RSP Architecture
Version 2.3
30 June 2021

This Industry Specification is a Non-Binding Permanent Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

This document provides an architecture approach as a proposed solution for the Remote SIM Provisioning of Devices across all markets.

The main goal of the Architecture is to define a mechanism for the Remote SIM Provisioning of Devices with the necessary credentials to gain mobile network access.

This version focuses on Devices for the consumer market.

Please note that SGP.21 V1.0 [23] has not been superceded.

1.2 Scope

The aim of this document is to define a common architecture framework to enable the Remote SIM Provisioning and management of the Embedded UICC (eUICC) in Devices. The adoption of this architecture framework will aim to provide the basis for ensuring global interoperability for Remote SIM Provisioning between Operators in different deployment scenarios.

1.3 Intended Audience

Technical experts working within Operators, SIM solution providers, Device vendors, standards organisations, network infrastructure vendors, Service Providers and other industry bodies.

1.4 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 for the download and installation of a Profile.
Activation Code Token	A part of the Activation Code information provided by the Operator/Service Provider to refer to 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 or direct Event Registration from a SM-DP+ for an installed Profile.
Bound Profile Package	A Protected Profile Package which has been cryptographically linked to a particular eUICC.
Certificate or Public Key Certificate	A certificate as defined in RFC.5280 [1] and GlobalPlatform specifications GPC_SPE_034 [15][9].
Certified eUICC	An eUICC meeting the GSMA requirements for Remote SIM Provisioning and certified according to SGP.25 GSMA eUICC Protection Profile [25].
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+ for the download of a Profile.

Term	Description
Confirmation Code Required Flag	A parameter to indicate whether the Confirmation Code is required or not.
Confirmation Level	Refers to the hierarchy of User Intent and Confirmation Request, where: • User Intent is the first and lowest level • Simple Confirmation is the second level • Strong Confirmation is the third and highest level Note: For examples of implementation, please refer to Annex C.
Confirmation Request	Describes a request for Strong Confirmation or a Simple Confirmation as defined in this specification.
Device	User equipment used in conjunction with an eUICC to connect to a mobile network. E.g. a tablet, wearable, smartphone or handset.
Device Manufacturer	An entity responsible for manufacturing Devices. The Device Manufacturer MAY be responsible for the selection and insertion of eUICCs in Devices.
Device Test Mode	A mode hidden from the End User that allows access to and use of Test Profiles.
Disabled Profile	The state of a Profile where all files and applications (e.g. NAA) present in the Profile are not selectable.
Discovery Request	An interrogation of the Discovery Service by a Device for Event Records that are registered for its eUICC.
Discrete eUICC	An eUICC implemented on discrete standalone hardware, including its own dedicated volatile and non-volatile memory. A Discrete eUICC can be removable or non-removable.
eUICC	A UICC which enables the local management of Profiles in a secure way. Note: The term originates from “embedded UICC”.
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.
End User Data	Information that pertains to the identity of an End User e.g. personal details, name, address, biometric characteristics, assigned identification numbers, etc.
eUICC Authorisation	Used by the SM-DS to authenticate the eUICC.
eUICC Certificate	A Certificate issued by the EUM for a specific eUICC. This Certificate can be verified using the EUM Certificate.
eUICC Eligibility Check Information	The information set sent from the eUICC to the SM-DP+ to allow eligibility checks.
eUICC Manufacturer (EUM)	The eUICC Manufacturer provides eUICC products.
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.

Term	Description
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.
Event-ID	Unique identifier of an Event for a specific EID generated by the SM-DP+/SM-DS.
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 Record Query	A query to the SM-DS (Root or Alternative) executed to verify Event Registration success or determine that an Event Record still exists.
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.
Form Factor	Physical manifestation of the UICC.
GSMA Certificate Issuer	A Certificate Authority accredited by GSMA.
IC Dedicated Software	As defined in BSI-CC-PP-0084 [29].
ICCID	Unique number to identify a Profile in an eUICC as defined by ITU-T E.118 [14][14].
Integrated eUICC	An eUICC implemented on an Integrated TRE.
Integrated eUICC Test Interface	An external interface for the purpose of testing eUICC functionality.
Integrated TRE	A TRE implemented inside a larger System-on-Chip (SoC), optionally making use of remote volatile and/or non-volatile memory.
International Mobile Subscriber Identity	Unique identifier owned and issued by Operators as defined in 3GPP TS 23.003 [3] Section 2.2.
Link Profile	The process that associates a Protected Profile Package with a specific eUICC so that a Profile Download including Bound Profile Package generation can be triggered. Note: This is normally an offline process, binding is an online process happening during the communication between the SM-DP+ and the eUICC.
Local Profile Assistant (LPA)	A functional element in the Device or in the eUICC that provides the LPD, LDS and LUI features.
Local Profile Management	Local Profile Management are operations that are locally initiated on the ESeu interface.
Local Profile Management Operation	Local Profile Management Operations are 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.

Term	Description
LPA Integrity	Assurance that the LPA has not been compromised or affected. The assurance SHALL be provided to the various Remote SIM Provisioning entities to ensure that the LPA can be trusted to execute the actions requested Note: This could be linked with a certification process.
LPA Mode	Defines the Operation LPA Mode which is either LPA in the eUICC or in the Device.
LPA Procedures	Refers to processes that trigger Local Profile Management Operations.
Mobile Network Operator	An entity providing access capability and communication services to its Subscribers through a mobile network infrastructure.
Mobile Virtual Network Operator	An entity providing access capability and communication services to its Subscribers through a mobile network infrastructure but does not have an allocation of spectrum.
Multi-Factor Authentication (MFA)	A method of authentication in which an End User is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
Network Access Application	Application residing in a Profile providing authorisation to access a network.
Network Access Credentials	Data required to authenticate to an ITU E.212 [4] network. This MAY include data such as Ki/K and IMSI stored within a NAA.
NFC Device	Device with NFC capability.
NFC eUICC	eUICC with NFC capability.
Nonce	An arbitrary random number generated for one time use, employed for cryptographic communication.
Notification	A report about a Profile download or Local Profile Management Operation processed by the eUICC.
Notification Receivers	A list of SM-DP+ defined in the Profile containing SM-DP+s that are to receive Notifications concerning the Profile.
Operational Profile	A combination of Operator data and applications to be provisioned on an eUICC for the purpose 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.
Operator Credentials	A set of credentials owned by the Operator, including Network Access Credentials, OTA Keys for Remote File/Application management, and authentication algorithm parameters.
OTA Keys	The credentials included in the Profile used in conjunction with OTA Platforms.

Term	Description
OTA Platform	A platform used by an Operator for the Remote File/Application management of enabled Profiles on eUICCs.
Policy Enforcement	A function that executes Policy Rules to implement a policy.
Policy Rule	Defines the atomic action of a policy and the conditions under which it is executed.
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 Description	The description of a Profile in a format specific to the Operator; example formats could be an Excel table, xml format, or plain text.
Profile Management	A combination of local and remote management operations (enable Profile, disable Profile, delete Profile, and query Profile Metadata)
Profile Metadata	Information pertaining to a Profile used for the purpose of Local Profile Management.
Profile Owner	The entity that controls the operations that can be performed upon its Profile. With the exception of Test Profile, this is always an Operator.
Profile Package	A personalised Profile using an interoperable description format that is transmitted to an eUICC to load and install a Profile [5][5].
Profile Policy Enabler	The functional element within the Profile management system that interprets and enforces Profile Policy Rules.
Profile Policy Management	A policy control system that allows the Service Provider to implement, manage and enforce its subscription terms and conditions associated with the installed 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 encrypted for storage but not to a specific eUICC.
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.
Remote Memory	Volatile or non-volatile memory residing outside of the TRE
Remote SIM Provisioning	The downloading, installing, enabling, disabling, and deleting of a Profile on an eUICC.
Replay Attack	An attack based on previously used or outdated data.
Root Certificate	A Certificate used to authenticate other entities within the Remote SIM Provisioning framework.
Root SM-DS	A globally identified central access point for finding Events from one or more SM-DP+(s).
Service Provider	The Service Provider provides Subscriptions to Subscribers either as part of an Operator or as a party with a wholesale agreement with an Operator. The Service Provider could also be the Operator.

Term	Description
Simple Confirmation	A secure and non-interceptable 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.
SMDPid	Identifier of the SM-DP+ that is globally unique and is included as part of the SM-DP+ Certificate. Note: This is referred to as the smdpOid in SGP.22 [24].
Strong Confirmation	A secure and non-interceptable mechanism to guarantee a higher level of User Intent than Simple Confirmation by which the End User confirms their action, e.g., by inputting PIN or fingerprint, repeating Simple Confirmation, entering Confirmation Code, etc.
Subscriber	An entity (associated with one or more users) that is engaged in a Subscription with an Operator. The Subscriber is allowed to subscribe and unsubscribe to services, as well as register an End User or a list of End Users authorised to use these services.
Subscriber Data	Information that pertains to the identity of a Subscriber such as contract details, authentication credentials, cryptographic keys etc. Note: In many instances, the Subscriber is also the End User and therefore Subscriber Data is likely to include End User Data.
Subscription	A Subscription describes the commercial relationship between the Subscriber and the Service Provider.
Subscription Manager Data Preparation+ (SM-DP+)	This role prepares Profile Packages, secures each with a Profile protection key, stores Profile protection keys in a secure manner as well as the Protected Profile Packages in a Profile Package repository, and links 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.
Tamper Resistant Element	A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data.
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.
Trusted Link	According to NIST SP 800-53r4 [18][18][18], a mechanism by which an End User (through an input Device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the End User or the security functions of the information system and cannot be imitated by untrusted software.

Term	Description
User Intent	Describes the direct, real time acquisition of the manual End User input on the LUI to trigger locally a Profile download or Profile Management operation.

1.5 Abbreviations

Abbreviation	Description
AC	Activation Code
ARA-M	Access Rule Application - Master
ARF	Access Rule File
AuC	Authentication Centre
BSS	Business Support Services
CI	Certificate Issuer
DNSCurve	Domain Name System Curve
DNSSEC	Domain Name System Security Extensions
ECASD	eUICC Certificate Authority Security Domain
EID	Embedded UICC Identifier
eSVN	embedded UICC Specification Version Number
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
EUM	eUICC Manufacturer
FASG	Fraud and Security Group
FFS	For Further Study
GSMA	GSM Association
GSMA CI	GSMA Certificate Issuer
HLR	Home Location Register
HTTP	Hypertext Transfer Protocol
ICCID	Integrated Circuit Card Identifier
IMSI	International Mobile Subscriber Identity
ISD-P	Issuer Security Domain - Profile
ISD-R	Issuer Security Domain - Root
ISIM	IP Multimedia Services Identity Module
ITU	International Telecoms Union
LDS	Local Discovery Service
LPA	Local Profile Assistant
LPD	Local Profile Download
LUI	Local User Interface
M4M	Mifare4Mobile
MFA	Multi-Factor Authentication

Abbreviation	Description
MNO	Mobile Network Operator
MNO-SD	Mobile Network Operator - Security Domain
MSISDN	Mobile Subscriber International Subscriber Directory Number
NAA	Network Access Application
OS	Operating System
OTA	Over The Air
PFS	Perfect Forward Secrecy
RAM	Remote Application Management
RAT	Rules Authorisation Table
RFM	Remote File Management
RMPF	Remote Memory Protection Function
SAS	Security Accreditation Scheme
SD	Security Domain
SIM	Subscriber Identity Module
SM-DP+	Subscription Manager - Data Preparation +
SM-DS	Subscription Manager - Discovery Server
SSD	Supplementary Secure Domain
TL	Trust Link
TRE	Tamper Resistant Element
USIM	Universal Subscriber Identity Module

1.6 References

Ref	Document Number	Title
[1]	RFC 5280	X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[2]	ETSI TS 102 221	UICC-Terminal interface; Physical and logical characteristics
[3]	3GPP TS 23.003	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification
[4]	ITU E.212	The international identification plan for public networks and Subscriptions
[5]	TCAAPP	Trusted Connectivity Alliance (former SIMalliance): eUICC Profile Package - Interoperable Format Technical Specification http://simalliance.org/euicc/euicc-technical-releases/
[6]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[7]	3GPP TS 21.133	3G security; Security threats and requirements

Ref	Document Number	Title
[8]	SGP.02	GSMA Remote SIM Provisioning of Embedded UICC Technical specification
[9]	GPC_SPE_034	GlobalPlatform Card Specification with its Amendments
[10]	3GPP TS 35.231	Specification of the TUAK Algorithm Set; Document 1: Algorithm Specification
[11]	3GPP TS 35.205	Specification of the MILENAGE Algorithm Set; Document 1: General
[12]	3GPP TS 35.206	Specification of the MILENAGE Algorithm Set; Document 2: Algorithm Specification
[13]	EUM SAS	FS.04 - Security Accreditation Scheme for UICC Production – Standard
[14]	ITU-T E.118	The International Telecommunication Charge Card
[15]	GPD_SPE_013	GlobalPlatform Device Technology Secure Element Access Control - Version 1.1
[16]	3GPP TS 22.022	Personalisation of Mobile Equipment - Mobile functionality specification
[17]	TS.26	GSMA NFC Handset Requirements
[18]	NIST SP 800-53r4	Security and Privacy Controls for Federal Information Systems and Organisations – Revision 4
[19]	OMAPI	Trusted Connectivity Alliance (former SIMalliance) Open Mobile API Specification
[20]	SGP.03	NFC UICC Requirements Specification V6.1
[21]	SGP.05	Embedded UICC Protection Profile
[22]	FS.08	FS.08 SAS-SM Standard v3
[23]	SGP.21	SGP.21 Architecture Specification - Version 1.0
[24]	SGP.22	SGP.22 Technical Specification - Version 2.2
[25]	SGP.25	SGP.25 RSP eUICC for Consumer Device Protection Profile NOTE: This document does not exist at the time of writing, reference will be valid once the document is available.
[26]	SGP.14	SGP.14 GSMA eUICC PKI Certificate Policy v1.1
[27]	EMVCo_Sec	EMVCo Security Evaluation Process 5.1 – June 2016
[28]	FS.09	FS.09 SAS-SM Methodology v3
[29]	BSI-CC-PP-0084	Security IC Platform Protection Profile with Augmentation Packages
[30]	NIST SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions
[31]	BSI TR-02102-1	Cryptographic Mechanisms: Recommendations and Key Lengths
[32]	ANSSI RGS v2 B1	Référentiel Général de Sécurité version 2.0 Annexe B1

Ref	Document Number	Title
[33]	JIL-Application-of-Attack-Potential-to-Smartcards-v2-9	Application of Attack Potential to Smartcards and Similar Devices Version 2.9, Jan 2013
[34]	NIST SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
[35]	SOG-IS	SOG-IS Smartcards and similar devices CC supporting documents at this link: https://www.sogis.eu/uk/supporting_doc_en.html
[36]	SGP.23	RSP Test Specification
[37]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174

1.7 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119 [6] and clarified by RFC8174 [37][37], when, and only when, they appear in all capitals, as shown here[6][6][6].

“FFS” or “For Further Study” means that it will be covered in the next version of SGP.21.

2 Principles

This section contains the principles related to the GSMA Remote SIM Provisioning system for the Embedded UICC.

The solution based on the requirements described within this document has to be provided in a non-discriminatory manner.

2.1 Basic Principles

Principle no.	Description
BAS1	Existing standards and specifications SHALL be used where possible for the specification of the eUICC and related provisioning systems.
BAS2	GlobalPlatform specifications SHALL be used as a framework of choice for the implementation of the eUICC.
BAS3	The overall security of the eUICC in combination with the related management processes SHALL at all times and under all circumstances be at least equivalent to the current removable UICC and its provisioning processes.
BAS4	The architecture of the eUICC and its Remote SIM Provisioning system SHALL comply with the requirements of 3GPP TS 21.133 [7].
BAS5	The architecture SHALL support a level of security with respect to the protection of Operator Credentials which is at least equivalent to the present levels of security. This applies in particular to: • the confidentiality of cryptographic keys and authentication parameters; • the integrity of Subscriber identities (e.g. IMSI).

Principle no.	Description
BAS6	The architecture SHALL support a level of security for all Profile content which is at least equivalent to the current state of the art level of security of the UICC.
BAS7	The architecture SHALL NOT compromise the security and privacy of Subscriber Data, nor the security and privacy of End User Data. Examples depending on territory include identities that can be used for tracking such as ICCID, MSISDN, EID, IMSI Ki etc.
BAS8	Regulatory issues are considered outside the scope of this document. However, any data which could be used to identify an individual SHALL be treated as personal data and subject to local regulations e.g. the EID, ICCID, etc.

Table 1: Basic Principles

2.2 Profile Principles

Principle no.	Description
PRO1	Profiles are the property of and SHALL be under the control of the issuing Operator.
PRO2	A Profile does not exist outside of an eUICC. I.e. a Profile is always located on a particular eUICC.
PRO3	A Profile SHALL be uniquely identified by its ICCID.
PRO4	An Enabled Profile in combination with an eUICC SHALL be able to carry all logical characteristics of a UICC.
PRO5	Once the Profile is enabled, all relevant UICC characteristics or features as described in ETSI 102 221 [2] specifications SHALL apply, with the exceptions as defined within this specification.
PRO6	It SHALL be possible to delete Profiles only when in a disabled state, with the exception of eUICC Memory Reset, and eUICC Test Memory Reset functions.
PRO7	Profile Management SHALL be governed by policy.
PRO8	A Profile SHALL be either an Operational Profile, a Provisioning Profile or a Test Profile.

Table 2: Profile Principles

3 Roles

3.1 eUICC Manufacturer

Role no.	Description
EUM1	The eUICC Manufacturer is responsible for the initial cryptographic configuration and security architecture of the eUICC.
EUM2	The eUICCs are delivered by the eUICC Manufacturer (EUM).
EUM3	Relevant parts of the eUICC Manufacturer's products and processes are certified by a GSMA-approved certification process.
EUM4	The EUM issues the eUICC Certificate to allow: • eUICC authentication and proof of certification to other entities; • authenticated keyset establishment between a SM-DP+ and an eUICC.

Role no.	Description
EUM5	The eUICC Manufacturer is responsible for the implementation of any LPA elements that reside in the eUICC and the compliance of the LPA with the requirements in Section 4.11.3.

Table 3: eUICC Manufacturer Role

3.2 Device Manufacturer

Role no.	Description
DM1	The Device Manufacturer is responsible for the implementation of any LPA elements that reside on the Device and the compliance of the LPA with the requirements in Section 4.11.
DM2	The Device Manufacturer is responsible for the implementation of any application that resides on the Primary Device allowing Local User Interface access to the Companion Device.

Table 4: Device Manufacturer Role

3.3 Operator and Service Provider

This section describes the characteristics of the Operator and Service Provider roles relevant to this architecture and its operation. Other characteristics exist but are considered out of scope.

Role no.	Description
OPE1	The Operator has access to a SM-DP+ via the ES2+ interface.
OPE2	In the event that a Subscriber has selected a Service Provider, that Service Provider will initiate the provisioning of a Profile Package.
OPE3	The Operator, potentially on behalf of the Service Provider, specifies the Profile characteristics and any features and applications analogous to removable UICCs.
OPE4	The Operator is able to use an OTA Platform to manage the content of its Enabled Profile in the eUICC (RAM, RFM).

Table 5: Operator Role

3.4 Subscriber and End User

Role no.	Description
SEU1	The Subscriber is the contract partner of the Service Provider for the Subscription. Note: The Subscriber MAY not be the End User.
SEU2	The End User is a human and uses the Device and/or the services related to the Enabled Profile.

Table 6: Subscriber and End User Role

3.5 Certificate Issuer

Role no.	Description
CIS1	The Certificate Issuer issues Certificates for GSMA accredited Remote SIM Provisioning entities and acts as a trusted third party for the purpose of authenticating the entities of the system.
CIS2	The Certificate Issuer communicates with the SM-DP+, SM-DS and the EUM through interfaces that are out of scope of this specification according to SGP.14 [26].

Table 7: Certificate Issuer Role

4 Remote SIM Provisioning System Architecture

This section contains the functional description of the Remote SIM Provisioning system architecture for the Embedded UICC.

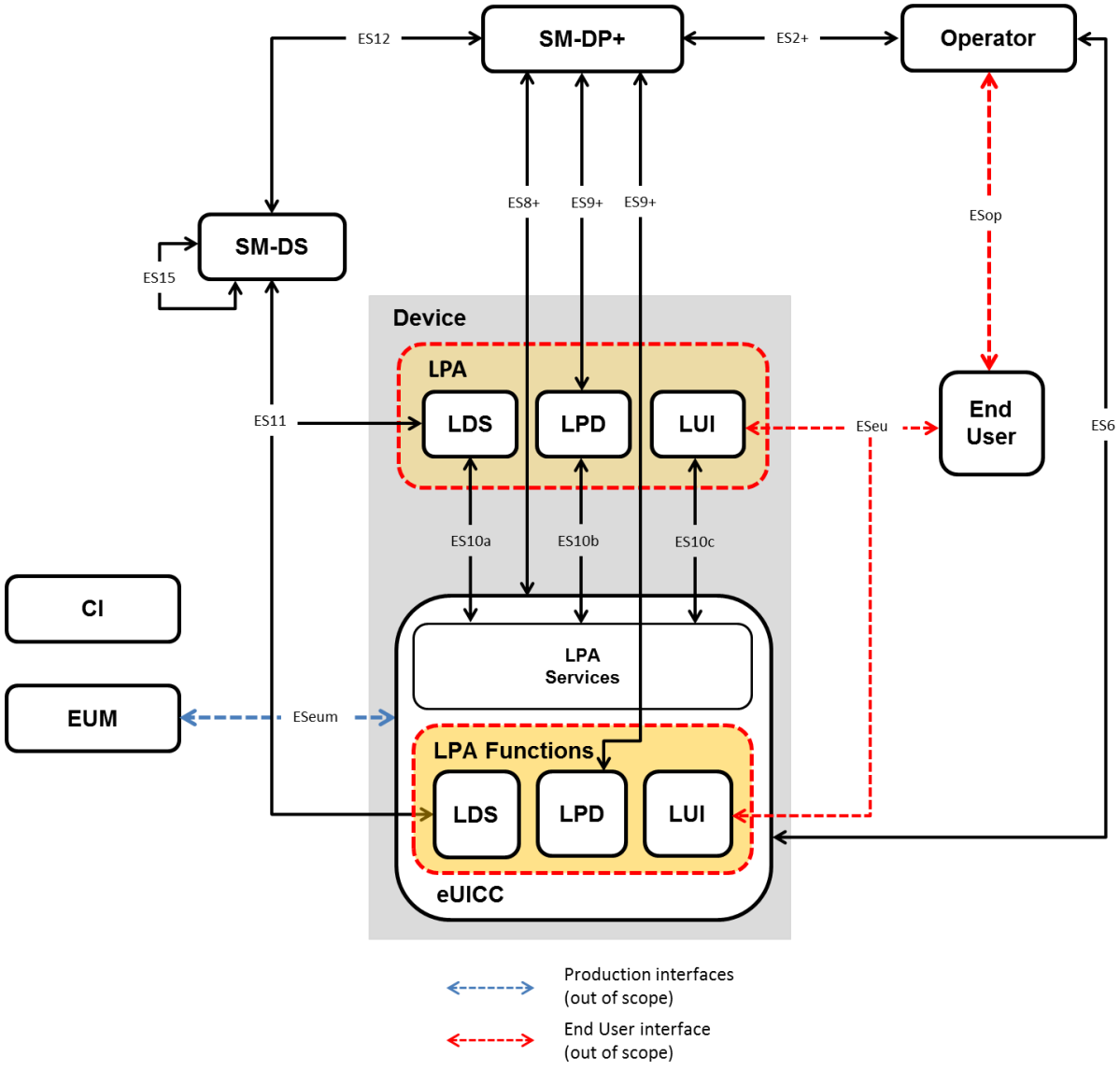


Figure 1: Remote SIM Provisioning System Architecture

4.1 eUICC Architecture

4.1.1 eUICC Architecture Overview

This section describes the internal high-level architecture of the eUICC. The eUICC architecture is similar to that used in the GSMA Remote SIM specification [8]. Profiles are provisioned based on the security framework defined in the GlobalPlatform Card Specification [9].

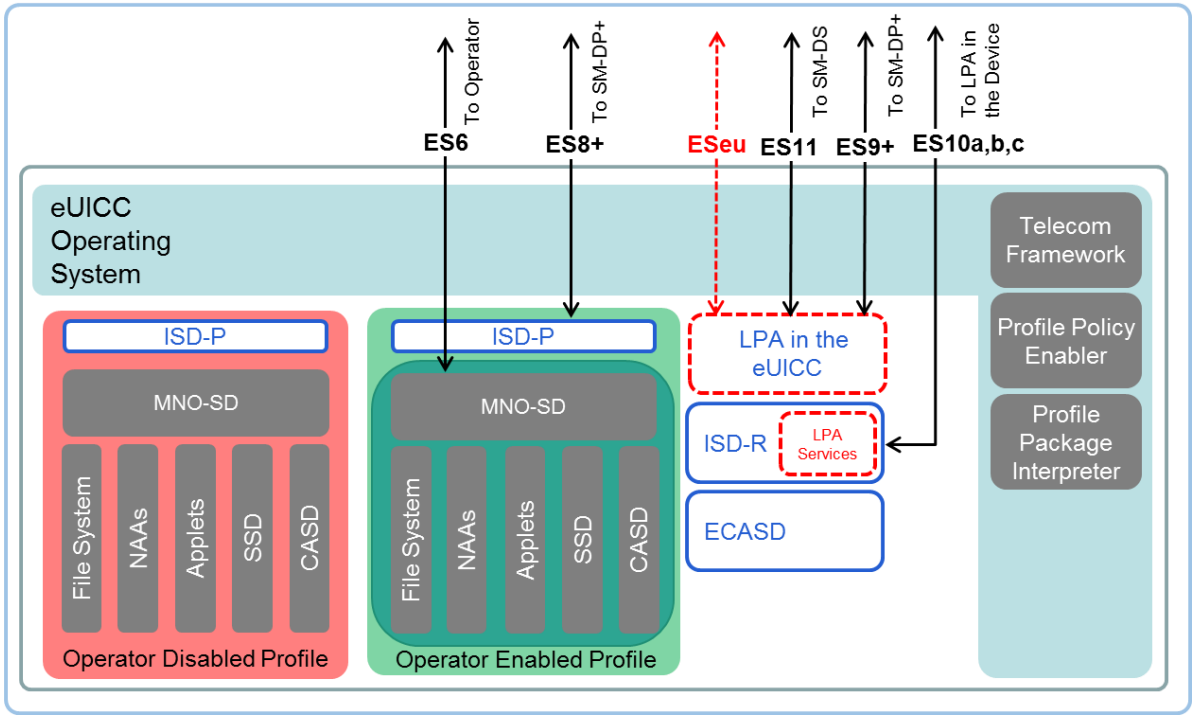


Figure 2: Schematic Representation of the eUICC

4.1.1.1 ECASD

The Embedded UICC Controlling Authority Security Domain (ECASD) is responsible for the secure storage of credentials needed to support the required security domains on the eUICC.

There SHALL only be one ECASD on an eUICC. The ECASD SHALL be installed and personalised by the EUM during the eUICC manufacturing as described in GlobalPlatform Card Specification [9].

The ECASD SHALL contain the following:

- eUICC private keys for creating signatures.
- Associated Certificates for eUICC authentication.
- The Certificate Issuers' (CI) root public keys for verifying SM-DP+ and SM-DS Certificates.
- eUICC Manufacturers' (EUMs) keyset for key/Certificate renewal.

Additionally, the ECASD SHALL provide security functions used during key establishment and eUICC authentication.

4.1.1.2 ISD-R

The ISD-R is responsible for the creation of new ISD-Ps and the lifecycle management of all ISD-Ps.

4.1.1.3 ISD-P

The ISD-P is a secure container (security domain) for the hosting of a Profile. The ISD-P is used for Profile download and installation in collaboration with the Profile Package interpreter for the decoding/interpretation of the received Bound Profile Package.

The ISD-P is the on-card representative of the SM-DP+.

4.1.1.4 MNO-SD

The MNO-SD is the on-card representative of the Operator. It contains the Operator's Over-The-Air (OTA) Keys and provides a secure OTA channel.

4.1.1.5 Profile Policy Enabler

The eUICC Operating System (OS) service which offers Profile Policy Rules validation and enforcement.

4.1.1.6 Telecom Framework

The telecom framework is an operating system service that provides standardised network authentication algorithms to the NAAs hosted in the ISD-Ps. Furthermore, it offers the capability to configure the algorithms with the necessary parameters.

4.1.1.7 Profile Package Interpreter

The Profile Package interpreter is an eUICC operating system service that translates the Profile Package data into an installed Profile using the specific internal format of the target eUICC.

4.1.1.8 LPA Services

The LPA services provide necessary access to the services and data required by the LPA functions for the following:

1. The Root SM-DS address.
2. The optionally stored default SM-DP+ address.
3. Facilitates the reception of the Bound Profile Package in transfer from the LPA.
4. Provide information regarding the installed Profiles and their Profile Metadata.
5. Provides Local Profile Management.
6. Provides functions for the LPA to authenticate and interact with the SM-DS.
7. Ensures access to the EID is restricted to only the LPA.

