RSP Architecture
Version 3.0
28 March 2022

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

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

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.

1 Introduction

1.1 Overview

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

This version focuses on eSIM Devices for the consumer market.

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 aim of this architecture framework is 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, Mobile Service Providers and other industry bodies.

1.4 Definition of Terms

Term	Description
Access Rules	Information stored on the eUICC that defines whether applications on the Device are denied or allowed access to applications on the eUICC as specified by Global Platform Secure Element Access Control [15].
Activation Code	Information issued by a Mobile Service Provider to a Subscriber or an End User. It is used by the End User to request the download and installation of a Profile.
Activation Code Token	The part of the Activation Code information provided by the Mobile Service Provider which refers to a Subscription.
Alternative SM-DS	SM-DS used in cascade mode with a Root SM-DS to redirect Event Registration from an SM-DP+ to that Root SM-DS or used directly to perform Event Registration from an SM-DP+ for an installed Profile.
Authorised Management	A privileged assignment as defined in GlobalPlatform Card Specification [9].
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][1][1].
Certified eUICC	An eUICC meeting the GSMA requirements for Remote SIM Provisioning and certified according to the GSMA compliance programme defined in SGP.24 [27]. Note: Unless stated otherwise, the word eUICC in this specification refers to a Certifed eUICC.

Term	Description
Companion Device	A Device that relies on the capabilities of a Primary Device for the purpose of Remote SIM Provisioning.
Confirmation Code	A code entered by an End User required by the SM-DP+ to validate the request to download a Profile.
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.
Delegated Management	A privileged assignment as defined in GlobalPlatform Card Specification [9].
Delegated Platform Identifier	Identifier of a third party platform used to delegate the management of a Profile.
Delegated Profile Content Management Platform (DPCMP)	Platform delegated by the Profile Owner and used for the same purpose as the Profile Content Management Platform: to manage the contents of an installed Profile.
Device	User equipment used in conjunction with an eUICC to connect to a mobile network. E.g. a tablet, wearable, smartphone or handset.
Device Application	An application installed in a Device.
Device Change	Given that one or more Profiles related to their respective Subscriptions are installed in an old Device, the process for installing one or more Profiles related to the same Subscriptions to a new Device.
Device Change Configuration	Set of rules that apply to a Profile to support Device Change.
Device Information Code	A set of Device-related information used for Remote SIM Provisioning operations (e.g. for Profile preparation between the SM-DP+ and the Operator).
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	A Profile in a state 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.

Term	Description
Eligibility Check	Procedure operated between the eUICC and the SM-DP+ to enable the SM-DP+ and the Operator or Mobile Service Provider to validate the eligibility of an eUICC and the Device for the installation of a Profile using information sent by the eUICC.
Eligibility Check Information	The information set sent from the eUICC to the SM-DP+ to allow eligibility checking of the combination of an eUICC and a Device.
Enabled Profile	A Profile in a state where all 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.
Enterprise	A business, organisation, or government entity that subscribes to mobile services to be utilised by its workforce in support of the business or activities of the Enterprise. The Enterprise, as the Subscriber, owns the relationship with the Mobile Service Provider(s).
Enterprise Capable Device	A Device that supports the installation and enforcement of Enterprise Rules.
Enterprise Profile	An Operational Profile for which the Subscriber is an Enterprise. This Profile may include restrictions on the End User of the Device.
Enterprise Rule	A rule stored in an Enterprise Profile that can be used by the Profile Owner to restrict End User controllability for enabling and installing Profiles on Enterprise Capable Devices.
eSIM	eSIM is the top level generic descriptor applied to the Devices and eUICCs that support Remote SIM Provisioning.
eSIM CA	A GSMA Certificate Issuer or an Independent eSIM CA.
eSIM Products	eUICC, Devices, and Servers defined in this specification.
eUICC	A UICC which enables the remote and/or local management of Profiles in a secure way. Note: The term originates from “embedded UICC”.
eUICC Authentication	Mechanism used by the SM-DP+ or 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 Form Factor Type	Defines the eUICC Type which is either removable or non-removable.
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 OS Update	A mechanism to correct existing features on the eUICC by the original OS manufacturer.

Term	Description
eUICC OS Manager	The eUICC OS Manager is a Device component that consolidates the functions dealing with the eUICC OS Update.
eUICC Test Memory Reset	An action that deletes all post-issuance Test Profiles on an eUICC.
EUM Certificate	A Certificate chaining to an eSIM CA, of a GSMA accredited EUM which can be used to verify eUICC Certificates.
EUM Keyset	Keyset used by the EUM to update ECASD content.
EUM Public Key	Public key included in the EUM Certificate (called PK.EUM.ECDSA in SGP.22 [24]).
EUM Private Key	Key used by the EUM to sign eUICC Certificates (called SK.EUM.ECDSA in SGP.22 [24]).
Event	A request for a Profile download or an RPM operation which is set by an SM-DP+ on behalf of a Mobile Service Provider or an Operator, to be processed by a specific eUICC.
Event Checking	A process for the LDS to query the SM-DS to determine the presence of Event Records registered for an 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 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.
Event Retrieval	A process for the LDS to retrieve Event Records for an eUICC from an SM-DS.
Field-Test eUICC	A pre-production eUICC whose functional or security certifications are not yet completed by the EUM.
Form Factor	Physical manifestation of the UICC.
GSMA Certificate Issuer	A Certificate Authority accredited by GSMA.
ICCID	Unique number to identify a Profile in an eUICC as defined by ITU-T E.118 [14][14].
IC Dedicated Software	As defined in BSI-CC-PP-0084 [40].
Independent eSIM CA	A non-GSMA CI that issues digital public key Certificates for a specific region, company or group of companies for eSIM purposes.
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 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.

Term	Description
Interoperable Application	An application that can be downloaded, installed, executed and removed on any eUICC compliant with technical requirements of a runtime environment (resources, APIs, version, ...), regardless of its Form Factor, its Manufacturer, Device type, Device Manufacturer, Operator, and Mobile Service Provider.
Issuer Security Domain	A Security Domain on the UICC as defined by GlobalPlatform Card Specification [9].
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.
Logical Interface	In case of MEP: logical connection between an endpoint in the Device and an Enabled Profile or another logical secure element.
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 operational LPA Mode which is either LPA in the eUICC or in the Device.
LPA Proxy	A component of the Device used as a proxy between an Operator authorised platform and the corresponding Profile to manage the Profile's content.
Managing SM-DP+	An SM-DP+ that is authorised by the Profile Owner to perform RPM on the Profile to the eUICC on which their Profile resides.
MatchingId	Reference data for an RSP Server which could be an Activation Code Token or the EventID.
MEP-capable Device	A Device where more than one enabled Profile can be used on the same eUICC.
Mobile Network Operator	An entity providing access capability and communication services to Subscribers through a mobile network infrastructure.
Mobile Service Provider	The Mobile Service Provider provides Subscriptions to Subscribers either as part of an Operator or as a party with a wholesale agreement with an Operator. The Mobile Service Provider could also be the Operator.

Term	Description
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. This refers to an MVNO with own IMSI range and core network.
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	A Device compliant with GSMA TS.26 [17].
NFC eUICC	An eUICC supporting the contactless functionalities defined in SGP.03 [20].
NFC Profile	A Profile containing contactless applications.
Non-Enterprise Capable Device	A Device that does not support the enforcement of Enterprise Rules.
Nonce	An arbitrary random number generated for one time use, employed for cryptographic communication.
Notification	A report about a Profile download or Remote/Local Profile Management Operation processed by the eUICC or about the progress of such an operation.
Notification Receivers	A list defined in the Profile containing SM-DP+s that are to receive Notifications concerning that Profile.
Operational Profile	A combination of data and applications to be provisioned on an eUICC for the purpose of providing services by a Mobile Service Provider. The Profile SHALL be in support of a Subscription with the relevant Mobile Service Provider 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. An Operator owns one or more IMSI ranges.
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.
OTA Platform	A platform for remote management of UICCs and the content of enabled Profiles on the 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.
Polling Address	Address configured in a Profile indicating where the Device needs to connect to retrieve RPM Events for this Profile.
Primary Device	A Device that can be used to provide some capabilities to a Companion Device for the purpose of Remote SIM Provisioning.

Term	Description
Profile	A combination of data and applications to be provisioned on an eUICC for the purpose of providing services.
Profile Content Management Platform (PCMP)	Platform owned by the Profile Owner, used to manage the content of an enabled Profile.
Profile Description	The description of a Profile in a format specific to the Mobile Service Provider or 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, list Profile information, and query Profile Metadata)
Profile Management Lifecycle	Encompasses all the procedures applied during the lifetime of a Profile.
Profile Management Operation	An operation related to the content and state update of a Profile in a dedicated ISD-P on the eUICC.
Profile Metadata	Information pertaining to a Profile used for the purpose of Local Profile Management and Remote 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 a Mobile Service Provider or an Operator.
Profile Package	A personalised Profile using an interoperable description format that is transmitted to an eUICC to load and install a Profile as defined by Trusted Connectivity Alliance [5][5].
Profile Policy Enabler	The functional element within the Profile Policy Management system that interprets and enforces Profile Policy Rules.
Profile Policy Management	A policy control system that allows the Mobile 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 cryptographically protected for storage but not linked to a particular eUICC.
Protection Profile	Defines an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumers' needs for IT security. A Protection Profile is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives.
Push Service	A service which is provided by a combination of a push server and a push client on the Device, to send a push notification from an SM-DS to an LDS.
Remote Memory	Volatile or non-volatile memory residing outside of the TRE
Remote Profile Management (RPM)	Profile Management operations performed by a Managing SM-DP+ at the request of the Profile Owner.
Remote SIM Provisioning	The downloading, installing, enabling, disabling, and deleting of a Profile on an eUICC.

Term	Description
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).
Security Domain	As defined in GlobalPlatform Card Specification [9].
Simple Confirmation	A secure and non-interceptable mechanism by which the End User confirms their action, e.g. by selecting Yes/No, OK/Cancel.
Simple Mode	A privileged assignment as defined in GlobalPlatform Card Specification [9].
SM-DP+ Certificate	A Certificate chaining to an eSIM CA of a GSMA accredited SM-DP+.
SM-DS Certificate	A Certificate chaining to an eSIM CA of 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 a Mobile Service Provider.
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 Mobile Service Provider.
Subscription Manager Data Preparation+ (SM-DP+)	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. The SM-DP+ is also capable of performing Remote Profile Management.
Subscription Manager Discovery Service (SM-DS)	This entity is responsible for providing addresses of one or more SM-DP+(s) to an LDS.
Tamper Resistant Element (TRE)	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.

Term	Description
Test Profile	A combination of data and applications to be provisioned on an eUICC to provide connectivity to test equipment for the purpose of testing the Device and the eUICC. A test Profile is not intended to store any Operator Credentials.
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.
User Intent	Describes the acquisition of the End User input.

1.5 Abbreviations

Abbreviation	Description
AC	Activation Code
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARA-M	Access Rule Application - Master
ARF	Access Rule File
AuC	Authentication Centre
BSS	Business Support Services
CA	Certificate Authority
CASD	Controlling Authority Security Domain
CAT	Card Application Toolkit
CC	Confirmation Code
CI	Certificate Issuer
CREL	Contactless Registry Event Listener
CRS	Contactless Registry Services
DNSCurve	Domain Name System Curve
DNSSEC	Domain Name System Security Extensions
DPCMP	Delegated Profile Content Management Platform
DPI	Delegated Platform Identifier
ECASD	eUICC Controlling Authority Security Domain
EID	Embedded UICC Identifier
eSVN	embedded UICC Specification Version Number
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
EUM	eUICC Manufacturer

Abbreviation	Description
FASG	Fraud and Security Group
FFS	For Further Study
FIFO	First In First Out
GSMA	GSM Association
GSMA CI	GSMA Certificate Issuer
HLR	Home Location Register
HR	High Resolution
HTTP	Hypertext Transfer Protocol
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISD-P	Issuer Security Domain - Profile
ISD-R	Issuer Security Domain - Root
ISIM	IP Multimedia Services Identity Module
ISO	International Standards Organisation
ITU	International Telecommunications Union
LDS	Local Discovery Service
LPA	Local Profile Assistant
LPD	Local Profile Download
LPR	LPA PRoxy
LUI	Local User Interface
M4M	Mifare4Mobile
MEP	Multiple Enabled Profiles
MNO-SD	Mobile Network Operator - Security Domain
MSISDN	Mobile Subscriber International Subscriber Directory Number
MSP	Mobile Service Provider
NAA	Network Access Application
NFC	Near Field Communication
OCR	Optical Character Recognition
OS	Operating System
OTA	Over The Air
PCMP	Profile Content Management Platform
PFS	Perfect Forward Secrecy
PPR	Profile Policy Rule
PPSE	Proximity Payment System Environment
QR Code	Quick Response Code
RAM	Remote Application Management
RAT	Rules Authorisation Table

Abbreviation	Description
RFM	Remote File Management
RMPF	Remote Memory Protection Function
RPM	Remote Profile Management
RSP	Remote SIM Provisioning
SEAC	(Global Platform) Secure Element Access Control
SAS	Security Accreditation Scheme
SCP	Secure Channel Protocol
SCWS	Smart Card Web Server
SD	Security Domain
SIM	Subscriber Identity Module
SM-DP+	Subscription Manager - Data Preparation +
SM-DS	Subscription Manager - Discovery Service
SoC	System-on-Chip
SSD	Supplementary Secure Domain
TRE	Tamper Resistant Element
UIMe	User Interface Module for LPAe
URL	Uniform Resource Locator
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]	TCAPP	Trusted Connectivity Alliance: eUICC Profile Package - Interoperable Format Technical Specification
[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
[8]	SGP.02	GSMA Remote Provisioning Architecture for Embedded UICC Technical specification
[9]	GPC_SPE_034	GlobalPlatform Card Specification with its Amendments

Ref	Document Number	Title
[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	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
[23]	[Void]	[Void]
[24]	SGP.22	SGP.22 RSP Technical Specification - Version 3.0
[25]	SGP.25	SGP.25 RSP eUICC for Consumer Device Protection Profile
[26]	SGP.14	SGP.14 GSMA eUICC PKI Certificate Policy v1.1
[27]	SGP.24	RSP Compliance Process
[28]	SCP02	GlobalPlatform Card Specifications V2.3, Appendix E
[29]	SCP03	GlobalPlatform Card Specification v2.2 – Amendment D, v1.1.1
[30]	SCP11	GlobalPlatform Card Specification v2.2 – Amendment F, v1.0
[31]	EMVCo_Sec	EMVCo Security Evaluation Process 5.1 – June 2016
[32]	FS.09	FS.09 SAS-SM Methodology
[33]	3GPP TS 31.111	USIM Application Toolkit
[34]	ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT)
[35]	SM2 algorithm	ISO/IEC 14888-3:2018 IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms
[36]	SM3 algorithm	ISO/IEC 10118-3:2018 IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions

Ref	Document Number	Title
[37]	SM4 algorithm	ISO/IEC 18033-3:2010/AMD1:2021 Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers – Amendment 1: SM4
[38]	OMA-TS-Smartcard_Web_Server-V1_2_1-20130913-A	OMA SpecWorks: Smartcard-Web-Server, Version 1.2.1 – 13 Sep 2013
[39]	GSMA TS.06	IMEI Allocation and Approval Process
[40]	BSI-CC-PP-0084	Common Criteria Protection Profile
[41]	NIST SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions
[42]	BSI TR-02102-1	Cryptographic Mechanisms: Recommendations and Key Lengths
[43]	ANSSI RGS v2 B1	Référentiel Général de Sécurité version 2.0 Annexe B1
[44]	JIL-Application-of-Attack-Potential-to-Smartcards-v2-9	Application of Attack Potential to Smartcards and Similar Devices Version 2.9, Jan 2013
[45]	NIST SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
[46]	SOG-IS	SOG-IS Smartcards and similar devices CC supporting documents at this link: https://www.sogis.eu/uk/supporting_doc_en.html
[47]	SGP.23	RSP Test Specification
[48]	TS.37	Requirements for Multi SIM Devices
[49]	3GPP TS 33.102	3G security; Security architecture
[50]	3GPP TS 33.401	3GPP System Architecture Evolution (SAE); Security architecture
[51]	3GPP TS 33.501	Security architecture and procedures for 5G System
[52]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[53]	ISO 15408-1:2009	Information technology — Security techniques — Evaluation criteria for IT security – Part1: Introduction and general model
[54]	TS.43	GSMA PRD, Service Entitlement Configuration
[55]	GPD_SPE_068	GlobalPlatform Device Technology Device API Access Control - Version 1.0

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 [52][52], when, and only when, they appear in all capitals, as shown here.

