP+ testing on ES9+ SHALL be
R_ERROR_SMXX_2_3_1
                                            #R ERROR 8 8 2 3 1
                                          for SM-DS testing on ES11 SHALL be
                                            #R_ERROR_8_9_2_3_1
                                     The error response will be as follows dependent on the entity
                                     under test:

    for SM-DP+ testing on ES9+ SHALL be

R_ERROR_SMXX_3_3_1
                                            #R_ERROR_8_8_3_3_1
                                          for SM-DS testing on ES11 SHALL be
                                            #R_ERROR_8_9_3_3_1
                                     The error response will be as follows dependent on the entity
                                     under test:
R_ERROR_SMXX_4_3_7
                                         • for SM-DP+ testing on ES9+ SHALL be
                                            #R ERROR 8 8 4 3 7
```

V1.4 Page 761 of 777

	for SM-DS testing on ES11 SHALL be #R_ERROR_8_9_4_3_7
R_SUCCESS	<pre>"header" : { "functionExecutionStatus" : { "status" : "Executed-Success" } }</pre>

Annex E Profiles

Profile	PROFILE_OPERATIONAL1
Description	Generic Operational Profile This Profile acts as an Operational Profile in the scope of this specification. NOTE: Milenage algorithm is used in this Profile
Details	The Profile Metadata SHALL be set to #METADATA_OP_PROF1, except if defined differently in the test sequence. The Unprotected Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that: • the iccid field SHALL be set to #ICCID_OP_PROF1 in the ProfileHeader element, in non-swapped format • the connectivityParameters field SHALL not be present in the ProfileHeader element • the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF1 • the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF1 • the pinAttributes of pinAppl1 present in the PE_PIN SHALL be set to 6 • the SCP80 encryption key configured in the PE-SecurityDomain that corresponds to the MNO-SD SHALL be set to #MNO_SCP80_ENC_KEY • the SCP80 message authentication key configured in the PE-SecurityDomain that corresponds to the MNO-SD SHALL be set to #MNO_SCP80_AUTH_KEY • the SCP80 data encryption key configured in the PE-SecurityDomain that corresponds to the MNO-SD SHALL be set to #MNO_SCP80_DATA_ENC_KEY • the instance AID configured in the PE-SecurityDomain that corresponds to the Supplementary Security Domain PE_SSD SHALL be set to #SSD_AID • the ef-dir present in the PE-MF SHALL be configured with the AID #USIM_AID • the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available) • the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H • the Token Verification and the Receipt Generation keys SHALL not be set in the PE-MNO-SD • the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H The PROFILE_OPERATIONAL1 UPP is named #UPP_OP_PROF1 in the scope of this document.

Profile	PROFILE_OPERATIONAL2
Description	Generic Operational Profile This Profile acts as an Operational Profile in the scope of this specification.

V1.4 Page 762 of 777

	NOTE: Milenage algorithm is used in this Profile
	The Profile Metadata SHALL be set to #METADATA_OP_PROF2, except if defined differently in the test sequence.
	The Unprotected Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that:
	the <i>iccid</i> field SHALL be set to #ICCID_OP_PROF2 in the <i>ProfileHeader</i> element, in non-swapped format
Details	 the connectivityParameters field SHALL not be present in the ProfileHeader element the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF2 the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF2
	 The pinAttributes of pinAppl1 present in the PE_PIN SHALL be set to 6 the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available)
	the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H
	the Token Verification and the Receipt Generation keys SHALL not be set in the PE- MNO-SD
	the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H
	The PROFILE_OPERATIONAL2 UPP is named #UPP_OP_PROF2 in the scope of this document.