4.2 Interfaces

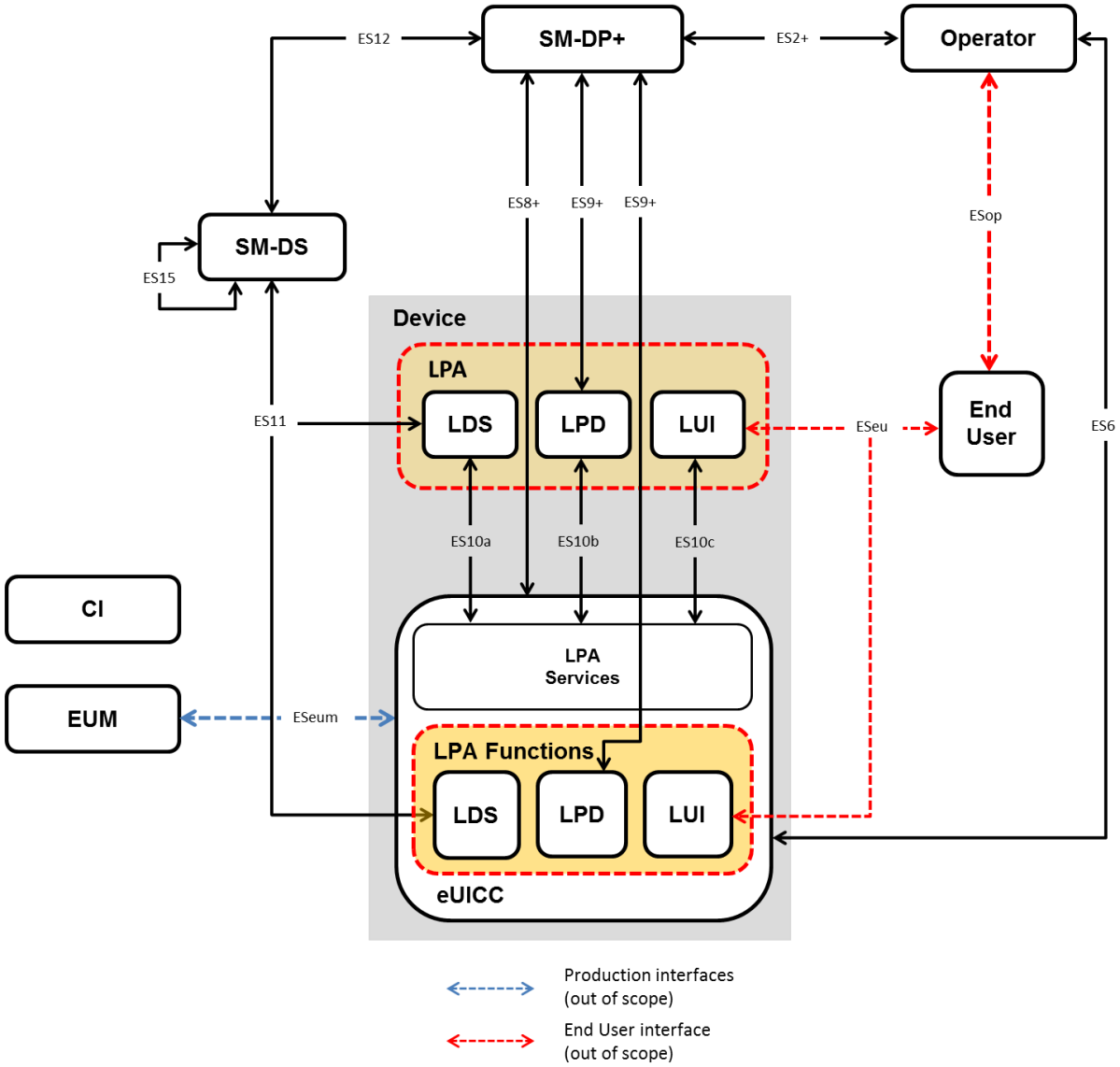


Figure 3: Interfaces on the eUICC Architecture with the LPA in the Device Configuration

4.2.1 Operator – SM-DP+ (ES2+)

The ES2+ interface is used by the Operator to order Profiles for specific eUICCs as well as other administrative functions.

4.2.2 Operator – End User (ESop)

ESop is the interface between the Operator and the End User.

This interface is out of scope of this specification.

4.2.3 End User - LUI (ESeu)

ESeu is the interface between the End User and the LUI.

In a Primary/Companion Device scenario the LUI used SHALL only reside within the Companion Device or its eUICC.

The ESeu interface is used to support the following requirements:

Req no.	Description
ESeu1	The Local Profile Management Operations SHALL be executed only over the ESeu interface.
ESeu2	Each Local Profile Management Operation SHALL be explicitly initiated by the End User, and verified by User Intent.
ESeu3	The ESeu interface SHALL support the triggering and confirmation of the Profile download and installation operation and Local Profile Management Operations requested by the End User.

Table 8: End User to LUI (ESeu) Interface Requirements

4.2.4 Operator – eUICC (ES6)

The ES6 interface is used by the Operator for the management of Operator services via OTA services.

4.2.5 SM-DP+ – LPD (ES9+)

The ES9+ interface is used to provide a secure transport for the delivery of the Bound Profile Package between the SM-DP+ and the LPD.

4.2.6 SM-DP+ – eUICC (ES8+)

The ES8+ interface 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.

4.2.7 SM-DP+ – SM-DS (ES12)

The ES12 interface allows any SM-DP+ to issue or remove Event Registrations on the SM-DS.

4.2.8 LDS – SM-DS (ES11)

The ES11 interface allows the LDS to retrieve Event Records for the respective eUICC.

4.2.9 EUM – eUICC (ESeum)

ESeum is the interface between the EUM and the eUICC. This interface is out of scope of this specification.

4.2.10 LDS – LPA Services (ES10a)

The ES10a interface is used by the LPA in the Device to get the configured addresses from the eUICC for Root SM-DS, and optionally the default SM-DP+.

4.2.11 LPD – LPA Services (ES10b)

The ES10b interface is used by the LPD in the Device and the LPA services to transfer a Bound Profile Package to the eUICC.

4.2.12 LUI – LPA Services (ES10c)

The ES10c interface is used between the LUI in the Device and the LPA services for Local Profile Management by the End User.

4.2.13 SM-DS – SM-DS (ES15)

In the case of deployments with cascaded SM-DSs, the ES15 interface is used to connect the SM-DSs.

4.2.14 Device – SM-DP+ (Established Connection)

This connection will be provided either by:

- An internet connectivity available or provided on the same Device where the LPA resides
  or
- An internet connection shared from another Device via a local go-between connection

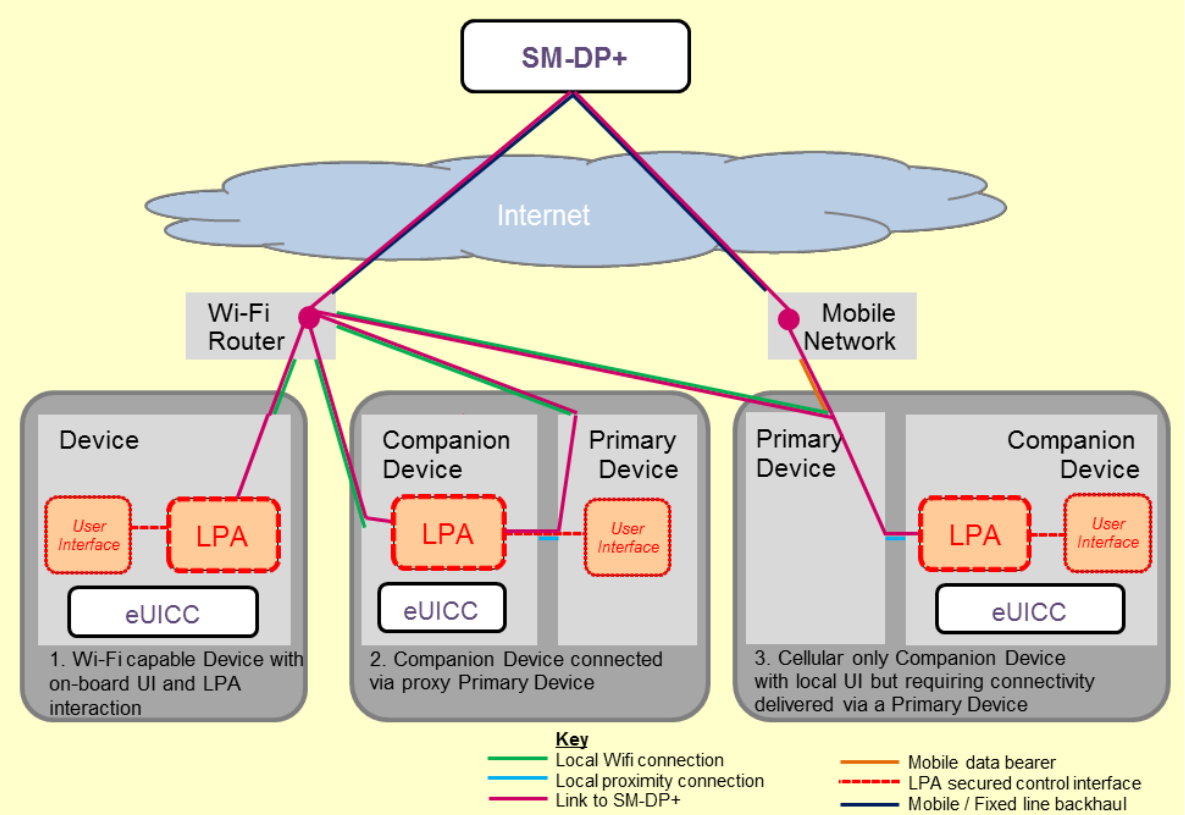


Figure 4: Example Connection Methods for Companion Devices to reach out to the SM-DP+

4.2.15 General Interface Requirements

Req no.	Description
INT1	All interfaces from the eUICC SHALL indicate the eSVN.
INT2	The behaviour of all interfaces SHALL support the indicated eSVN.
INT3	During the indication of the supported eSVN from the eUICC to the SM-DP+, the eUICC version SHALL be used or the procedure SHALL fail. See table below.
INT4	All communicating entities involved in Remote SIM Provisioning SHALL be mutually authenticated. The Device and the eUICC are considered as one entity in this context.

Table 9: General Interface Requirements

Platform	Version 1 (V1)	Version 2 (V2)	Version 3 (V3)
eUICC V1	Platform uses V1	Platform uses V1 or fails.	Platform uses V1 or fails.
eUICC V2	X	Platform uses V2	Platform uses V2 or fails.
eUICC V3	X	X	Platform uses V3

Table 10: eUICC Version vs. Platform

4.3 eUICC Requirements

Req no.	Description
EUICC1	The eUICC SHALL be a discrete or integrated tamper resistant component consisting of hardware and software, capable of securely hosting applications as well as confidential and cryptographic data. Note: Wherever a distinction is required, the former is referred to as Discrete eUICC, and the latter as Integrated eUICC.
EUICC2	A removable eUICC is packaged in a standardised ETSI Form Factor [2].
EUICC3	The Discrete eUICC SHALL be either removable or non-removable.
EUICC4	The behaviour of the eUICC with an Enabled Profile SHALL be equivalent to the UICC.
EUICC5	The eUICC SHALL be able to contain zero or more Profiles.
EUICC6	At a maximum, only one Profile SHALL be enabled at any point in time.
EUICC7	The behaviour of a NAA USIM or ISIM within a Profile on an eUICC SHALL be identical to a removable UICC NAAs USIM or ISIM. Note: No changes to existing 3GPP/3GPP2 USIM, CSIM and ISIM specifications are expected.
EUICC8	The eUICC SHALL support Milenage [11][12] and TUAK [10] algorithm sets[10][10].
EUICC9	The ownership of the eUICC MAY change throughout its lifetime as can the Device. Note: According to CERTEU11, the EUM keyset belongs to the EUM for the lifetime of the eUICC.

Req no.	Description
EUICC10	If any Profile Management operation does not complete successfully, the eUICC SHALL maintain the state it was in before it received the request.
EUICC11	The eUICC SHALL contain an ECASD and ISD-R security domains installed and personalised during manufacture.
EUICC12	It SHALL not be possible to delete or disable the ECASD after eUICC manufacture.
EUICC13	The ISD-R SHALL be responsible for the creation of new ISD-Ps and the lifecycle management of all ISD-Ps.
EUICC14	The ISD-R SHALL be installed and personalised by the EUM during eUICC manufacturing as described in GlobalPlatform Card Specification [9].
EUICC15	The eUICC SHALL support an eUICC Memory Reset. This can only be requested by the End User.
EUICC16	If the eUICC supports Test Profiles, the eUICC SHALL support eUICC Test Memory Reset.
EUICC17	The eUICC SHALL support the eUICC Profile Package Interoperable format as defined by Trusted Connectivity Alliance [5].
EUICC18	An ISD-R SHALL: • be created within an eUICC at the time of manufacture; • NOT be deleted or disabled; • NOT be able to perform any operations inside an ISD-P.
EUICC19	An eUICC MAY provide LPA functions.
EUICC20	An ISD-P SHALL be created by the ISD-R at the request of the SM-DP+.
EUICC21	Communication between the eUICC and the SM-DP+ SHALL be protected in authenticity, integrity and confidentiality.
EUICC22	The eUICC SHALL NOT export Profiles installed on the eUICC.
EUICC23	The eUICC SHALL enforce an isolation of Profiles and prevent Profiles from operating outside of their execution environment i.e. Profile SHALL run in a sandbox.
EUICC24	The integrity of the Bound Profile Package SHALL be ensured during its installation on the eUICC.
EUICC26	Profile keys and algorithm parameters SHALL NOT be extractable from the eUICC.
EUICC27	All cryptographic functions SHALL be implemented in a robust tamper-resistant way and be resistant to side-channel attacks.
EUICC28	The Operator SHALL be able to update the OTA Keys in its Profile on the eUICC in a secure and confidential way, reusing existing OTA Platform mechanisms.
EUICC29	A downloaded Profile Package SHALL be installed on the eUICC in a disabled state.
EUICC30	The eUICC SHALL always report its eSVN in the first communication during the commencement of each session with the SM-DP+ or SM-DS.
EUICC31	The EUM SHALL install an eUICC Certificate in the eUICC used to authenticate the eUICC and verify the eUICC certification.

Req no.	Description
EUICC32	The EUM SHALL install an EUM Certificate in the eUICC used to verify the eUICC Certificate.
EUICC33	The eUICC SHALL have a means to authenticate itself to the SM-DS.
EUICC34	The eUICC SHALL protect itself against unauthorised access.
EUICC35	Upon Profile deletion, the eUICC SHALL ensure a complete deletion of all data related to the Profile.
EUICC36	The eUICC SHALL only accept Profile Management operations sent from the LPA in either the eUICC, or the Device.
EUICC37	The eUICC SHALL reject any Profile Management operations that are in conflict with the Profile Policy Rules of the respective Profile.
EUICC38	If any Bound Profile Package download or installation does not complete successfully, the eUICC SHALL maintain the state it was in before it received the request.
EUICC39	The eUICC SHALL support GlobalPlatform Secure Element Access Control [15].
EUICC40	There SHALL be a means to pre-set a default SM-DP+ address in the eUICC.
EUICC41	The eUICC SHALL store the Root SM-DS address.
EUICC42	The eUICC SHALL be able to send a delete Notification to the LPA to notify the Notification Receivers that the Profile has been deleted.
EUICC43	In EUICC42, if connectivity is not available to send the Notification of deletion to the Notification Receivers, each Notification SHALL be retained and sent as soon as connectivity becomes available again.
EUICC44	The delete Notification process SHALL also be executed for each deleted Profile in case of eUICC Memory reset.
EUICC45	The eUICC SHALL support a set of standard functions and services including, but not limited to Java Applications, USIM Toolkit functions and GlobalPlatform features. The list of supported functions and services (e.g. API package names and versions) SHALL be explicitly referenced within the technical specification (SGP.22 [24]). A different set of functions and services MAY be defined/supported according to the different Embedded UICC categories as defined in Annex D.
EUICC46	The eUICC SHALL support at least the following USIM Toolkit commands: • PROVIDE LOCAL INFORMATION including the following fields: local info, IMEI, network measure results, date & time, access technology • TERMINAL PROFILE • ENVELOPE (SMS-PP DOWNLOAD) • SEND SHORT MESSAGE • DISPLAY TEXT • GET INPUT • RING TONE
EUICC47	An eUICC SHALL support at least two sets of elliptic curve parameters preloaded by the EUM during eUICC manufacturing, defined in GSMA SGP.22 [24].

Req no.	Description
EUICC48	Each Notification SHALL be uniquely identifiable and SHALL be signed by the eUICC.
EUICC49	Each Notification SHALL be protected against re-play attacks and signed by the eUICC.
EUICC50	[Void]
EUICC51	[Void]
EUICC52	The Profile SHALL be able to contain a list of zero or more Notification Receivers for each type of Notification.
EUICC53	The eUICC SHALL support SHA-1. Usage of SHA-1 SHALL be strictly limited to applications inside the Profile where the use of SHA-1 is required.
EUICC54	The EID SHALL not be modifiable. The EID SHALL not be affected by any of the procedures, including the change of the eUICC Private keys.
EUICC55	An Integrated eUICC SHALL conform to the additional requirements defined in Annex J.
EUICC56	The Integrated eUICC SHALL be based on an Integrated TRE.
EUICC57	An Integrated eUICC SHALL be able to execute the test cases defined in SGP.23 [36].

Table 11: eUICC Requirements

4.4 eUICC Eligibility Check

The eUICC eligibility check enables a SM-DP+ to validate the eligibility of an eUICC for the installation of a Profile using information sent by the eUICC. The set of information sent by the eUICC to the SM-DP+ for eligibility checking purposes is referenced herein as the eUICC Eligibility Check Information. Some eUICC eligibility check parameters MAY be required due to Device capabilities which must be supported by the Profile/eUICC and delivered as part of the eUICC Eligibility Check Information set.

Note: Device capability refers to a Device feature or service-enabling function provided by the Device that MAY have a direct effect on the content of the Profile or the procedure used to download the Profile, and consequently requires support from the eUICC.

4.3.1 eUICC Eligibility Check Requirements

Req no.	Description
ELG1	The eUICC SHALL indicate the specification version it is supporting. This parameter SHALL be transmitted to the SM-DP+ during the eUICC eligibility check.
ELG2	The eUICC SHALL include the available memory in the eUICC Eligibility Check Information.
ELG3	The eUICC SHALL declare in the Eligibility Check Information if it is unable to accept an additional Profile.
ELG4	The eUICC SHALL provide a valid current Certificate to the SM-DP+ signed by the EUM with the Eligibility Check Information.

ELG5	The eUICC SHALL provide an identification of the EUM with the Eligibility Check Information.
ELG6	The eUICC SHALL provide in the Eligibility Check Information, the current OS version.
ELG7	The eUICC SHALL provide in the Eligibility Check Information Device enabler information relating to services that MAY need Profile support (e.g. NFC enablers).
ELG8	Eligibility Check Information SHALL be integrity and authenticity protected by the eUICC for its sending to the SM-DP+.
ELG9	The eUICC SHALL indicate the application runtime environment version and libraries versions supported in eUICC Eligibility Check Information.
ELG10	The eUICC SHALL indicate cryptographic algorithms and their respective key lengths supported in the eUICC Eligibility Check Information.
ELG11	The eUICC SHALL declare in the Eligibility Check Information the list of supported CIs.
ELG12	The eUICC SHALL indicate its current certification status in the Eligibility Check Information.
ELG13	If the eUICC is NFC capable (e.g. CAT3) the Device SHALL indicate its support for the relevant NFC services including its current certification status during the eUICC Eligibility Check.
ELG14	The eUICC SHALL indicate its category (see Annex D). This parameter SHALL be transmitted to the SM-DP+ during the eUICC Eligibility Check.
ELG15	An eUICC SHALL provide information indicating if it is a Discrete eUICC or an Integrated eUICC.

Table 12: eUICC Eligibility Check Requirements

Note: It is assumed that the EID is normally shared to the SM-DP+ by other means and could be used for the eligibility check procedure.

4.5 Device Requirements

Req no.	Description
DEV1	The Device SHALL conform to the terminal requirements within ETSI TS 102 221 [2] with the exceptions as defined in this specification.
DEV2	There SHALL be a means for the End User to obtain the EID through the Device software. This SHALL only be possible through the LUI.
DEV3	If an eUICC is within the Device packaging, then the EID SHALL be printed in machine readable form on the Device packaging.
DEV4	Bearer connection of the Companion Device to the SM-DP+ SHALL only be determined by the bearer availability. Note: The Companion Device MAY use any connectivity method available to connect to the SM-DP+.
DEV5	Devices compliant with the GSMA NFC Handset Requirements [17] SHALL support the Open Mobile API [19] used by the Device applications to exchange data with their counterpart applications running in the Enabled Profile on the eUICC.

Req no.	Description
DEV6	The implementation of the Remote SIM Provisioning specification in the Device SHALL not impact the potential use of the SIM Lock mechanism defined in 3GPP TS 22.022 [16].[16]
DEV7	In the case where the Device supports both the LPA in the Device, and the LPA in the eUICC, the Device SHALL have a mechanism (setting or configuration parameter) that sets which LPA SHALL be used.
DEV8	The End User SHALL be able to modify the parameter defined in DEV7.
DEV9	A Device that supports an embedded UICC without an LPA in the eUICC, SHALL provide LPA functions.
DEV10	A Device that supports only an embedded UICC with an LPA in the eUICC, MAY provide LPA functions.
DEV11	If the Device supports Device Test Modes, the Device SHALL support eUICC Test Memory Reset. eUICC Test Memory Reset can only be requested by the End User when the Device is in Device Test Mode.
DEV12	Where technically feasible, the Device SHALL implement a mechanism allowing the End User to protect the access to the Device and its Profile Management Operations with personal data. Implementation is OEM specific. Note: This can be achieved by the implementation of a Device PIN lock, fingerprint, password, facial recognition (etc.)
DEV13	The End User SHOULD be able to enable/disable the mechanism described in DEV12. Implementation is OEM specific. Note: The mechanism described in DEV12 should be enabled by default.
DEV14	With respect to LPA41, a Device containing any additional feature that affects the status of Operational Profiles SHOULD enforce the Confirmation Level of the equivalent Local Profile Management Operations defined in this specification. The mechanism and process of the Confirmation Level is implementation specific. The End User SHOULD be able to revoke/unset a cached Confirmation previously given, if any. NOTE: In case the LPA or a Device application performs automatic Profile management, the Device or the application must ensure that the End User has been made fully aware of the conditions under which the service operates. NOTE: The Device protects against abuse or malevolence of management of profiles as compared to the specified LPA functionalities.

Table 13: Device Requirements

4.5.1 Device Capability Requirements

Req no.	Description
DEVCAP1	There SHALL be a mechanism that is able to provide the Device capabilities to the SM-DP+.

Table 14: Device Capability Requirements

4.5.2 Device with Integrated eUICC

Req no.	Description
DIE1	Access to any Remote Memory used by the TRE to store software and data as defined in GS01 SHALL be protected against attacks on availability (e.g. Denial of Service, memory corruption, tampering) by other Device components.
DIE2	All Integrated TRE software and data stored in Remote Memory outside the SoC, per GS01 SHALL be protected against access by non Integrated TRE components.

Table 15: Device with Integrated eUICC Requirements

4.6 Device Initialisation

4.6.1 Device Reset Requirements

Req no.	Description
FAC1	It SHALL be possible for the End User to perform any type of Device reset without affecting the status of the eUICC.
FAC2	The Device SHALL by means of a secured procedure, trigger/request the eUICC Memory Reset.
FAC3	The Device SHALL by means of a secured procedure, trigger/request the eUICC Test Memory Reset.

Table 16: Device Reset Requirements

4.6.2 eUICC Memory Reset Requirements

Req no.	Description
MEM1	eUICC Memory Reset SHALL delete all Profiles on the eUICC apart from pre-installed Profiles that are flagged as permanent.
MEM2	eUICC Memory Reset SHALL delete all Profiles on the eUICC regardless of their Profile Policy Rules but not the Provisioning Profile or preinstalled Test Profiles.
MEM3	Strong Confirmation SHALL be verified in order to initiate eUICC Memory Reset.
MEM4	In addition to MEM3, other secure means MAY be provided to perform the eUICC Memory Reset function. The same level of security as is offered by the LUI based reset function SHALL apply. User Intent and Confirmation Request SHALL apply.

Table 17: eUICC Memory Reset Requirements

4.6.3 eUICC Test Memory Reset Requirements

Req no.	Description
MEMT1	eUICC Test Memory Reset SHALL delete all post-issuance installed Test Profiles on the eUICC including the Enabled Test Profile if any.
MEMT2	Simple Confirmation SHALL be verified in order to enable eUICC Test Memory Reset.

MEMT3	If Test Profiles are not supported, then eUICC Test Memory Reset is not required.

Table 18: eUICC Test Memory Reset Requirements

4.7 Profile Requirements

4.7.1 Test Profile Requirements

Req no.	Description
TPRO1	It is OPTIONAL for the removable eUICC to support the requirements of Test Profiles described in this section. If Test Profiles are not supported, it SHALL not be possible to download Test Profiles into the eUICC.
TPRO2	Test Profiles SHALL NOT be able to authenticate to an Operator's mobile network using Operator Credentials. The eUICC SHALL ensure that such Profiles cannot be used to connect to any Operator's mobile network even if authentication information is contained in the Test Profile.
TPRO3	A Test Profile SHALL be installed in its own individual ISD-P.
TPRO4	Test Profiles MAY be pre-installed on the eUICC.
TPRO5	Test Profiles SHALL only be visible and usable when the Device is in Device Test Mode.
TPRO6	It SHALL be possible to download, install, enable, disable or delete Test Profiles in the eUICC only in Device Test Mode with the exception of the eUICC Memory Reset operation.
TPRO7	Test Profiles, as with any other Profile, SHALL be managed through a certified SM-DP+.
TPRO8	The enabling of a Test Profile SHALL override the 'Disabling of this Profile is not allowed' (POL RULE1) Profile Policy Rule.
TPRO9	When the Device Test Mode is deactivated, the LPA SHALL disable any enabled Test Profile.
TPRO10	When the Test Profile is disabled, the eUICC SHALL enable the Operational Profile that was previously enabled, if any.
TPRO11	The Device Test Mode activation SHALL be obfuscated from the End User.
TPRO12	When exiting Device Test Mode, an End User notice SHALL be presented to prompt the tester to perform an eUICC Test Memory Reset.

Table 19: Test Profiles Requirements

The Device MAY implement a mechanism for connecting an external SIM card for the purpose of testing in the context of Device repair, without affecting the state of the eUICC.

4.7.2 Provisioning Profile Requirements

Req no.	Description
PPRO1	Provisioning Profiles SHALL be based on the same format structure as described for the Profile (Figure 2).
PPRO2	A Provisioning Profile MAY be enabled by the LPA upon End User request for operations defined in PPRO6 if establishment of the connectivity using the currently Enabled Profile is unsuccessful. If this results in an Operational

	Profile being disabled, the End User SHALL first give consent to the loss of communication provided by the Enabled Profile.
PPRO3	Provisioning Profiles and their associated Profile Metadata SHALL not be visible to the End User on the LUI.
PPRO4	Provisioning Profiles SHALL not be selectable by the End User.
PPRO5	Provisioning Profiles SHALL not be deleted through any action by the End User including the use of eUICC Memory Reset.
PPRO6	Provisioning Profile SHALL only be used for the intended purposes of Profile downloading and related Profile maintenance functions. The Provisioning Profile SHALL not be used as an Operational Profile.
PPRO7	PPRO6 SHALL be enforceable in the RSP architecture.

Table 20: Provisioning Profile Requirements

4.8 Profile Metadata Requirements

Req no.	Description
META1	All Profiles SHALL have associated Profile Metadata.
META2	The Profile Metadata SHALL be stored in the eUICC.
META3	The Profile Metadata SHALL be accessible irrespective of the state of the Profile.
META4	The Profile Metadata SHALL include a field for the Service Provider name. Note: EFSPN is already used in a different context outside of this specification and could be blank.
META5	The Profile Metadata SHALL include a field for the ICCID of the Profile.
META6	The Profile Metadata SHALL include a field for the End User nickname of the Profile.
META7	The Profile Metadata SHALL include a field for containing a short description of the Profile defined by the Operator/Service Provider.
META8	The eUICC SHALL support the ‘set/edit nickname’ function.
META9	The Profile Metadata SHALL always be available to the LUI.
META10	The Profile Metadata SHALL include an OPTIONAL field to allow the display of an icon defined by the Operator/Service Provider for the respective Profile.
META11	The Profile Metadata SHALL be able to include a copy of the Profile Policy Rules associated to the Profile.
META12	All Profiles SHALL be uniquely identified in the Profile Metadata as Operational, Provisioning or Test Profile.
META13	An Operator SHALL be able to access and update the following Profile Metadata of its Profile using the ES6 interface if the Profile is Enabled: • Service Provider name • Short description of the Profile • Icon of the Profile

Table 21: Profile Metadata Requirements

4.9 NFC Requirements

An NFC Device and an NFC eUICC SHALL be compliant with the following list of requirements:

Req no.	Description
NFC1	An NFC Device SHALL be compliant with GSMA TS 26 [17][17][17].
NFC2	After installation of an Operational Profile, the NFC eUICC SHALL support all requirements as specified in the SGP.03 GSMA NFC UICC Requirements Specification [20].
NFC3	The NFC Device SHALL retrieve and enforce access control rules as specified in the GlobalPlatform SEAC specification [15].
NFC4	The eUICC SHALL be able to generate proof that the Operational Profile has been deleted.
NFC5	All NFC applications and NFC enabling applications (e.g. ARA-M, PPSE, CRS, CREL, etc.) attached to an Operational Profile SHALL be included under the ISD-P created for the Profile, either under the MNO-SD or in an SD hierarchy with a self-extradited SSD with authorised management privilege.
NFC6	The NFC eUICC solution SHALL be able to provide assurance to NFC application Service Providers that the combination of an eUICC and Operational Profile is trusted. This solution SHALL be based on the CASD that is part of the Operational Profile and scenario Push 2B and scenario 3 as specified by SGP.03 [20].
NFC7	If the NFC eUICC is compliant with M4M, the eUICC SHALL reset all the M4M virtual cards associated to that Profile when a Profile containing M4M applications is disabled.
NFC8	The appropriate NFC related certification information SHALL be part of the information shared with the SM-DP+ during the eUICC Eligibility Check.
NFC9	A NFC Device SHALL at least have an embedded eUICC or have the capability to support a removable eUICC that is compliant with CAT3 and SGP.03 [20] in either instance.

Table 22: NFC Requirements

4.10 Subscription Manager Data Preparation + (SM-DP+)

4.10.1 SM-DP+ Overview

The SM-DP+ is responsible for the creation, generation, management and the protection of resulting Profiles upon the input/request of the Operator. It is also responsible for the delivery of a Profile within a Bound Profile Package, making the Bound Profile Package available for the secure delivery. In addition, the SM-DP+ is responsible for requesting the creation of the ISD-P in the eUICC into which the Profile will be installed. The SM-DP+ will also be the off-card entity that will be responsible for the lifecycle management of the ISD-P that was created at its request. This is performed via the distinct functions listed below.

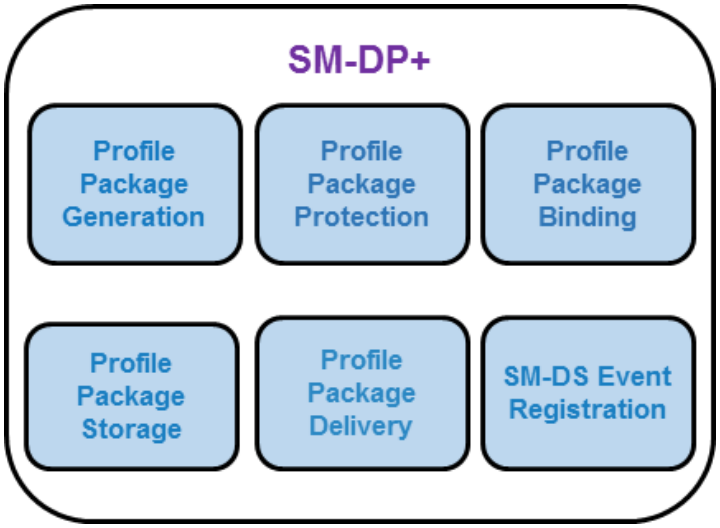


Figure 5: SM-DP+ Functions

Function name	Description
Profile Package Generation	Creates Profile Packages [i.e. Personalised Profiles, including (IMSI, Ki, ICCID…)] from Profile Descriptions agreed with Operators. This can be an off-line batch or real time process.
Profile Package Protection	Secures each Profile Package according to the security process creating the Protected Profile Package.
Profile Package Binding	Binds the Protected Profile Package to a target eUICC using the security process thus creating the Bound Profile Package.
Profile Package Storage	Temporarily stores Protected Profile Packages or Bound Profile Packages for subsequent delivery to the eUICC.
Profile Package Delivery	Securely transmits and installs the Bound Profile Package to the eUICC through the LPA.
SM-DS Event Registration	Notifies the SM-DS of a pending operation for a specific eUICC.