"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

All parties either implementing or operating systems based on these specifications should be aware that any data items passed between system elements that can be used to identify an individual can be classified as personal data (as defined in the General Data Protection Regulation (EU) 2016/679). Responsibility for the management of Personal Data and compliance with any necessary legislation lies with implementing and operating organisations, according to each organisation's respective legal status with respect to the data processes (i.e. whether the entity acts as a data controller or as a data processor).

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 33.102 [49], 3GPP TS 33.401 [50] and 3GPP TS 33.501 [51].
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).
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, IMEI, IMSI etc.

Principle no.	Description
BAS9	The RSP Session SHALL prevent sending IMEI and EID information to a non-authenticated RSP Server.
BAS10	The SM-DP+ acts on behalf of the Profile Owner.

Table 1: Basic Principles

2.2 Profile Requirements

Req no.	Description
PRO1	[Void]
PRO2	[Void]
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	[Void]
PRO8	A Profile SHALL be either an Operational Profile or a Test Profile.

Table 2: Profile Requirements

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	[Void]
EUM3	Relevant parts of the eUICC Manufacturer's products and processes are certified by a GSMA-specified certification process.
EUM4	The EUM issues the eUICC Certificate to allow: • eUICC Authentication and proof of certification to other entities; • authenticated keyset establishment between an SM-DP+ and an eUICC.
EUM5	[Void]
EUM6	Field-Test eUICCs SHALL be tracked by the EUM.

Table 3: eUICC Manufacturer Role

3.2 [Void]

3.3 Operator and Mobile Service Provider

This section describes the characteristics of the Operator and Mobile Service Provider roles relevant to this architecture and its operation. Other characteristics exist but are considered out of scope. Note: The commercial and support system interfaces needed between the Mobile Service Provider and the supporting Operator (e.g. for Profile ordering and distribution) are out of scope.

Role no.	Description
OPE1	The Operator has access to an SM-DP+ via the ES2+ interface.
OPE2	In the event that a Subscriber has selected a Mobile Service Provider, that Mobile Service Provider will initiate the provisioning of a Profile Package. The details of this are out of scope.
OPE3	The Operator, potentially on behalf of the Mobile Service Provider, specifies the Profile characteristics and any features and applications analogous to removable UICCs.
OPE4	The Operator potentially on behalf of a Mobile Service Provider, is able to use an OTA Platform via the ES6 interface to manage the content of its Enabled Profile in the eUICC (RAM, RFM).

Table 4: Operator Role

3.4 [Void]

3.5 Certificate Issuer

Role no.	Description
CIS1	A Certificate Issuer issues Certificates for Remote SIM Provisioning system entities and acts as a trusted root for the purpose of authentication of 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 5: 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.

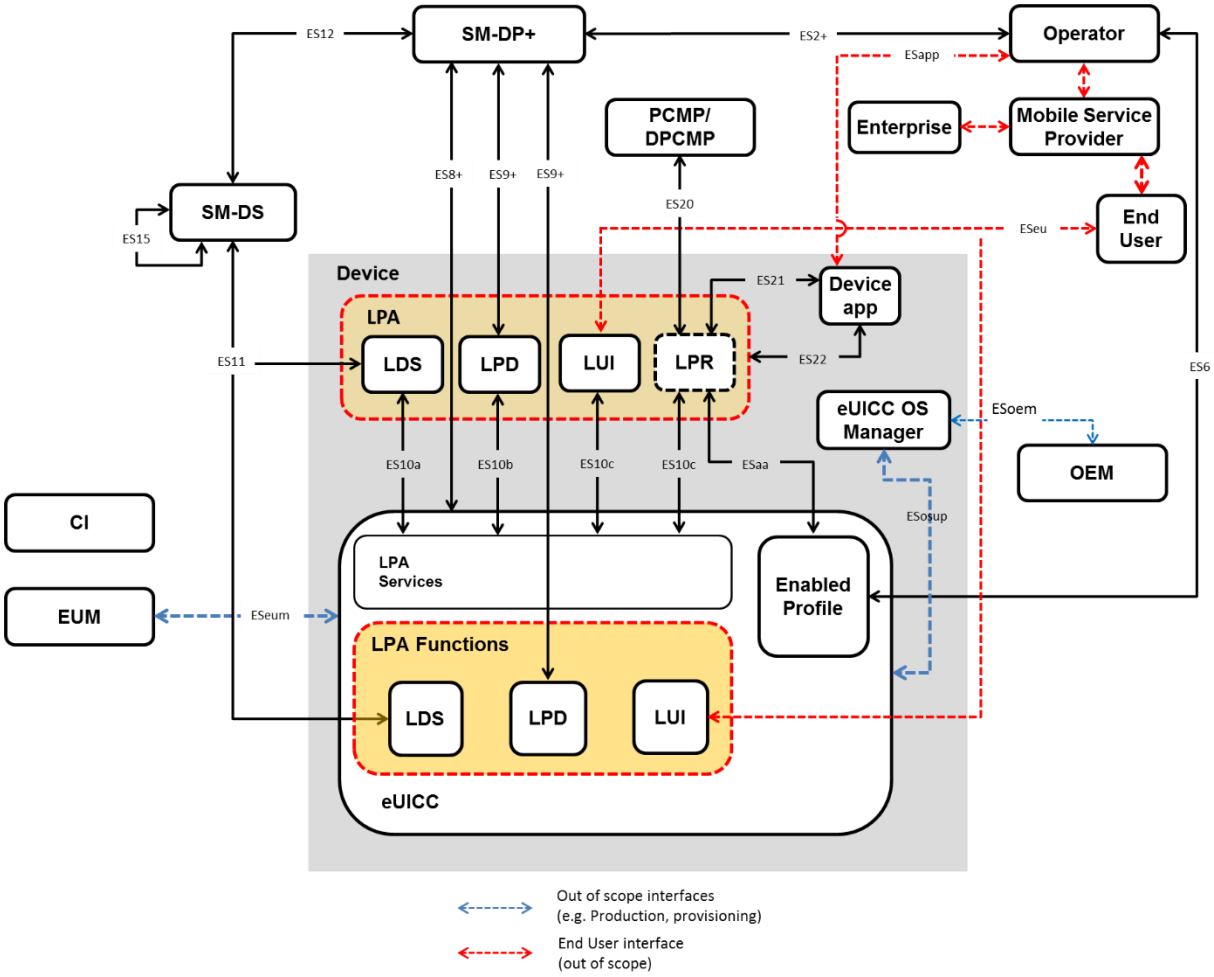

Figure 1: Remote SIM Provisioning System Architecture

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 Provisioning of Embedded UICC Technical specification [8]. Profiles are provisioned based on the security framework defined in the GlobalPlatform Card Specification [9][15].

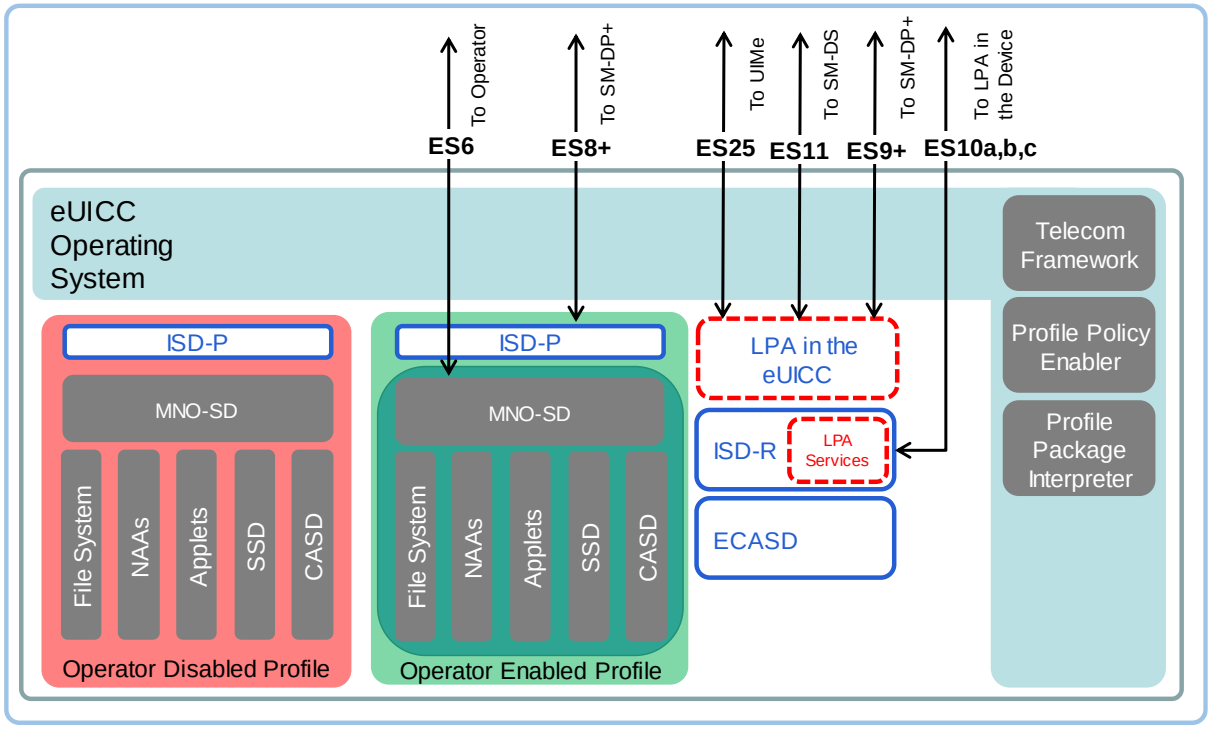

Figure 2: Schematic Representation of the eUICC

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 which issued the Profile. 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(es).
3. Facilitates the reception of the Bound Profile Package in transfer from the LPA.
4. Provides information regarding the installed Profiles and their Profile Metadata.
5. Provides Local Profile Management
6. Supports Remote Profile Management operations
7. Provides functions for the LPA to authenticate and interact with the SM-DS.
8. Ensures access to the EID is restricted to only the LPA.

4.2 Interfaces

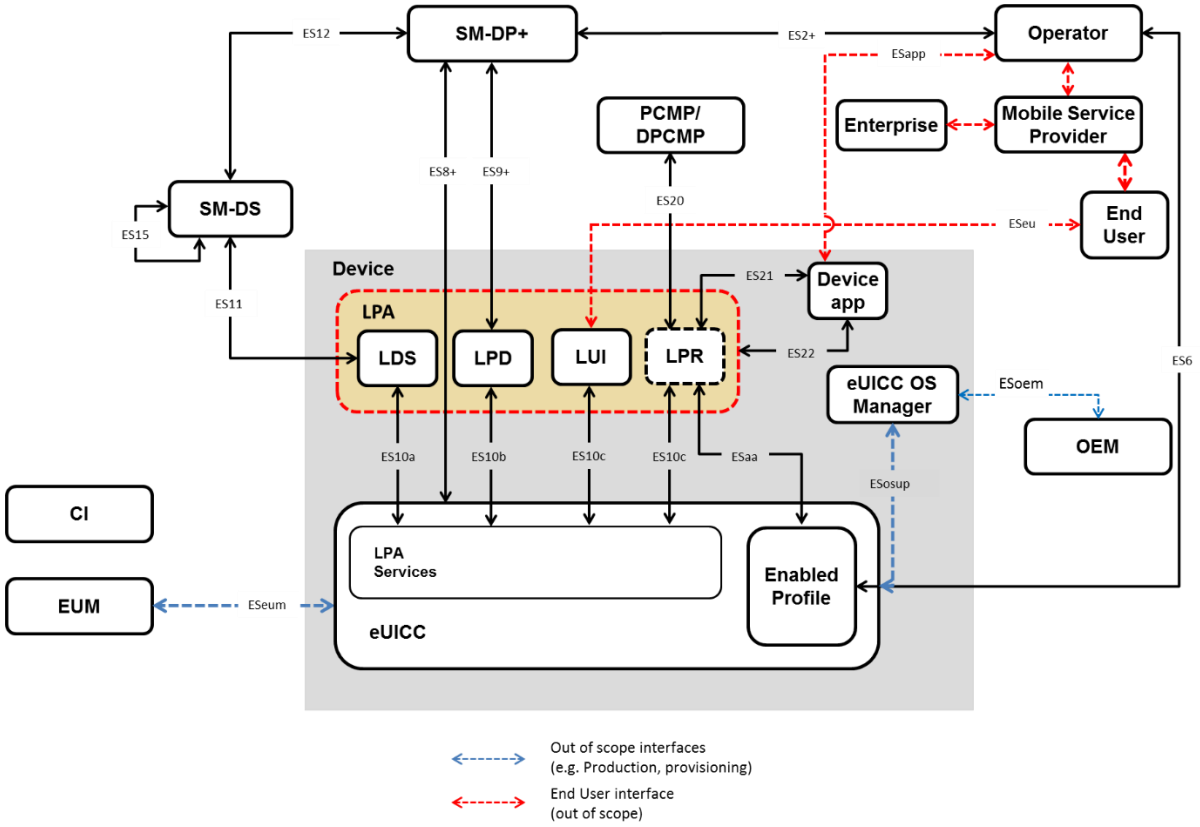

Figure 3: Interfaces on the eUICC Architecture with the LPA in the Device Configuration

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 [Void]

4.2.3 End User - LUI (ESeu)

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

The ESeu interface is used to support the following requirements:

Req no.	Description
ESeu1	[Void]
ESeu2	All Local Profile Management Operations of the LPA defined in Section 4.11.3 SHALL be explicitly initiated or authorised by the End User or Device owner.
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 6: 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, and for RPM and ReM.

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 the SM-DP+ to register Event Records with the SM-DS and to delete its Event Records.

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+(s).

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.
- between the LPR in the Device and the LPA services to retrieve Metadata that would be needed for Profile content management through LPA Proxy.