Profile	PROFILE_OPERATIONAL3
Description	Operational Profile with PPR2 but without notification This Profile acts as an Operational Profile in the scope of this specification. NOTE: Milenage algorithm is used in this Profile
Details	The Profile Metadata SHALL be set to #METADATA_OP_PROF3, except if defined differently in the test sequence. The Unprotected Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that: • the iccid field SHALL be set to #ICCID_OP_PROF3 in the ProfileHeader element, in non-swapped format • the connectivityParameters field SHALL not be present in the ProfileHeader element • the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF3 • the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF3 • the pinAttributes of pinAppl1 present in the PE_PIN SHALL be set to 6 • the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available) • the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H • the Token Verification and the Receipt Generation keys SHALL not be set in the PE-MNO-SD • the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H The PROFILE_OPERATIONAL3 UPP is named #UPP_OP_PROF3 in the scope of this document.

Profile	PROFILE_OPERATIONAL4
Description	Operational Profile with PPR1 and notification

V1.4 Page 763 of 777

	This Profile acts as an Operational Profile in the scope of this specification. NOTE: Milenage algorithm is used in this Profile
	The Profile Metadata SHALL be set to #METADATA_OP_PROF4, except if defined differently in the test sequence.
	The Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that:
Details	the <i>iccid</i> field SHALL be set to #ICCID_OP_PROF4 in the <i>ProfileHeader</i> element, in non-swapped format
	the connectivityParameters field SHALL not be present in the ProfileHeader element the of incidence at the RF MF SHALL has get to #ICCID_OR_RROLL
	 the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF4 the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF4
	the pinAttributes of pinAppl1 present in the PE_PIN SHALL be set to 6
	the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available)
	the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H
	the Token Verification and the Receipt Generation keys SHALL not be set in the PE- MNO-SD
	the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H
	The PROFILE_OPERATIONAL4 UPP is named #UPP_OP_PROF4 in the scope of this document.

Profile	PROFILE_OPERATIONAL5
Description	Generic Operational Profile with pinAppl1 enabled. This Profile acts as an Operational Profile in the scope of this specification. NOTE: Milenage algorithm is used in this Profile
Details	The Profile Metadata SHALL be set to #METADATA_OP_PROF5, except if defined differently in the test sequence. The Unprotected Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that: • the iccid field SHALL be set to #ICCID_OP_PROF5 in the ProfileHeader element, in non-swapped format
	 the connectivityParameters field SHALL not be present in the ProfileHeader element the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF5 the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF5 the pinAppl1 present in the PE_PIN SHALL be enabled and has the value #PO1_PIN1 the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available)
	 the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H the Token Verification and the Receipt Generation keys SHALL not be set in the PE-MNO-SD the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H

Profile	PROFILE_OPERATIONAL6
Description	Generic Operational Profile with pinAppl1 enabled. This Profile acts as an Operational Profile in the scope of this specification.

V1.4 Page 764 of 777

Official Document SGP.23 - SGP.23 RSP Test Specification

	NOTE: Milenage algorithm is used in this Profile
	The Profile Metadata SHALL be set to #METADATA_OP_PROF6, except if defined differently in the test sequence.
	The Unprotected Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that:
	the <i>iccid</i> field SHALL be set to #ICCID_OP_PROF6 in the <i>ProfileHeader</i> element, in non-swapped format
	the connectivityParameters field SHALL not be present in the ProfileHeader element
	the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF6
Details	the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF6
	The pinAppl1 present in the PE_PIN SHALL be enabled and has the value #PO2_PIN1
	the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available)
	the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H
	the Token Verification and the Receipt Generation keys SHALL not be set in the PE- MNO-SD
	the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H

Non-confidential

Profile	PROFILE_OPERATIONAL7
Description	Operational Profile with PPR2 and notification This Profile acts as an Operational Profile in the scope of this specification. NOTE: Milenage algorithm is used in this Profile
Details	The Profile Metadata SHALL be set to #METADATA_OP_PROF7, except if defined differently in the test sequence. The Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that: • the iccid field SHALL be set to #ICCID_OP_PROF7 in the ProfileHeader element, in non-swapped format • the connectivityParameters field SHALL not be present in the ProfileHeader element • the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF7 • the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF7 • the pinAttributes of pinAppl1 present in the PE_PIN SHALL be set to 6 • the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available) • the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H • the Token Verification and the Receipt Generation keys SHALL not be set in the PE-
	MNO-SD the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H

Profile	PROFILE_OPERATIONAL8
Description	Operational Profile with PPR2, pinAppl1 enabled and notification This Profile acts as an Operational Profile in the scope of this specification. NOTE: Milenage algorithm is used in this Profile

V1.4 Page 765 of 777

	The Profile Metadata SHALL be set to #METADATA_OP_PROF8, except if defined differently in the test sequence.