Table 23: SM-DP+ Function Descriptions

4.10.2 SM-DP+ Requirements

Req no.	Description
SMDP1	The SM-DP+ SHALL act on behalf of an Operator.
SMDP2	The SM-DP+ SHALL be able to initiate the request for ISD-P creation as part of the Bound Profile Package delivery.
SMDP3	The SM-DP+ SHALL establish an end-to-end secure channel to the eUICC to download and install Bound Profile Packages on the eUICC.
SMDP4	The SM-DP+ SHALL link a Protected Profile Package for binding to a specific eUICC only at the request of the respective Operator.
SMDP5	The SM-DP+ SHALL create a Bound Profile Package from the linked Protected Profile Package only at the request of the respective eUICC.
SMDP6	The SM-DP+ SHALL be able to create a Bound Profile Package for any Certified eUICC.

Req no.	Description
SMDP7	Only the target eUICC SHALL be able to decrypt the content of a Bound Profile Package delivered by the SM-DP+.
SMDP8	Profile Packages SHALL only leave the SM-DP+ after completing all production steps, Profile Package Protection, and binding.
SMDP9	Communication session between the SM-DP+ and the LPA SHALL be terminated by the SM-DP+ after execution of intended Operation(s).
SMDP10	End-to-end communication between the SM-DP+ and the eUICC involved in the Profile download and installation SHALL be protected in terms of integrity, authenticity and confidentiality.
SMDP11	Profile Packages stored within the SM-DP+ SHALL always be protected through encryption.
SMDP12	On the SM-DP+, backups as well as used data within the Profile creation and storage infrastructure SHALL be discarded using secure deletion procedures (logically and physically).
SMDP13	SM-DP+/eUICC communication SHALL incorporate Perfect Forward Secrecy (PFS).
SMDP14	The transport used for the Bound Profile Package SHALL implement anti-replay mechanisms between the SM-DP+ and the eUICC.
SMDP15	Connectivity to the SM-DP+ SHALL be aborted and an explicit error message SHALL be triggered by the SM-DP+ upon failure to verify authenticity of the connecting party. (No message SHALL be sent to the connecting party)
SMDP16	After a configurable number of failed attempts to download a Bound Profile Package to the LPA, the transport encryption procedure SHALL be renewed. If subsequent attempts to download the Bound Profile Package fail more than a configurable number of times, the provisioning transaction SHALL be terminated and the Operator SHALL be notified.
SMDP17	The SM-DP+ SHALL use a secure version of Internet protocols whenever available (e.g. DNSSEC, DNSCurve, etc.).
SMDP18	The SM-DP+ SHALL prepare Profile Packages following the eUICC Profile Package Interoperable Format Specification as defined by Trusted Connectivity Alliance [5].
SMDP19	The SM-DP+ SHALL be able to create Bound Profile Packages on demand.
SMDP20	It SHALL be possible for the SM-DP+ to create Profile Packages in bulk.
SMDP21	The SM-DP+ SHALL send a confirmation of the successfully completed download and installation of a Profile to the Operator.
SMDP22	There SHALL be a mechanism to remove any relationship between any SM-DP+ and the ISD-P following the successful installation of the Profile. Such a mechanism SHALL either be ordered by the Operator or be performed by the Operator itself. If such deletion mechanism is used, there will be no off-card entity responsible for managing the ISD-P of the installed Profile.
SMDP23	The SM-DP+ SHALL be globally uniquely identified by its SMDPid.
SMDP24	The SM-DP+ Certificate SHALL include the SMDPid.

Req no.	Description
SMDP25	The SM-DP+ SHALL be able to send a Notification to the Operator informing them that a specific Bound Profile Package download is about to start.
SMDP26	The SM-DP+ SHALL be able to send an eUICC Eligibility Check Information report and other relevant information (e.g. Activation Code, ICCID, etc.) to the Operator ahead of/prior to the eUICC Bound Profile Package download.
SMDP27	The SM-DP+ SHALL be able to perform Event Registrations to the SM-DS.
SMDP28	The SM-DP+ SHALL be able to request from an Alternative SM-DS not to propagate the Event Registration to the Root SM-DS.
SMDP29	The SM-DP+ SHALL be able to send a Profile delete Notification to the Operator owning a Profile when a related delete Notification is received from the eUICC.
SMDP30	The SM-DP+ SHALL support the following states for a Profile Package, triggered by the Profile Owner: • A Profile Package is not released for Profile Package download. • A Profile Package is released for Profile Package download.
SMDP31	The SM-DP+ SHALL be able to select the elliptic curve parameter in the Profile download procedure.
SMDP32 (FFS)	It SHALL be possible for a SM-DP+ to conduct an Event Record Query to a SM-DS (Root or Alternative) for the purpose of auditing Event Registrations it owns.
SMDP33 (FFS)	The SM-DP+ SHALL be able to query the existence of an Event Record on the Root SM-DS or the Alternative SM-DS, identified by the EID or the Event-ID over the ES12 interface.
SMDP34 (FFS)	Response to a SM-DP+ Event Record Query SHALL only occur where the Root SM-DS or Alternative SM-DS validates the Event Record ownership.
SMDP35 (FFS)	Ownership validation of a SM-DP+ Event Record Query SHALL only use the requester's address or the submitted Event-ID against the components of the Event Record held.
SMDP36	A SM-DP+ SHALL support all sets of elliptic curve parameters as defined in GSMA SGP.22 [24].
SMDP37	If a Profile Package is not yet released for download then the LPA SHALL be informed by means of a specific error code.

Table 24: SM-DP+ Requirements

4.10.3 Default SM-DP+ Address on the eUICC Requirements

Req no.	Description
DF1	The default SM-DP+ address in the eUICC SHALL be ignored if an SM-DP+ address is present in an AC being presented to the LUI.
DF2	The default SM-DP+ address in the eUICC SHALL be accessible by the LPA to establish a connection to this SM-DP+.
DF3	The default SM-DP+ address in the eUICC MAY be left blank.

DF4	If the default SM-DP+ address in the eUICC is blank, then the use of the SM-DS discovery procedure or an SM-DP+ address in an AC SHALL be required to establish the target SM-DP+.
DF5	[Void]

Table 25: Default SM-DP+ Address on the eUICC Requirements

4.11 Local Profile Assistant (LPA)

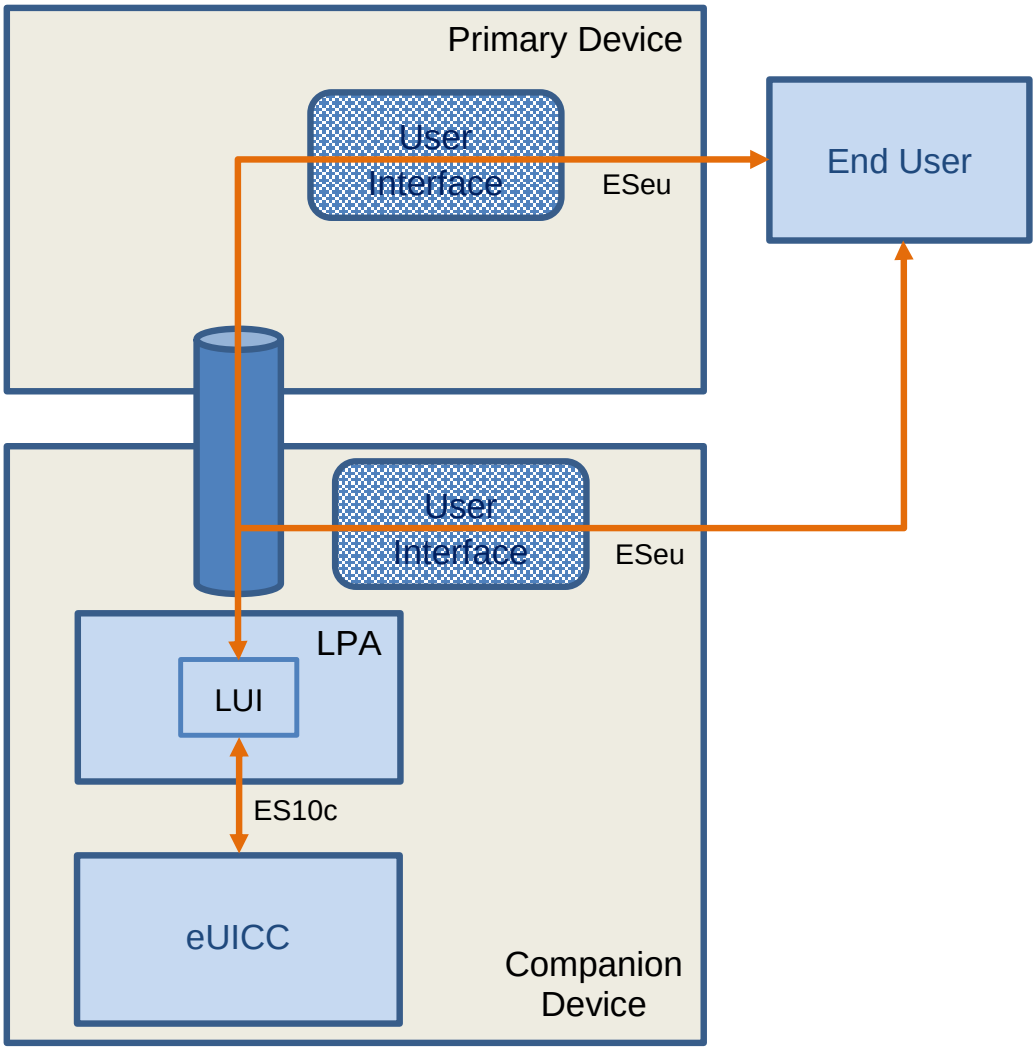


Figure 6: End User Interaction and Interfaces between a Primary and Companion Device, where the Companion Device MAY have a UI

4.11.1 LPA Overview

This role exists both within the Device in conjunction with LPA Services provided by the eUICC, and within the eUICC with the LPA function provided by the eUICC. It provides three distinct functions, the Local User Interface (LUI), the Local Profile Download (LPD) and the Local Discovery Service (LDS) as described below. Whilst the eUICC alone cannot provide any of these functions without Device interaction, the specific level of interaction will depend upon the capability within the Device. The way this variability is implemented across different Devices and Device types is for further study.

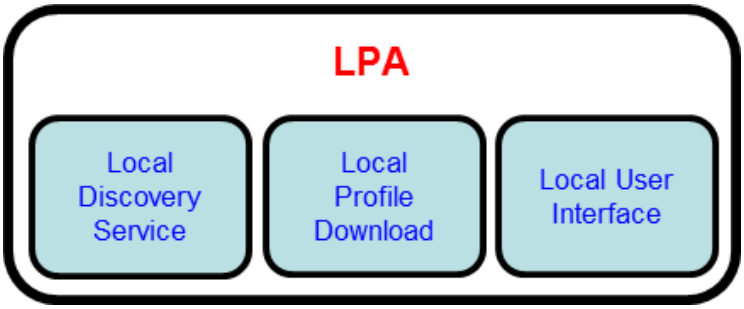


Figure 7: LPA Functions

Function name	Description
Local Discovery Service (LDS)	Where required, the LDS is responsible for retrieving pending Event Records from the SM-DS.
Local Profile Download (LPD)	This plays a proxy role for the efficient download of a Bound Profile Package in two stages: (i) the download of a Bound Profile Package from the SM-DP+ to the LPD in a single transaction, and (ii) the onward transfer of the Bound Profile Package into the eUICC in segments. This function will depend on network, Device, and eUICC capabilities.
Local User Interface (LUI)	This function allows the End User to perform Local Profile Management on the Device. User Intent SHALL be enforced.

Table 26: LPA Function Descriptions

4.11.2 Operational LPA Modes

When there is an LPA in the Device and in the eUICC, then the LPA to be used is specified by the Device settings (DEV7):

- LPA in the Device
- LPA in the eUICC

4.11.2.1 LPA in the eUICC

LPA functions are provided by the eUICC.

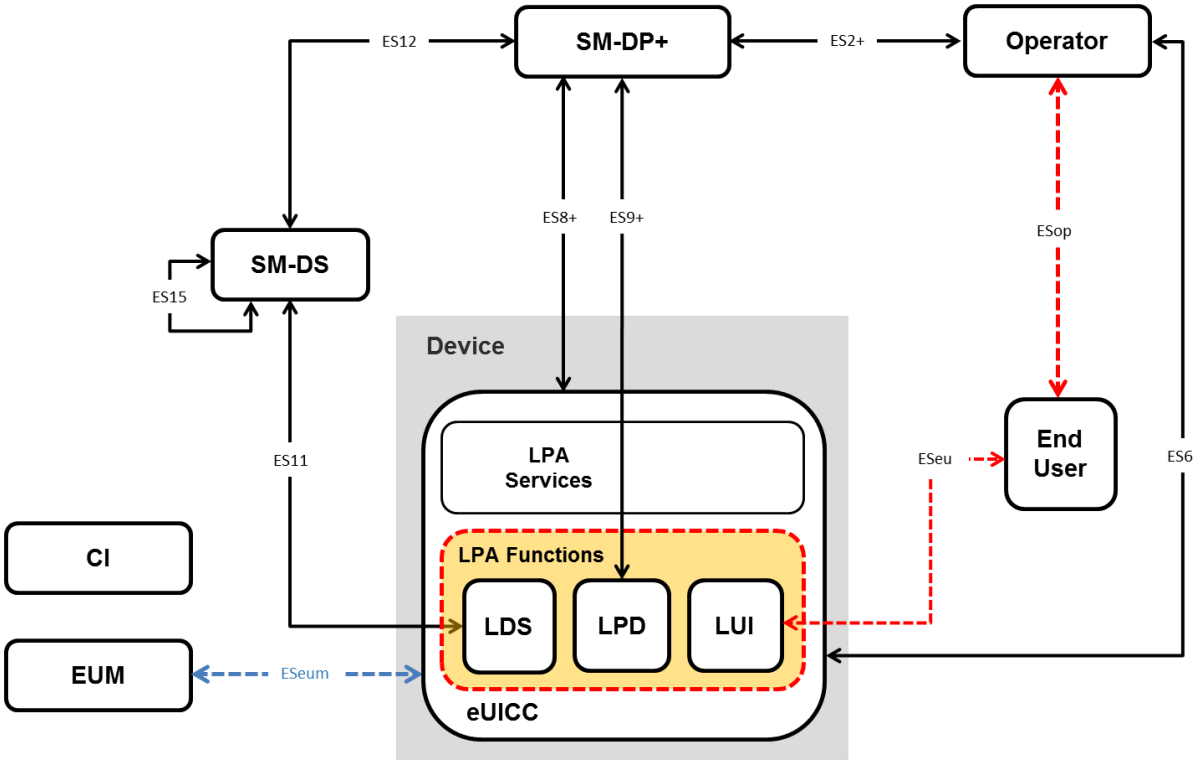


Figure 8: LPA in the eUICC

4.11.2.2 LPA in the Device

LPA functions are provided by the Device.

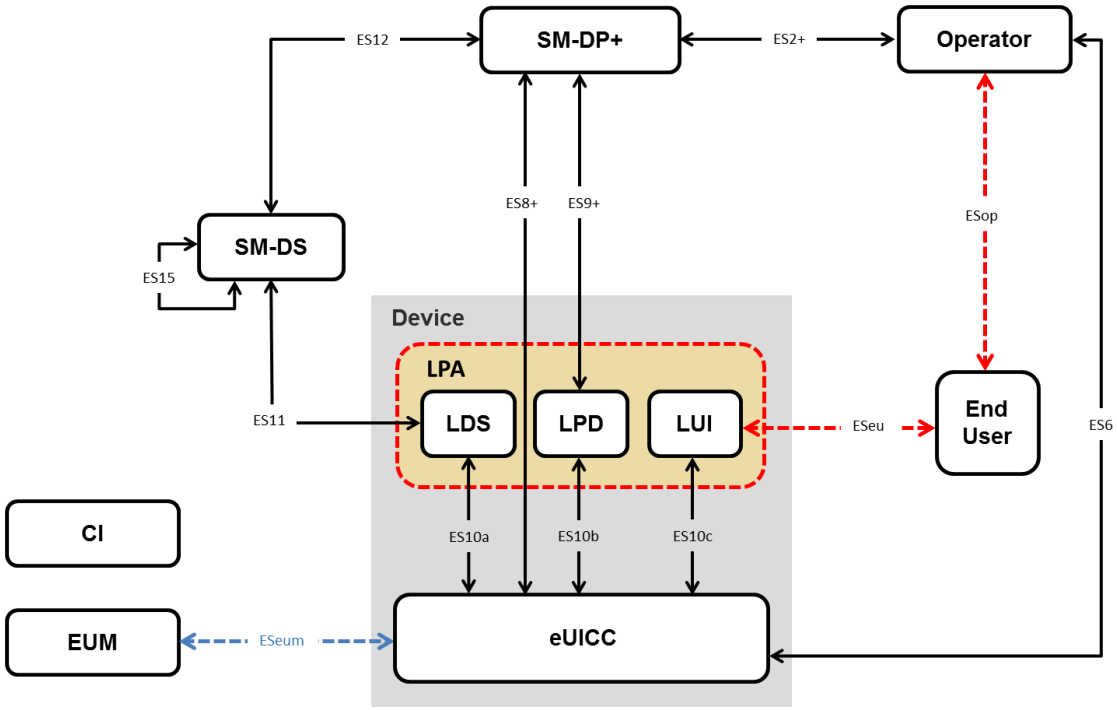


Figure 9: LPA in the Device

4.11.3 LPA Requirements

Req no.	Description
LPA1	The LPA SHALL be responsible for instructing the eUICC to perform Local Profile Management Operations as per End User request.
LPA2	A mechanism SHALL be implemented between any LPA elements outside the eUICC, and the eUICC to ensure that the communication is not compromised wherever the LPA is located.
LPA3	A secure mechanism SHALL be implemented between the LUI and the associated display or input applications on the Device.
LPA4	Access to the LUI SHALL be protected according to current best practices. This SHALL be enforced by the Device OS.
LPA5	All Local Profile Management Operations SHALL require User Intent.
LPA6	LUI access SHALL require User Intent.
LPA7	The End User SHALL be able to easily access the list of installed Profiles.
LPA8	The LPA SHALL protect Profile Metadata from unauthorised access.
LPA9	The Local Profile Management Operation, ‘enable’ SHALL be supported. This operation SHALL allow the End User to select the Profile to be enabled.
LPA10	The Local Profile Management Operation, ‘disable’ SHALL be supported.
LPA11	The Local Profile Management Operation, ‘delete’ SHALL be supported. This operation SHALL allow the End User to delete a Disabled Profile from the eUICC. The End User SHALL acknowledge the message of consequences for the deletion of the Profile. Strong Confirmation SHALL be enforced.
LPA12	The Local Profile Management Operation ‘query’ SHALL be supported. This operation SHALL allow the End User to view the list of installed Operational Profiles on the eUICC and relevant associated information through their Profile Metadata.
LPA13	The Local Profile Management Operation, ‘edit default SM-DP+ address’ SHOULD be supported. When supported, this operation SHALL allow the End User to edit the default SM-DP+ address. Simple confirmation SHALL be enforced. If the LPA does not support ‘edit default SM-DP+ address’, alternative Device-specific method(s) to edit the default SM-DP+ address SHALL be provided to the End User.
LPA14	The Local Profile Management Operation ‘eUICC Memory Reset’ SHALL be supported. This operation SHALL execute the eUICC Memory Reset as described in Section 4.6.2. The End User SHALL acknowledge the message of consequences of ‘eUICC Memory Reset’. Strong Confirmation SHALL be enforced.
LPA15	The Local Profile Management Operation ‘eUICC Test Memory Reset’ SHALL execute the eUICC Test Memory Reset as described in Section 4.6.3. Simple Confirmation SHALL be enforced.
LPA16	The Local Profile Management Operation ‘set/edit nickname’ SHOULD be supported. This operation SHALL allow the End User to add or modify a nickname for the selected Profile. The operation SHALL NOT modify the Service Provider name. If the LPA does not support ‘set/edit nickname’, alternative vendor-specific methods to distinguish Profiles on the LUI SHOULD be provided by the LPA.

LPA17	The Local Profile Management Operation ‘add Profile’ SHALL be supported. This operation SHALL allow the LPA to download and install a new Profile to the eUICC. At least three mechanisms SHALL be supported by the LPA depending on the type of Device where technically capable: • Profile download from default SM-DP+ • Profile download via SM-DS service discovery • Profile download with Activation Code Simple Confirmation SHALL be enforced.
LPA18	The LPA SHALL NOT be accessible by any applications other than those provided by the provider of the LPA for the sole purpose of enabling the services and functions of the LPA.
LPA19	[Void]
LPA20	The LPA provider SHALL enforce a secure and non-interceptable Simple Confirmation located on the Device as described in this document.
LPA21	[Void]
LPA22	[Void]
LPA23	[Void]
LPA24	[Void]
LPA25	[Void]
LPA26	[Void]
LPA27	When enforced, any Confirmation Request SHALL allow the End User to cancel the Local Profile Management Operation.
LPA28	It SHALL be possible to expose the LUI of a Companion Device allowing input from an End User interface on the Primary Device.
LPA29	When a Companion Device LUI allows input from a Primary Device, the Companion Device LUI SHALL be able to restrict the actions that can be applied. For example: • not offer the eUICC Memory Reset; • only ‘enable’ and ‘disable’ operation are exposed. • Profile enabling is exposed only if no Profile is already enabled on the Companion Device.
LPA30	The LUI of the Companion Device SHALL be able to request an End User initiated action on the Companion Device before the establishment of any proximity secure link (used for inputs into the LUI from another Device).
LPA31	A point-to-point proximity secure link initiated by the End User and offering confidentiality and integrity SHALL be established between the Companion and Primary Device for any input executed from the Primary Device.
LPA32	When operating a Companion Device LUI from a Primary Device, any required User Intent or Confirmation Request SHALL only be executed by the LPA on the Companion Device. The physical End User input MAY be done in either the Primary or the Companion Device.
LPA33	The Device Manufacturer of the Companion Device SHALL implement a secure measure to ensure integrity and eligibility of any application accessing the LUI.
LPA34	[Void]

LPA35	The LPA SHALL be able to utilise any on-Device and existing connection to the internet, such as Wi-Fi or Wi-Fi direct, in order to reach out to the SM-DP+. Over such connection, ES8+ and ES9+ interfaces can be established.
LPA36	The LPA SHALL be able to utilise any internet connection offered by another Device, via other connectivity mechanisms such as cabled tethering, locally shared Wi-Fi connections or Bluetooth in order to reach out to the SM-DP+. Over such connection, ES8+, and ES9+ interfaces can be established.
LPA37	The LPA SHALL be able to determine if connectivity to the SM-DP+ is available by any means.
LPA38	The LPA SHALL be able to notify the End User that there is no connection to the internet and or no connection to the SM-DP+ in order to allow the End User to enable or troubleshoot required connectivity.
LPA39	The LPA SHALL only be able to access the eUICC if it has assigned privileges.
LPA40	There SHALL only be one LPA on the Device.
LPA41	The LPA MAY be extended to support additional features which are not described in this specification. NOTE: These additional features could be (but not limited to) interaction with entities external to LPA, automation or batch processing of Local Profile Management Operations, etc.
LPA41a	The LPA including additional features SHALL maintain the interoperability of the solution defined in this specification.
LPA42	[Void]
LPA43	When multiple Operational Profiles are installed, the Local Profile Management Operation ‘enable’ SHALL first initiate the ‘disable’ operation for any Enabled Profile prior to initiating the ‘enable’ operation for the selected Profile.
LPA44	The LPA SHALL be able to read the Profile Policy Rules.
LPA45	When a Profile with Profile Policy Rules is installed, in the case where End User consent is requested, the LPA SHOULD display the consequences of the Profile Policy Rule to the End User. This message SHALL be formulated in a descriptive and non-discriminatory manner (e.g. for “Non-Delete” Profile Policy Rule: “The profile that you are about to install cannot be deleted under the terms you have agreed with your service provider. Approve installation YES/NO?”). Strong Confirmation SHOULD be enforced.
LPA46	Prior to downloading a new Profile, the LPA SHALL check the condition for whether the Enabled Profile, if any, has enabled POL RULE1. If this is the case, a dedicated message SHALL be displayed identifying the consequences to the End User. Examples of information that may be displayed would be: • Enabling of the new Profile will not be possible because the currently Enabled Profile cannot be disabled. • The Profile name of the Enabled Profile. • For more information, the End User should contact the Profile Owner of this Profile. With displaying this message, the End User SHALL be able to decide on whether to continue the download or to cancel the operation. This dialogue MAY be combined with the regular End User Intent for confirming a Profile download.

LPA47	The communication between the End User interface of the Primary Device and the LUI of the Companion Device SHALL be protected (confidentiality, integrity and authentication).
LPA48	[Void]
LPA49	Confirmation Requests for consecutive Local Profile Management Operations MAY be achieved in one step as long as the different actions are clearly explained to the End User. For instance, 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")
LPA50	When consecutive operations are achieved in one single step (LPA49), the highest level of confirmation SHALL be applied - i.e. in the case of two operations having respectively Strong and Simple Confirmation Requests, the single step SHALL use the Strong Confirmation Request.
LPA51	The Local Profile Management Operations 'enable' (LPA9), 'disable' (LPA10), and 'delete' (LPA11) SHALL be able to trigger a Notification to the Notification Receivers of the respective Profile being managed to indicate that this operation was actioned. These Notifications are sent on a best effort basis and SHALL not impact otherwise the operation.
LPA52	The LPA SHALL provide a Trusted Link from the End User to the eUICC through the LUI.
LPA53	The End User SHALL be able to configure the LPA such that the automatic Event Record retrieval from the SM-DS is disabled.
LPA54	The LPA SHALL be able to read any SM-DS and SM-DP+ addresses configured in the eUICC.
LPA55	It SHALL be possible to check the LPA Integrity. If the integrity check fails, communication between the eUICC and the LPA SHALL not occur.
LPA56	LPA Integrity SHALL be ensured using the best practice methods on the targeted platform. See Annex G.
LPA57	The polling mechanism in the LPA SHALL have two types of triggers; those that are event based, and those that are End User initiated.
LPA58	Event based triggers for polling SHOULD include Device power-up when no Operational Profile is installed; in addition other triggers MAY be provided. Event based triggers MAY be disabled by the End User.
LPA59	End User initiated triggers for polling SHALL include: • The 'Add Profile' operation to trigger the default SM-DP+ if configured, and the Root SM-DS. • In addition, other manual triggers MAY be provided.
LPA60	[Void]
LPA61	Error/retry handling of the LPA polling mechanism SHALL be implemented e.g. advise the End User to retry or automatically retry as appropriate. The corresponding confirmation needs to be enforced in the retry cases.
LPA62	As part of the initial Device setup, if no Operational Profile is already installed, means SHALL be provided to the End User to retrieve pending Profiles waiting on the Default SM-DP+ if configured, via the Root SM-DS, and via the Activation Code procedure.

	Simple Confirmation is required. Note: Implementation is left to the OEM and retrieval does not need to happen exactly during the initial Device setup if the End User, as an example, is informed on how to retrieve these profiles after the setup.
LPA63	The End User SHALL always be able to manually request the retrieval of any waiting Event Record via the LPA if there is no default SM-DP+ address. Note: This may be achieved through the combination with existing operations – e.g. pressing “Add Profile” would contact the server to retrieve an Event.
LPA64	The Operator/Service Provider name SHALL be given in the signalling information from the SM-DP+ to the LPA when initiating the download of a Profile and shown to the End User before the Profile is downloaded. Simple Confirmation SHALL be enforced.
LPA65	The LPA SHOULD present the EID to the End User as both text and in a defined scannable format (e.g. QR Code).
LPA66	[Void]
LPA67	If the SM-DP+ stops the Profile download procedure, the LPA SHALL notify the End User.
LPA68	[Void]

Table 27: LPA Requirements

4.11.4 LDS Requirements

Req no.	Description
LDS1	The LDS SHALL be able to read out the address described in EUICC **Error! Reference source not found.** and only use the address to connect to the SM-DS

Table 28: LDS Requirement

4.12 Subscription Manager – Discovery Service (SM-DS)

4.12.1 SM-DS Overview

The role of the SM-DS is to provide mechanisms that allow an SM-DP+ to inform the LDS within any Device that an SM-DP+ wishes to communicate with it. The purpose of the SM-DS to LDS communication SHALL be informing the LDS of a pending Event.

The principle of operation remains the same for all use cases. The SM-DP+ will send an Event Registration message for a target Device to a SM-DS.

In a simple deployment, only the Root SM-DS is configured on the eUICC. The Root SM-DS address is unique and filled in the eUICC. The LDS in the target Device polls the Root SM-DS using the same logical location. When the Root SM-DS has an Event-ID for the target Device it will respond with the SM-DP+ address, or if there is no Event-ID the response will be a null response.

In a deployment with cascaded SM-DSs, the SM-DP+ will send an Event Registration to an Alternative SM-DS, which may not be configured as the Root SM-DS on the eUICC. This Alternative SM-DS will cascade the Event Registration to the Root SM-DS. The LDS in the target Device polls the Root SM-DS and will receive the Alternative SM-DS address. It will

then request the Event from the Alternative SM-DS, which will respond with the SM-DP+ address.