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

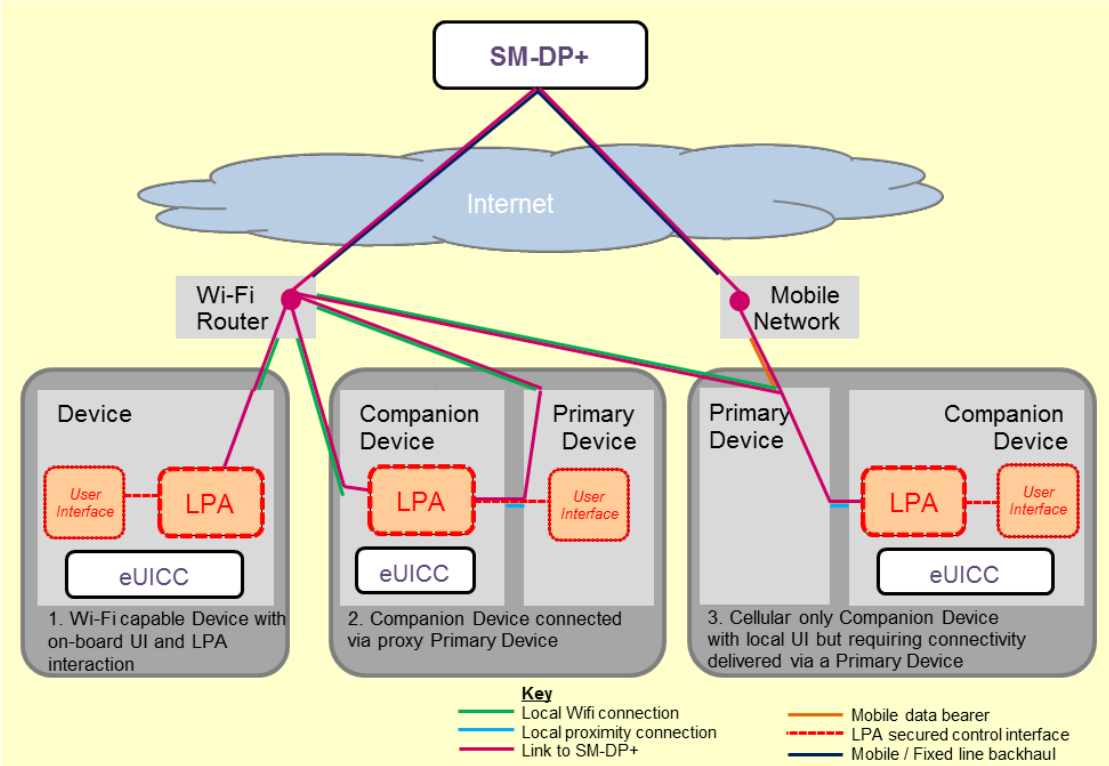

Figure 4: Example Connection Methods for Companion Devices to reach out to the SM-DP+

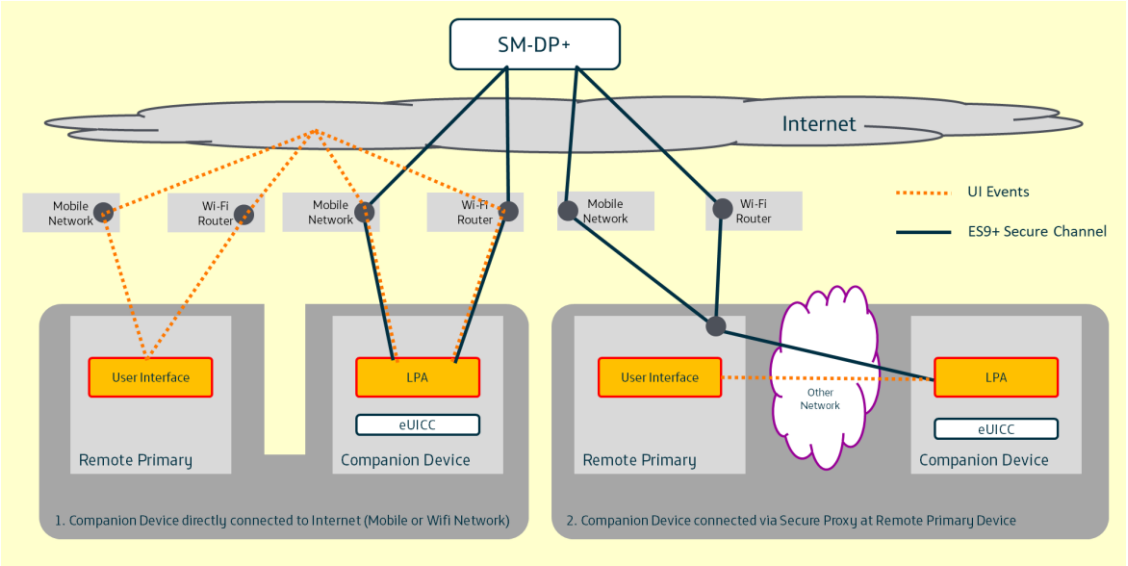

Figure 5: Example Connection Methods for Companion Devices to reach out to the SM-DP+ with a Remote Primary Device

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	The SM-DP+ and SM-DS SHALL use the capabilities indicated by the eUICC to determine its response to the eUICC.
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 7: General Interface Requirements

4.2.16 (D)PCMP – LPR (ES20)

The ES20 interface is used by the PCMP or DPCMP to manage Profile contents through the use of the LPA as a proxy.

4.2.17 LUI in the eUICC – UIMe (ES25)

The ES25 interface is used between the LUI in the eUICC and the UIMe to transfer End User related interaction. This interface uses one of the following options:

- The LUI uses CAT commands (e.g. CAT menu navigation) as defined in ETSI TS 102 223 [34] and the UIMe is the CAT interpreter. Besides the support of these commands, there are no additional requirements for the UIMe.
- The LUI uses SCWS as defined by OMA SpecWorks [38] and the UIMe is a browser. Besides the support of these commands, there are no additional requirements for the UIMe.
- The LUI uses a limited set of specific CAT Envelopes and the UIMe is a tailored application.

The following specific requirement applies for ES25:

Req no.	Description
ES25 REQ1	If the LUI in the eUICC uses specific CAT Envelopes defined in SGP.22 [24], then the UIMe SHALL fulfil the requirements related to the LUI.

Table 8: LUI in the eUICC – UIMe (ES25) Interface Requirements

4.2.18 Device Application – LPR (ES21)

The ES21 interface is used for exchanges between the LPR and a Device Application to trigger from the Device Application, a Profile content management session between a (D)PCMP and a Profile, or to send Notifications to the Device Application.

4.2.19 Device Application – LPA (ES22)

The ES22 interface is an LPA API used for exchanges between the LPA and a Device Application.

4.2.20 LPR – eUICC (ESaa)

The ESaa interface is used between the LPR in the Device and the Profile of the eUICC for Profile content management through the use of the LPA as a proxy.

4.2.21 eUICC – eUICC OS Manager (ESosup)

The eUICC OS Manager communicates with the eUICC through the ESosup interface. The ESosup interface delivers to the eUICC the commands to perform the eUICC OS Update. The implementation of the eUICC OS Manager and the ESosup are out of the scope of this specification

4.2.22 OEM – eUICC OS Manager (ESoem)

ESoem is the interface betweem OEM and the eUICC OS Manager. This interface can be used to receive the eUICC OS Update package(s) from the OEM and to dispatch it to the eUICC OS Manager in charge of the eUICC OS Update. The implementation of this interface is out of the scope of this specification but it has to deliver, together with the eUICC OS Update package(s), a minimum set of information.

4.2.23 Device Application – Operator (ESapp)

The ESapp interface is used for exchanges between a Device Application and the Operator. The exchanges are triggered by the Device Application.

GSMA PRD Specification TS.43 [54] is an example for the protocol to use on the ESapp interface.

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	[Void]
EUICC7	The behaviour of a NAA USIM, ISIM or CSIM within a Profile on an eUICC SHALL be identical to a removable UICC NAAs USIM, ISIM or CSIM. 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 EUM Keyset shall be issued by the EUM.

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 security domain as well as an ISD-R security domain 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.
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 Specification as defined by Trusted Connectivity Alliance [5].
EUICC18	An ISD-R SHALL: • 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.
EUICC25	[Void]
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	[Void]
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 to authenticate the eUICC.
EUICC32	The EUM SHALL install an EUM Certificate in the eUICC to verify the eUICC Certificate.

Req no.	Description
EUICC33	The eUICC SHALL have a means to authenticate itself to the SM-DS.
EUICC34	[Void]
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), and from Managing SM-DP+s.
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	[Void]
EUICC40	The eUICC SHALL be able to store one or more default SM-DP+ address(es).
EUICC41	The eUICC SHALL be able to store one or more Root SM-DS addresses.
EUICC41a	A removable eUICC SHALL have at least one Root SM-DS address configured.
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 SHOULD support Java Card. If supported, the specifics of these functions and features SHALL be explicitly referenced within the technical specification (SGP.22 [24]).
EUICC46	The eUICC SHALL support USIM Toolkit functions and GlobalPlatform features. The specifics of these functions and features SHALL be explicitly referenced within the technical specification (SGP.22 [24]).
EUICC47	An eUICC SHALL support at least two elliptic curves preloaded by the EUM during eUICC manufacturing.
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	[Void]
EUICC54	The EID SHALL NOT be modifiable. The EID SHALL NOT be affected by any of the procedures, including the change of eUICC Private keys.

Req no.	Description
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 [47].
EUICC58	For the purpose of integration and/or end-to-end testing, a Field-Test eUICC MAY contain certificates that chain up to the GSMA CI.
EUICC59	The eUICC MAY provide a means by which the Profile Owner of an Enabled Profile can request the LPA to check for Events (Root SM-DS(s)) or pending RSP operations (Default SM-DP+(s)).
EUICC60	The eUICC MAY provide a means by which the Profile Owner of an Enabled Profile can request the LPA to check for Events or pending RSP operations on the Polling Address configured in the Enabled Profile.
EUICC61	The eUICC SHALL support the 'set/edit nickname' function.
EUICC62	The eUICC SHALL support at least one eSIM CA for: • Profile binding • mutual authentication between eUICC and SM-DP+ • mutual authentication between eUICC and SM-DS.
EUICC63	An eUICC MAY support SM2, SM3 and SM4 cryptographic algorithms, defined in [35][35][35][35], [36] and [37] for mutual authentication and data encryption between the SM-XX and eUICCs. Note: TLS is used between the LPA and the SM-XX and is not considered in this requirement.
EUICC64	A non-removable eUICC MAY support Multiple Enabled Profiles (MEP). NOTE: Support of Multiple Enabled Profiles on a removable eUICC is FFS.
EUICC65	The eUICC MAY provide a means by which the LPA is able to determine the current estimated size of an installed Profile.
EUICC66	An eUICC SHOULD support Interoperable Applications.
EUICC67	An eUICC implementing EUICC66 SHALL support an application runtime environment facilitating interoperability, e.g. Java Card. The application runtime environment(s) SHALL be explicitly indicated to the SM-DP+.
EUICC68	The Enabled/Disabled state of a Profile SHALL remain unchanged when the eUICC undergoes the following operations outside of an 'Enable Profile' or 'Disable Profile' procedure: • Powering down or powering up the eUICC • Removing the eUICC from the Device • Inserting the eUICC in the Device (whether the same Device or a different Device)

Table 9: eUICC Requirements

4.4 Eligibility Check

Eligibility Check enables an SM-DP+ to validate the eligibility of an eUICC and the Device 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

Eligibility Check Information. Some Eligibility Check parameters MAY be required due to Device capabilities which must be supported by the Profile/eUICC and delivered as part of the 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.

4.4.1 Eligibility Check Requirements

Req no.	Description
ELG1	The eUICC SHALL indicate the specification versions it is supporting. This parameter SHALL be transmitted to the SM-DP+ during the Eligibility Check.
ELG2	The eUICC SHALL include the available memory in the 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.
ELG5	The eUICC SHALL provide an identification of the EUM.
ELG6	The eUICC SHALL provide the current OS version in the Eligibility Check Information.
ELG7	The eUICC SHALL provide in the Eligibility Check Information, Device enabler information relating to services that may require Profile support (e.g. NFC enablers).
ELG8	Eligibility Check Information SHALL be integrity and authenticity protected by the eUICC before it is sent to the SM-DP+.
ELG9	The eUICC SHALL indicate the application runtime environment version and libraries versions supported in Eligibility Check Information.
ELG10	The eUICC SHALL indicate cryptographic algorithms and their respective key lengths supported in the Eligibility Check Information.
ELG11	The eUICC SHALL declare in the Eligibility Check Information the list of supported CIs.
ELG12	[Void]
ELG13	The eUICC SHALL declare in the Eligibility Check Information if it is a NFC eUICC.
ELG14	[Void]
ELG15	An eUICC SHALL provide information indicating if it is a Discrete eUICC or an Integrated eUICC.
ELG16	An eUICC SHALL indicate in the Eligibility Check Information if it is a Field-Test eUICC.
ELG17	The eUICC SHALL declare which LPA Mode is being used during the secure session with the SM-DP+.

Req no.	Description
ELG18	The eUICC SHALL declare in the Eligibility Check Information if it supports eUICC OS Update.
ELG19	The eUICC SHALL declare permitted Profile Policy Rules in the Eligibility Check Information.
ELG20	The Eligibility Check Information MAY include the Device's IMEI.
ELG21	Eligibility Check Information SHALL include the Device Type allocation code.
ELG22	Eligibility Check Information SHALL include the Device radio access technologies, including release.
ELG23	The eUICC SHALL declare the eUICC Form Factor Type in the Eligibility Check Information.
ELG24	Eligibility Check Information SHALL include the Device letter class(es) according to 3GPP TS 31.111 [33] and ETSI TS 102 223 [34].
ELG25	When the Device is Enterprise Capable, this SHALL be indicated in the Eligibility Check Information
ELG26	There SHALL be a means to retrieve the certifications (functional and security) of the eUICC.

Table 10: 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	When technically feasible, the EID SHALL be accessible by the End User in a defined human readable format via the Device (e.g. On a Primary Device, printed on the Device itself, displayed on the screen etc.), otherwise, the EID SHALL be accessible by the End User via alternate forms out of scope of this specification (e.g. printed in the Device's packaging, accessible via a support web site etc.).
DEV3	If an eUICC is within the Device packaging, then the EID SHOULD be printed in machine readable form on the Device packaging. If the EID is not printed in machine readable form, a mechanism SHOULD be provided to retrieve the EID from the other information on the packaging (e.g. a database of correspondence between EIDs and IMEIs)
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	[Void]

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	[Void]
DEV8	[Void]
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	[Void]
DEV15	IMEIs SHALL be assigned by the Device Manufacturer to and used by the Device in compliance with TS.06 [39].
DEV16	There SHALL be a means on the Device for the End User to access the ICCID of the enabled Operational Profile(s).
DEV17	The EID and/or the Device Information Code SHOULD be accessible by the End User in a defined machine readable format (e.g. OCR, QR Code, etc.) via the Device (e.g. On a Primary Device, printed on the Device itself, displayed on the screen etc.).
DEV18	IMEIs SHALL be assigned by the Device Manufacturer to and used by the Device in compliance with TS.06 [39].
DEV19	There SHALL be a means for the Device supporting LDS to present the associated Root SM-DS address(es). The presentation is implementation specific (e.g., it could be displayed on the screen, or printed on the Device itself or packaging of the Device).
DEV20	If both the Device and its eUICC supports MEP, then each Enabled Profile SHALL be associated with a different IMEI.
DEV21	If the eUICC supports EUICC64, it SHALL be possible to enable more than one profile on the same eUICC for a MEP-capable Device.
DEV22	There MAY be a means to store one or more default SM-DP+ address(es) in the Device.