	The Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that:
	the <i>iccid</i> field SHALL be set to #ICCID_OP_PROF8 in the <i>ProfileHeader</i> element, in non-swapped format
	the connectivityParameters field SHALL not be present in the ProfileHeader element
	the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF8
Details	the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF8
	The pinAppl1 present in the PE_PIN SHALL be enabled and has the value #PO2_PIN1
	the ef-ust SHALL be set in accordance to #EF_UST1 (service 17 and 18 are not available)
	the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H
	the Token Verification and the Receipt Generation keys SHALL not be set in the PE- MNO-SD
	the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H

Profile	PROFILE_OPERATIONAL9		
Description	Generic Operational Profile with GID1 and GID2 set This Profile acts as an Operational Profile in the scope of this specification. NOTE: Milenage algorithm is used in this Profile		
Details	The Profile Metadata SHALL be set to #METADATA_OP_PROF9, except if defined differently in the test sequence. The Unprotected Profile Package content SHALL follow the ASN.1 structures specified in Annex B.7 of SGP.11 [21] except that: • the iccid field SHALL be set to #ICCID_OP_PROF9 in the ProfileHeader element, in non-swapped format • the connectivityParameters field SHALL not be present in the ProfileHeader element • the ef-iccid present in the PE-MF SHALL be set to #ICCID_OP_PROF9 • the ef-imsi present in the PE-USIM SHALL be set to #IMSI_OP_PROF9 • the pinAppl1 present in the PE_PIN SHALL be enabled and has the value #PO1_PIN1 • the ef-ust SHALL be set to #EF_UST2 (service 17 and 18 are available) • the applicationPrivileges in PE-MNO-SD SHALL be set to '82DC00'H • the Token Verification and the Receipt Generation keys SHALL not be set in the PE-MNO-SD • the applicationSpecificParametersC9 in PE-MNO-SD SHALL be set to '810280008201F08701F0'H • the following new Profile Element PE_OPT_USIM SHALL be inserted right after PE_USIM:		
	PE_OPT_USIM		

V1.4 Page 766 of 777

```
optusimValue ProfileElement ::= opt-usim : {
  optusim-header {
   mandated NULL,
   identification 15
  },
  templateID id-OPT-USIM,
  ef-gid1 {
   fileDescriptor {
     efFileSize '04'H
    fillFileContent #GID1
  },
  ef-gid2 {
   fileDescriptor {
     efFileSize '04'H
    fillFileContent #GID2
}
Note: The following OIDs are used:
```

```
id-OPT-USIM OBJECT IDENTIFIER ::=
{joint-iso-itu-t(2) international-organizations(23)
simalliance(143) euicc-profile(1) template(2) opt-usim(5)}
```

The PROFILE_OPERATIONAL9 UPP is named #UPP_OP_PROF9 in the scope of this document.

V1.4 Page 767 of 777

Annex F IUT Settings

F.1 eUICC Settings

In order to execute the test cases defined in this document, the eUICC Manufacturer SHALL deliver following settings:

eUICC Setting name	Description		
IUT_DLOA_URL	Discovery Base URL of the SE default DLOA Registrar as defined in GlobalPlatform DLOA specification [19] (optional)		
IUT_EUICC_CATEGORY	The category, if provided, SHALL be either not present or: • other(0) • or basicEuicc(1) • or mediumEuicc(2) • or contactlessEuicc(3)		
IUT_EUICC_FIRMWARE_VER	eUICC Firmware version coded as binary value (3 bytes representing major/minor/revision).		