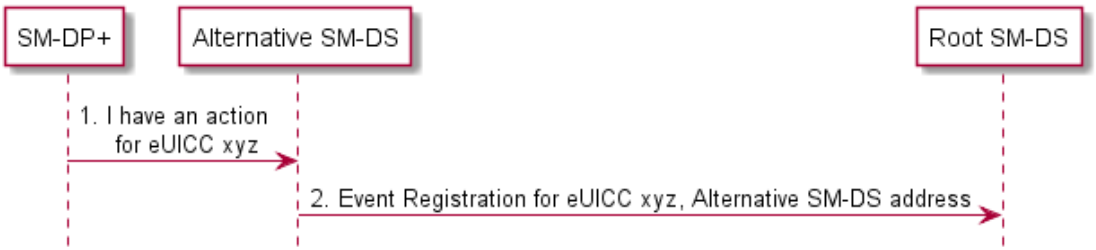


Figure 10: Alternative Device to Root SM-DS Event Registration

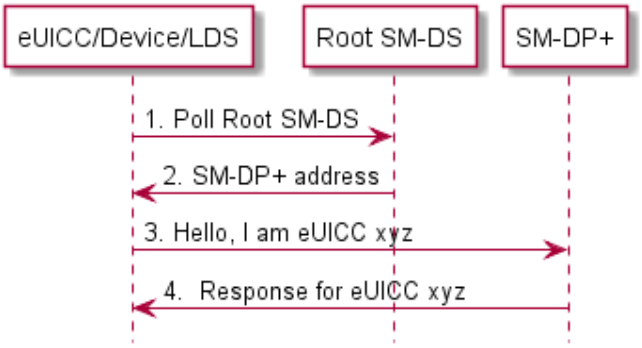


Figure 11: Root SM-DS Event Registration

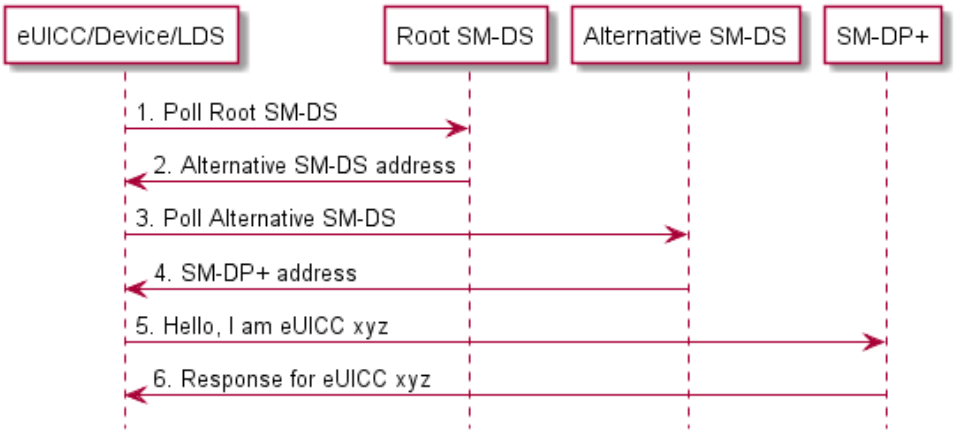


Figure 12: Alternative SM-DS Discovery

4.12.2 SM-DS Implementation

Two configurations of the SM-DS MAY exist:

- A Root SM-DS
- An Alternative SM-DS

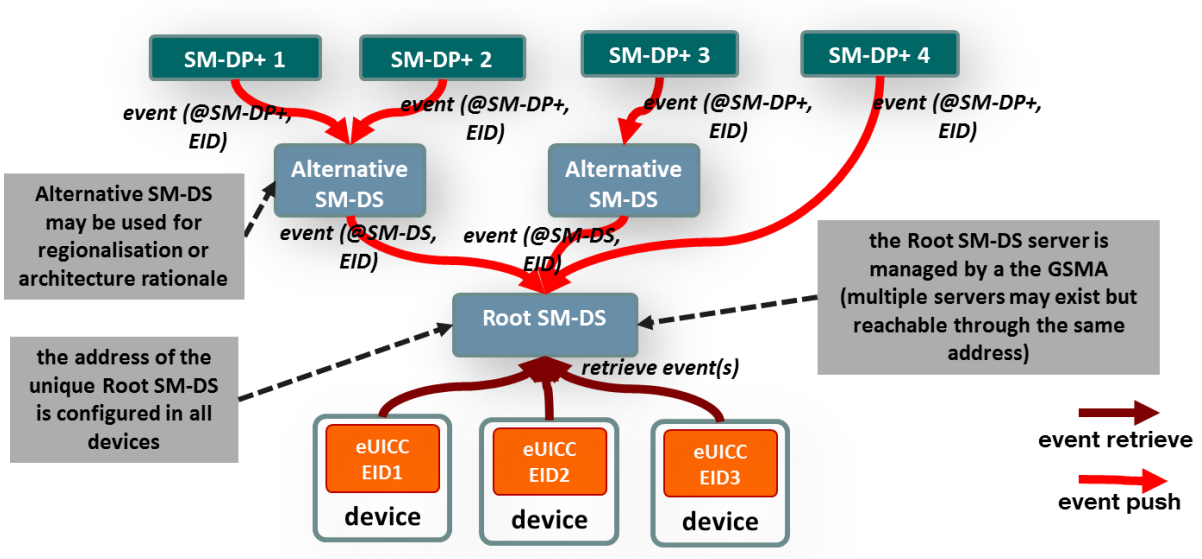


Figure 13: SM-DS Implementation

Figure 13 shows both configurations. The Root SM-DS is configured at the time of Device manufacture and is invariant.

4.12.3 SM-DS Implementation Guidelines

The following statements SHOULD be considered when defining a technical implementation:

- A competitive environment on the supply of SM-DS services SHOULD be favoured by the approach.
- There SHOULD be no single-points-of-failure.
- Implementation SHOULD inherently provide both vertical and horizontal performance/scalability.
- There SHOULD be no need for pre-registration of Devices or eUICCs at a certain SM-DS as required in SGP.02 [8] (GSMA Embedded SIM for the SM-SR).

4.12.4 SM-DS functions

The SM-DS has three distinct functions:

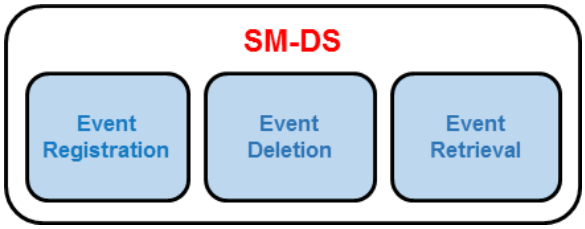


Figure 14: SM-DS Functions

Function name	Description
Event Registration	Process by which an Event Record received from a SM-DP+ is stored.
Event Deletion	Process by which an SM-DP+ can delete its own Event Record.
Event Retrieval	Provides all registered Event Records, upon Discovery Request from any enquiring LDS.

Table 29: SM-DS Function Descriptions

4.12.5 SM-DS Requirements

Req no.	Description
SMDS1	The SM-DS SHALL enable a LDS to discover its own Event Records registered by SM-DP+(s) or by Alternative SM-DS(s).
SMDS2	The SM-DS SHALL not be able to identify the nature of an Event. Note: The nature of the Event may be 'Profile Package available for download'.
SMDS3	All valid Discovery Requests and Event Registrations SHALL be processed in a non-discriminatory manner.
SMDS4	The SM-DS SHALL only accept Event Registrations from • any authorised and authenticated SM-DP+(s) having a valid Certificate. • any authorised and authenticated SM-DS(s) having a valid Certificate.
SMDS5	The SM-DS SHALL only accept Discovery Requests authenticated by an eUICC via the corresponding LDS.
SMDS6	The SM-DS and the SM-DP+ as well as connected SM-DSs SHALL be mutually authenticated.
SMDS7	The SM-DS SHALL NOT have visibility of any data that may be used to compromise the End User´s privacy.
SMDS8	The SM-DS SHALL support multiple concurrent Event Registrations per eUICC and SHALL present to the LDS all currently valid Event Records in the same order as they were received by the SM-DS (first in, first out).
SMDS9	The SM-DS SHALL only store Event Records destined for specific EIDs.
SMDS10	Subscriber Specific data and Profile related contents SHALL NOT be stored within the SM-DS.
SMDS11	The SM-DS SHALL NOT allow the harvesting of any information such as Operator, EIDs, Device Manufacturers, Devices, etc.
SMDS12	The SM-DS SHALL only return to the LDS, the Event Records related to the served eUICC.
SMDS13	The SM-DS SHALL NOT have any contact with the Profile Packages e.g. SHALL NOT store or process any Profile Package.
SMDS14	The SM-DS SHALL provide the same data regardless of the status of the Device that queries it (i.e. consistent in time and in geographic location).
SMDS15	The SM-DS SHOULD NOT significantly impact the end-to-end provisioning time.
SMDS16	The SM-DS SHALL provide defence against DoS attacks.
SMDS17	All communications to, from and between entities of the SM-DS SHALL be encrypted.
SMDS18	The SM-DP+ SHALL be able to delete any of its own Event Records registered on the SM-DS.
SMDS19	An Alternative SM-DS SHALL be able to delete any of its own Event Records registered on the Root SM-DS (In response to an SM-DP+ delete operation defined in SMDS18).

Req no.	Description
SMDS20	An Alternative SM-DS SHALL propagate the Event Record to the Root SM-DS if requested by the SM-DP+.
SMDS21	If there are multiple Event Records registered on the SM-DS for one eUICC, these SHALL all be sent as a single response.
SMDS22	An SM-DP+ SHALL be able to send an Event Record to an LDS either by the Root SM-DS or via any Alternative SM-DS selected by the SM-DP+. If an Alternative SM-DS is selected, the Event Record to the LDS SHALL come from this Alternative SM-DS.
SMDS23	There SHALL be a unique Root SM-DS. Note: This requirement does not forbid the potential load-balancing of this Root SM-DS.
SMDS24	The Root SM-DS SHALL be managed by the GSMA.
SMDS25 (FFS)	It SHALL be possible for the Alternative SM-DS to conduct an Event Record Query to the Root SM-DS for the purpose of auditing Event Registrations it owns.
SMDS26 (FFS)	A SM-DS response to an Event Record Query SHALL only confirm Event Record existence and SHALL NOT include additional information.
SMDS27 (FFS)	An Alternative SM-DS SHALL be able to query the existence of an Event Record on the Root SM-DS, identified by the EID or the Event-ID over the ES15 interface.
SMDS28 (FFS)	Response to a SM-DS Event Record query SHALL only occur where the responder validates the Event Record ownership.
SMDS29 (FFS)	Ownership validation of a SM-DS Event Record Query SHALL only use the requester's address or the submitted Event-ID against the components of the Event Record held.
SMDS30 (FFS)	The SM-DS (Root or Alternative) MAY inform the SM-DP+ directly or via another SM-DS, that a Discovery Request from an authorised LDS has been answered by issuing an Event Record.
SMDS31 (FFS)	The SM-DS SHALL only inform the Event Record's owning SM-DP+ or SM-DS that it has replied to a Discovery Request.

Table 30 SM-DS Requirements

4.12.6 Event Registration/Deletion Procedure

The figure below shows the procedure for a deployment with the Root SM-DS and an Alternative SM-DS (cascade mode).

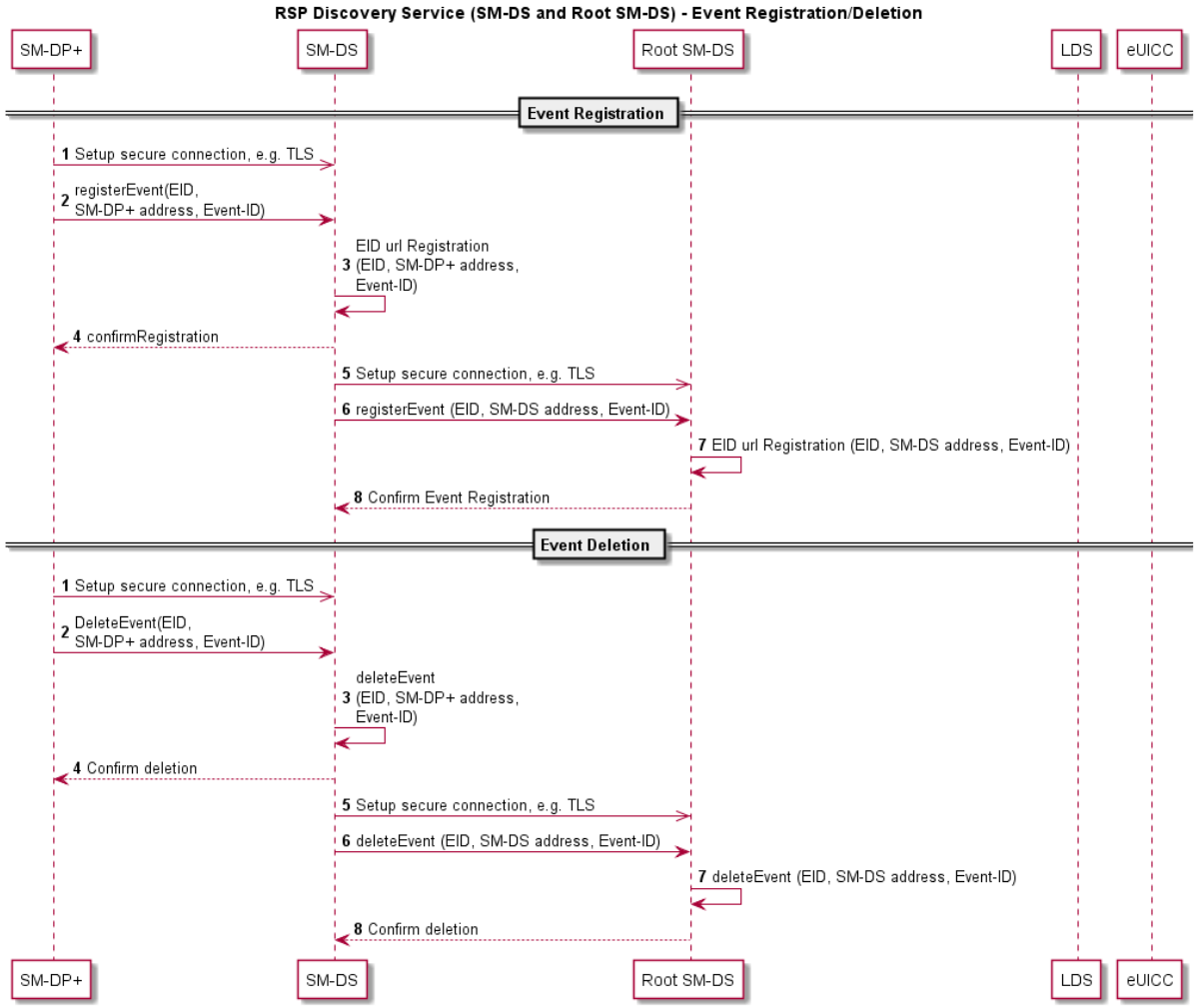


Figure 15: Event Registration/Deletion Procedure

4.12.6.1 Event Registration Procedure

Starting Condition:

a. The SM-DP+ has an Event Registration action waiting for a target eUICC identified by the EID.

Procedure:

1. The SM-DP+ establishes a secure connection to an Alternative SM-DS of the Profile Owner´s choice.
2. The SM-DP+ notifies the Alternative SM-DS about an Event Registration action.

3. to 4. The Alternative SM-DS registers and confirms the Event Registration.

5. The Alternative SM-DS establishes a secure connection to the Root SM-DS.
6. The Alternative SM-DS informs the Root SM-DS that for the given EID, an Event Record is waiting at the Alternative SM-DS.

7. The Root SM-DS registers the Event Registration.
8. The Root SM-DS confirms the receipt of the information.

4.12.6.2 Event Deletion Procedure

Starting Condition:

a. The SM-DP+ has an Event Deletion action waiting for a target eUICC identified by the EID

Procedure:

1. The SM-DP+ establishes a secure connection to an Alternative SM-DS of the Profile Owner´s choice.
2. The SM-DP+ notifies the Alternative SM-DS about an Event Deletion action.
3. to 4. The Alternative SM-DS deletes the Event Record and confirms the Event Deletion.
5. The Alternative SM-DS establishes a secure connection to the Root SM-DS.
6. The Alternative SM-DS informs the Root SM-DS that for the given EID, an Event Record has to be deleted.
7. The Root SM-DS deletes the Event Record.
8. The Root SM-DS confirms the deletion of the Event Record.

4.12.7 Discovery Request Procedure

The figure below shows the procedure for a deployment with an Alternative SM-DS and the Root SM-DS (cascade mode).

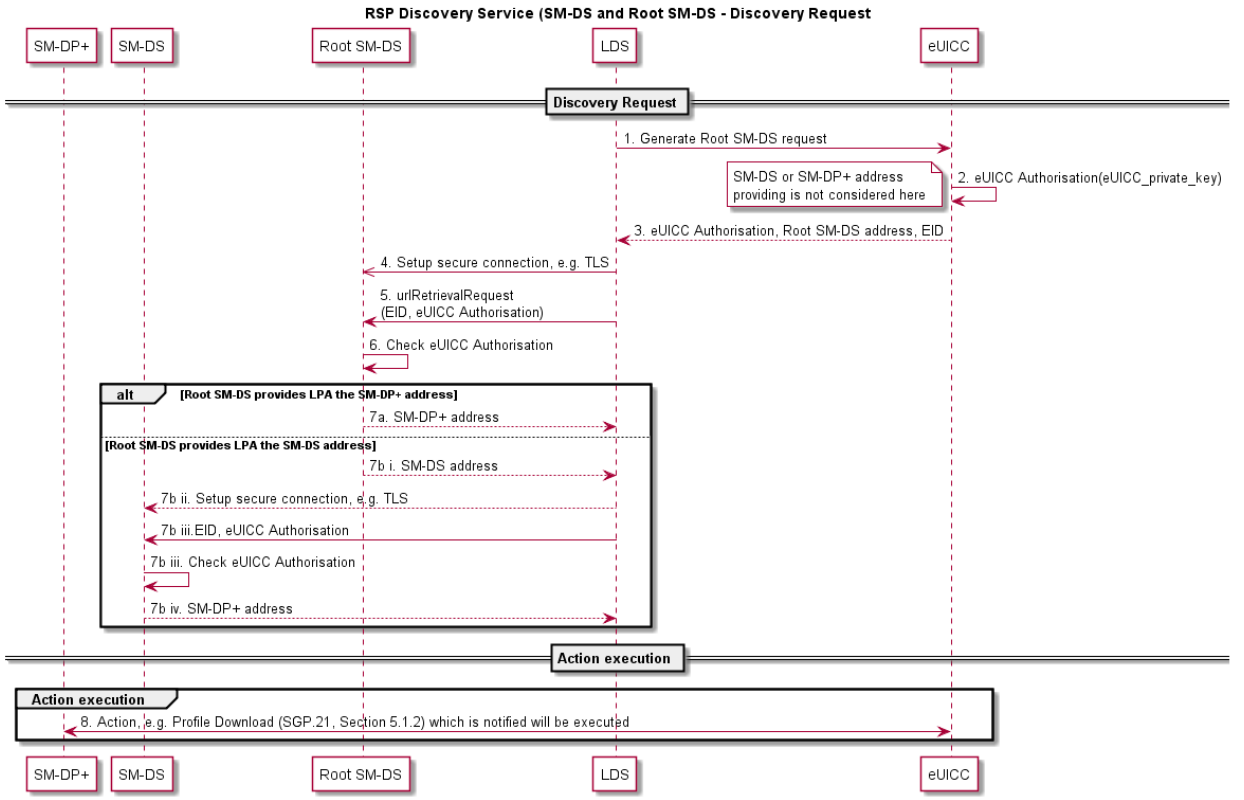


Figure 16: Discovery Request Procedure

Procedure:

1. to 3. In order to generate a Discovery Request, the LDS requests the eUICC to generate an eUICC Authorisation which contains (at least) the eUICC-Certificate and is signed by the eUICC.
4. to 5. The LDS establishes a secure communication to the Root SM-DS.
6. The Root SM-DS verifies the authenticity of the eUICC by checking the eUICC Authorisation.
7. In case the eUICC is authentic and an Event Record is waiting, it delivers back:
    a. The address of the SM-DP+, where an action is waiting.
    or
    b. The rest of the following actions:
        i. The address of the Alternative SM-DS, where an Event Record can be retrieved.
        ii. The LDS establishes a secure connection to the Alternative SM-DS.
        iii. The Alternative SM-DS verifies the authenticity of the eUICC by checking the eUICC Authorisation.
        iv. In case the eUICC is authentic and an Event Record has been received, it delivers back the address of the SM-DP+, where an action is waiting.
8. The LPA establishes a connection to the SM-DP+ and the waiting action can be performed.

4.13 Profile Policy Management

4.13.1 Introduction

The Profile Policy Management function provides mechanisms by which Service Providers are able to reinforce the conditions or policies (operational and business) under which services are provided to the Subscriber. In some instances this MAY also include the enforcement of the policies set by the Subscriber.

Profile Policy Management MAY also be applied with other already existing policy enforcement technologies which are also subject to agreement by the Subscriber.

The realisation of the Profile Policy Management function is based on two key elements. The first element is the Profile Policy Enabler which is contained within the eUICC. The second element is a set of defined Profile Policy Rules which are required for the actual enforcement of specific policies.

4.13.2 Profile Policy Management Requirements

Policy no.	Description
POL1	A Profile Policy Rule SHALL only be configured within a Profile.
POL2	Each Profile MAY have Profile Policy Rules associated to itself.
POL3	A Profile Policy Rule SHALL only apply to the Profile that contains it.
POL4	Profile Policy Enforcement SHALL be consistent across implementations.
POL5	Profile Policy Enforcement SHALL be able to resolve any Profile Policy Rule conflict.

Policy no.	Description
POL6	The updating of a Profile's Policy Rules SHALL be restricted to the Profile Owner.
POL7	The mechanism used for the update of a Profile Policy Rule SHALL be atomic.
POL8	The set of Profile Policy Rules SHALL be extensible for future releases.
POL9	There SHALL be a Profile Policy Rule scheme to allow extensibility of the Policy Rules, e.g. described like 'operational command, scope of application, qualification'
POL10	A Profile Policy Rule SHALL be enforced whenever a Profile state change is attempted.
POL11	Downloading and installing a Profile with the Profile Policy Rule 'Disabling of this Profile is not allowed' (POL RULE1) SHALL only be possible if no other Operational Profile is currently installed.
POL12	The LPA and the eUICC SHALL prevent the downloading and installation of a Profile containing Profile Policy Rules that conflict with the Profile Policy Rules of the already installed Profiles. Note: The technical specification SHALL describe exhaustively each conflict that MAY occur.
POL12a	The LPA MAY cancel the Profile download procedure if it does not support the downloading of Profiles containing Profile Policy Rules to a removable eUICC regardless of its RAT.
POL13	An Operator SHALL be able to deactivate the Profile Policy Rules of its Profile using the ES6 interface if the Profile is enabled. Note: The activation of Profile Policy Rules on the ES6 interface is a potential feature for a future release.
POL14	Before a Profile is installed with Profile Policy Rules, the End User SHALL be able to be notified about the Profile Policy Rules and if notified, the installation SHALL thereafter be conditional on End User Strong Confirmation. This prompting may not be needed if the installation is directly allowed by the RAT.
POL15	The request for End User consent for the installation of Profile Policy Rules and Profile download MAY be combined into a single prompt therefore requiring a single confirmation by the End User.
POL16	Profile Policy Rules SHALL be enforced by the Profile Policy Enabler in the eUICC.
POL17	The Profile Policy Enabler SHALL only support the Profile Policy Rules defined in this specification.
POL18	The Profile Policy Enabler SHALL be capable of supporting all the Profile Policy Rules as defined in this specification.
POL19	POL RULE3 SHALL be enforceable in all cases with the exception of the enabling of a Provisioning Profile. Note: POL RULE3 is defined for use in specific use cases that have not yet been fully defined and is not applicable for this version of the specification.

Policy no.	Description
POL20	Allowing the installation of a Profile with Profile Policy Rules SHALL be subject to compliance with local regulatory requirements.

Table 31: Profile Policy Management Requirements

4.13.3 Policy Rules

Policy no.	Description
POL RULE1	The Profile Policy Rule 'Disabling of this Profile is not allowed' SHALL be supported.
POL RULE2	The Profile Policy Rule 'Deletion of this Profile is not allowed' SHALL be supported.
POL RULE3	The Profile Policy Rule 'Deletion of this Profile is required upon its successful disabling' SHALL be supported. Note: POL RULE3 is defined for use in specific use cases that have not yet been fully defined and is not applicable for this version of the specification.

Table 32: Policy Rules Requirements

4.13.4 Profile Policy Enabler Requirements

Policy no.	Description
POLPPE1	The Rules Authorisation Table (RAT) SHALL be stored in the Profile Policy Enabler in the eUICC.
POLPPE2	The Profile Policy Enabler SHALL enforce the contents of the installed RAT, if any, only at Profile installation time.
POLPPE3	The RAT SHALL allow multiple Profile Owners to have Profile Policy Rules enabled in their Profiles.
POLPPE4	The RAT SHALL be able to support specific configurations which allow a set of or all Profile Policy Rules for any Profile Owner.
POLPPE5	The RAT SHALL only be installed at pre-issuance or during the initial Device setup provided there are no Operational Profiles installed.
POLPPE6	The RAT SHALL not be affected by the eUICC Memory Reset function.
POLPPE7	To support identifiable regulatory requirement, a RAT SHALL be able to support a specific configuration which MAY forbid any Profile Owner to set a specific Profile Policy Rule.
POLPPE8	If POLPPE7 is set, this information SHALL be part of the eligibility check information shared between the SM-DP+ and the eUICC.
POLPPE9	Where the RAT allows the Profile Policy Rules for the Profile being installed, installation SHALL proceed as stated in POL14.
POLPPE10	The RAT SHALL be able to support a setting to display the consequences of the Profile Policy Rules to the End User before installation of the Profile.
POLPPE11	The OEM or EUM SHALL be responsible for providing the RAT.
POLPPE12	A fixed RAT SHALL be implemented in the eUICC. Note: RAT configuration examples are described in Annex H.

Table 33: Profile Policy Enabler Requirements

4.14 Certification

4.14.1 eUICC Certification Requirements

Req no.	Description
CERTEU1	The EUM SHALL be GSMA SAS UP certified [13][13][13].
CERTEU2	The EUM SHALL be required to declare eUICC product compliance with GSMA SGP.22 [24].
CERTEU3	The eUICC SHALL be certified according to the Protection Profile defined by the GSMA [25].
CERTEU4	The eUICC Protection Profile SHALL at least include the following elements: ISD-R, Profile storage, isolation of Profiles, and Telecom Framework.
CERTEU5	The eUICC protection Profile SHALL be equivalent to the eUICC Protection Profile defined in SGP.05 [21][21][21].
CERTEU6	The Evaluation Assurance Level of the eUICC Protection Profile SHALL be (at least) EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 (EAL 4+). Note: A study needs to be performed in terms of assurance level by FASG.
CERTEU7	The eUICC public key Certificate used for authentication SHALL contain the EID.
CERTEU8	It SHALL be possible to obtain the technical reference of the product, for example the Common Criteria certification report number and if applicable, the EMVco PCN (Platform Certification Number) associated with a specific eUICC.
CERTEU9	The EUM Public Key Certificate(s) SHALL be signed by a GSMA CI.
CERTEU10	The eUICC Certificate(s) SHALL be signed by the EUM using its EUM private key corresponding to its Certificate (CERTEU9**Error! Reference source not found.**).
CERTEU11	The eUICC private key(s) SHOULD not be modifiable. If they are, they should be modifiable only by the EUM that issued the corresponding Certificate.
CERTEU12	If the eUICC private key(s) are modifiable, it SHALL use the mechanism defined in the GlobalPlatform specification with a minimum security level corresponding to the AES algorithm using a key length of 128 bits.
CERTEU13	If the eUICC's EUM Certificate is updatable, then the eUICC SHALL support a secure mechanism to update its EUM Certificate.
CERTEU14	If the eUICC's CI public keys are updatable, then the eUICC SHALL support a secure mechanism to update its CI public keys.
CERTEU15	If the eUICC's Certificate is updatable, then the eUICC SHALL support a secure mechanism to update its eUICC Certificate.
CERTEU16	Where appropriate, the eUICC SHOULD be certified according to EMVCo Security Evaluation process [27].

Table 34: eUICC Certification Requirements

4.14.2 Device Compliance Requirement

Req no.	Description
CERTDEV1	There SHALL be a compliance process for all parts of Local Profile Management implementations in accordance with the GSMA.
CERTDEV2	The certification process for Integrated TRE using Remote Memory residing outside the SoC as per DIE1 SHALL cover the Integrated TRE, internal and external SoC interfaces used for Integrated eUICC implementation, and Remote Memory residing outside the SoC.
CERTDEV3	The certification process for Integrated TRE implementions SHALL ensure that software and data stored in Remote Memory residing outside the SoC as per DIE1 are protected against confidentiality, integrity, and availability attacks.
CERTDEV4	The certification process for Integrated TRE implementions SHALL ensure that any interfaces between the Integrated TRE and the SoC are protected against confidentiality and integrity attacks.

Table 35: Device Compliance Requirement

4.14.3 SM-DP+ Certification Requirements

Req no.	Description
CERTDP1	The SM-DP+ provider SHALL be required to declare product (SM-DP+) compliance with GSMA SGP.22 V2.2 [24].
CERTDP2	The SM-DP+ SHALL be certified according to FS.08 SAS-SM Standard v3 [22] and FS.09 SAS-SM Methodology v3 [28].
CERTDP3	SM-DP+ elements SHALL use Hardware Security Modules (HSM) for cryptographic related operations (key storage, derivation, cryptographic operations). Note: This is to be covered by the SAS documents “HSM certified according to FIPS 140-2 level 3 or higher”
CERTDP4	The SM-DP+ SHALL implement privileges isolation (Log, Audit, Operation, and Administration).
CERTDP5	The SM-DP+ SHALL implement operating system hardening mechanisms.
CERTDP6	The SM-DP+ SHALL implement separation of control, user and administrative planes.
CERTDP7	The SM-DP+ SHALL use Multi-Factor Authentication and administration operation.
CERTDP8	SM-DP+ hard drives and backup mediums used for storing Profiles SHALL be ciphered.
CERTDP9	The private keys of SM-DP+ Certificates used for mutual authentication and Profile Binding with eUICC SHALL be protected and stored in HSM according to CERTDP3.
CERTDP10	The SM-DP+ SHALL implement rate-limiting mechanisms to mitigate against DoS attacks.
CERTDP11	The SM-DP+ SHALL log all Certificate authentication failures.
CERTDP12	The SM-DP+ Public Key Certificate(s) SHALL be signed by a GSMA CI.

Table 36: SM-DP+ Certification Requirements

4.14.4 SM-DS Certification Requirements

Req no.	Description
CERTDS1	The SM-DS provider SHALL be required to declare product compliance with GSMA SGP.22 [24].
CERTDS2	The SM-DS SHALL be certified according to FS.08 SAS-SM Standard v3 [22] and FS.09 SAS-SM Methodology v3 [28].
CERTDS3	The SM-DS SHALL implement isolation of privileges (Log, Audit, Operation, and Administration).
CERTDS4	The SM-DS SHALL implement operating system hardening mechanisms.
CERTDS5	The SM-DS SHALL implement separation of control, user and administrative planes.
CERTDS6	The SM-DS SHALL use Multi-Factor Authentication and administration operation.
CERTDS7	SM-DS hard drives and backup mediums SHALL be ciphered.
CERTDS8	The SM-DS Public Key Certificate(s) SHALL be signed by a GSMA CI.