Table 11: 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 12: Device Capability Requirements

4.5.2 Devices 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 13: Device with Integrated eUICC Requirements

4.5.3 Device Information Code Requirements

Req no.	Description
DEV-IC1	The Device Information Code SHALL include a field listing the available EID(s).
DEV-IC2	The Device Information Code SHALL be able to include a field listing the available TAC(s) or IMEI(s).
DEV-IC3	The Device Information Code SHALL be able to include a field for the SM-DS FQDN(s) where SM-DS Events can be registered by the SM-DP+ on behalf of the Mobile Service Provider.
DEV-IC4	The Device Information Code SHALL be able to include additional proprietary information e.g. Device brand,
DEV-IC5	In case of multiple EIDs, the Device Information Code SHALL be able to indicate which EID has to be used for SM-DS Event Registration.

4.6 Device Initialisation

4.6.1 Device Reset Requirements

Req no.	Description
FAC1	It SHALL be possible for the End User to perform a 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 14: Device Reset Requirements

4.6.2 eUICC Memory Reset Requirements

Req no.	Description
MEM1	[Void]
MEM2	eUICC Memory Reset SHALL delete all Operational Profiles on the eUICC regardless of their Profile Policy Rules and of their state.
MEM3	Strong Confirmation SHALL be verified in order to initiate eUICC Memory Reset.
MEM4	In addition to MEM3**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 15: 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 regardless of their state.
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 16: eUICC Test Memory Reset Requirements

4.7 Profile Requirements

4.7.1 Test Profile Requirements

Req no.	Description
TPRO1	It is OPTIONAL for the 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 17: Test Profiles Requirements

Note: 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 [Void]

4.8 Profile Metadata Requirements

Req no.	Description
META1	All Profiles SHALL have associated Profile Metadata.
META2	Unless specified otherwise in the below requirements, 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 Mobile 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 or Mobile Service Provider.
META8	[Void]
META9	The Profile Metadata SHALL always be available to the LPA. The display to the End User is implementation-specific.
META10	The Profile Metadata SHALL include an OPTIONAL field to allow the display of an icon defined by the Operator or Mobile 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.
META11a	The Profile Metadata SHALL be able to include a message that is to be displayed to the End User when the Profile contains a Profile Policy Rule. It SHALL NOT be stored after Profile download.

Req no.	Description
META12	All Profiles SHALL be uniquely identified in the Profile Metadata as Operational, Provisioning or Test Profile.
META13	An Operator, potentially on behalf of a Mobile Service Provider SHALL be able to access and update the following Profile Metadata of its Profile using the ES6 interface if the Profile is Enabled: • Mobile Service Provider name • Short description of the Profile • Icon of the Profile • HR icon reference • List of Managing SM-DP+ and their respective authorisations to update individual Profile Metadata items • Profile Owner OIDs that are allowed to implicitly disable this Profile by RPM 'Enable' • Polling Address • Profile Policy Rules (unset only) • Enterprise ID (access only) • Enterprise Name • Enterprise Rules • Device Change Configuration of the Profile The content of the respective Profile SHALL reflect the updated Profile Metadata.
META14	The Profile Metadata SHALL include an OPTIONAL field (named HR icon reference) that enables access to high resolution icons. The icons MAY be hosted by the SM-DP+ that handles the Profile.
META15	The HR icon reference SHALL allow the LPA to retrieve one or several icons for a Profile in the format(s) best suited for presentation on the user interface. Best fitting icons are intended to be shown during Profile download, Profile selection etc.
META16	The HR icon solution SHALL provide an option to allow the HR icon(s) to be provided during the Profile download procedure.
META17	The Profile Metadata SHALL include an OPTIONAL field for Device Change Configuration of the Profile. This field SHALL include OPTIONAL sub-fields for: • The address of the SM-DP+ that processes Device Change request • The Activation Code to be used by the new Device for Device Change • An indication of whether the Profile has to be deleted before the Activation Code is made available for the new Device, where the Activation Code is either from the present sub-field or what was used to trigger the original Profile Download procedure Note: If an Activation Code is present in the sub-field, then it supersedes the Activation Code that was used to trigger the original Profile Download procedure.
META18	The Profile Metadata SHALL be able to include an optional field for the estimated installed size of the Profile.

Req no.	Description
META19	The Profile Metadata SHALL be able to include a list of Managing SM-DP+(s).
META20	The Profile Metadata SHALL include an optional field to allow for the inclusion of the Enterprise ID.
META21	The Profile Metadata SHALL include an optional field to allow for the inclusion of the Enterprise Name.
META22	The Profile Metadata SHALL be able to include additional proprietary information. The additional proprietary information SHALL include a field for uniquely identifying the issuer of the additional proprietary information.
META23	With regard to META22, the eUICC SHALL ignore fields it does not support.
META24	With regard to META22, the LPA SHALL ignore fields it does not support.
META25	The information defined in META22 SHALL NOT impact the functionalities and Profile Management Operations defined in this specification that are not Vendor specific.
META26	The information defined in META22 SHALL NOT impact the interoperability of the solution defined in this specification (incl. Devices, Profiles and SM-DP+).
META27	With regard to META22, the eUICC SHALL store the additional proprietary information in its memory if indicated by the Profile Owner

Table 18: 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	In combination with an enabled Operational NFC Profile, the NFC eUICC SHALL support all requirements as specified in the SGP.03 GSMA NFC UICC Requirements Specification [20].
NFC3	[Void]
NFC4	[Void]
NFC5	[Void]
NFC6	[Void]
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	[Void]
NFC9	[Void]

Table 19: 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 on behalf of served Mobile Service Providers. 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.

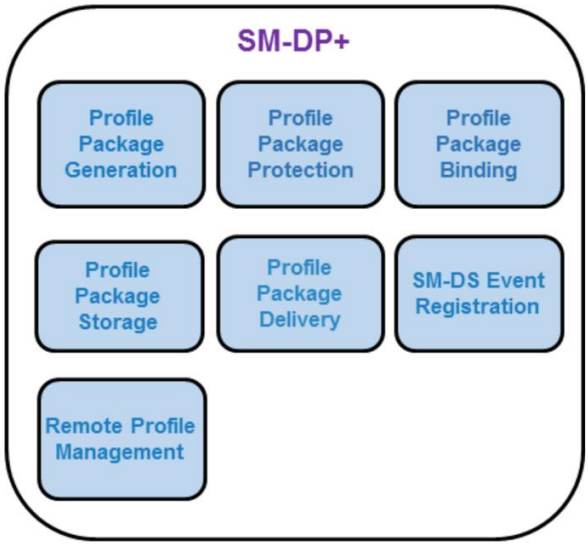

Figure 6: SM-DP+ Functions

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.
Remote Profile Management	Profile Management operations (Enabling, Disabling, deleting, list Profile information, query, update Metadata) within the eUICC managed by the Managing SM-DP+. RPM command authorisation is enforced by the eUICC.

Table 20: SM-DP+ Function Descriptions

4.10.2 SM-DP+ Requirements

Req no.	Description
SMDP1	[Void]
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.
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.
SMDP14a	The SM-DP+ SHALL check the information referenced by the digital identification in ELG26.
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 or failure to verify the information referenced by the digital identification in ELG26 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

Req no.	Description
	SHALL be terminated and the Mobile Service Provider and the supporting 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 Mobile Service Provider and the supporting 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.
SMDP25	The SM-DP+ SHALL be able to send a Notification to the Operator informing them that a specific Bound Profile Package download is starting. Such notifications MAY be forwarded by the Operator to the Mobile Service Provider.
SMDP26	The SM-DP+ SHALL be able to send an Eligibility Check Information report and other relevant information (e.g. Activation Code, ICCID, etc.) to the Mobile Service Provider and the supporting 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 that is requested by the Operator.
SMDP27a	It SHALL be possible for the SM-DP+ to indicate to the Operator lists of Root SM-DSs and Alternate SM-DSs to which the SM-DP+ can perform the (cascade) Event Registration associated with an RSP operation. Note: This could be part of the static configuration between the SM-DP+ and the Operator.
SMDP27b	It SHALL be possible for the Operator to determine and indicate to the SM-DP+ lists of Root SM-DSs and Alternate SM-DSs to which the SM-DP+ has to perform the (cascade) Event Registration associated with an RSP operation.
SMDP28	The SM-DP+ SHALL be able to request an Alternative SM-DS not to propagate an Event Registration to a specific Root SM-DS.
SMDP29	The SM-DP+ SHALL be able to send a Profile delete Notification to the Mobile Service Provider and the supporting Operator owning a Profile when a related delete Notification is received from the eUICC.

Req no.	Description
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)	[Void]
SMDP33 (FFS)	[Void]
SMDP34 (FFS)	[Void]
SMDP35 (FFS)	[Void]
SMDP36	A SM-DP+ SHALL support all sets of elliptic curve parameters for the CAs that it uses.
SMDP37	If a Profile Package is not yet released for download then the LPA SHALL be informed by means of a specific error code.
SMDP38	An SM-DP+ SHALL be able to distinguish a Field-Test eUICC from a Certified eUICC through eUICC Eligibility Check Information.
SMDP39	The SM-DP+ SHALL be able to be instructed by the Profile Owner to reject an RSP operation to Field-Test eUICCs. Note: The mechanism is out of the scope of this document and it is left to implementation.
SMDP40	The SM-DP+ SHALL NOT perform an RSP operation to a Field-Test eUICC if it has been instructed so by the Profile Owner as per SMDP49.
SMDP41	The Managing SM-DP+ SHALL be able to send a Notification to the Profile Owner informing them that a requested RPM command is about to be executed.
SMDP42	Only a Managing SM-DP+ SHALL be allowed to perform RPM on a Profile.
SMDP43	If RPM is supported by the Managing SM-DP+, the LPA and the eUICC: the Managing SM-DP+ SHALL establish a secure channel to the eUICC to perform Remote Profile Management (RPM) providing authentication, authorisation, and integrity checking. Ciphering SHALL be provided between the SM-DP+ and the LPA.
SMDP44	The SM-DP+ SHALL be able to send a Profile enabled Notification to the Mobile Service Provider and the supporting Operator owning a Profile when a related enabled Notification is received from the eUICC.
SMDP45	The SM-DP+ SHALL be able to send a Profile disabled Notification to the Mobile Service Provider and the supporting Operator owning a Profile when a related disabled Notification is received from the eUICC.
SMDP46	The SM-DP+ SHALL provide means for the Operator to query about the current status of a Profile Package. The search criteria and level of details of the returned information are implementation-dependent.
SMDP47	In the Event Registration, the SM-DP+ SHALL indicate to the SM-DS the RSP operation type (i.e., Profile download or RPM).

Req no.	Description
SMDP48	In the Event Registration, the SM-DP+ SHALL be able to provide to the SM-DS information that can be used by the LPA to identify the target Profile(s) upon Event Retrieval. Note: See BAS7 and the text at the beginning of Basic Principles 2.1 for privacy requirements to be covered.
SMDP49	The information in SMDP48 SHALL NOT disclose to the SM-DS any private or confidential data of the target Profile.
SMDP50	In the Event Registration, the SM-DP+ SHALL be able to provide the Mobile Service Provider Name to the SM-DS to be forwarded to the LPA upon Event Retrieval.
SMDP51	The SM-DP+ SHOULD ensure that repeated Profile or RPM download attempts due to expired/outdated Event Records are prevented (as per SMDP52 and SMDP53).
SMDP52	The SM-DP+ SHALL request the deletion of the associated Event Record (if any) of a successful Profile or RPM download.
SMDP53	The SM-DP+ SHOULD request the deletion of the associated Event Record (if known) of an expired/outdated Profile or RPM download attempt.

Table 21: SM-DP+ Requirements

4.10.3 Default SM-DP+ Address on the eUICC Requirements

Req no.	Description
DF1	[Void]
DF2	The default SM-DP+ address(es) in the eUICC or Device SHALL be accessible by the LPA to establish a connection to an SM-DP+.
DF3	The default SM-DP+ address(es) in the eUICC or Device MAY be left blank.
DF4	[Void]
DF5	[Void]

Table 22: Default SM-DP+ Address on the eUICC Requirements

4.11 Local Profile Assistant (LPA)

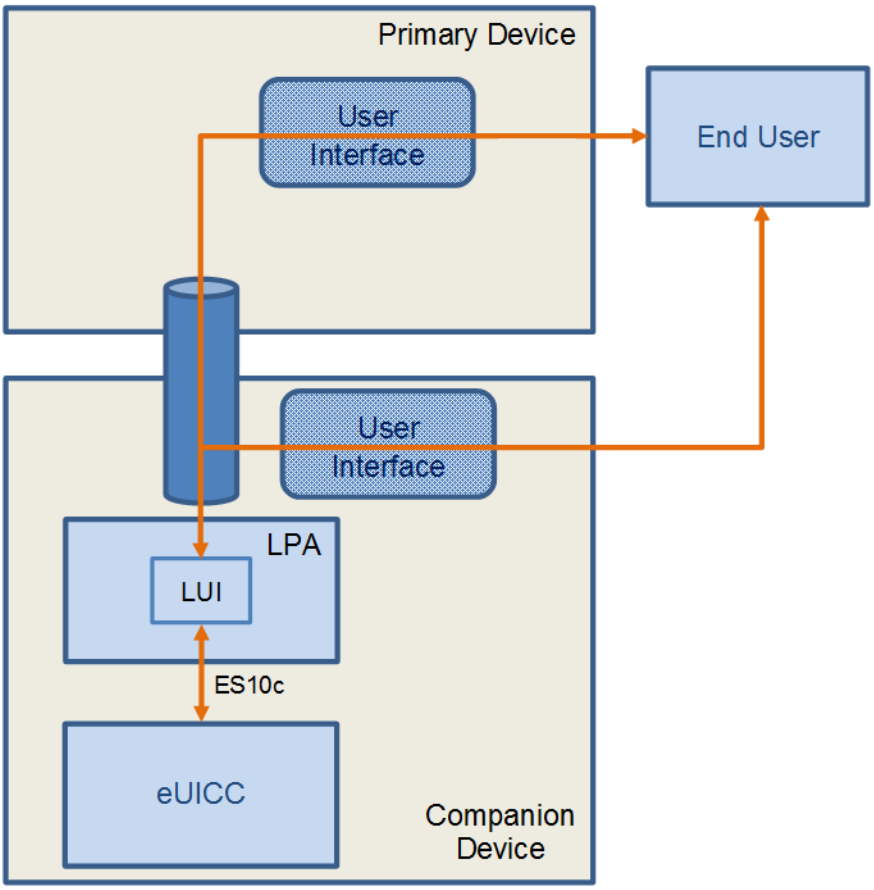

Figure 7: End User Interaction and Interfaces between a Primary and Companion Device, where the Companion Device MAY have a UI

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 four distinct functions, the Local Discovery Service (LDS), the Local Profile Download (LPD), the Local User Interface (LUI), and the LPA PRoxy (LPR) 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.

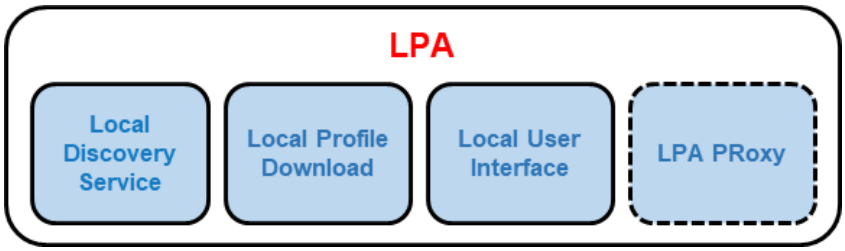

Figure 8: LPA Functions

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.
LPA PRoxy (LPR)	This plays a proxy role for the efficient management of Profile contents from a Profile Content Management Platform, or a Delegated Profile Content Management Platform.