IUT_GLOBALPLATFORM_VERSION	GlobalPlatform version coded as binary value (3 bytes representing major/minor/revision, 2.3.0 or higher). The support of GlobalPlatform is considered as mandatory in the scope of this specification.		
IUT_PLATFORM_LABEL	Platform_Label as defined in GlobalPlatform DLOA specification [19] (optional)		
IUT_PP_VERSION	Protection Profile version coded as binary value (3 bytes representing major/minor/revision).		
IUT_SAS_ACCREDITATION_NUMBE R	SAS Accreditation Number, coded as ASN.1 UTF8String		
IUT_TS102241_VERSION	The ts102241 version field is coded as binary value (3 bytes representing major/minor/revision, 9.0.0 or higher). The support of Java Card is considered as mandatory in the scope of this specification. The ts102241 Version field indicates the latest version of ETSI TS102 241[17] supported by the eUICC.		
IUT_UICC_CAPABILITY	Sequence is derived from ServicesList[] defined in SIMalliance PEDefinitions, coded as ASN.1 BIT STRING (19 bits).		
IUT_SIMA_VERSION	Version of SIMalliance [4] supported by the eUICC (3 bytes representing major/minor/revision) e.g. 0x020100		

F.2 Platforms Settings

In order to execute the test cases defined in this document, the Platform (i.e. SM-DP+ or SM-DS) provider SHALL deliver following settings:

SM-DP+ Setting name	Description		
IUT_CLIENT_TLS_VER	Highest TLS protocol version supported by the Client (SM-DP+ or SM-DS) under test, which SHALL be at least v1.2. For versions higher than TLS v1.2 backwards compatibility is assumed.		
IUT_SM_DP_ADDRESS	FQDN of the SM-DP+ Under Test.		

V1.4 Page 768 of 777

IUT_SM_DP_HOST_ID	SM-DP+ Host ID of the SM-DP+ Under Test coded as an ASN.1 octet string.
IUT_SM_DP_OID	SM-DP+ OID (as defined in section 1.3) of the SM-DP+ Under Test.
IUT_SM-DP+_MAX_NUMBER_DOWNLOA D_ATTEMPTS	Maximum number of download attempts allowed by the SM-DP+. After this number, no further download is allowed.
SM-DS Setting name	Description
SM-DS Setting name IUT_SM_DS_ADDRESS	Description FQDN of the SM-DS Under Test.

F.3 Device Settings

Device Setting name	Description
IUT_CDMA2000_1X_REL	If cdma2000 1X is supported, this SHALL be encoded as the octet string {1, 0, 0}.
IUT_CDMA2000_EHRPD_REL	If cdma2000 eHRPD, is supported this SHALL be the highest 3GPP release N fully supported by the Device, encoded as the octet string {N, 0, 0}.
IUT_CDMA2000_HRPD_REL	If cdma2000 HRPD is supported, this SHALL be encoded as the octet string {R, 0, 0}. The value R SHALL represent the EVDO revision as follows: Rev 0 SHALL be encoded as 1 Rev A SHALL be encoded as 2 Rev B SHALL be encoded as 3
IUT_EU_CONFIRMATION_TIMEOUT	Timeout in seconds for LPAd for the End User Intent confirmation starting when the LPAd displays the dialog for confirmation.
IUT_GSM_GERAN_REL	If GSM/GERAN is supported, this is the highest 3GPP release N fully supported by the Device, encoded as the octet string {N, 0, 0}.
IUT_LPAd_CI	CI subjectPublicKeyInfo of CERT.CI.ECDSA (used to verify CERT.DP.TLS) stored in LPAd. Based on NIST [11] in this version of specification.
IUT_LPAd_AuthenticatedConfirmation	Description of the way to perform Authenticated Confirmation
IUT_LPAd_NOTIFICATION_TIMEOUT	Timeout in seconds for LPAd to send a Notification to the SM-DP+ on ES9+ interface assuming IP connection is available.
IUT_LPAd_READY_AFTER_REBOOT_TIMEOUT	Timeout in seconds for the LPAd to be ready after a reboot. The time starts from the power off at the start of the reboot and ends when the LPAd is ready after the reboot.