Table 37: SM-DS Certification Requirements

4.14.5 LPA Certification Requirements

Req no.	Description
CERTLPA1	There SHALL be a certification process for all the LPA elements communicating with Remote SIM Provisioning entities.
CERTLPA2	The certification process SHALL ensure that Local Profile Management Operations are sent by authorised LPA elements only.
CERTLPA3	The certification process SHALL ensure a mechanism exists to block compromised LPAs.
CERTLPA4	The LPD SHALL authenticate the SM-DP+ during the TLS session.
CERTLPA5	The LDS SHALL authenticate the SM-DS during the TLS session.
CERTLPA6	The LPA SHALL only accept valid TLS Certificates as defined in CERTPK10a for SM-DP+ and SM-DS authentication.

Table 38: LPA Certification Requirements

4.14.6 Public Key Certificates Management Requirements

Req no.	Description
CERTPK1	The eUICC SHALL verify the Public Key Certificate of the SM-DP+.
CERTPK2	The LPD SHALL verify the Public Key Certificate of the SM-DP+.
CERTPK3	The LDS SHALL verify the Public Key Certificate of the SM-DS.
CERTPK4	The LDS authentication of an SM-DS using an invalid Public Key Certificate SHALL fail (see CERTPK11), and on-going communication SHALL stop.

Req no.	Description
CERTPK5	The LPD authentication of an SM-DP+ using an invalid Public Key Certificate SHALL fail (see CERTPK11**CERTPK1**), and on-going communication SHALL stop.
CERTPK6	The SM-DP+ authentication of an eUICC using an invalid Public Key Certificate SHALL fail (see CERTPK11), and on-going communication SHALL stop.
CERTPK7	The eUICC authentication of an SM-DP+ using an invalid Public Key Certificate SHALL fail (see CERTPK11), and on-going communication SHALL stop.
CERTPK8	The GSMA CI SHALL revoke the Public Key Certificate of any entities (SM-DP+, SM-DS, EUM) if it is compromised (e.g. private key theft).
CERTPK9	The eUICC SHALL be able to support a set of GSMA CIs.
CERTPK10	A Public Key Certificate SHALL be considered as valid if: • it has a valid signature • it is signed by a GSMA CI, or a trusted chain of Certificates up to a GSMA CI. Certificate Path validation SHALL follow the process defined in RFC 5280 0**Error! Reference source not found.**. • it has not been revoked, and no Certificate in the trust chain has been revoked • it has not expired If any of these applicable verifications fail, the Public Key Certificate SHALL be considered as invalid.
CERTPK10a	A TLS Public Key Certificate SHALL be considered as valid if: • it has a valid signature • it is signed by a GSMA CI, or a public trusted CA, or a trusted chain of Certificates up to a GSMA CI or a public trusted CA. Certificate Path validation SHALL follow the process defined in RFC 5280 0**Error! Reference source not found.**. • it has not been revoked, and no Certificate in its trust chain has been revoked • it has not expired If any of these applicable verifications fail, the TLS Public Key Certificate SHALL be considered as invalid.
CERTPK11	The eUICC, LPA, SM-DS and SM-DP+ SHALL have knowledge of revoked Public Key Certificates. Note: This requirement also applies to TLS Certificates that chain to either the GSMA CI or a public trusted CA.

Table 39: Public Key Certificates Management Requirements

5 Operational Procedures

5.1 LPA Initiated Download

5.1.1 LPA Initiated Download Requirements

Req no.	Description
LID1	The LPA SHALL use any Root SM-DS or default SM-DP+ address populated on the eUICC if it has not been provided already by the Activation Code.
LID2	In the context of LID1, if both a Root SM-DS and a default SM-DP+ address are populated, the LPA SHALL first contact the SM-DP+ and then SM-DS to initiate a Remote SIM Provisioning transaction.

Table 40: LPA Initiated Download Requirements

5.1.2 LPA Initiated Download Procedure

This following procedure describes the Events that are part of the Profile Package download and installation procedure initiated by the LPA.

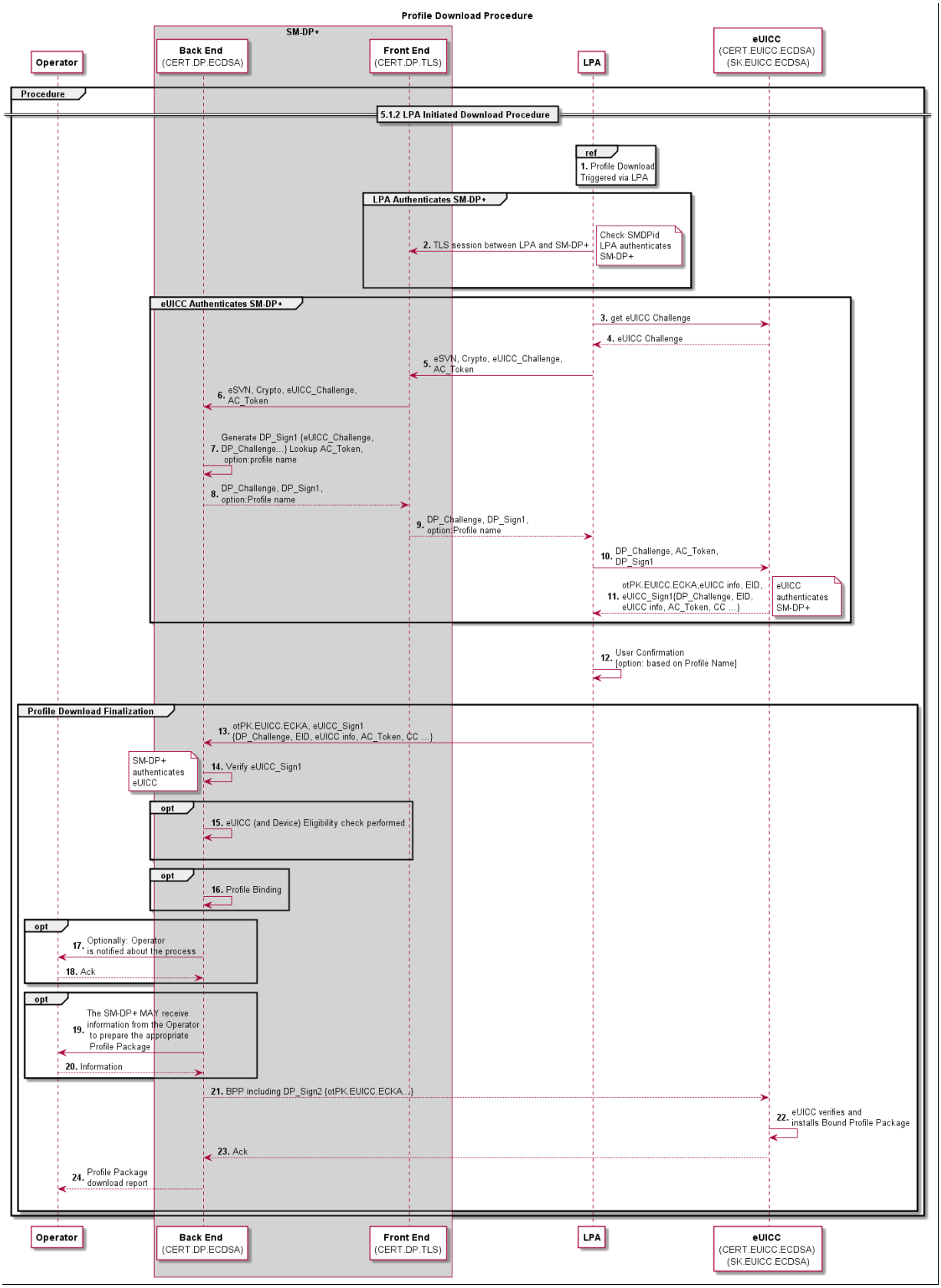


Figure 17: Profile Download Procedure

Start conditions:

a. The Subscriber has completed the Subscription process to the selected Operator/Service Provider offer.
b. The Profile ordering process related to this Subscription has been completed (i.e. an assigned Protected Profile Package is stored on the SM-DP+).

Procedure:

1. The LPA initiates Profile Package download and identifies the address of the SM-DP+ where the Profile is stored and available for download (via e.g. URL, QR code, manual input, etc.) as well as other information provided (e.g. Token, SMDPId, Confirmation Code).
2. The LPA authenticates the SM-DP+ through establishing a TLS connection with the SM-DP+, and verifying the SMDPid if such information has been provided.
3. to 4. The LPA gets an eUICC challenge
5. to 6. The LPA sends the eUICC challenge and any other relevant information to the SM-DP+.
7. to 9. The SM-DP+ signs the eUICC challenge, and generates a DP_Challenge to be sent back to the eUICC.
10. The LPA sends the material received by the SM-DP+ and the AC Token to the eUICC; the eUICC checks the SMDPid and authenticates the SM-DP+.
11. The eUICC sends back a signed set of information including the DP_Challenge, the AC Token, the EID and its Certificate to the LPA.
12. The End User confirms the download of the Profile, optionally with the display of the Profile name of the Operator.
13. The LPA sends the set of information received in Step 11 from the eUICC to the SM-DP+.
14. The SM-DP+ verifies the signature; the eUICC is authenticated.
15. to 16. OPTIONAL: The eUICC Eligibility Check and Profile binding functions are performed by the SM-DP+.

17. to 22. OPTIONAL

17. The Operator is notified about the Profile Package that is about to be downloaded.
18. If the Operator has been notified, it MAY request to stop the download process by indicating an error code to the SM-DP+.
19. If the Operator sends an error code to the SM-DP+, the SM-DP+ stops the download process and indicates the error code to the LPA.
20. The LPA notifies the End User with an appropriate message.
21. to 22. The SM-DP+ MAY receive information from the Operator to prepare the appropriate Profile Package.
23. to 25. The Bound Profile Package is sent to the eUICC and installed on the eUICC.
26. The Profile Package download report is sent from the SM-DP+ to the Operator.

End Condition:

a. The Profile is installed in the eUICC in a Disabled state

5.2 Profile Download with Activation Code

5.2.1 Activation Code Requirements

Req no.	Description
AC1	Where used, the Activation Code SHALL trigger the download of a Bound Profile Package from a specific SM-DP+.
AC2	The Activation Code SHALL comprise of the following parameters: • SM-DP+ address • Activation Code Token (Includes OPTIONAL Confirmation Code Required Flag) • SMDPid (OPTIONAL)
AC3	The Activation Code Token SHALL be able to include a parameter indicating whether a Confirmation Code is required or not. If such a Confirmation Code is required, the LPA SHALL ask the End User to input a Confirmation Code. The SM-DP+ SHALL verify the Confirmation Code before delivering the Bound Profile Package. Note: How the Confirmation Code is created and provided to the End User is out of scope of this specification.
AC4	The Activation Code SHALL be verified by the SM-DP+ before delivering the Bound Profile Package.
AC5	The Activation Code input in the LPA by the End User SHALL support at least manual typing and QR code scanning.
AC6	All Activation Code procedures SHALL be implemented natively as part of the LPA.
AC7	[Void]
AC8	Following the Activation Code procedure, the Profile Package download procedure SHALL be used.
AC9	The Activation Code procedure SHALL preserve eco-system security, privacy and validation of User Intent.
AC10	The Activation Code procedure SHALL be used for the sole purpose of downloading a Profile package to the targeted eUICC. The Activation Code procedure SHALL prevent sending IMEI and EID information to a non-authenticated SM-DP+.
AC11	The Activation Code SHALL uniquely identify the Operator/Service Provider.
AC12	The Activation Code request to the SM-DP+ SHALL be extended by the LPA with the EID after the specific SM-DP+ has been authenticated.

Table 41: Activation Code Requirements

5.2.2 Profile Download with Activation Code Procedure

The Activation Code procedure defines a common functionality which allows the Subscriber or the End User on behalf of the Subscriber to “activate” a Device by means of requesting the download of an Operational Profile from the Device itself.

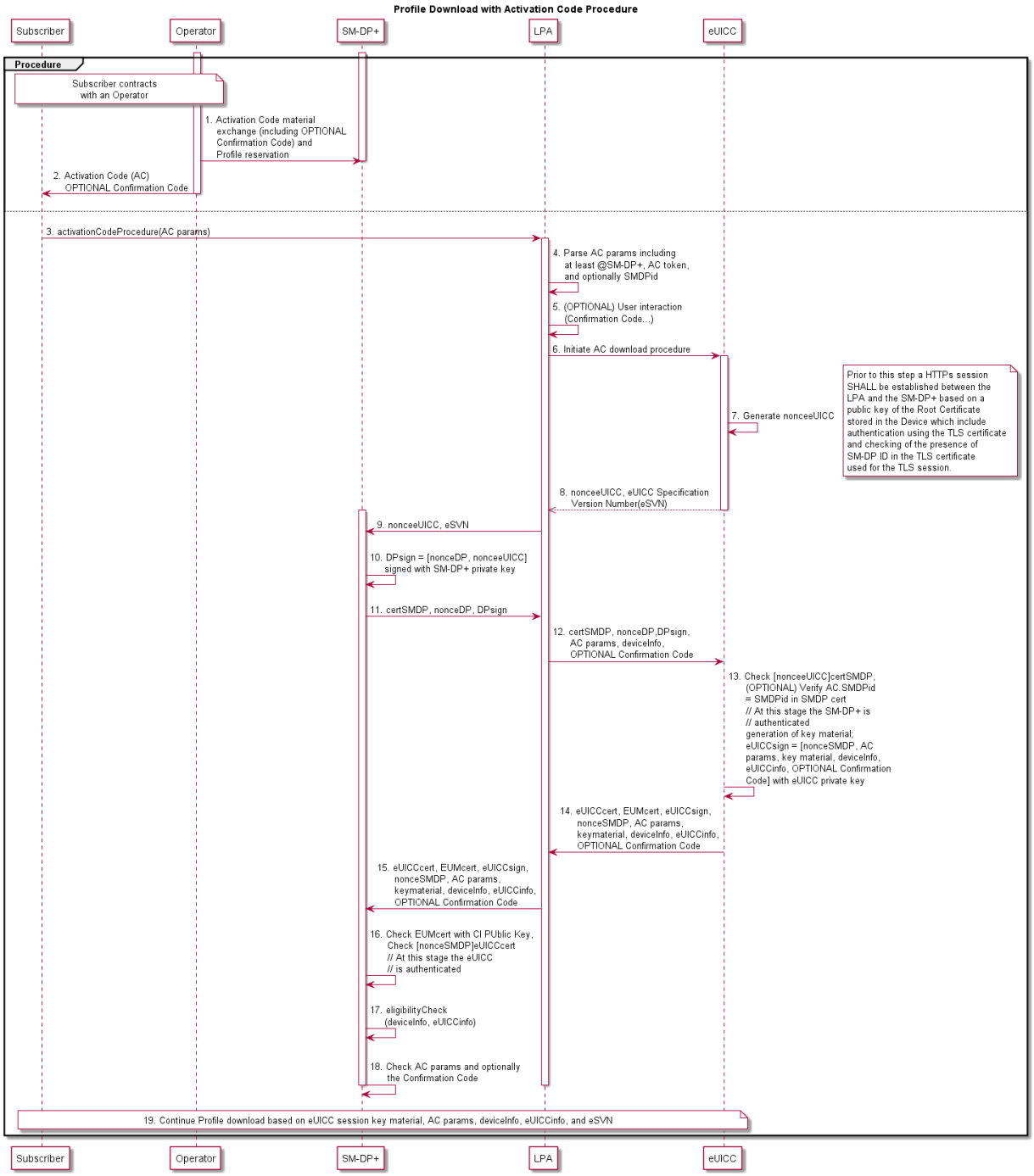


Figure 18: Profile Download with Activation Code Procedure

Start Conditions:

a. A Subscription has been established by the Subscriber.
b. Activation Code material and optionally a Confirmation Code has been provided to the SM-DP+ (Step 1), and an Activation Code has been provided to the End User and optionally a Confirmation Code (side channel) (Step 2).

Procedure:

3. The End User inputs the Activation Code to the LPA through the LUI.

4. The LPA parses the Activation Code parameters to recognise the SM-DP+ address, the Activation Code Token, the LPA Mode and optionally the SMDPid. In addition, the LPA MAY parse in the Activation Token the information that a Confirmation Code is required.
5. If the Confirmation Code parameter in the Activation Code Token is set to “require Confirmation Code”, the End User is prompted to input a Confirmation Code provided to them by the issuing Operator/Service Provider.
6. The Activation Code download procedure is initiated by the LPA. The LPA requests a nonceeUICC from the eUICC.
7. The eUICC creates a nonceeUICC associated with the supported eUICC Specification Version Number (eSVN).
8. The eUICC transmits the nonceeUICC associated with the supported eSVN to the LPA.
9. The LPA sends the nonceeUICC associated with the supported eSVN to the SM-DP+.

Note: Prior to this step a HTTPs session SHALL be established between the LPA and the SM-DP+ based on a public key of the Root Certificate stored in the Device which includes authentication using the TLS Certificate and checking for the presence of the SMDPid in the TLS Certificate used for the TLS session.

10. Upon receiving the nonceeUICC and the associated eSVN, the SM-DP+ creates nonceSMDP and signs both the nonceSMDP and the nonceeUICC.
11. The SM-DP+ sends the signed nonceeUICC and nonceSMDP to the LPA.
12. The LPA collects the Activation Code parameters as well as the Device information needed for the eligibility procedure and optionally the Confirmation Code and transmits them with the signed nonceeUICC and nonceSMDP to the eUICC.
13. The eUICC checks the signature attached to the nonceeUICC. If the SMDPid is configured in the AC, the eUICC checks that the SMDPid provided by the LPA and the SMDPid in the SM-DP+ Certificate correspond. The SM-DP+ is at this stage authenticated by the eUICC. The eUICC generates key material that will be used for the session key establishment. The eUICC signs a set of information with the eUICC private key which includes:
    a. The nonceSMDP
    b. Key material created by the eUICC to calculate session keys for the preparation of the Bound Profile Package
    c. Activation Code parameters
    d. The Device and eUICC information
    e. Optionally the Confirmation Code
14. The eUICC sends the signed set of information to the LPA in addition to:
    a. The nonceSMDP
    b. Key material created by the eUICC to calculate session keys for the preparation of the Bound Profile Package
    c. Activation Code parameters
    d. The Device and eUICC information
    e. The eUICC Certificate which includes the EID
    f. The EUM Certificate
    g. Optionally the Confirmation Code

15. The LPA sends the whole set of information received from the eUICC to the SM-DP+.
16. The SM-DP+ checks the EUM Certificate with the CI Public Key. The SM-DP+ checks the signature of the nonceSMDP; the eUICC is at this stage authenticated by the SM-DP+.
17. The SM-DP+ proceeds with the eligibility check based on the transmitted information (EID, Device information, eUICC information, eSVN).
18. The SM-DP+ checks the Activation Code parameters and optionally the Confirmation Code to retrieve the referenced Profile Package.
19. The Profile Package is downloaded to the eUICC:
    a. The SM-DP+ establishes session keys with the eUICC.
    b. A Bound Profile Package is prepared on the basis of the eUICC session key material and is downloaded and installed on the eUICC.
    c. Successful installation of the Profile on the eUICC is acknowledged and the Operator is notified by the SM-DP+.
    d. Successful installation of the Profile on the eUICC is acknowledged by the eUICC to the LPA which notifies the End User of the status.

End Conditions:

a. A Bound Profile Package has been downloaded and installed on the eUICC in a Disabled state.
b. The LPA MAY offer the Profile for enablement by the End User.

5.3 Local Profile Management

5.3.1 Local Profile Management Procedures

5.3.1.1 Enable Profile

This procedure performs the enabling of a target Profile. The request is given by the End User to the LPA.

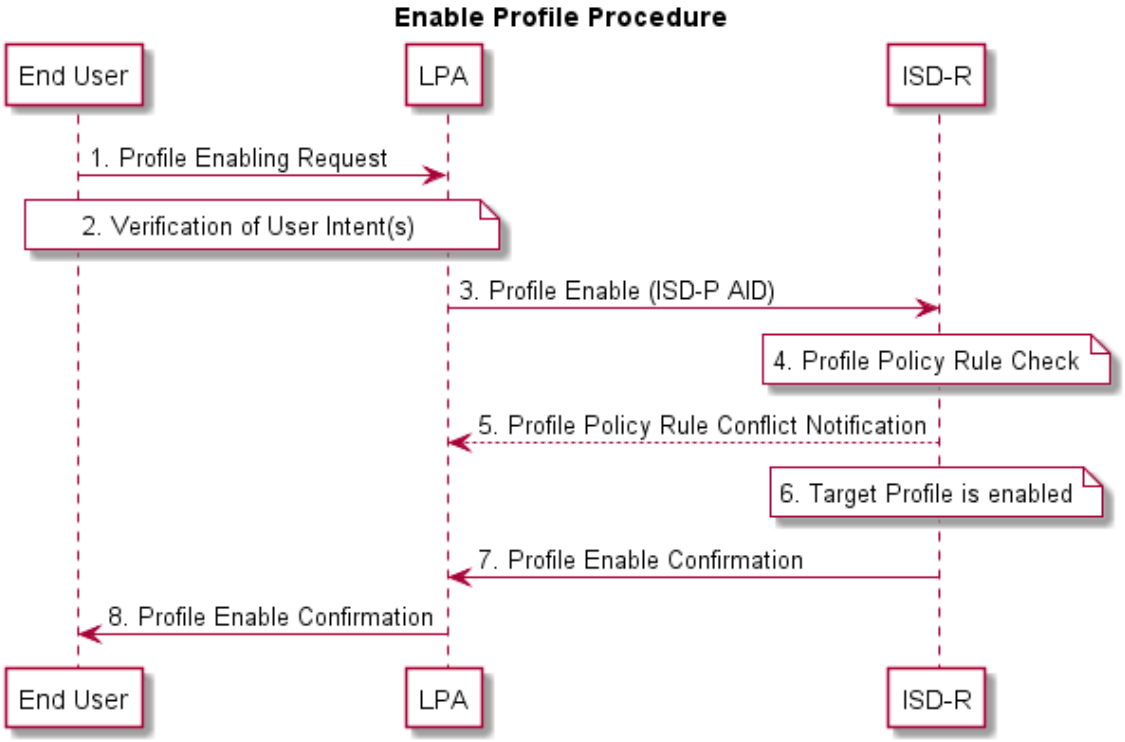


Figure 19: Enable Profile Procedure

Start conditions:

a. The target Profile is disabled on the eUICC.
b. The target Profile has been chosen by the End User.
c. The LPA is authenticated to the eUICC as legitimate for performing Local Profile Management.

Procedure:

1. The End User makes a Profile enable request on the LPA.
2. User Intent is verified.
3. The LPA sends a Profile enable operation for the target Profile to the ISD-R on the eUICC.
4. The ISD-R checks if applied Profile Policy Rules on the target Profile permits the Profile to be enabled
5. If there is a conflict with Profile Policy Rules, the ISD-R aborts the procedure and informs the End User via the LPA.
6. The target Profile is enabled.
7. The ISD-R informs the LPA of the enabling of the Profile.
8. The End User is informed via the LPA.

End conditions:

a. The target Profile is enabled.

5.3.1.2 Disable Profile

Profile disabling can be achieved with the following procedure. The request is given by the End User on the LPA.

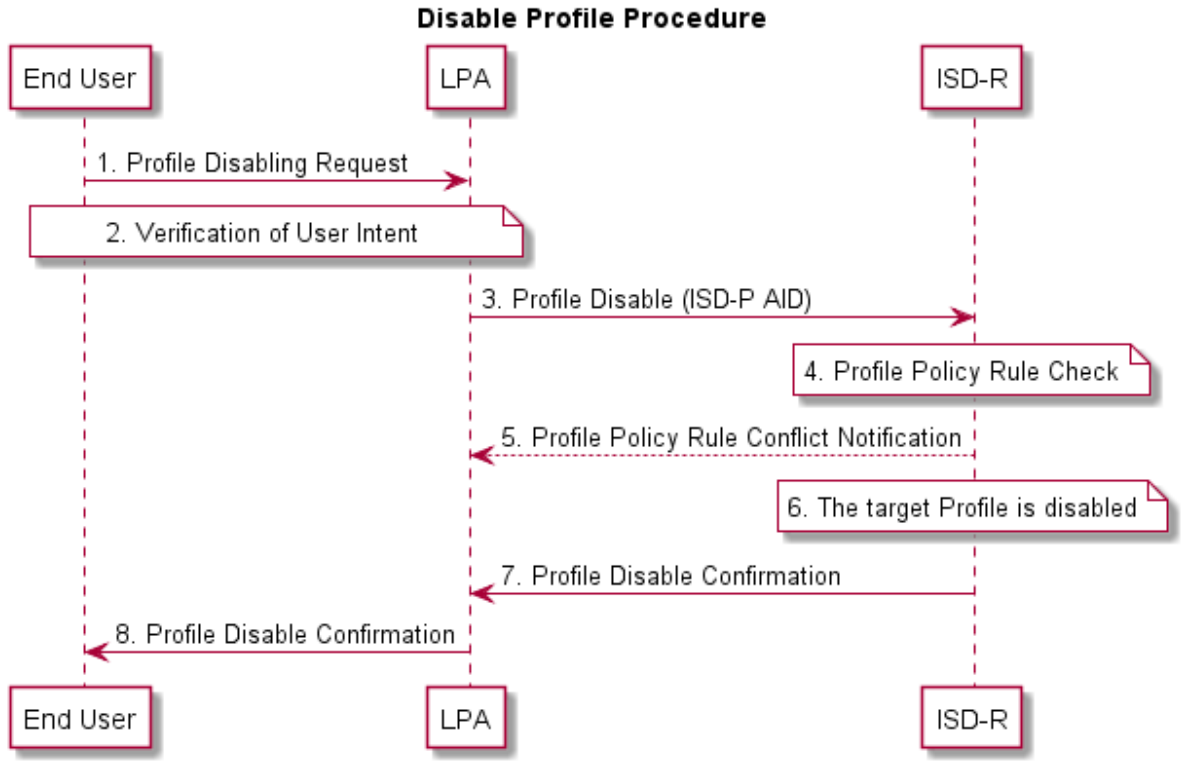


Figure 20: Disable Profile Procedure

Start conditions:

a. The target Profile is enabled on the eUICC.
b. The target Profile has been chosen by the End User.
c. The LPA is authenticated to the eUICC as legitimate for performing Local Profile Management.

Procedure:

1. The End User makes a Profile disable request on the LPA.
2. User Intent is verified.
3. The LPA sends a Profile disable operation to the ISD-R on the eUICC.
4. The ISD-R checks if applied Profile Policy Rules on the target Profile permits the Profile to be disabled.
5. If there is a conflict with Profile Policy Rules, the ISD-R aborts the procedure and informs the End User via the LPA.
6. The ISD-R disables the target Profile.
7. The ISD-R informs the LPA of the disabling of the Profile.
8. The End User is informed via the LPA.

End conditions:

a. The target Profile is disabled.

5.3.1.3 Delete Profile

Profile deletion can be achieved with the following procedure. The request is given by the End User on the LPA.

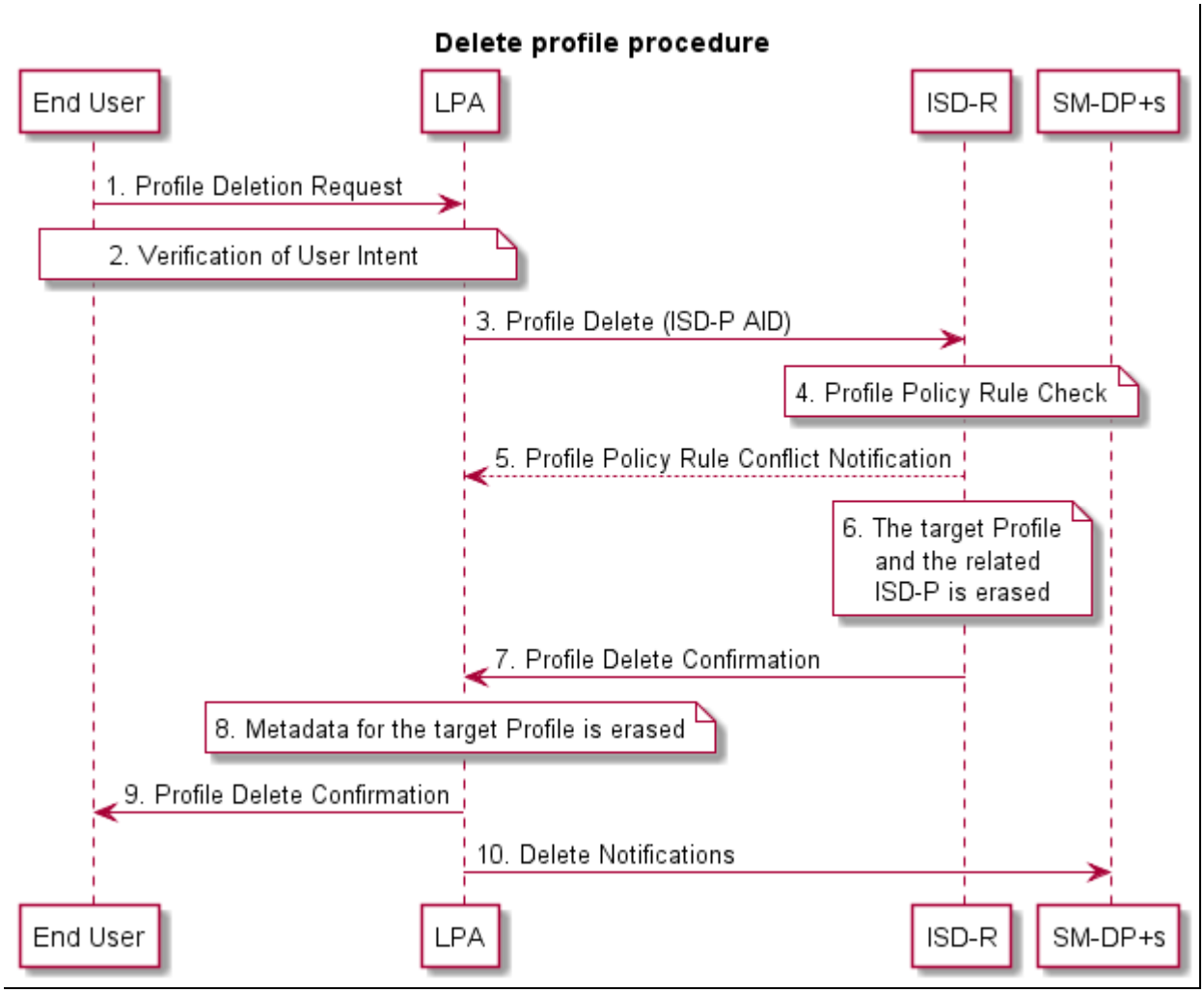


Figure 21: Delete Profile Procedure

Start conditions:

a. The target Profile is disabled.
b. The target Profile has been chosen by the End User
c. The LPA is authenticated to the eUICC as legitimate for performing Local Profile Management.

Procedure:

1. The End User makes a Profile deletion request on the LPA.
2. User Intent is verified.
3. The LPA sends a Profile deletion operation for the target Profile to the ISD-R on the eUICC. The request includes the ISD-P AID of the target Profile.
4. The ISD-R checks if applied Profile Policy Rules permits the Profile to be deleted.
5. If there is a conflict with Profile Policy Rules, the ISD-R aborts the procedure and informs the End User via the LPA.
6. The ISD-R erases the target Profile and the related ISD-P.