Table 23: 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:

- LPA in the Device
- LPA in the eUICC

4.11.2.1 LPA in the eUICC

LPA functions are provided by the eUICC.

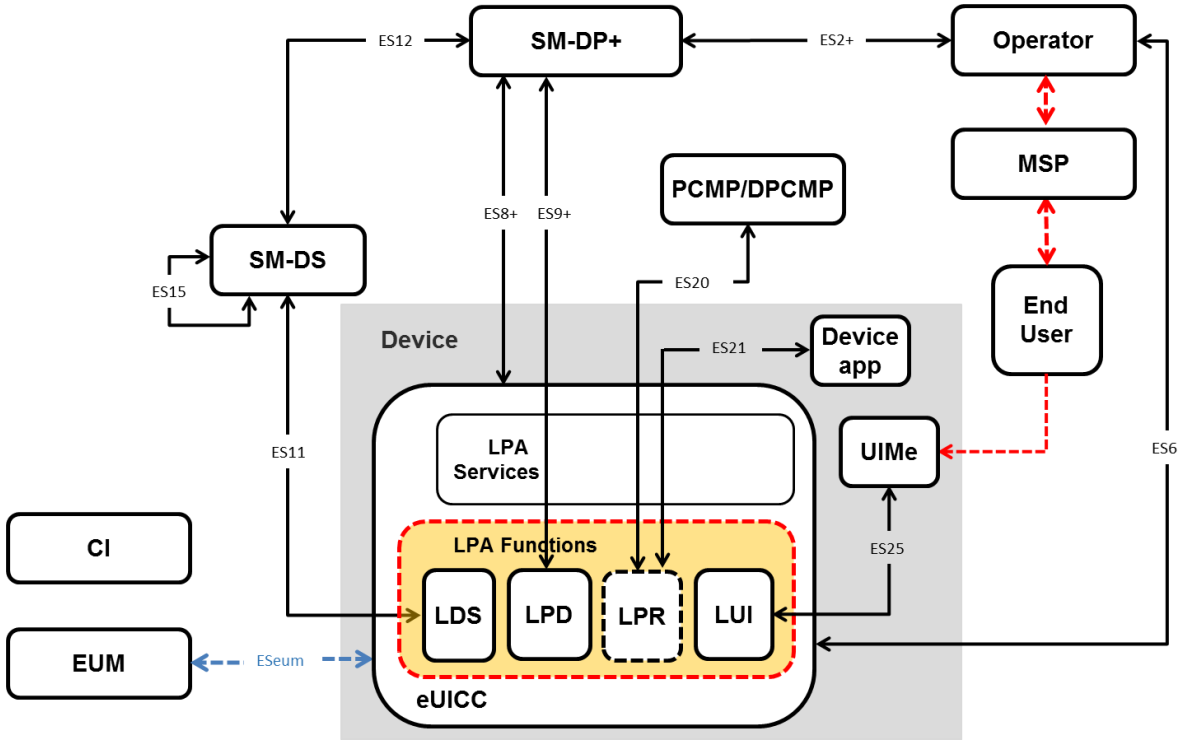

Figure 9: LPA in the eUICC

4.11.2.2 LPA in the Device

LPA functions are provided by the Device.

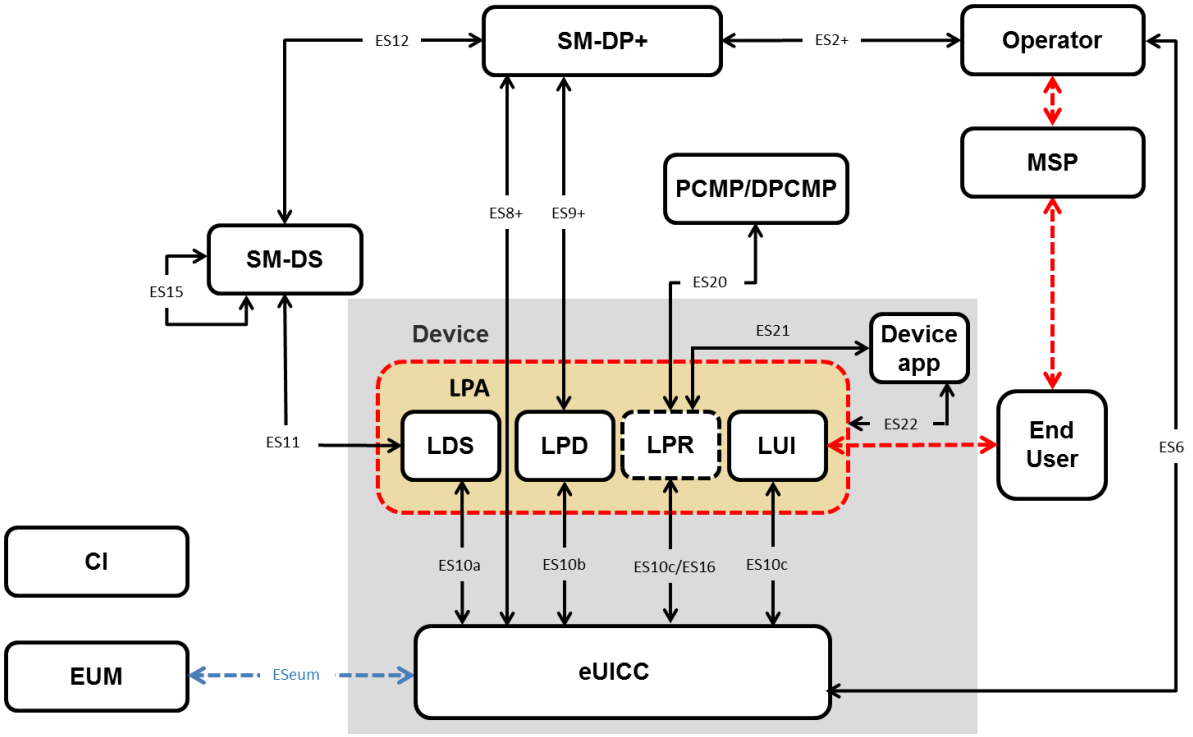

Figure 10: LPA in the Device

4.11.3 LPA Requirements

Req no.	Description
LPA1	[Void]
LPA2	[Void]
LPA3	Security between the LUI and the associated display or input applications on the Device SHALL be provided according to current industry best practices.
LPA4	Access to the LUI SHALL be protected according to current industry best practices.
LPA5	All Local Profile Management Operations SHALL require User Intent except where otherwise noted in this specification.
LPA6	[Void]
LPA7	[Void]
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 the 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 a default SM-DP+ address. Simple confirmation SHALL be enforced. If the LPA does not support 'edit default SM-DP+ address', alternative vendor-specific methods to edit a 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. When supported, this operation SHALL allow the End User to add or modify a nickname for the selected Profile. The operation SHALL NOT modify the Mobile 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.
LPA16a	The Local Profile Management Operation ‘add Profile via Default SM-DP+’ SHALL be supported and available to the End User if a Default SM-DP+ is

Req no.	Description
	populated. This operation SHALL allow the LPA to download and install a new Profile to the eUICC using the Default SM-DP+ address(es) configured on the eUICC or the Device. Simple Confirmation SHALL be enforced. Note: The presentation of Profile management operations to the End User on the LUI is OEM specific. For example two Profile management operations could be combined within one menu item.
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.
LPA17a	An LPA with an LDS SHALL support the Local Profile Management Operation 'add Profile via SM-DS' and make it available to the End User. Note: The presentation of Profile management operations to the End User on the LUI is OEM specific. For example, two Profile management operations could be combined within one menu item.
LPA17b	Operation in LPA17a**LPA17** SHALL allow the LPA to download and install a new Profile to the eUICC by contacting a Root SM-DS fetched by the LPA to retrieve pending events. Simple Confirmation SHALL be enforced.
LPA17c	The Local Profile Management Operation 'add Profile via Activation Code' SHALL be supported and available to the End User. This operation SHALL allow the LPA to download and install a new Profile to the eUICC with the use of an Activation Code. Simple Confirmation SHALL be enforced. Note: The presentation of Profile management operations to the End User on the LUI is OEM specific. For example, two Profile management operations could be combined within one menu item.
LPA17d	If RPM is supported by the LPA and the eUICC: the Local Profile Management Operation 'update Profile' SHOULD be supported and available to the End User. This operation SHALL trigger Event retrieval(s) from the Polling Address (Managing SM-DP+/SM-DS address) stored in the selected Profile to retrieve RPM operations for this specific Profile. Note: The presentation of Profile management operations to the End User on the LUI is OEM specific. For example, two Profile management operations could be combined within one menu item.
LPA18	[Void]
LPA19	[Void]
LPA20	[Void]
LPA21	[Void]

Req no.	Description
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	[Void]
LPA30	[Void]
LPA31	A point-to-point 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	[Void]
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	[Void]
LPA40	There SHALL be at most one active LPA per eUICC.
LPA41	[Void]
LPA42	[Void]
LPA43	[Void]
LPA44	The LPA SHALL be able to read the Profile Policy Rules.
LPA45	[Void]
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:

Req no.	Description
	• 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 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 of the separate operations are clearly explained and offered 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 SHOULD 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	[Void]
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	[Void]
LPA60	[Void]

Req no.	Description
LPA61	Error/retry handling of the LPA polling mechanism SHOULD 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. This includes means such as checking for pending Profiles from Default SM-DP(s)+ if configured, pending profiles registered to Root/Alternative SM-DS(s), and/or using Activation Codes provided by the Mobile Service Provider. Simple Confirmation is required. Note: This is implementation dependent 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 are no default SM-DP+ addresses. 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 Mobile 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	[Void]
LPA66	[Void]
LPA67	If the SM-DP+ stops the Profile download procedure, the LPA SHALL notify the End User.
LPA68	[Void]
LPA69	As part of the process of downloading a new Profile, the LPA SHOULD offer the choice to the End User to enable or not enable the new Profile.
LPA70	The LUI SHOULD provide a local configuration option that allows the End User to turn on/off RPM operations.
LPA71	The LPA MAY provide a means by which the eUICC can request the LPA to check for Events or pending RSP operations as described by EUICC55 and EUICC56.
LPA72	An LPA with an LDS SHALL retrieve one or more Root SM-DS addresses, either stored on the eUICC or stored within the Device.
LPA73	It SHALL NOT be required for the LPA to maintain state for any transactions from the SM-DS(s) except the cascade Event Retrieval(s).

Table 24: LPA Requirements

4.11.4 LDS Requirements

Req no.	Description
LDS1	The LDS SHALL be able to read out the root SM-DS address configured in the eUICC and the Alternative SM-DS address configured in the installed Profiles.

LDS2	The LDS MAY support the Event Checking procedure. If the Event Checking procedure is supported by the LDS, requirements LDS3 to LDS6 SHALL apply.
LDS3	The Event Checking procedure SHALL provide a means for the LDS to query the SM-DS to determine the presence of any Event Records registered for an eUICC, without requiring the eUICC and SM-DS to perform the common mutual authentication procedure.
LDS4	During the Event Checking procedure, the LDS SHALL provide the SM-DS an information for identifying the eUICC in order to check the presence of Event Record(s) registered for that eUICC, without compromising the privacy of the EID.
LDS5	There SHALL be a means for the LDS to determine whether the SM-DS supports the Event Checking (e.g. by a pre-configuration by the OEM or by a response from the SM-DS).
LDS6	If both the LDS and the SM-DS support Event Checking, the LDS SHOULD perform the Event Checking procedure prior to the Event Retrieval against that SM-DS.
LDS7	The LDS MAY support a Push Service. If a Push Service is supported by the LDS, requirements LDS8 and LDS9 SHALL apply.
LDS8	There SHALL be a means for the LDS to request an SM-DS to be notified about Events registered for the eUICC.
LDS9	With regard to LDS8, the request SHALL include the information for identifying the corresponding eUICC and the information about the Push Service to be used by the SM-DS for the notification.

Table 25: LDS Requirement

4.11.5 LPA API Requirements

This section describes requirements for an Application Programming Interface offered by the LPA in the Device. API requirements for the LPA in the eUICC are FFS.

4.11.5.1 LPA API Access Control Requirements

Req no.	Description
LPAAPIAC1	A Device supporting an LPA API SHALL provide a mechanism which can authorise applications' access to LPA API.
LPAAPIAC2	The Device MAY refer to GP SEAC [15] or GP DAC [55] to implement the LPA API access control mechanism.

Table 26: LPA API Access Control Requirements

4.11.6 APDU Access API Requirements

This section describes requirements for an APDU access interface on the Device. This interface MAY be provided by some other Device component external to the LPA (e.g. a smart-card interface) provided that when it is used with an eUICC it satisfies the following requirements.

Req no.	Description
APDUAPI1	A Device MAY support the APDU Access API requirements in this section. NFC Devices SHALL support the APDU Access API requirements in this section.
APDUAPI2	If the Device supports APDU Access API as per requirement APDUAPI1, the Device SHALL provide a mechanism by which authorised applications can send APDUs to the Enabled Profile.
APDUAPI3	The Device SHALL authorise applications by retrieving and enforcing Access Rules of the corresponding Profile as specified in the GlobalPlatform SEAC specification [15].
APDUAPI4	The Access Rules for the Enabled Profile SHALL be stored as part of the Profile.
APDUAPI5	Within the Enabled Profile only the contents of the Profile itself SHALL be accessible to authorised applications.

Table 27: APDU Access API Requirements

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 an 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.