IUT_LPAd_SESSION_CLOSE_TIMEOUT	Timeout in seconds for LPAd to send a next command for Profile Download to the SM-DP+ (or SM-DS) on ES9+ (or ES11) interface assuming IP connection is

V1.4 Page 769 of 777

	available. The timeout SHALL start after sending of the previous command by the LPAd.		
IUT_LTE_EUTRAN_REL	If LTE/E-UTRAN is supported, this SHALL be the highest 3GPP release N fully supported by the Device, encoded as the octet string {N, 0, 0}.		
IUT_NFC_REL	If NFC is supported, this SHALL be the highest (version, revision) number of TS.26 [15], encoded as the octet string {version, revision, 0}.		
IUT_TAC	Type Allocation Code defined by the Device		
IUT_TLS_VERSION	Highest TLS protocol version supported by LPAd, at least v1.2. By versions higher then TLS v1.2 backwards compatibility is assumed.		
IUT_UMTS_UTRAN_REL	If UMTS/UTRAN is supported, this SHALL be the highest 3GPP release N fully supported by the Device, encoded as the octet string {N, 0, 0}.		

F.4 Common Settings

In order to execute the test cases defined in this document, the IUT provider SHALL deliver following settings:

IUT Setting name	Description
IUT RSP VERSION	Version of SGP.22 supported by the IUT encoded as a string of three integers separated with dots (for example: 2.1.0).
IUI_RSF_VERSION	In the scope of this specification, this value SHALL be either 2.1.0 or 2.2.x (x≥0).

V1.4 Page 770 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

Annex G Initial States

Unless it is defined differently in a particular test case, the IUTs SHALL be set in the following initial state before the test case execution.

G.1 Device

G.1.1 Device (default)

The Device is "powered on".

The Device is in the normal execution mode after Device boot-up and Device initial configuration. The Device is NOT in the Test Mode.

The LPAd has access to the root CI key #CERT_CI_ECDSA (or the CI public key) for verification of the TLS certificates of SM-DP+ or SM-DS. No CRL is loaded.

• The Device contains a Test eUICC pre-configured as defined below in G.1.3.

G.1.2 Companion Device connected to a Primary Device

The Companion Device is connected to the Primary Device as defined by the Device vendor

Companion Device and the connected Primary Device are "powered on"

The Companion Device and Primary Device are in the normal execution mode (NOT in the boot-up mode)

The LPAd of the Companion Device has access to the root CI #CERT_CI_ECDSA (or the CI public key) for verification of the TLS certificates of SM-DP+ or SM-DS. No CRL is loaded.

The Companion Device contains a Test eUICC preconfigured as defined below in G.1.3.

G.1.3 Test eUICC Settings

Depending on the test cases and on the supported options, the Test eUICC SHALL be configured according to the following Initial States.

- The Test eUICC is configured with the ISD-R AID #ISD_R_AID and the EID #EID1.
- The Test eUICC does not contain any Profile.
- The Test eUICC is configured with the default SM-DS address #TEST_ROOT_DS_ADDRESS.
- The Test eUICC contains #TEST_DP_ADDRESS1 as default SM-DP+ address.

The ECASD is configured with at least the following Keys and Certificates based on NIST P-256 [11] or on brainpoolP256r1 [8] for this version of the SGP.23:

- The Test eUICC's Private Key #SK EUICC ECDSA (for creating ECDSA signatures)
- The Test eUICC's Certificate #CERT_EUICC_ECDSA (for eUICC authentication) containing the eUICC's Public Key #PK EUICC ECDSA
- The GSMA Certificate Issuer's Public Key #PK_CI_ECDSA (for verifying off-card entities certificates)
- The Certificate of the EUM #CERT_EUM_ECDSA

V1.4 Page 771 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Other Certificates and Keys MAY be present. No CRL is loaded on the Test eUICC.