7. The ISD-R informs the LPA of the Profile deletion.
8. The Profile Metadata for the target Profile is erased.
9. The End User is informed via the LPA.
10. The LPA sends delete Notifications to the Notification Receivers for Profile deletion in the Profile.

End conditions:

a. The target Profile is deleted.

5.3.1.4 Add/Update Profile Nickname

Add/update nickname will allow the Subscriber or End User to attribute a nickname to a Profile for ease of use. Note that adding or changing a nickname SHALL NOT affect any other data or other Profile Metadata for that Profile.

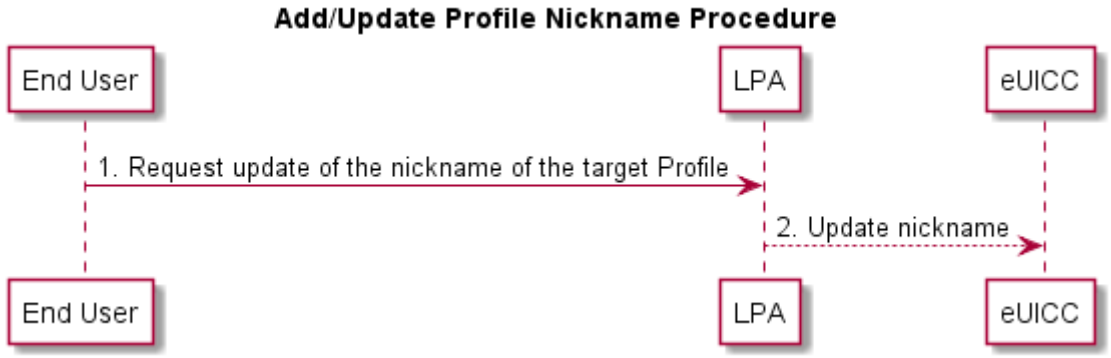


Figure 22: Add/Update Profile Nickname Procedure

Start conditions:

a. User Intent has been verified.
b. The target Profile has been chosen by the End User.
c. The LPA is authenticated to the eUICC as legitimate for performing Local Profile Management.

Procedure:

1. The End User requests the update of the nickname on the LPA.
2. The LPA updates the Profile Metadata of the target Profile with the End User's choice of nickname in the eUICC.

End conditions:

a. Profile Metadata of the target Profile has been updated with the End User's choice of nickname.

5.3.1.5 Query Profile Metadata

This procedure will allow the End User to query the Profile Metadata of the Profiles accessible to the End User. The result SHALL display all (or parts of) the Profile Metadata for the selected Profile on the eUICC at the time of querying. No changes are made to any data on the eUICC as a result of this procedure.

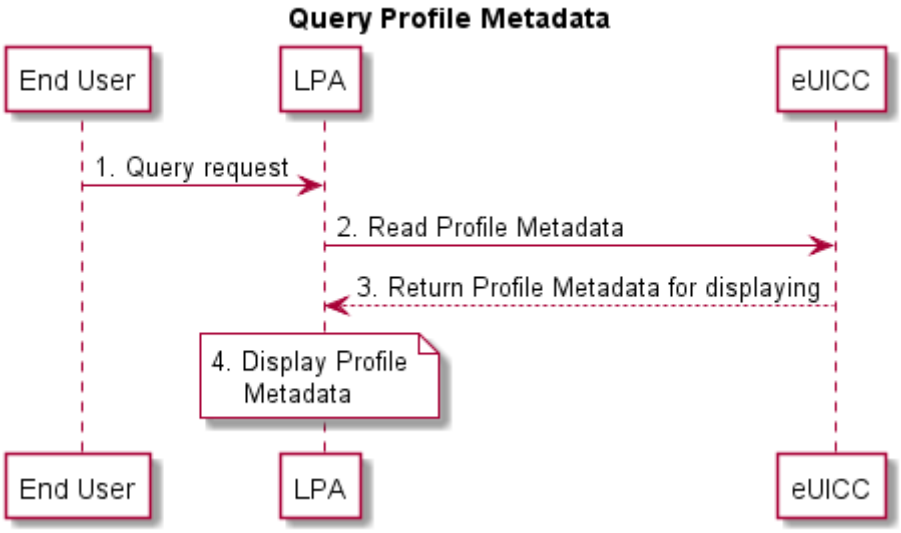


Figure 23: Query Profile Metadata Procedure

Start conditions:

a. The LPA is authenticated to eUICC as legitimate for performing Local Profile Management.
b. The list of Profiles accessible to the End User is displayed by the LPA (LUI).

Procedure:

1. The End User selects a Profile to query.
2. The LPA receives a query request from the End User.
3. The LPA requests Profile Metadata from the eUICC.
4. The LPA displays the Profile Metadata to the End User on the LUI.

End conditions:

a. No change to Profile Metadata.

5.3.1.6 eUICC Memory Reset

This procedure performs the eUICC Memory Reset of the eUICC including its associated Profile Metadata. The request is given by the End User to the LPA.

Note: A similar procedure will apply to perform the eUICC Test Memory Reset of the eUICC**.**

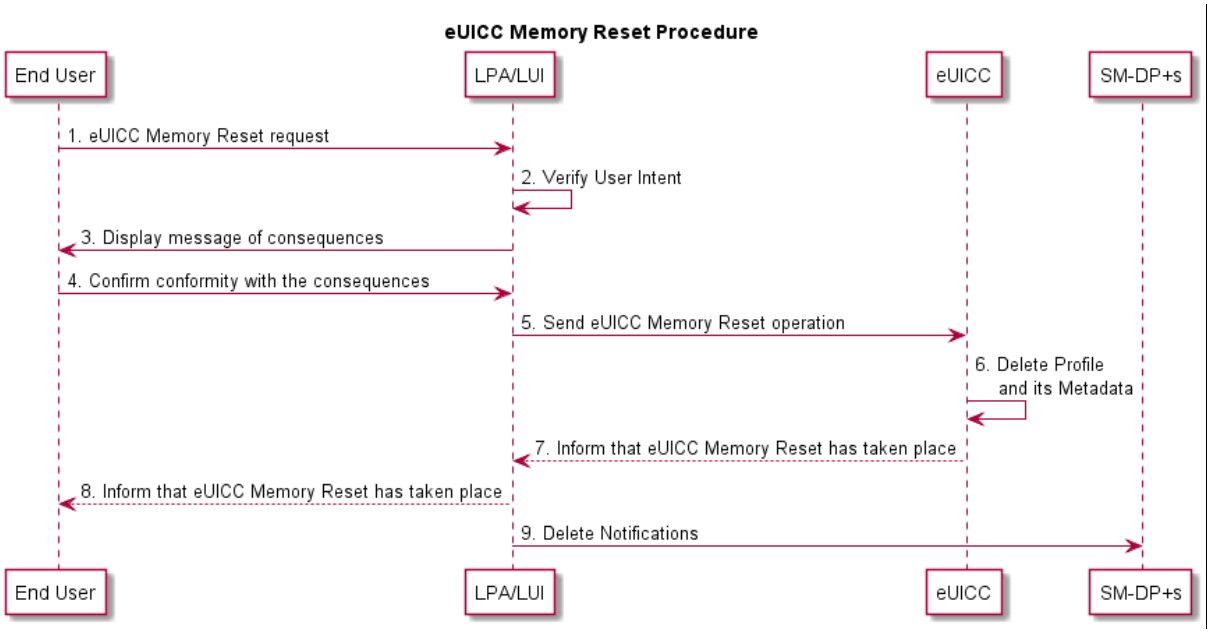


Figure 24: eUICC Memory Reset Procedure

Start conditions:

a. The LPA is authenticated to the eUICC as legitimate for performing Local Profile Management.
b. The eUICC Memory Reset option is displayed by the LPA (LUI).

Procedure:

1. The End User makes an eUICC Memory Reset request on the LPA (LUI).
2. User Intent is verified.
3. The LPA (LUI) displays a message of consequences of ‘eUICC Memory Reset’ to the End User.
4. The End User confirms the conformity with the consequences to the LPA.
5. The LPA sends an eUICC Memory Reset operation to the eUICC.
6. The eUICC deletes the Profile on the eUICC even if it is an Enabled Profile including the Profile Metadata associated with it.
7. The eUICC informs the LPA of the eUICC Memory Reset of the eUICC.
8. The End User is informed via the LPA (LUI).
9. The LPA sends delete Notifications to all Notification Receivers for Profile deletion in the Profile.

End conditions:

a. The Profile is deleted from the eUICC.

5.3.1.7 Add Profile with Activation Code

This procedure will allow the Subscriber to add a single Profile. This procedure will not enable the downloaded Profile, nor disable an Enabled Profile. Network connectivity is assumed. The download can be initiated by the input of an Activation Code.

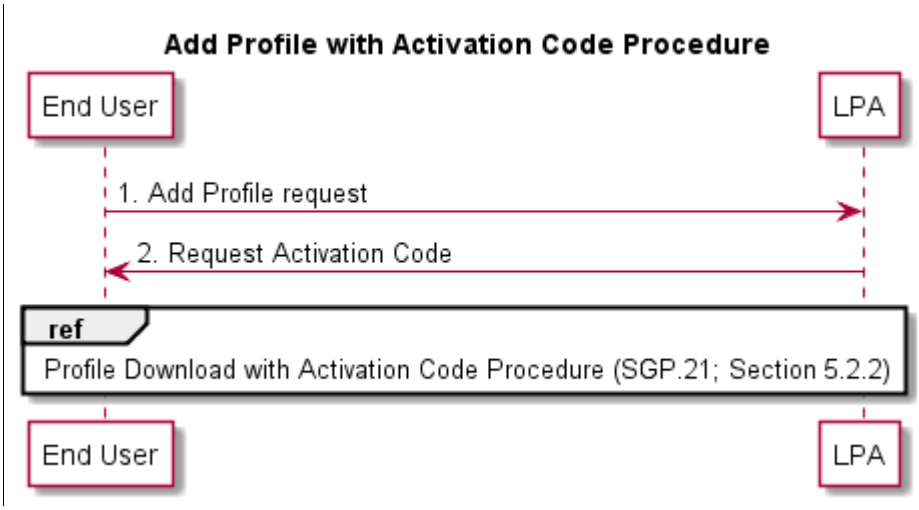


Figure 25: Add Profile with Activation Code Procedure

Start conditions:

a. User Intent has been verified.
b. The download of a new Profile is allowed on the eUICC.
c. The LPA is authenticated to the eUICC as legitimate for performing Profile download.

Procedure:

1. The End User obtains an Activation Code to add a Profile to their Device.
2. The LPA requests the End User to enter the Activation Code.
3. Profile Download with Activation Code Procedure as described in Section 5.2.2 starts.

End conditions:

a. The Profile has been installed on the End User's Device.
b. Profile Metadata has been updated from the Profile.

5.3.1.8 Edit SM-DP+ Address

This procedure will allow the End User to edit a default SM-DP+ address on to the eUICC.

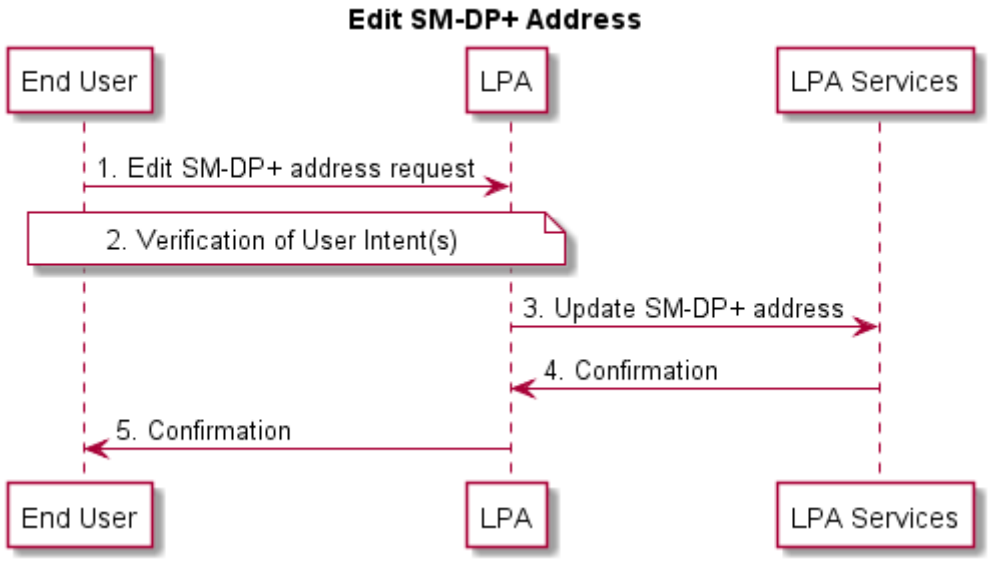


Figure 26: Edit SM-DP+ Address

Start conditions:

a. There is a default SM-DP+ address in the LPA.
b. The End User is willing to edit the default SM-DP+ address

Procedure:

1. The End User edits the SM-DP+ Address via the LPA.
2. Simple Confirmation from the End User is required.
3. The LPA sends the default SM-DP+ address for storage in the LPA Service.
4. The LPA Service informs the LPA of the storage of the default SM-DP+ address.
5. The End User is informed via the LPA.

End conditions:

a. The target default SM-DP+ Address is edited in the LPA Services.

Annex A Security Threats, Risks and Creation Process Requirements (Informative)

New Profile on New Primary Device (Off Device Activation)

Risk no.	Risk description
INI1	Incomplete or corrupted Profile being pushed to the Subscriber.
INI2	Malicious eUICC party using privileged position in order to push unsolicited Profiles to Devices.

Table 42: New Profile on New Primary Device Risks

Profile Deletion

Risk no.	Risk description
IND1	Long term gathering of key materials due to a long term storage of delivered Profiles after their disabling.
IND2	Loss of sensitive data from discarded media supports (hard drives…)
IND3	Malware launching coordinated or isolated deletion of one or several Profiles leading to a loss of connectivity to an End User.
IND4	Accidental Profile deletion (e.g. unattended children…) leading to a loss of connectivity to an End User.
IND5	Non-tech-savvy or malicious Subscriber repeatedly deleting Profiles and asking for them to be reloaded leading to surcharge of provisioning servers.

Table 43:Profile Deletion Risks

Profile Switch

Risk no.	Risk description
INP1	Malicious Profile switching originating from an internal party.
INP2	Human error leading to the switching of alternate Profiles leading to a loss of connectivity.
INP3	Malware launching coordinated or isolated switching of one or several Profiles leading to a loss of connectivity.
INP4	Malware launching coordinated or isolated switching of one or several Profiles leading to major fraud scenarios.

Table 44: Profile Switching Risks

Profile Swap

Risk no.	Risk description
INS1	Race condition leading to the deactivation of all Profiles and a loss of connectivity.

Table 45: Profile Swapping Risks

Cryptographic Related Risks

Risk no.	Risk description
INO1	Loss or theft of private keys in one or several Profile Management components leading to the loss of confidentiality on the whole chain.
INO2	Inability to revoke compromised Certificates leading to the loss of trust on the whole Certificate chain.
INO3	Local law enforcement requests leading to the forceful disclosure of key materials.
INO4	Local law enforcement requests leading to the forceful compromise of key components.
INO5	Malicious or accidental revocation of Certificates leading to the denial of service on the whole provisioning Certificate chain.
INO6	Use of temporary symmetric cryptographic or “generic” key material during the Profile creation, temporary storage, transport, or long-term storage leading to single point of failure and attack being created.

Table 46: Cryptographic Related Risks

Quality of Service

Risk no.	Risk description
QoS1	Profile creation burst leading to the inability for the eUICC platforms to deliver expected service level.
QoS2	Denial of service on delivery platforms leading to the inability to deliver expected service level.
QoS3	Inability to recover from management communication failures leading to a temporary or permanent inability to deliver a Profile.

Table 47: Quality of Service Risks

Non-human or Unpredictable

Risk no.	Risk description
EXC1	Catastrophic event such as floods, earthquakes, etc. leading to the destruction of a datacentre.
EXC2	Geopolitical/Human events leading to the destruction of a datacentre.
EXC3	Change of regulation leading to partial or total loss of trust for an actor of the provisioning delivery chain (Operator, OEM, SIM vendor…).

Table 48: Non-human or Unpredictable Risks

New Profile during Subscriber Journey

Risk no.	Risk description
EXN1	Malicious pairing of new Device using unattended Primary or Companion Device.
EXN2	Use of public Wi-Fi for internet connectivity leading to the loss of confidentiality during the provisioning of Profile operations.

Risk no.	Risk description
EXN3	Use of public Wi-Fi for internet connectivity leading to the tampering of registration information during provisioning of Profile operations.
EXN4	Social engineering leading to the communication of OTP materials to attackers.
EXN5	Man-in-the-middle or eavesdropping during Profile provisioning leading to the loss of confidentiality.
EXN6	“Implicit authentication” (e.g. HTTP MSISDN enrichment) leading to the loss of authentication or Profile material.

Table 49: New Profile during Subscriber Journey Risks

Device Swap

Risk no.	Risk description
EXS1	Malicious Subscriber using race condition scenarios leading to Profiles being activated on both Devices.
EXS2	Malicious entity using weak swap procedures in order to compromise authentication vectors.

Table 50: Device Swapping Risks

Loss of Privacy

Risk no.	Risk description
PRI1	Improper handling, transport or disclosure of the EID or any user related data information leading to the use of the latter as a “super” user tracking identifier.
PRI2	eUICC management commands leading to the creation of unexpected and unpredicted « remote paging » or « remote control » commands used by 3rd parties to spy or compromise Devices or the Subscriber themselves.

Table 51: Loss of Privacy Risks

Others

Risk no.	Risk description
EXO1	Compromising of exchanges between Profile Management actors leading to the critical loss of private keys.
EXO2	Profile cloning due to unpredicted implementation routines for specific scenarios.

Table 52: Other Risks

Creation Process

Req no.	Requirement description
CRE1	Profiles failing to be created SHALL be securely deleted or at least purged of authentication vectors.

Req no.	Requirement description
CRE2	Communication between systems participating in the Profile creation SHALL be protected in integrity and confidentiality.

Table 53: Creation Process Requirements

Annex B Profile Production Procedure (Informative)

B.1 Profile Production Procedure

This section describes a generic implementation. It should be regarded as an example only; specific implementation MAY be required to address specific security concerns.

Within the eUICC, the current functionality of the UICC is represented by a Profile. Just as with current UICCs, Profiles are the responsibility of the Operator and Profile production is performed upon their request and permission (if not produced by the Operators themselves).

The same Operator procedures as in the current UICCs SHALL apply.

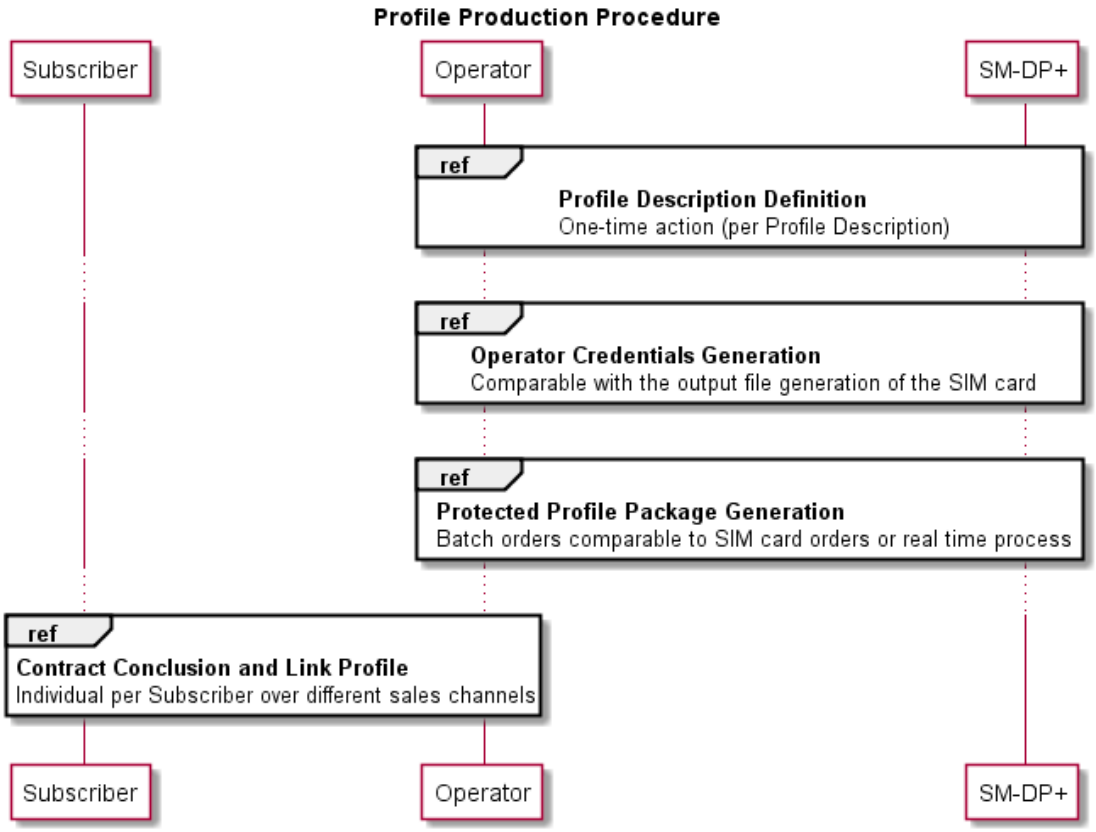


Figure 27: Profile Production Procedure

Profile Production consists of three steps:

- **Profile Description definition:** The SM-DP+ creates and registers a Profile Description based on the Operational Profile Description.
- **Operator Credentials generation:** The Operator asks the SM-DP+ to generate Operator Credentials that will be used in the next step. This procedure is OPTIONAL and will not be used if the Operator wants to generate the Operator Credentials during Protected Profile Package generation.
- **Protected Profile Package generation:** The Profile Packages will be created, protected and stored. This step (batch type of operation or real time process) is only performed after an order with the respective Operator.

- **Contract conclusion and Link Profile:** At the end of the contract conclusion, an Activation Code is delivered to the End User and the Profile MAY be allocated for this contract.

Note: The generation of the Bound Profile Package is part of the Profile download with Activation Code procedure in Section 5.2.2.

B.1.1 Profile Description Definition

The Profile description definition MAY comprise of the following sequence:

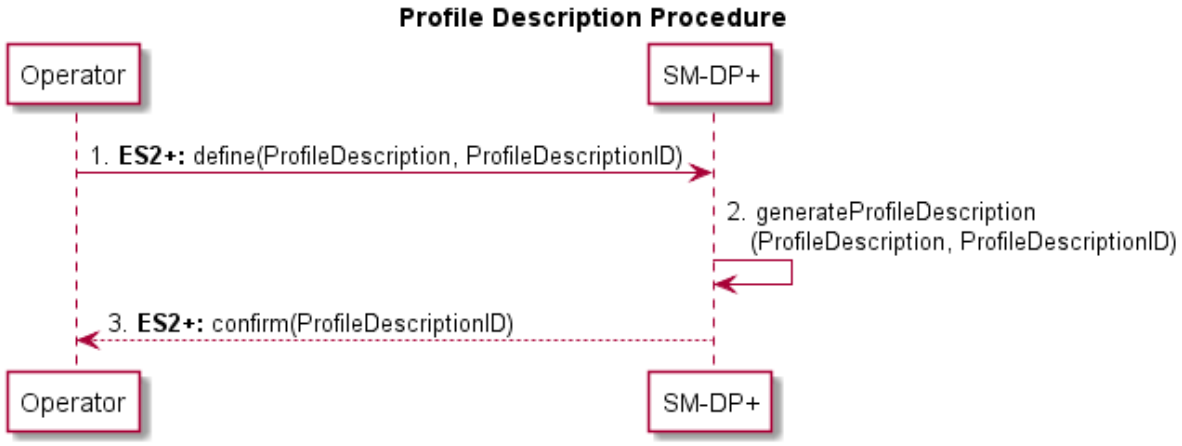


Figure 28: Profile Description Procedure

Start Condition:

a. Contractual relationship between the Operator and the SM-DP+.

Procedure:

1. The Operator defines its different Profile types (identified by a [non-standardised] Profile Description ID) which contains the Network Access Application like USIM, file structure, data and applications, etc.
2. The SM-DP+ creates the Profile Descriptions based on the Operators input with the corresponding Profile Description ID.
3. The SM-DP+ confirms the Profile Description definition e.g. by sending the corresponding Profile Description ID.

Note: An Operator can define multiple Profile Descriptions with the SM-DP+

End Condition:

a. The Operator is able to order Protected Profile Packages based on Profile Description IDs.

B.1.2 Operator Credentials Generation

This procedure allows the Operator to allocate a set of Operator Credentials on the SM-DP+ without associating them to a specific ProfileDescriptionID.

Operator Credentials generation MAY comprise of the following sequence:

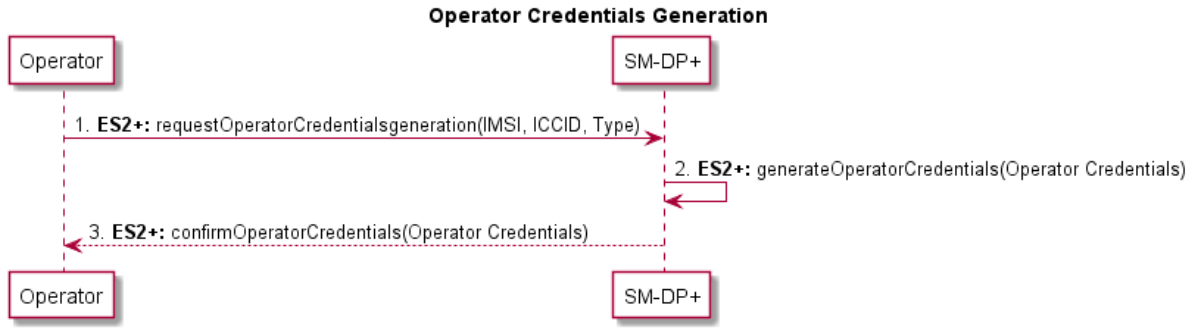


Figure 29: Operator Credentials Generation

Start Condition:

a. IMSI, ICCID and other resources have been allocated by the Operator.

Procedure:

1. The Operator provides the IMSI, ICCID, type of credential to be created (e.g. Milenage [11][12], TUAK [10] etc.) and other resources that MAY already be allocated to the SM-DP+. It asks the SM-DP+ to securely generate and store a set of Operator Credentials.
2. The SM-DP+ securely generates and stores a set of Operator Credentials based on the Operator's input with the corresponding IMSI, ICCID and other resources provided.
3. The SM-DP+ confirms the generation of Operator Credentials and provides them to the Operator.

B.1.3 Protected Profile Package Generation

The Protected Profile Package Generation MAY comprise of the following sequence:

This procedure MAY apply between the Profile Description definition, and the Contract conclusion and Link Profile, depending on whether the Protected Profile Package is created on demand or prepared in advance.

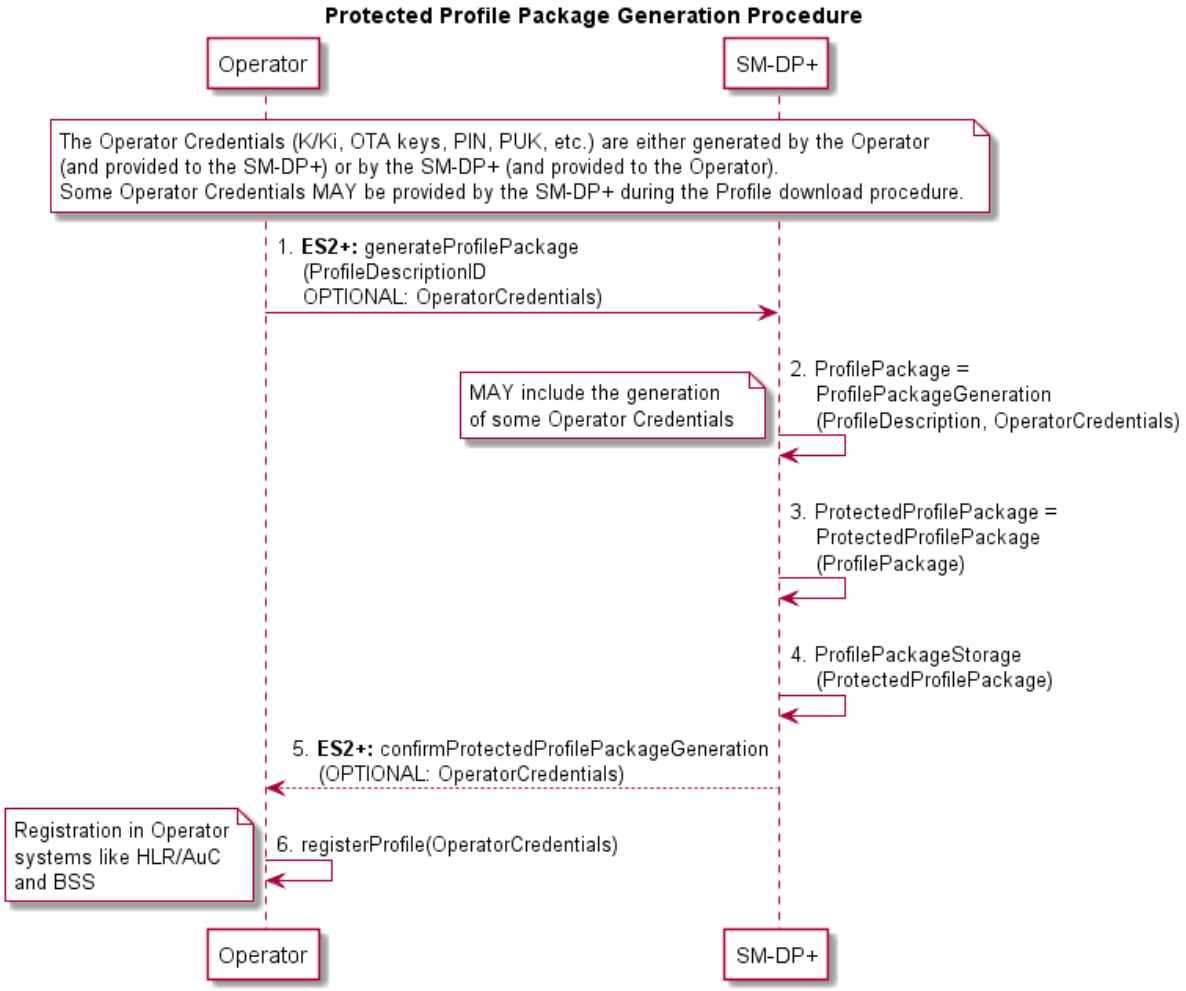


Figure 30: Protected Profile Package Generation Procedure

Start Conditions:

a. Profile Description definition

Procedure:

1. The Operator orders the Protected Profile Package generation by providing the SM-DP+ with the Profile Description ID and some corresponding Operator input data (credentials e.g. ICCID, IMSI).The Operator input data required for Protected Profile Package generation (IMSI, ICCID, K/Ki, OTA Keys, PIN, PUK, etc.) is either created by the Operator (and provided to the SM-DP+) or by the SM-DP+ (and provided to the Operator).
2. The SM-DP+ creates the Profile Packages.
3. The SM-DP+ creates the Protected Profile Packages.
4. The SM-DP+ stores the Protected Profile Packages (securely).
5. The SM-DP+ confirms the Protected Profile Package generation, and eventually sends the additional Operator input data created by the SM-DP+.
6. The Operator registers the Operator data in the Operator systems like HLR/AuC and BSS.