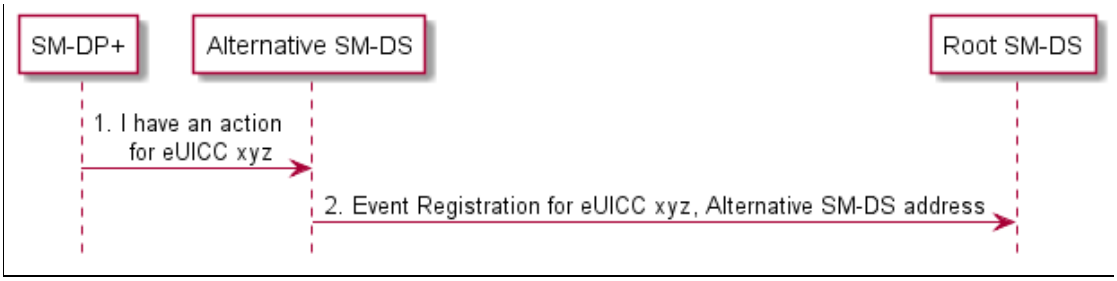

Figure 11: Alternative SM-DS Event Registration

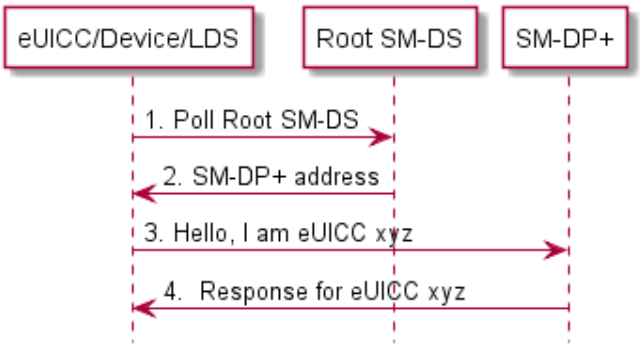

Figure 12: Device to Root SM-DS Event Discovery

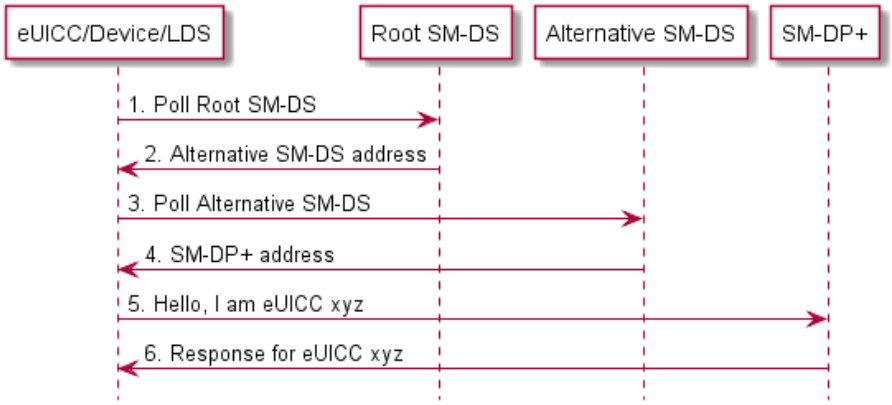

Figure 13: Alternative SM-DS Event Discovery

4.12.2 SM-DS Implementation

Two configurations of the SM-DS MAY exist:

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

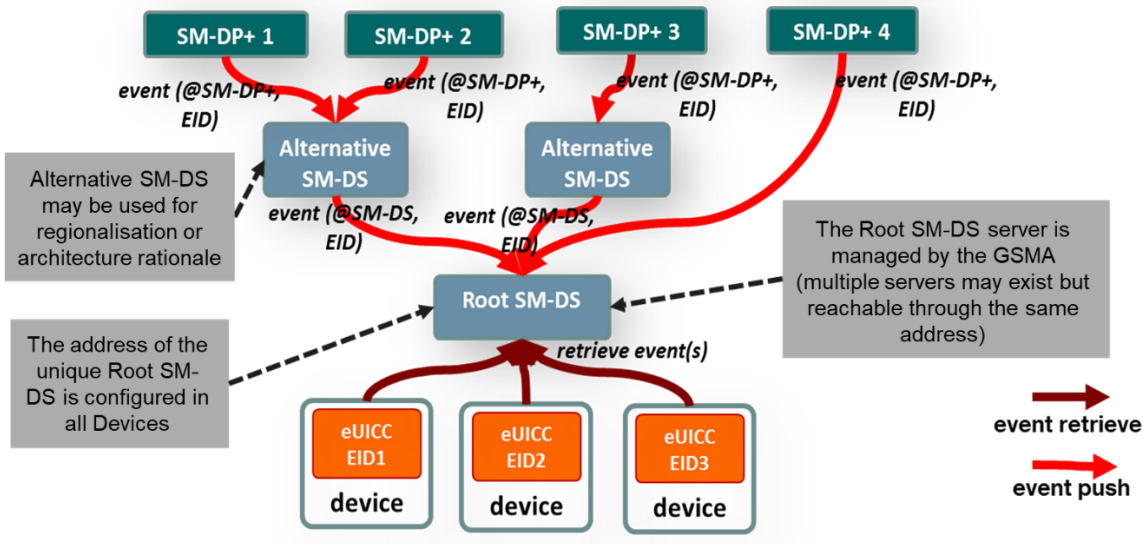

Figure 14: SM-DS Implementation

Figure 14 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.

4.12.4 SM-DS functions

The SM-DS has four distinct functions:

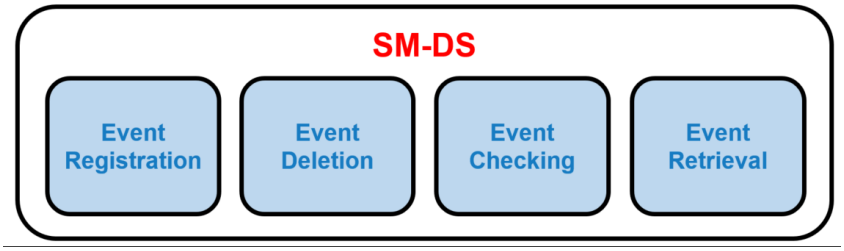

Figure 15: SM-DS Functions

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

Table 28: 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	[Void]
SMDS3	All Discovery Requests and Event Registrations SHALL be processed by any Root SM-DS in a non-discriminatory manner.
SMDS4	The SM-DS SHALL 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.

Req no.	Description
SMDS5	The SM-DS SHALL only accept Discovery Requests authenticated by the 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).
SMDS8a	As per SMDS8, the valid Event Records SHALL be filtered by the RSP operation type provided by the LDS (if any).
SMDS9	The SM-DS SHOULD protect itself to avoid becoming a point of injection for DoS or spam attacks.
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 Mobile Service Provider, 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, or RPM commands.
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 Denial of Service attacks.
SMDS17	All communications to, from and between entities of the SM-DS SHALL be encrypted and integrity protected.
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).
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 unless the discovery operation requests a specific event to be returned, in which case only that Event SHALL be sent.
SMDS22	An SM-DP+ SHALL be able to send an Event Record to an LDS either by a Root SM-DS or via any Alternative SM-DS selected by the SM-

Req no.	Description
	DP+. If an Alternative SM-DS is selected, the Event Record to the LDS SHALL come from this Alternative SM-DS.
SMDS23	[Void]
SMDS24	A Root SM-DS SHALL be managed by the GSMA. This Root SM-DS MAY be used as a default Root SM-DS.
SMDS25 (FFS)	[Void]
SMDS26 (FFS)	[Void]
SMDS27 (FFS)	[Void]
SMDS28 (FFS)	[Void]
SMDS29 (FFS)	[Void]
SMDS30 (FFS)	[Void]
SMDS31 (FFS)	[Void]
SMDS32	The SM-DS MAY support the Event Checking procedure. If the Event Checking procedure is supported by the SM-DS, SMDS33 SHALL apply.
SMDS33	Upon the request from an LDS for Event Checking, the SM-DS SHALL provide the information to the LDS whether it has any Event registered for the corresponding eUICC.
SMDS34	The SM-DS MAY support none, one, or multiple kinds of Push Services available in the industry. If a Push Service is supported by the SM-DS, SMDS35 and SMDS36 SHALL apply.
SMDS35	If requested by the LDS as per LDS8, the SM-DS SHALL return the indication whether it accepts or rejects the request.
SMDS36	If accepted by the SM-DS as per SMDS35, the SM-DS SHALL notify the LDS about the Event Registration using the Push Service, whenever an Event is newly registered for the eUICC.

Table 29: 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).

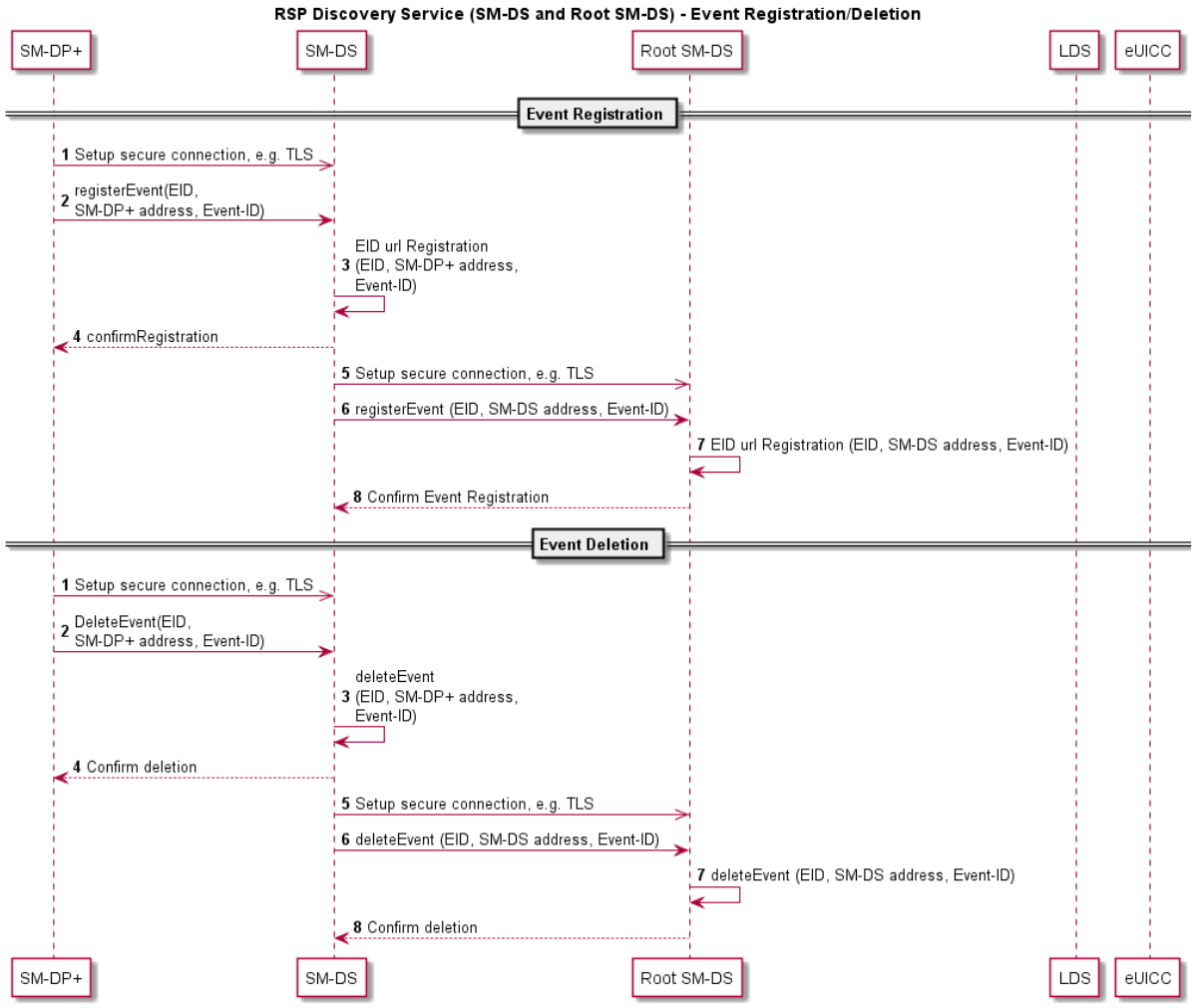

Figure 16: Event Registration/Deletion Procedure

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).

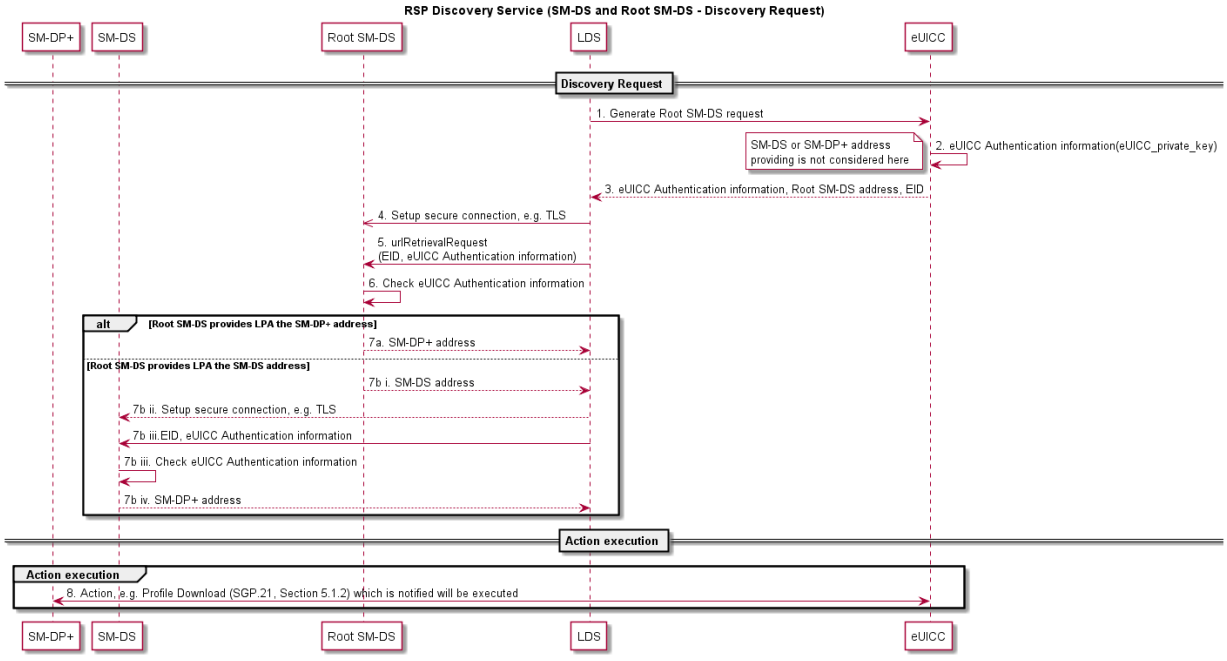

Figure 17: Discovery Request Procedure

Procedure:

1. to 3. In order to generate a Discovery Request, the LDS requests the eUICC to generate its Authentication information 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 Authentication information.

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 Authentication information.
      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 Mobile 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	[Void]
POL5	Profile Policy Enforcement SHALL be able to resolve any Profile Policy Rule conflict.
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	[Void]

Policy no.	Description
POL10	A Profile Policy Rule SHALL be enforced whenever a Profile state change is attempted.
POL11	Downloading and installing a Profile in a non-MEP-capable eUICC 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.
POL11a	Downloading and installing a Profile with the POL RULE1 in an MEP-capable eUICC SHALL NOT be allowed.
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.
POL13	A Profile Owner SHALL be able to unset the Profile Policy Rules of its Profile using the ES6 interface.
POL13a	If RPM is supported by the Managing SM-DP+, the LPA and the eUICC: a Profile Owner SHALL be able to unset the Profile Policy Rules of its Profile via a Managing SM-DP+ using the ES9+ interface. Note 1: For details refer to Section 5.4.2 Remote Profile Management RequirementsFigure 32. Note 2: The setting of Profile Policy Rules on the ES9+ 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 if needed about the Profile Policy Rules and if notified, the installation SHALL thereafter be conditional on End User Strong Confirmation.
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.
POL15a	Where End User consent is required for the download of the Profile which includes Policy Rules, the Mobile Service Provider SHALL be able to provide a message for the End User that MAY be displayed by the Device. Note: Consideration should be made for the display of lengthy text on a Device with a limited display.
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	[Void]
POL20	Allowing the installation of a Profile with Profile Policy Rules SHALL be subject to compliance with local regulatory requirements.

Table 30: 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 only be supported by non MEP-capable eUICCs.
POL RULE2	The Profile Policy Rule 'Deletion of this Profile is not allowed' SHALL be supported.
POL RULE3	[Void]

Table 31: Policy Rules Requirements

4.13.4 Profile Policy Enabler Requirements

The Rules Authorisation Table (RAT) contains the description of the Profile Policy Rules (PPR) that can be set in a Profile to be installed in that eUICC. The RAT is defined at eUICC platform level and is used by the Profile Policy Enabler (PPE) and the LPA to determine whether or not a Profile that contains PPRs is authorised and can be installed on the eUICC.

The RAT is provisioned at eUICC manufacturing time; or during the initial Device setup provided that there is no installed Operational Profile. The OEM or EUM is responsible for setting the content of the RAT.