The CI, identified as highest priority in euiccCiPKIdListForSigning, is also selectable in the euiccCiPKIdListForVerification (i.e. all EUM and eUICC Certificates lead to a Root CI certificate linked to a #PK_CI_ECDSA contained in the eUICC).

This CI corresponds to the SubjectKeyldentifier of one of the #CERT_CI_ECDSA defined in sections G.2.2 and G.2.3.

The default RAT configuration as detailed in SGP.21 Annex H applies for all test sequences except if the Test Case overrides it:

 Only one PPAR authorizing PPR1 and PPR2 for all MNOs with End User consent required i.e. #PPRS_ALLOWED

A separate Test eUICC needs to be provided for each additional RAT configuration (not used in this version of the test specification). In case the Test eUICC is non-removable the additional Device SHALL contain the same software and hardware except the Test eUICC configuration.

G.2 eUICC

Depending on the test cases and on the supported options, the EUM SHALL configure the eUICC according to the following Initial States. The initial conditions SHALL be restored, as described in the following subsections, after each test sequence.

G.2.1 Common Initial States

The following initial states apply for all test cases defined in this Test Plan whatever the options supported by the eUICC:

- The eUICC is configured with the ISD-R AID #ISD_R_AID and the EID #EID1.
- The eUICC does not contain any Profile.
- The eUICC's Pending Notifications List is empty.
- No RSP session is ongoing.
- The eUICC is configured with the default SM-DS address #TEST_ROOT_DS_ADDRESS.
- The eUICC is configured without Default SM-DP+ address.
- No CRL is loaded on the eUICC.
- The ECASD is configured as defined in section G.2.2 and/or G.2.3 depending on the support of the options O_E_NIST and O_E_BRP.
 - If the eUICC only supports O_E_NIST, the ECASD is configured as defined in section G.2.2.
 - If the eUICC only supports O_E_BRP, the ECASD is configured as defined in section G.2.3.
 - If the eUICC supports O_E_NIST and O_E_BRP, the ECASD is configured as defined in sections G.2.2 and G.2.3 (i.e. several EUM / eUICC Certificates and Keys are configured in the eUICC).

V1.4 Page 772 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

The CI, identified as highest priority in euiccCiPKIdListForSigning, is also selectable in the euiccCiPKIdListForVerification (i.e. all EUM and eUICC Certificates lead to a Root CI certificate linked to a #PK_CI_ECDSA contained in the eUICC).

This CI corresponds to the SubjectKeyldentifier of one of the #CERT_CI_ECDSA defined in sections G.2.2 and G.2.3.

The default RAT configuration defined in section G.2.4 applies for all test sequences except if the Test Case overrides it. Particular RAT configurations for those specific Test Cases are defined in section G.2.5.

G.2.2 For eUICC supporting NIST P-256

If the eUICC supports O_E_NIST, the ECASD contains at least:

- The eUICC's Private Key #SK_EUICC_ECDSA (for creating ECDSA signatures) based on NIST P-256 [11]
- The eUICC's Certificate #CERT_EUICC_ECDSA (for eUICC authentication)
 containing the eUICC's Public Key #PK_EUICC_ECDSA based on NIST P-256 [11]
- The GSMA Certificate Issuer's Public Key #PK_CI_ECDSA (for verifying off-card entities certificates) based on NIST P-256 [11]
- The Certificate of the EUM #CERT_EUM_ECDSA based on NIST P-256 [11]

Other Certificates and Keys MAY be present.

G.2.3 For eUICC supporting BrainpoolP256r1

If the eUICC supports O_E_BRP, the ECASD contains at least:

- The eUICC's Private Key #SK_EUICC_ECDSA (for creating ECDSA signatures) based on brainpoolP256r1 [8]
- The eUICC's Certificate #CERT_EUICC_ECDSA (for eUICC authentication) containing the eUICC's Public Key #PK_EUICC_ECDSA based on brainpoolP256r1
 [8]
- The GSMA Certificate Issuer's Public Key #PK_CI_ECDSA (for verifying off-card entities certificates) based on brainpoolP256r1 [8]
- The Certificate of the EUM #CERT_EUM_ECDSA based on brainpoolP256r1 [8]
- Other Certificates and Keys MAY be present.