End Condition:

a. The ordered Protected Profile Packages are available at the SM-DP+. The Operator is able to activate these Subscriptions and a Profile download can be triggered upon binding to an EID.

B.1.4 Contract Conclusion and Link Profile

The Activation Code has to be provided to the End User in order to achieve the Profile download procedure. The contract conclusion and Link Profile procedure describes different scenarios to link a contract with the Activation Code process. The following options are described below:

- **Activation Code with known EID:** The EID is given by the Subscriber to the Operator during the conclusion of the contract.
- **Activation Code with unknown EID:** The EID is not given by the Subscriber to the Operator during the conclusion of the contract. The EID is only provided to the SM-DP+ during the Profile download procedure and is given back from the SM-DP+ to the Operator.
- **Activation Code with EID provided to the Operator:** The EID is not immediately given by the Subscriber during the contract conclusion, but provided in step two to the Operator.

The contract reference MAY be, but not necessarily, any Activation Code parameter (e.g. token), ICCID or the IMSI.

In any case, the SM-DP+ SHALL be able to allocate and link a Profile to the corresponding eUICC during the Profile download procedure.

B.1.4.1 Activation Code with Known EID

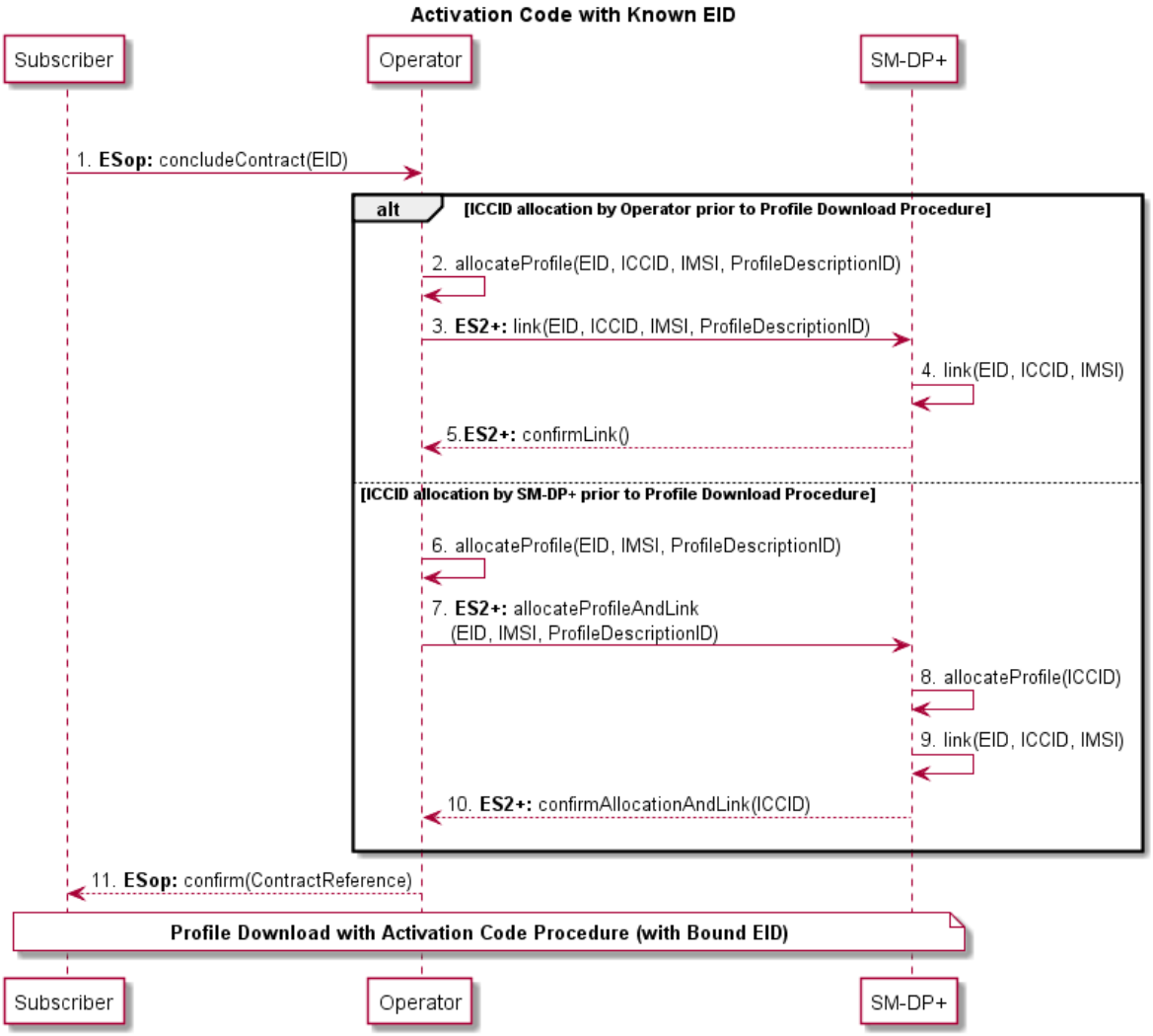


Figure 31: Activation Code with Known EID Procedure

Procedure:

Steps 1-11 in Figure 31: Contract conclusion with known EID

1. The Subscriber concludes a contract with the Operator and provides the EID during this process.
2. to 5. **Alternatively 'ICCID allocation by Operator prior to Profile download procedure':** The Operator allocates the Profile and sends the EID, IMSI and ICCID to the SM-DP+. The SM-DP+ links the different parameters and confirms this to the Operator.
6. to 10. **Alternatively 'ICCID allocation by SM-DP+ prior to Profile download procedure':** The Operator sends the EID, the IMSI and the Profile Description ID to the SM-DP+. The SM-DP+ allocates an ICCID to a corresponding Profile, links the different parameters and confirms the allocated ICCID and the link to the Operator.
11. The Operator confirms the contract conclusion to the Subscriber with the corresponding information (contract reference).

End Condition:

a. The Subscriber has concluded a contract and a valid Subscription with the Operator.
b. The SM-DP+ is informed about a future Profile download procedure request.

B.1.4.2 Activation Code with Unknown EID

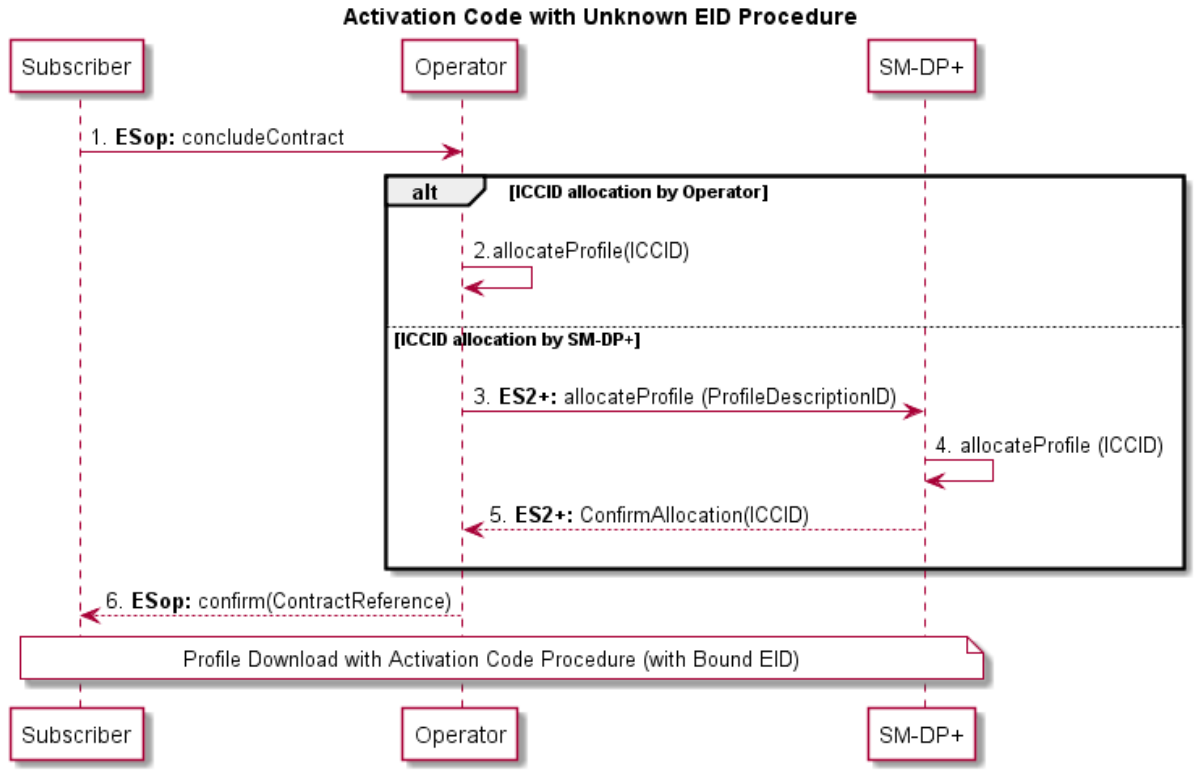


Figure 32: Activation Code with Unknown EID Procedure

Procedure:

Steps 1-6 in Figure 32: Contract conclusion without EID

1. The Subscriber concludes a contract with the Operator without knowledge of the target eUICC (EID).
2. **Alternatively 'ICCID allocation by Operator':** The Operator allocates the Profile (ICCID)
3. to 5. **Alternatively 'ICCID allocation by SM-DP+':** The Operator sends the Profile template (ID) to the SM-DP+. The SM-DP+ allocates a corresponding Profile (ICCID) and sends the allocated ICCID to the Operator.
6. The Operator confirms the contract conclusion to the Subscriber with the corresponding information (contract reference).

End Condition:

a. The Subscriber has concluded a contract and a valid Subscription with the Operator.

b. The SM-DP+ is informed about a future Profile download procedure request.

B.1.4.3 Activation Code with EID Provided to the Operator

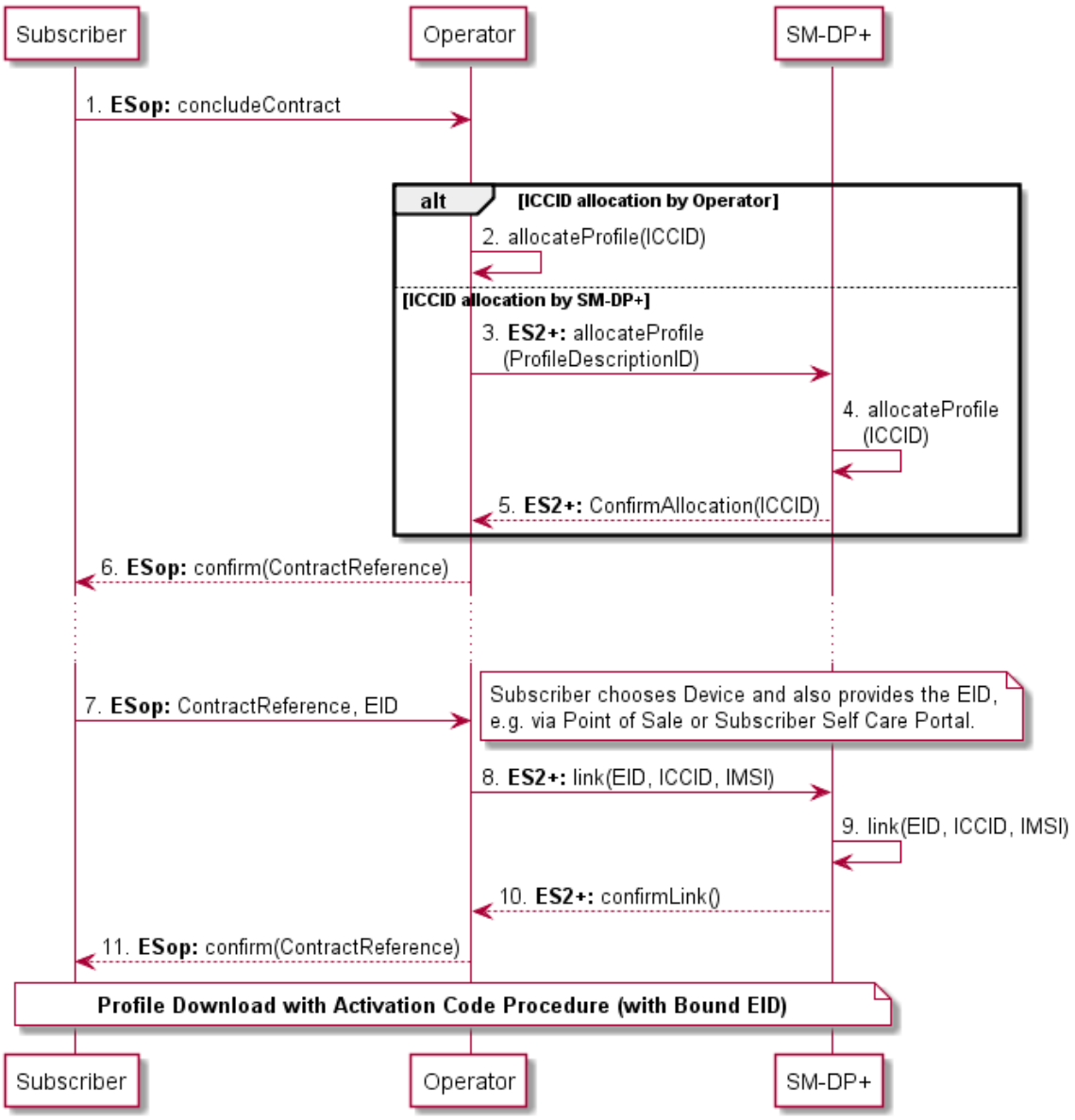


Figure 33: Activation Code with EID Provided to the Operator

Procedure:

Steps 1-11 in Figure 33 Error! Reference source not found.**: Activation Code with EID provided to the Operator**

1. The Subscriber concludes a contract with the Operator without knowledge of the target eUICC (EID).
2. **Alternatively 'ICCID allocation by Operator':** The Operator allocates the Profile (ICCID)
3. to 5. **Alternatively 'ICCID allocation by SM-DP+':** The Operator sends the Profile template (ID) to the SM-DP+. The SM-DP+ allocates a corresponding Profile (ICCID) and sends the allocated ICCID to the Operator.

6. The Operator confirms the contract conclusion to the Subscriber with the corresponding information (contract reference).
7. After the Subscriber has chosen the Device/eUICC, the EID is provided together with the contract reference to the Operator.
8. to 10. The Operator requests the linking of the eUICC (EID) and Profile (ICCID) by the SM-DP+. The SM-DP+ links the EID and the ICCID and confirms this to the Operator.
11. The Operator confirms the linking of the EID to the corresponding contract to the Subscriber.

End Condition:

a. The Subscriber has concluded a contract and a valid Subscription with the Operator.
b. The SM-DP+ is informed about a future Profile download procedure request.

Annex C Local Profile Management Operations implementation (Informative)

This annex provides an example diagram for the implementation of Local Profile Management Operations and describes how the different Confirmation Levels MAY be applied.

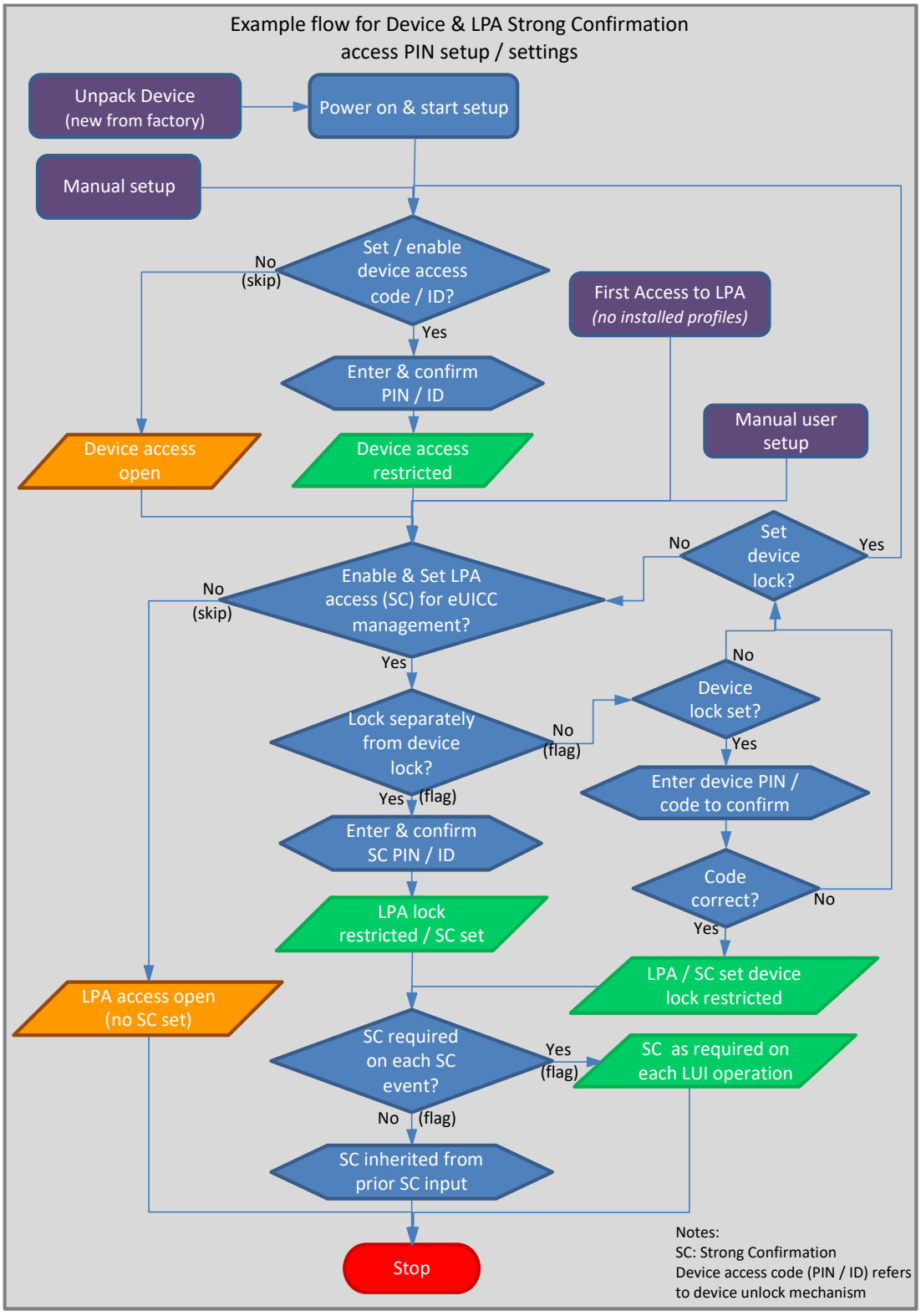


Figure 34: Example Flow for Device & LPA Strong Confirmation Access PIN Setup / Settings

Annex D eUICC Categories (Normative)

The following table provides eUICCs categories defined for Remote SIM Provisioning products.

Role no.	Description
CAT1	Basic eUICCs SHALL be compliant with at least the following features: • Memory size available when no Profiles are installed (EEPROM) : 64kB • ISO interface PPS 96 • BIP over HTTPS features
CAT2	Medium eUICCs SHALL be compliant with at least the following features: • Memory size available when no Profiles are installed (EEPROM) : 384kB • ISO interface PPS 97 • BIP over HTTPS features • Processor >= 25MHz • Crypto processor >= 100MHz • Memory Protection Unit
CAT3	Contactless eUICCs SHALL be compliant with at least the following features: • Memory size available when no Profiles are installed (EEPROM) : 1024kB • ISO interface PPS 97 • BIP over HTTPS features • Processor >= 25MHz • Crypto processor >= 100MHz • Memory Protection Unit

Table 54: eUICC Categories

Annex E LPA Settings (Informative)

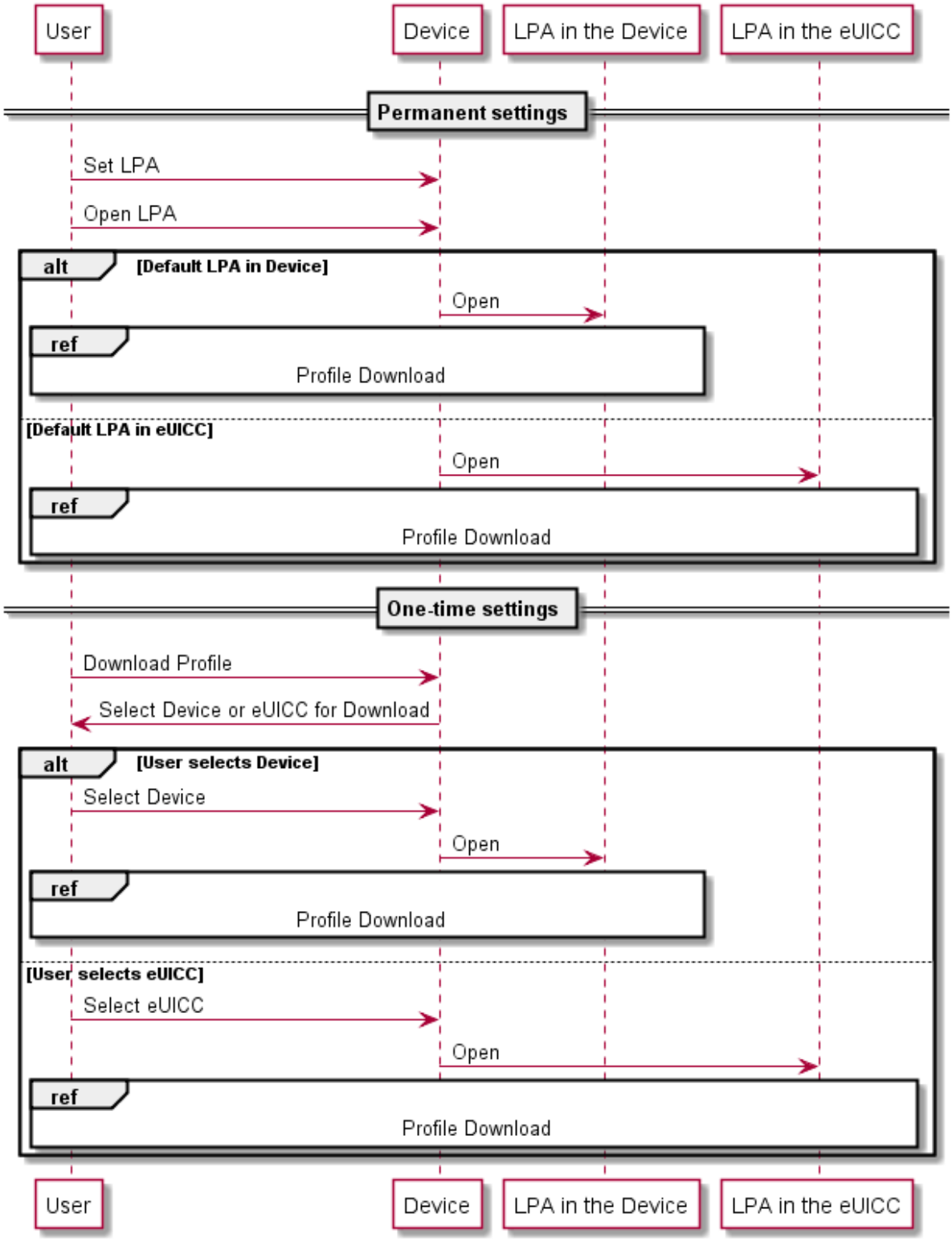


Figure 35: LPA Settings

Annex F Certifications Chain and Security Model (Normative)

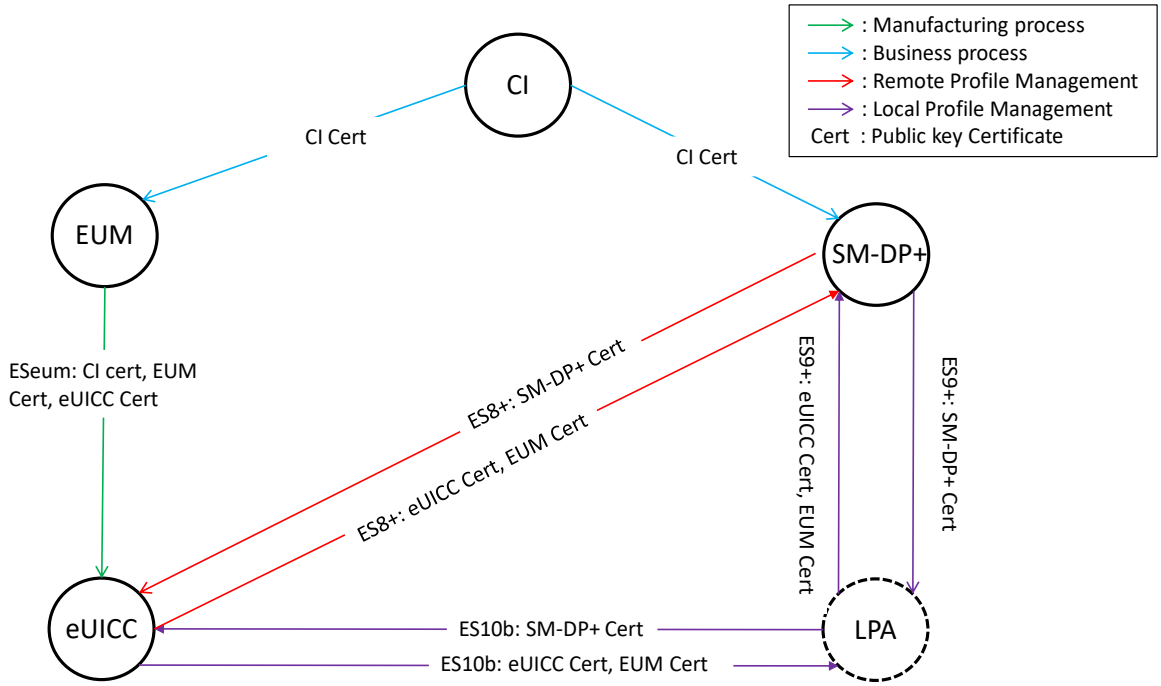


Figure 36: Certificate Exchange with LPA in the Device

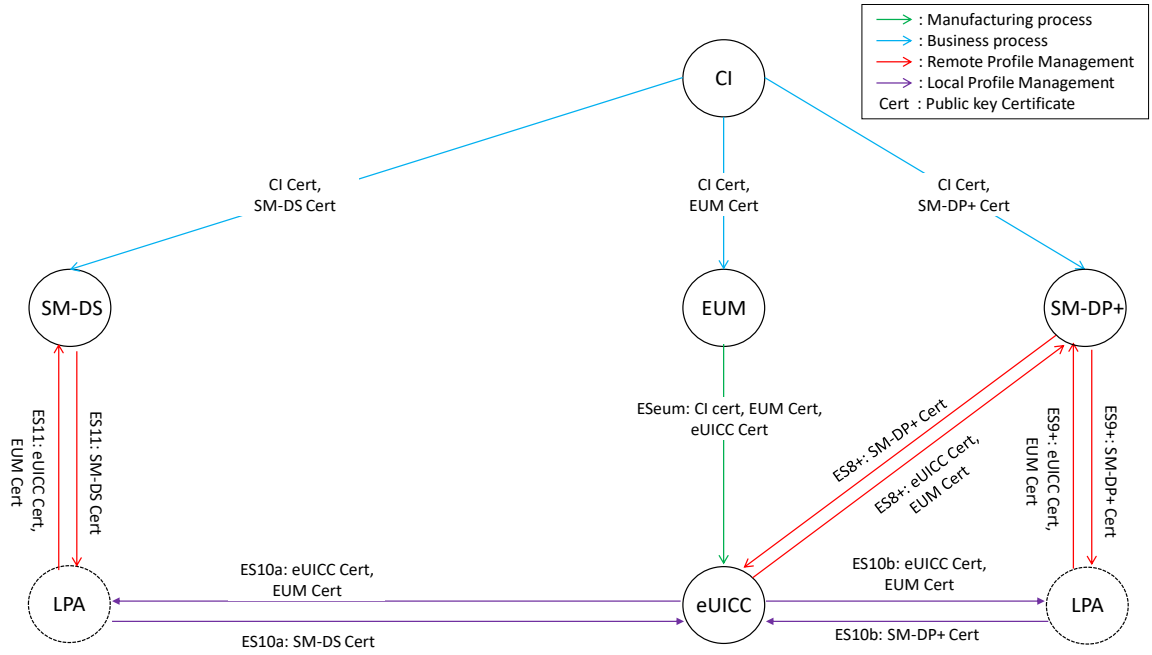


Figure 37: Certificate Exchange with LPA in the eUICC

F.1 Security Model

The Security Model defines the trust relationships between all the active components of the eUICC ecosystem with an LPA in the Device.

The figure below shows only the end-to-end logical links where cryptographic keys and sensitive data are sent. The different links define the end-to-end trust relationship between entities. We distinguish a hierarchy of seven trust links with link 1 being the most significant and link 7 being the least significant.

If trust link 1 is broken, all trust links will be broken as a result. If trust link 2 is broken, trust link 1 remains intact however all other Trusted Links are compromised or broken.