The RAT contains a set of entries that are mandatory for all eUICCs. In addition optional entries MAY be included:

- For Profile Policy Rules that are optional to implement (e.g. POL4), the RAT contains additional entries permitting the use of these Profile Policy Rules.
- The RAT may also contain Operator-specific entries that provide exceptions to the requirement to obtain Authenticated User Confirmation prior to download and installation of a Profile that contains specific Profile Policy Rules.

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 at (and 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	[Void]

Policy no.	Description
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 and require Strong Confirmation before the download of the Profile.
POLPPE11	The OEM or EUM SHALL be responsible for provisioning the RAT into the eUICC.
POLPPE12	A RAT MAY be configured in the eUICC. If the RAT is not present, the eUICC SHALL regard this as a RAT with no entry.

Table 32: 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].
CERTEU3a	The EUM compliance to CERTEU1 and the eUICC product compliance to CERTEU2 and CERTEU3 SHALL be referenced via a digital identification associated to the eUICC product.
CERTEU3b	The eUICC SHALL be certified according to the compliance programme defined in SGP.24 [27].
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+) [44].
CERTEU7	The eUICC public key Certificate used for authentication SHALL contain the EID.
CERTEU8	The eUICC public key Certificate(s) SHALL contain the technical reference of the product, for example the Common Criteria certification [53] report number.
CERTEU9	The EUM Public Key Certificate(s) SHALL chain to eSIM CA(s).
CERTEU10	The eUICC Certificate(s) SHALL be signed by the EUM using its EUM Private Key corresponding to its Certificate (CERTEU9).
CERTEU10a	Any eUICC Certificate(s) modification SHALL be end-to-end protected between the eUICC and issuing EUM.

Req no.	Description
CERTEU11	[Void]
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 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.
CERTEU13a	If the digital identification stored on the eUICC as defined in ELG26 is updatable, then the eUICC SHALL support a secure mechanism to update this digital identification.
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 [31].
CERTEU17	Field-Test eUICCs SHALL use a certified hardware according to SGP.24 [27].
CERTEU18	An eUICC certified according to SGP.24 [27] SHALL be eligible to be issued with an eUICC certificate that chains up to GSMA CI.
CERTEU19	The eUICC SHALL provide a means to uniquely identify its certification(s).

Table 33: eUICC Certification Requirements

4.14.2 Device Compliance Requirement

Req no.	Description
CERTDEV1	The LPA SHALL comply with SGP.24 [27].
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 34: 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 [24].
CERTDP2	The SM-DP+ SHALL be certified according to GSMA FS.08 SAS-SM Standard [22] and FS.09 SAS-SM Methodology [32].
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	[Void] Note: Based on CERTDP2, this is covered by SAS-SM.
CERTDP8	[Void] Note: Based on CERTDP2, this is covered by SAS-SM.
CERTDP9	The private key 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 Denial of Service attacks.
CERTDP11	[Void] Note: Based on CERTDP2, this is covered by SAS-SM.
CERTDP12	The SM-DP+ Public Key Certificate(s) for authentication and Profile binding SHALL chain to eSIM CA(s).
CERTDP13	The SM-DP+ SHALL support at least one eSIM CA for the purpose of the operations listed in CERTDP12.

Table 35: 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 GSMA FS.08 SAS-SM Standard [22] and FS.09 SAS-SM Methodology [32].
CERTDS3	The SM-DS SHALL implement isolation of privileges (Log, Audit, Operation, and Administration).
CERTDS4	The SM-DS SHALL implement operating system hardening mechanisms.

Req no.	Description
CERTDS5	The SM-DS SHALL implement separation of control, user and administrative planes.
CERTDS6	[Void] Note: Based on CERTDS2, this is covered by SAS-SM.
CERTDS7	[Void] Note: Based on CERTDS2, this is covered by SAS-SM.
CERTDS8	The SM-DS Public Key Certificate(s) for authentication SHALL chain to eSIM CA(s).
CERTDS9	The SM-DS SHALL support at least one eSIM CA for the purpose of the operations listed in CERTDS8.

Table 36: 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	[Void]
CERTLPA3	[Void]
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 accept Certificates signed by a GSMA CI for SM-DP+ and SM-DS authentication used in TLS session.

Table 37: 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.
CERTPK5	The LPD authentication of an SM-DP+ using an invalid Public Key Certificate SHALL fail (see CERTPK11), 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.

Req no.	Description
CERTPK8	The eSIM CA(s) 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 support at least one eSIM CA for the purpose of the operations listed in EUICC62.
CERTPK10	A Public Key Certificate SHALL be considered as valid if: • it has a valid signature • it is signed by a GSMA CI, or by an Independent eSIM CA, or a trusted chain of Certificates up to a GSMA CI or an Independent eSIM CA. Certificate Path validation SHALL follow the process defined in RFC 5280 [1]. • 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 an eSIM CA or a public trusted CA, or a trusted chain of Certificates up to an eSIM CA or to a public trusted CA. Certificate path validation SHALL follow the process defined in RFC 5280 [1]. • 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 an eSIM CA or a public trusted CA.
CERTPK12	It SHALL be possible for the Profile Owner to ensure that the Certificates of the SM-DP+ servers used during the Profile Management Lifecycle of a Profile (e.g. download of a Profile, RPM) chain to a specific eSIM CA Certificate.
CERTPK13	The eUICC SHOULD support at least one GSMA CI.
CERTPK14	The use of the Independent eSIM CA Certificate SHALL NOT compromise any operations that use the Certificate provided by the GSMA CI.

Table 38: Public Key Certificates Management Requirements

4.15 eUICC OS Update

At the time of writing this specification it is understood that other industry bodies may be developing standards that will define harmonised and more robust methods of updating UICC operating system software. Accordingly, readers of this specification are advised that

the publishers reserve the right to explicitly amend features in this specification related to software update in future versions.

There may need to be some industry procedures to manage eUICC OS Updates that affect installed Profiles.

Note: Such a mechanism cannot be included in the RSP Test Specification, nor can it be restricted by the Protection Profile.

Req no.	Description
OSUpd1	An eUICC SHOULD support a mechanism to allow an eUICC OS Update. This mechanism SHALL be secure.
OSUpd2	If such a mechanism is used, the eSIM Products for which the compliance is affected by the eUICC OS update SHALL maintain compliance as specified in SGP.24 [27].
OSUpd3	If such a mechanism is used, after applying an eUICC OS Update, the eUICC OS Manager SHALL receive the status of the execution of the eUICC OS Update.

Table 39: eUICC OS Update Requirements

4.15.1 eUICC OS Update Information

If the eUICC support a mechanism to allow an eUICC OS Update, the Device needs to know some information in order to properly schedule the eUICC OS Update and to handle the eUICC services.

To perform the eUICC OS Update and manage the End User interactions according to the Device Manufacturer's choice of user experience, the following information are needed:

- The Device needs to know if an eUICC OS Update is available for its eUICC; and also which supplier is providing the eUICC OS Update. When and how this detection is performed is out of scope of this specification.
- Before the eUICC OS Update is applied to the eUICC, the Device needs to know if the update will impact the eUICC services, and whether eUICC reboot(s) will be needed.
- At the end of the eUICC OS Update, the Device needs to have a confirmation that the eUICC OS Update is finished and a status to know if it was successful or not.

These information are provided to the eUICC OS Manager delivered over the ESoem interface.

The management of the eUICC OS Update itself (including the deployment process, the way the Device triggers the eUICC OS Update, the retry policy in case of failure (if applicable) and the internal management inside the eUICC) is out of scope of this specification.

Req no.	Description
INFOOS1	The eUICC OS Update package(s) SHALL have associated eUICC OS Update information.
INFOOS2	The eUICC OS Update information SHALL include a field for the identification of the EUM which provides the eUICC OS Update
INFOOS3	The eUICC OS Update information SHALL include a field for the the version of the GSMA SGP.22 specification [24] supported by the eUICC after the OS Update.
INFOOS4	The eUICC OS Update information SHALL include the impact of the eUICC OS Update on the eUICC services.
INFOOS5	The eUICC OS Update information SHALL indicate if eUICC reboots will be needed during or after the eUICC OS Update

Table 40: eUICC OS Update Information Requirements

4.16 Enterprise Requirements

The requirements contained in this section are intended to be used solely in support of the Subscriptions obtained by the Enterprise for its internal use as part of its business operations.

These requirements are to be considered as complementary to the consumer solution.

The following principles apply to Enterprise:

- An Enterprise can request the installation and management of Profiles from more than one Profile Owner on the eUICC
- The Enterprise can request the Profile Owner to remotely manage (enable, disable, delete) their own Profiles, on Enterprise Capable Devices.

Req no.	Description
ENT1	Enterprise Capable Device requirements SHALL only apply to Devices owned by an Enterprise. Implementation and/or related processes are Device Manufacturer specific.
ENT2	It is Optional for the Device, the eUICC and the SM-DP+ to support the Enterprise requirements defined in this document.
ENT3	It SHALL NOT be possible to associate more than one Enterprise to a Device at any point in time.
ENT4	The Enterprise SHALL be able to request that only Enterprise Profiles can be installed on an Enterprise Capable Device; this has no impact on other already installed Profiles. When MEP is supported by both the Device and its eUICC, this requirement SHALL only be enforced if the number of non-Enterprise Profiles that can be enabled according to ENT14 is zero.
ENT5	Where both the Enterprise Capable Device and its eUICC support Multiple Enabled Profiles (MEP), it SHALL be possible to enable more than one Enterprise Profile on that Device.

ENT6	Only the Profile Owner, acting on behalf of the Enterprise, SHALL be able to set Enterprise Rules for its Enterprise Profile(s), at the Profile ordering phase.
ENT7	For an Enterprise Capable Device, it SHALL be possible for the Enterprise to control whether the End User can locally: enable any Profile, enable only Enterprise Profiles, or enable only the specific Enterprise Profile. Strong Confirmation SHALL be enforced.
ENT8	When receiving a request to: • restrict the End User to Enterprise Profiles only and a non-Enterprise Profile is already enabled, or • restrict the End User to the specific Enterprise Profile and a different Profile is enabled, the eUICC SHALL reject the requested restriction.
ENT9	A globally unique identifier and associated Enterprise name SHALL be provided in the Profile Metadata of the Enterprise Profile.
ENT10	The download and installation of the Enterprise Profile SHALL require user confirmation in response to a prompt indicating the type of Profile and the associated consequences of installing this Enterprise Profile.
ENT11	On a Non-Enterprise Capable Device: • It SHALL be possible for an Enterprise Profile without Enterprise Rules to be installed and used. • It SHALL NOT be possible to install an Enterprise Profile with Enterprise Rules • It SHALL NOT be possible to update Enterprise Rules of an installed Enterprise Profile
ENT12	The eUICC SHALL reject the download of an Enterprise Profile when a Profile with POL RULE1 set is already installed.
ENT13	For an Enterprise Capable Device, there SHALL be a mechanism for the End User to allow or disallow the installation of an Enterprise Profile with Enterprise Rules. This mechanism SHALL only be in effect if there is no Enterprise Profile with Enterprise Rules already installed.
ENT14	It SHALL be possible for the Enterprise to indicate the number of non-Enterprise Profiles that can be enabled on the Enterprise Capable Device when MEP is supported by both the Device and its eUICC.

Table 41: Enterprise Requirements

4.17 LPA PRoxy

4.17.1 LPA PRoxy Overview

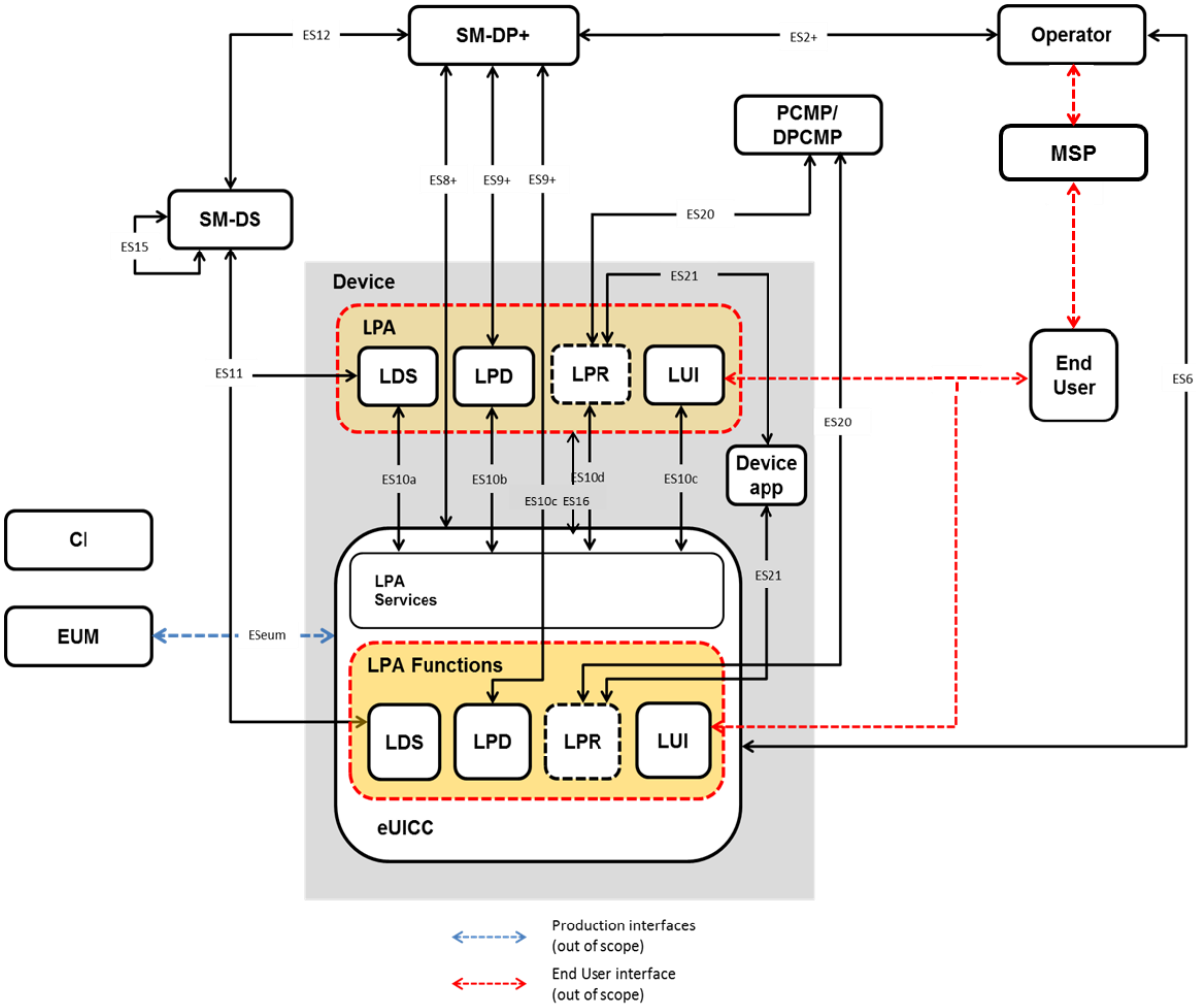

Figure 18: LPA PRoxy Architecture (with LPA configuration in the Device)

The LPR is a “LPA PRoxy” acting as an intermediary between a Profile Content Management Platform hosted by the Profile Owner and the Enabled Profile of the eUICC to improve performance, in the same way the LPD is used between the SM-DP+ and the eUICC for Profile download purposes.

While the Profile Content Management Platform of the Profile Owner has the role of managing the content of the Profile, it might redirect the LPR towards a Delegated Profile Content Management Platform used by a third party to manage a subset of the Profile that has been delegated. This is applicable in Simple Mode, Delegated Management, or Authorised Management.