G.2.4 With default RAT configuration

The eUICC's RAT is configured as detailed in SGP.21 Annex H:

 Only one PPAR authorizing PPR1 and PPR2 for all MNOs with End User consent required i.e. #PPRS ALLOWED

G.2.5 With Additional PPARs in the RAT

The eUICC's RAT is configured as below (following this order):

- Additional PPARs representing custom agreements between MNOs and OEMs:
 - #PPR1_WITH_OWNER_GID

V1.4 Page 773 of 777

GSM Association Non-confidential

Official Document SGP.23 - SGP.23 RSP Test Specification

- #PPR1 WITHOUT GID
- o #PPR2 WITHOUT CONSENT
- The last PPAR authorizes PPR1 and PPR2 for all MNOs with End User consent required i.e. #PPRS_ALLOWED

G.2.6 Clean-up procedure

Unless differently specified in the test case, the following procedure SHALL be executed after each test sequence to bring the eUICC back to its Common Initial State:

- eUICC Memory Reset to delete all profiles and reset the SM-DP+ Address
- Retrieve and Remove all pending notifications

Where necessary, in addition to the above, other steps may be executed to restore the initial state specified in this Annex.

G.3 SM-DP+ and SM-DS

The SM-DP+ SHALL be configured with #CERT_SM_DPauth_ECDSA, #CERT_SM_DPpb_ECDSA and #CERT_SM_DP_TLS for both NIST and BRP.

The SM-DP+ provider SHALL provide the capability to provision the SM-DP+ with Profiles as required by the specific test cases, with the following associated data where required:

- Profile Metadata
- MatchingID
- EID
- Confirmation Code
- Protected with random keys in advance, or with session keys during an RSP session, as required
- Number of retries for receipt of a valid Confirmation Code.

The SM-DP+ provider SHALL provide the capability to expire a download order.

NOTE: as ES2+ is out of scope in the current version of the present document, proprietary means MAY be used to provide these capabilities.

The SM-DS SHALL be configured with #CERT_SM_DSauth_ECDSA and #CERT_SM_DS_TLS for both NIST and BRP.

The SM-DS provider SHALL provide the capability to register an event.

The SM-DS provider SHALL provide the capability to remove the record of a particular EventID having been used from the SM-DS.

V1.4 Page 774 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Annex H Icons and QR Codes

The files for the eUICC Consumer Devices Icons and QR Codes are provided within in SGP.23_AnnexH_Icons.zip and SGP.23_AnnexH_QRCodes.zip packages, which accompany the present document.

V1.4 Page 775 of 777

GSM Association Non-confidential Official Document SGP.23 - SGP.23 RSP Test Specification

Annex I Requirements

The requirements used in the specified test cases are provided within SGP_23_AnnexI_Requirements_v1_3.zip package, which accompanies the present document.

V1.4 Page 776 of 777

Annex J Document Management

J.1 Document History

Versi on	Date	CR No	Brief Description of Change	Entity	Appro val Autho rity	Editor / Company
v1.0	9 th June 2017		Initial version of SGP.23 v1.0 Test Specification		PSMC	Yolanda Sanz, GSMA
v1.1	28 th Sept 2017		Minor version of SGP.23 Test specifications		RSPL EN	Yolanda Sanz, GSMA
v1.2	3 rd Jan 2018		Minor version of SGP.23 Test specifications		RSPL EN	Yolanda Sanz, GSMA
V1.3	01 th Augu st		Minor version of SGP.23 Test specification		RSPL EN	Yolanda Sanz, GSMA
V1.4	18 th Dec		Minor version of SGP.23 Test specification		RSPL EN	Yolanda Sanz, GSMA

Туре	Description
Document Owner	Yolanda Sanz
Editor / Company	GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.

V1.4 Page 777 of 777