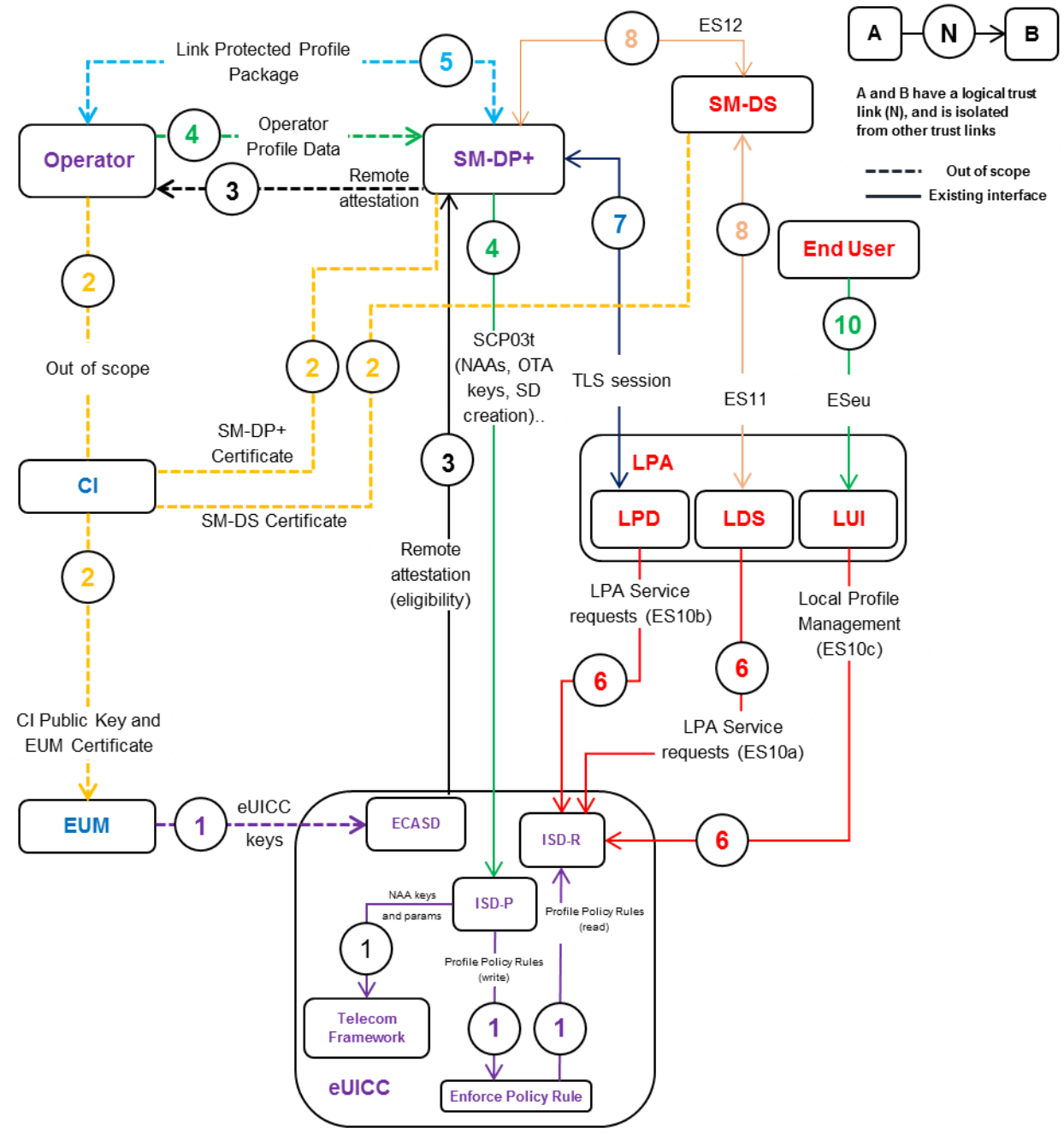


Figure 38: Trusted Link with LPA in the Device

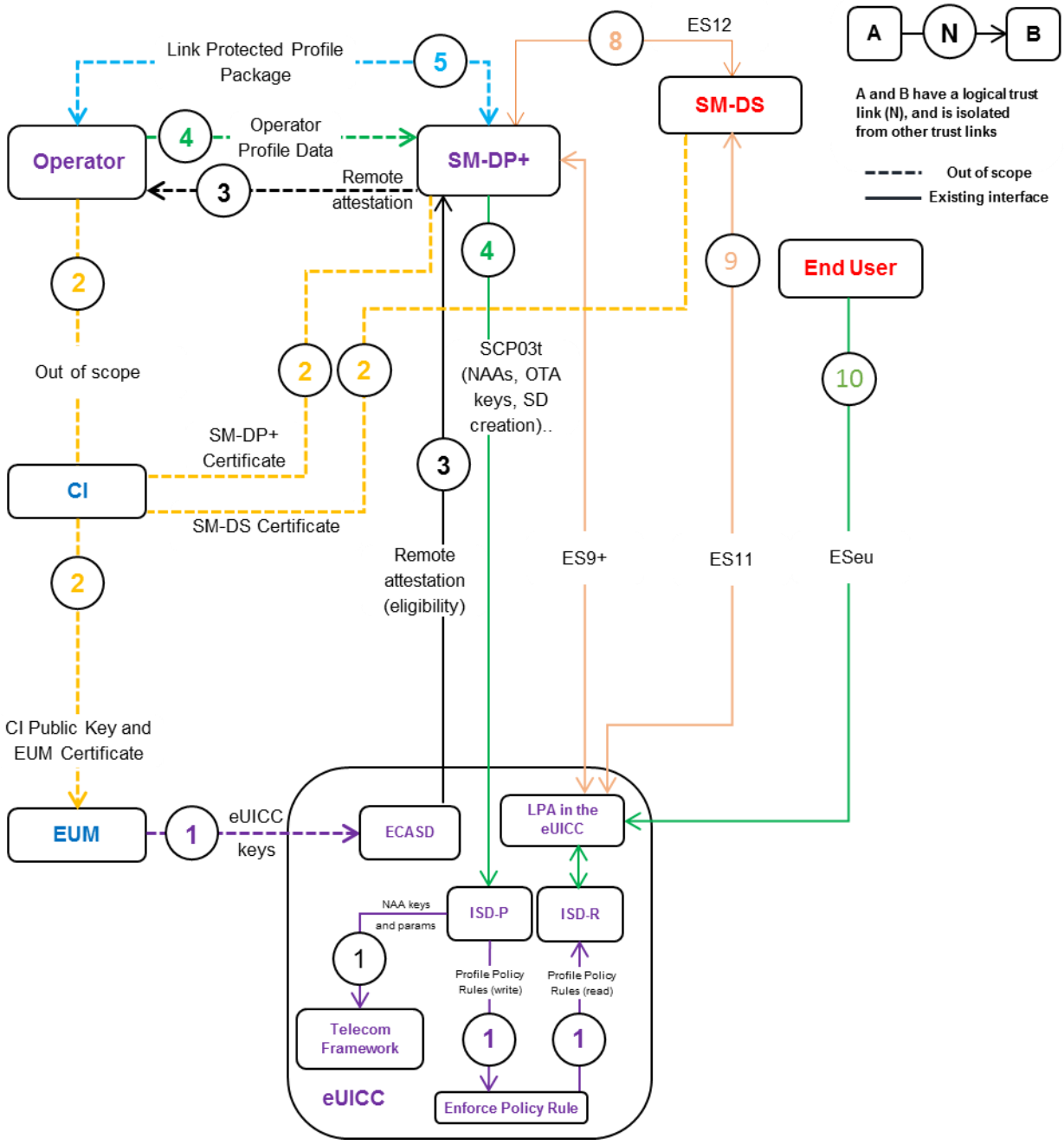


Figure 39: Trusted Link with LPA in the eUICC

Trust link	Description	Interfaces involved	Possible compromises	Impact of loss of trust link
TL1	Trust introduced onto the eUICC by the issuing EUM to enable future remote management and authorisation by the SM-DP+ and possibly the EUM: eUICC keys	Out of scope	The CI public key, the EUM's Certificate, the EUM's keyset, the eUICC keys, the OS, and the Security Domains.	The trust of the entire security model is breached and all eUICCs issued under the model cannot be trusted.

Trust link	Description	Interfaces involved	Possible compromises	Impact of loss of trust link
	(EUM & CI keyset eUICC Certificates).			
TL2	Trust placed in the CI's verification of the EUM, SM-DP+, and the resulting Certificate issuance.	Out of scope	The EUM and SM-DP+ Certificates.	Loss of Operator trust on the EUM and SM-DP+
TL3	Trust placed in the activities for eUICC eligibility and remote attestation from the ISD-R on the target eUICC to the Operator via the SM-DP+. Provides eUICC Certificate, EID, reference to its certification and EUM to the Operator and SM-DP+.	ES2+ ES8+	The eUICC Certificate or eligibility check failure.	Loss of Operator trust on the eUICC and/or SM-DP+.
TL4	Trust placed in the activities for Profile data transfer from the Operator via the SM-DP+ to the ISD-R on the target eUICC. Protects the Profile and associated credentials and keys (NAAs, OTA keys, ISD-R access, ISD-P SD creation …) with only the Operator, SM-DP+ and the eUICC.	ES2+ ES8+	SM-DP+ Certificate eUICC Certificate or eligibility check failure.	Loss of Operator trust on the SM-DP+ and/or eUICC.
TL5	Trust placed in the information exchange between the Operator and the SM-DP+ for Link Profile requests.	ES2+	SM-DP+ Certificate	Operator loss of trust on SM-DP+.
TL6	Trust placed in the mechanisms provided by the LPA: Local Profile Management, Local Profile	ESeu	LPA security	eUICC loss of trust on LPA.

Trust link	Description	Interfaces involved	Possible compromises	Impact of loss of trust link
	Management Operations			
TL7	Trust placed in the TLS session	ES9+	LPA security or SM-DP+ security.	SM-DP+ loss of trust on LPA (in the Device or the eUICC) or LPA loss of trust on the SM-DP+.
TL8	Trust in the discovery process	ES11	LDS security or SM-DS security.	LDS loss of trust on the SM-DS and vice versa.
TL9	Trust in the discovery process	ES11	eUICC security or SM-DS security.	SM-DS loss of trust on the eUICC and vice versa.
TL10	Trust in the UI	ESeu	Device security	Loss of trust on the Device

Table 55: Trusted Link Descriptions

Compromised element	Impacted Links	Description	Impact of loss of trust	Countermeasures
eUICC	TL1, TL3, TL4, TL9	The eUICC keys and EUM's Keyset.	The eUICC can no longer be trusted. MNO and SM-DP+ loss of trust on eUICC.	Revoke the Certificate of the eUICC.
CI	TL2	The EUM, SM-DS, and SM-DP+ Certificates.	Loss of Operator trust in the EUM, SM-DS and SM-DP+.	Repair/Replace CI. Generate new CI Certificate and new Certificate for the EUM, SM-DS and SM-DP+ following the SAS process. Remote repair of already issued eUICCs: new CI public key.
EUM	TL1, TL2	Loss of SAS certification.	Loss of trust from the Operator and SM-DP+ on the EUM and its eUICCs.	New SAS for the EUM. Remote repair of already issued eUICCs: new EUM Certificate, new eUICC Certificate.

Compromised element	Impacted Links	Description	Impact of loss of trust	Countermeasures
SM-DP+	TL3, TL4, TL5, TL7, TL8	Loss of SAS certification.	Loss of trust from the Operator, LPA, SM-DS and eUICC on the SM-DP+.	New SAS for the SM-DP+. New SM-DP+ Certificate.
SM-DS	TL8	Loss of SAS certification.	Loss of trust from the Operator, LPA, SM-DP+ and eUICC on the SM-DS.	New SAS for the SM-DS. New SM-DS Certificate.
LPA	TL6, TL7, TL8	LPA security failure.	Loss of trust from the SM-DP+, SM-DS and eUICC on the LPA.	LPA repair by the Device Manufacturer.
Device	TL10	Device security failure	Loss of trust in the Device UI	LUI in the eUICC self-protected with User Intent capture mechanisms (i.e. Captcha Code)

Table 56: Impact of Compromising Trusted Links and Countermeasures

The signer is responsible for the revocation of the Certificates it has signed. This section describes how the new Certificates are pushed to concerned entities according to the security model.

- SM-DP+ trusts the CI
- EUM trusts the CI
- eUICC trusts the EUM and the CI

Req no.	Description
CERT1	The new SM-DP+ Public Key Certificate(s) SHALL be issued to the SM-DP+ by a GSMA CI upon achievement of the GSMA SAS or CI repair.
CERT2	The new SM-DS Public Key Certificate(s) SHALL be issued to the SM-DS by a GSMA CI upon achievement of the GSMA SAS or CI repair.
CERT3	The new EUM Certificate(s) SHALL be issued to the EUM by a GSMA CI upon achievement of the GSMA SAS or CI repair.
CERT4	The EUM Certificate(s) SHALL be loaded securely to the eUICC by the EUM Note: See details in Section 4.1.1.1.
CERT5	The CI Certificate(s) SHALL be loaded securely to the eUICC by the EUM Note: See details in Section 4.1.1.1.
CERT6	Certificates SHALL be revocable.
CERT7	Neither the End User nor any other party SHALL be able to prevent Certificate revocation.
CERT8	The End User SHALL not be allowed to use Remote SIM Provisioning functions with revoked Certificates.

Req no.	Description
CERT9	The Public Key Certificate of the SM-DP+ SHALL be revoked if required (e.g. loses or subsequently fails to achieve the GSMA Remote SIM Provisioning certification requirements).
CERT10	The Public Key Certificate of the SM-DS SHALL be revoked if required (e.g. loses or subsequently fails to achieve the GSMA Remote SIM Provisioning certification requirements).
CERT11	The Public Key Certificate of the EUM SHALL be revoked if required (e.g. loses or subsequently fails to achieve the GSMA Remote SIM Provisioning certification requirements).

Table 57: Certificate Requirements

Annex G LPA Integrity (Normative)

The LPA SHALL be protected against misuse or being compromised by means of implementing standard procedures.

For cases where the LPA is in the Device, the LPA integrity SHALL be guided by the following Device classes:

Device class	Description	Example of Devices
Advanced	Devices with an open operating system where mechanisms such as secure boot and platform signing of applications are available and used to protect the LPA.	Smartphones, Tablets, Laptops, Advanced Wearables
Basic	Devices without possibility to install applications. The attack surface of the LPA is minimal due to the locked down nature of these Devices. Simple mechanisms to ensure that the LPA is not compromised SHALL be taken.	Connected sensors, Simple Wearables, Single use case devices

Table 58: Device Classes

Annex H Rules Authorisation Table (Informative)

Annex H reflects the RAT table configuration(s) that MAY be configured in embedded UICC.

The RAT entries shown in Table 58 MAY be provisioned:

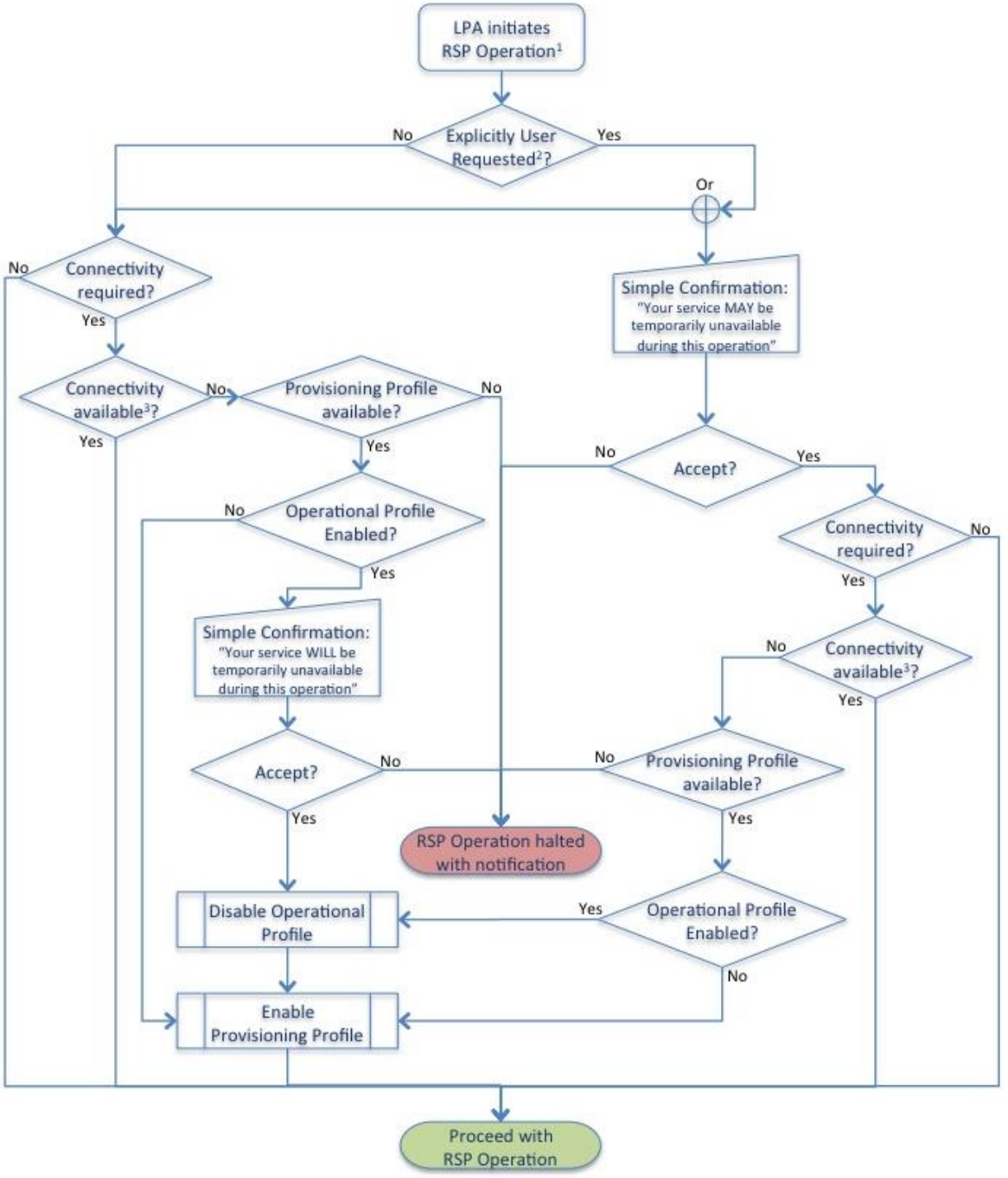
PR	Operators	User consent
POL RULE1	*	YES
POL RULE2	*	YES

Table 59: RAT configuration

Additional lines can be added to the RAT table to reflect agreement between some Operators and OEMs as needed. The OEM can also decide to add lines to the RAT table.

Note: POL RULE3 is defined for use in specific use cases that have not yet been fully defined and is not applicable for this version of the specification.

Annex I LPA Invocation of the Provisioning Profile Example Flow (Informative)



[1] RSP Operation inc. Discovery Request, Profile Download & RPM and may not be explicitly user requested at the point of occurrence, for example SM-DS polling.
[2] Explicit means not event driven i.e. non system generated.
[3] Via the Enabled Operational Profile or Wifi
Note 1. This does not cover re-enablement of the Operational Profile upon completion of the RSP Operation)
Note 2. Simple Confirmation text is an example for the purpose of the flow.

Annex J Integrated eUICC Security Requirements (Normative)

J.1 General Security Requirements

Requirement	Description
GS01	An Integrated TRE MAY use a Remote Memory within the Device, dedicated to the Integrated TRE, to store software and data.
GS02	All Integrated eUICC software and data which are stored outside the Integrated TRE SHALL be protected by the Integrated TRE in order to ensure their confidentiality, their integrity, and software side channel protection. This includes protection against side-channel attacks such as cache-timing attacks.
GS03	All Integrated TRE software and data, including context, SHALL only be stored in protected memory as requested in paragraph 36 in BSI-CC-PP-0084 [29].
GS04	All Integrated TRE software and data stored outside an Integrated TRE SHALL be protected against replay attacks.
GS05	The Integrated TRE internal instruction and data buses SHALL be isolated from the rest of the SoC.
GS06	The other SoC components SHALL have no access to the Integrated TRE internal buses.
GS07	The Integrated TRE SHALL be the only entity to expose TRE data outside the Integrated TRE.
GS08	The Integrated TRE SHOULD have priority access to Remote Memory as defined in GS02 in cases of shared resource contention
GS08a	All the credentials used to protect the data stored in the Remote Memory, dedicated to the Integrated TRE as per requirements GS02 and GS03, SHALL only be stored and used in the Integrated TRE.
GS09	The Integrated TRE SHALL be isolated from all other SoC components such that no other SoC components can have access to assets inside the Integrated TRE.
GS10	The Integrated TRE SHALL have a hardware and software protection means that controls the access to every function of the Integrated TRE (e.g. cryptographic unit).
GS11	The Integrated TRE SHALL process/execute its data/software in a dedicated secure CPU contained within the Integrated TRE.
GS12	The Integrated TRE SHALL be resistant against hardware and software side-channel attacks (e.g. DPA, cache-timing attacks, EMA etc.).
GS13	All Integrated TRE software and data SHALL be exclusively processed within the Integrated TRE.
GS14	The Integrated TRE SHALL include in its security target the following threats for software and data managed by the TRE, but stored outside the TRE: • leakage • probing • manipulation

Requirement	Description
GS15	The protection of software and data stored in Remote Memory as defined in GS02 SHALL be managed by the Integrated TRE using means which are independent of the Remote Memory implementation.
GS16	All cryptographic processing used by the Integrated TRE SHALL be contained within the Integrated TRE.
GS17	All security mechanisms within the Integrated TRE SHALL withstand state of the art attacks.
GS18	If Remote Memory outside the SoC is used, the combination of Integrated TRE and Remote Memory SHALL implement mechanisms protecting access to Remote Memory.
GS19	Integrated TRE implementations using Remote Memory outside the SoC SHALL implement mechanisms protecting the integrity of Remote Memory contents as defined in GS02.

Table 60: General Security Requirements

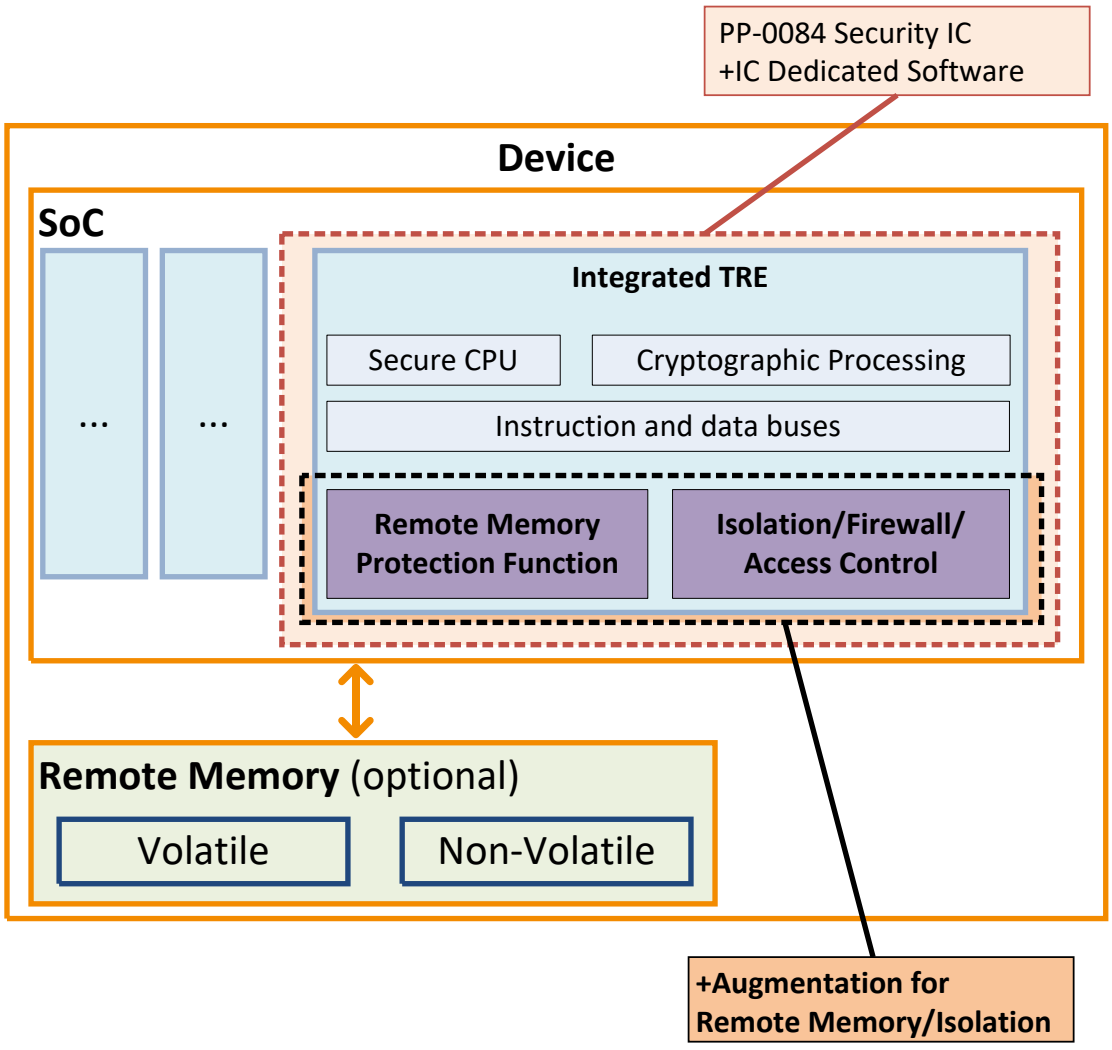


Figure 40: Example of Optional Remote Memory Usage

Note: IC Dedicated Software including its authentication by the TRE, is covered by BSI-CC-PP-0084 [29] and is not required to be augmented by this annex.

J.2 Security Certification

Requirement	Description
SC01	An Integrated TRE together with the RMPF SHALL be evaluated according to BSI-CC-PP-0084 [29] augmented with the requirements defined in this annex. Note: The requirements relating to Remote Memory are only applicable when that type of memory is used by the Integrated TRE.
SC02	Evidence of Isolation (for example GS05, GS06, GS07, GS09) SHALL be assessed during evaluation.
SC03	Evidence of proper Life Cycle management of the Integrated TRE SHALL be assessed during evaluation.

Table 61: Security Certification Requirements

J.3 Conformance Claims

Requirement	Description
CC01	The Integrated TRE SHALL claim in its security target, that it comprises of Security IC and IC Dedicated Software regarded as a Security Integrated Circuit which implements all functional aspects specified by the BSI-CC-PP-0084 [29] protection profile augmented with the requirements defined in this annex.
CC02	The Integrated TRE SHALL provide resistance to attackers with “high” attack potential as defined by AVA_VAN.5 and ALC_DVS.2 in [33].
CC03	The Integrated TRE SHALL be evaluated against the requirements, methods of attacks and evaluation documents for smartcards and similar devices published by SOG-IS [35].

Table 62: Conformance Claims

J.4 Security Objectives

BSI-CC-PP-0084 [29] defines security problems related to the Security IC being evaluated and corresponding security objectives. Within BSI-CC-PP-0084 [29], the definitions do not take into account the implementation of the TRE within a SoC and the use of Remote Memory. In particular, Integrated TRE has to include additional security problems and objectives in its security target. The security target shall include the following in its security objectives:

Requirement	Description
SO01	The Integrated TRE SHALL define, in its security target, a security objective to protect software and data managed by the TRE and stored outside the TRE against: • leakage • probing • manipulation

Table 63: Security Objectives

J.5 Security Functional Requirements

Requirement	Description
IESFR01	The Integrated TRE SHALL contain a Remote Memory Protection Function (RMPF) to protect software and data to be stored in Remote Memory, outside the TRE.
IESFR02	The RMPF SHALL reside in the Integrated TRE.
IESFR03	The RMPF SHALL ensure the following security properties: (1) confidentiality (2) integrity and (3) replay-protection. Note: these properties are intended to cover a range of possible attacks, including replay of commands on the Remote Memory, rollback of data stored in the Remote Memory, cloning the content of a Remote Memory from another device, swapping or corrupting data within the Remote Memory, etc.
IESFR04	The RMPF SHALL use keys that are either: • derived from a secret TRE-unique seed(s), or; • randomly generated within the Integrated TRE
IESFR05	TRE-unique seed(s) used by RMPF SHALL be generated using a certified random number generator as required by BSI-CC-PP-0084 [29].
IESFR06	TRE-unique seed(s) used by the RMPF SHALL be generated inside the TRE.
IESFR07	The entropy of the TRE-unique seed(s) used by the RMPF SHALL be at least 256 bits.
IESFR08	Randomly generated keys used by the RMPF shall be at least 256 bits.
IESFR09	The key derivation mechanism used by the RMPF SHALL be compliant with NIST SP 800-108 [30][30] and SHALL use: • a block cipher with security strength equivalent to or greater than AES-256, or • a hash function with security strength equivalent to or greater than SHA-256,
IESFR10	The keys used by the RMPF SHALL be protected by the TRE.
IESFR11	Seed(s) used by the RMPF SHALL be restricted to the RMPF.
Confidentiality Requirements	
IESFR12	The RMPF SHALL provide confidentiality based on encryption using a cipher with security strength equivalent to, or greater than AES-256 and using a suitable mode of operation approved by NIST in NIST SP 800-175B [34][18] or recommended by BSI in BSI TR-02102-1 [31] or recommended by ANSSI RGS v2 B1 [32].
Integrity and Authenticity	
IESFR13	The RMPF SHALL use a cryptographic integrity mechanism with security strength equivalent to, or greater than SHA-256.
IESFR14	The RMPF SHALL provide authentication using a MAC of at least 128 bits based • on a block cipher using a cipher with security strength equivalent to or greater than AES-256, or

Requirement	Description
	• on a hash function with security strength equivalent to or greater than SHA-256, and using a mode of operation approved by NIST in NIST SP 800-175B [34] or recommended by BSI in BSI TR-02102-1 [31] or recommended by ANSSI RGS v2 B1 [32].
IESFR15	IESFR12 and IESFR14 MAY also be provided in combination by an authenticated encryption mode fulfilling both requirements.
Replay protection	
IESFR16	The RMPF SHALL detect any replay attack on the Integrated TRE.
IESFR17	The Integrated eUICC SHALL be resistant to replay attacks on the data stored in Remote Memory.
IESFR18	The Integrated eUICC SHALL be able to verify that the data received from the Remote Memory is not unsolicited. Note: Solicited data received from the Remote Memory is data that the Integrated eUICC did intend to retrieve at runtime from Remote Memory and/or retrieved data that the Integrated eUICC was able to verify according to the requirements set in this Annex.
IESFR19	The RMPF SHALL NOT process data if it is unable to detect a replay attack. Note: Such a situation may arise e.g. if the RMPF uses a counter to detect replay attacks and the counter expired or became unreliable for any other reason.
Test Interface	
IESFR20	The Integrated eUICC Test Interface SHALL NOT affect the security requirements defined in this annex.
IESFR21	The Integrated eUICC Test Interface SHALL be compatible with commonly used interfaces for smartcard testing.

Table 64: Security Functional Requirements

J.6 Identification

Requirement	Description
ID01	The Integrated eUICC SHALL allow the SM-DP+ to identify the type of the Integrated TRE including its component configuration (e.g. use of internal or Remote Memory, use of other optional components), its manufacturer, in addition to the RSP OS provider.

Table 65: Identification Requirement

Annex K Document Management

K.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	23/12/15	First Release with amendments from Security review.	PSMC	Carmen Kwok, GSMA
V2.0	25/08/16	Includes Phase 2 content	PSMC	Carmen Kwok, GSMA
V2.1	29/02/17	Phase 2 maintenance release	Technology Group	Carmen Kwok, GSMA
V2.2	31/08/17	Phase 2 maintenance release	RSPLEN	Carmen Kwok, GSMA
V2.3	30/06/21	Phase 2 maintenance release	ISAG	Carmen Kwok, GSMA

Other Information

Type	Description
Document Owner	Carmen Kwok
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.