The Device Application may be used to trigger the LPR and may receive status regarding the information exchanged between the Management Platform and the eUICC.

The LPA Proxy MAY be implemented partially outside the LPA.

4.17.2 LPR Procedures

The figure below shows the expected behavior of the LPR and its involvement in the end to end processes. In addition, it highlights the optional use of a Delegated Platform Identifier (DPI) during triggering that allows redirection to a Delegated Profile Content Management Platform. The following management modes SHALL be supported: Simple Mode, Delegated Management, or Authorised Management.

Three methods may trigger the connection request from the LPA to the Profile Content Management Platform

- An automatic triggering after the enabling of a Profile (this mode is configured in the Profile to be activated or not activated)
- An RPM command sent from a SM-DP+ to the LPA
- A specific API command sent from a Device Application to the LPA

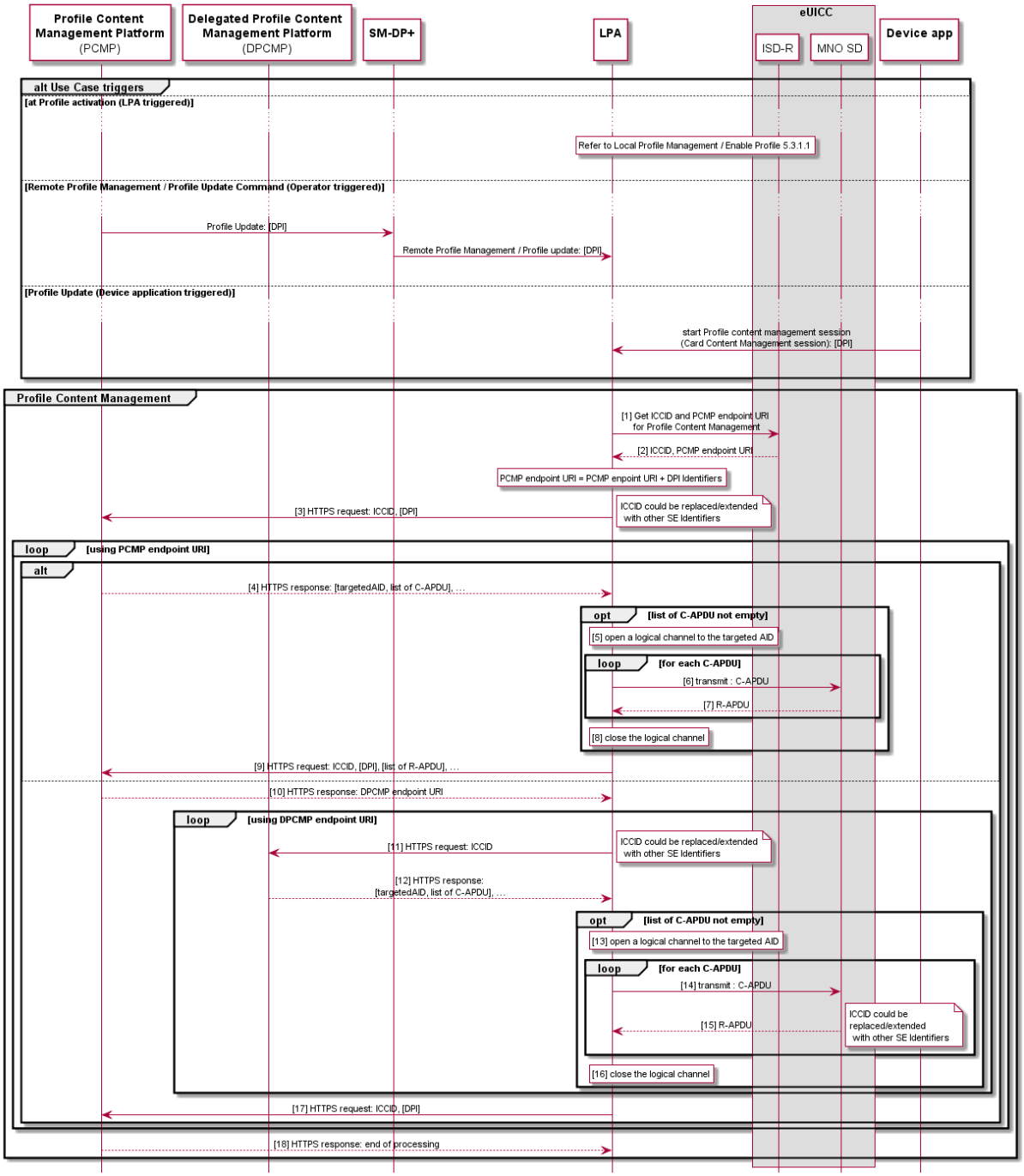

Figure 19: LPA Proxy Procedure

Start Conditions:

a. A Profile which requests the automatic trigger of the LPR procedure is enabled; an optional parameter DPI may be attached to this request to signify an expected connection to a Delegated PCMP.
OR

b. A RPM Profile update command which triggers the LPR procedure is received from the SM-DP+; an optional parameter DPI may be attached to this request to signify an expected connection to a Delegated PCMP.

OR

c. A specific API command sent from a Device Application to the LPA to trigger the LPR procedure to initiate a Profile content management session (Card Content Management Session); an optional parameter DPI may be attached to this request to signify an expected connection to a Delegated PCMP.

Procedure:

1. The LPR requests the ICCID and the PCMP endpoint URI associated to the Profile Content Management Platform from the eUICC.
2. The eUICC sends the ICCID of the Enabled Profile and the PCMP address to the LPR.
3. The LPR connects to the PCMP, with the DPI as a parameter if provided during the initialisation of the LPR Procedure. This step is followed by step 4 (sending the lists of C-APDU from the PCMP) or 10 (sending the URI of a Delegated PCMP) or 18 (end of processing).

Note: Steps 4 to 9 MAY be skipped if the PCMP requests a redirection to the DPCMP

4. The PCMP provides a list of Command APDUs (C-APDUs) and the AID of the targeted application of the Enabled Profile.
5. The LPR opens a logical channel to the AID of the targeted application of the Enabled Profile.
6. The LPR transmits the list of C-APDUs to the targeted application of the Enabled Profile within the MNO-SD.
7. The targeted application sends back the list of Response APDU (R-APDU) to the LPR.
8. The LPR closes the logical channel.
9. The LPR sends the list of R-APDUs to the PCMP, and in addition, the DPI parameter if provided during the LPR procedure initialisation request. Additionally, this step is equivalent to step 3: the LPR connects to the PCMP, with the DPI as a parameter, if provided during the initialisation of the LPR procedure.
   This step is followed by step 4 (sending a new list of C-APDUs from the PCMP) or 10 (sending the URI of a Delegated PCMP) or 18 (end of processing).

Note: Steps 10 to 17 MAY be skipped if the DPI parameter is not provided during the LPR procedure initialisation request.

10. The PCMP provides the address of the DPCMP to the LPR to initialise the redirection.
11. The LPR connects to the DPCMP address.
12. The DPCMP provides a list of Command APDUs (C-APDUs) and the AID of the targeted application of the Enabled Profile.
13. The LPR opens a logical channel to the AID of the targeted application of the Enabled Profile.

14. The LPR transmits the list of C-APDUs to the targeted application of the Enabled Profile within the MNO-SD
15. The targeted application sends back the list of Response APDUs (R-APDUs) to the LPR.
16. The LPR closes the logical channel,
17. This step is equivalent to step 3: The LPR connects to the PCMP, with the DPI as a parameter if provided during the initialisation of the LPR Procedure.
    This step is followed by step 4 (sending the lists of C-APDU from the PCMP) or 10 (sending the URI of a Delegated PCMP) or 18 (end of processing).

Note: Step 18 is used by the PCMP to end the processing

18. The PCMP sends an acknowledgement to the LPR about the end of processing.

Note: When initialising the connection between the LPR and the PCMP or the DPCMP, a HTTPs session SHALL be established between the LPR and respectively the PCMP and DPCMP based on a public key of the Root Certificate stored in the Device which includes authentication using the TLS Certificate, and may check for the presence of the adequate platform identifier in the TLS Certificate used for the TLS session.

End Condition:

a. The contents of the Enabled Profile have been updated according to updates received from either the PCMP, the DPCMP or both.

The following flow highlights the specific use of Notifications sent from the LPR to a specific Device Application(s). These Notifications can be used to inform the End User about the progress of the Profile management process.

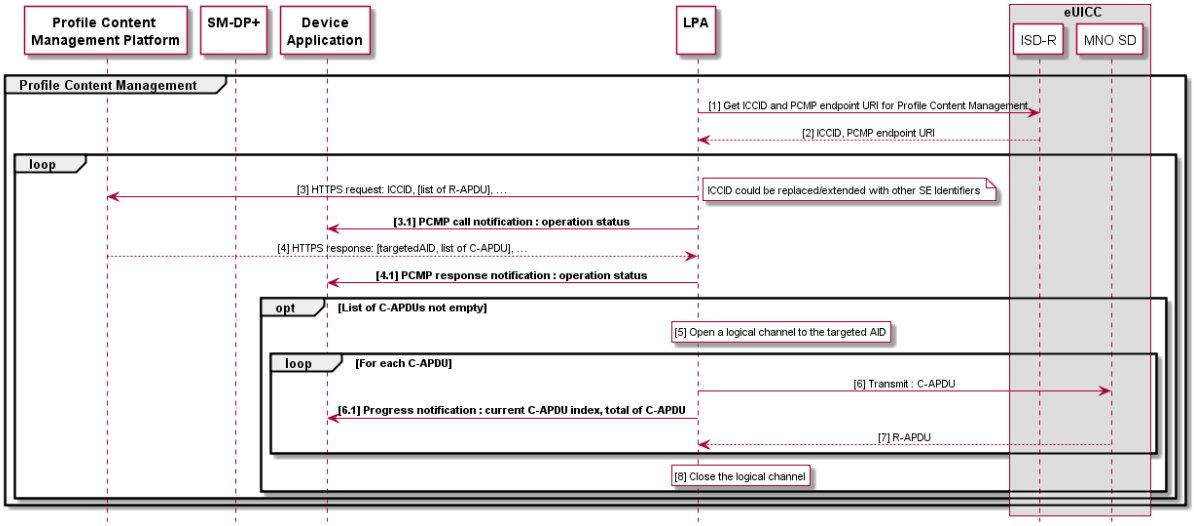

Figure 20: Device Application Interaction with a LPA PRoxy

Start Conditions:

a. One of the triggers to start a connection between a (D)PCMP and the eUICC has been initiated.
b. A Device Application has been registered to receive Notifications during the Profile content management session.

Procedure:

1. The LPR requests the ICCID and the (D)PCMP endpoint URI associated to the Profile Content Management Platform from the eUICC.
2. The eUICC sends the ICCID of the Enabled Profile and the (D)PCMP address to the LPR.
3. The LPR connects to the (D)PCMP.

3.1 The LPR sends a Notification about the operation status to the registered Device Application.

4. The (D)PCMP provides a list of Command APDUs (C-APDUs) and the AID of the targeted application of the Enabled Profile.

4.1 The LPR sends a Notification about the operation status to the registered Device Application

5. The LPR opens a logical channel to the AID of the targeted application of the Enabled Profile.
6. The LPR transmits the list of C-APDUs to the targeted application of the Enabled Profile within the MNO-SD.

6.1 The LPR sends a Notification about the operation status to the registered Device Application

7. The targeted application sends back the list of Response APDU (R-APDU) to the LPR.
8. The LPR closes the logical channel.

End Condition:

c. The application of the Enabled Profile has been updated according to updates received from the (D)PCMP. The Device Application has been notified during the procedure execution.

4.17.3 LPA PRoxy Requirements

Req no.	Description
LPAPR1	It is OPTIONAL for the Device, the eUICC, and the SM-DP+ to support the LPA Proxy requirements defined in this document.
LPAPR2	The LPR SHALL be able to forward APDUs remotely sent from a Profile Content Management Platform or from a Delegated Profile Content Management Platform to any application on the Enabled Profile. Note: The mechanism cannot address a Disabled Profile
LPAPR3	A mechanism allowing the LPR to connect to a Profile Content Management Platform address, each time the Profile is Enabled, SHALL

Req no.	Description
	exist. This mechanism SHALL be executed on a best effort basis and SHALL NOT impact otherwise the pending RSP operations.
LPAPR4	The DPI used for redirection from a PCMP to a DPCMP, SHALL be able to be included in the Profile.
LPAPR5	The Profile Content Management Platform address and the configuration (LPAPR3/deactivated) of the mechanism described in LPAPR3 SHALL be included in the Profile.
LPAPR6	The mechanism described in LPAPR3 SHALL be activated/deactivated by the Profile Owner.
LPAPR7	It SHALL be possible for the PCMP to request redirects to some Delegated Profile Content Management Platform(s). A redirection MAY happen at any point of time during the data exchange between the PCMP and the LPR. The PCMP internal routing logic MAY use the DPI parameter, if provided, the ICCID and any other contextual data.
LPAPR8	The identifier parameter for the routing to a Delegated Profile Content Management Platform, called the DPI, SHALL be globally unique.
LPAPR9	The protocol used between the LPR and its Profile Content Management Platform SHALL be able to transport all types of SCP designed to address the Enabled Profile through logical channels. E.g. this may include SCP03 [29] and SCP11 [30].
LPAPR10	When triggered, the LPR SHALL connect to the PCMP address retrieved from the Enabled Profile. If the triggering method includes a DPI as a parameter, this parameter SHALL be added to the PCMP address. If a DPI parameter is filled in the Enabled Profile, this parameter SHALL also be added to the PCMP address.
LPAPR11	The capability to use mobile network data for the LPA Proxy MAY be enabled/disabled by the End User. The Default state SHALL be ‘enabled’.
LPAPR12	The Device SHALL provide a means to Device Application to interact with LPA Proxy through this API. The requirements about this API are detailed in LPAPR13 to LPAPR17.
LPAPR13	The access to the LPA Proxy API by a Device Application SHALL be authorised by the Profile Owner of the Enabled Profile.
LPAPR14	The Device SHALL offer a means for Device Applications to detect whether the LPA Proxy is deployed on the Device or not.
LPAPR15	A triggering Device Application SHALL be able to register interest for receiving Notifications during the triggered session.
LPAPR16	The LPA Proxy SHALL be able to send Notifications to the triggering Device Application. These Notifications SHALL either • be contained in the command sequence retrieved from the Profile Content Management Platform (e.g. for task overview message, initialisation or end of the process) • or generated locally (e.g. error Notifications)

Req no.	Description
LPAPR17	The LPA SHOULD provide a mechanism to allow a Device Application to get progress or result information about an LPA Proxy operation which it requested through an API.

Table 42: LPA Proxy Requirements

4.18 Device Change Support

This section describes use cases and requirements for the Device Change support.

4.18.1 Overview

An End User subscribes to a mobile service with a Mobile Service Provider, and installs one or more Profiles in their Device. After a while when the End User needs to use their Subscriptions on another Device, they can perform a Device Change process in order to install one or more Profiles related to their Subscriptions in the new Device.

The underlying mechanism for the Device Change process is based upon the download of the Profiles from the SM-DP+(s) as in the general Profile download procedure. As such, the Mobile Service Providers may need to update their backend systems such as HSS/AuC and BSS with respect to the newly installed Profiles, where the details are out of scope of the specification.

4.18.2 Device Change Procedure

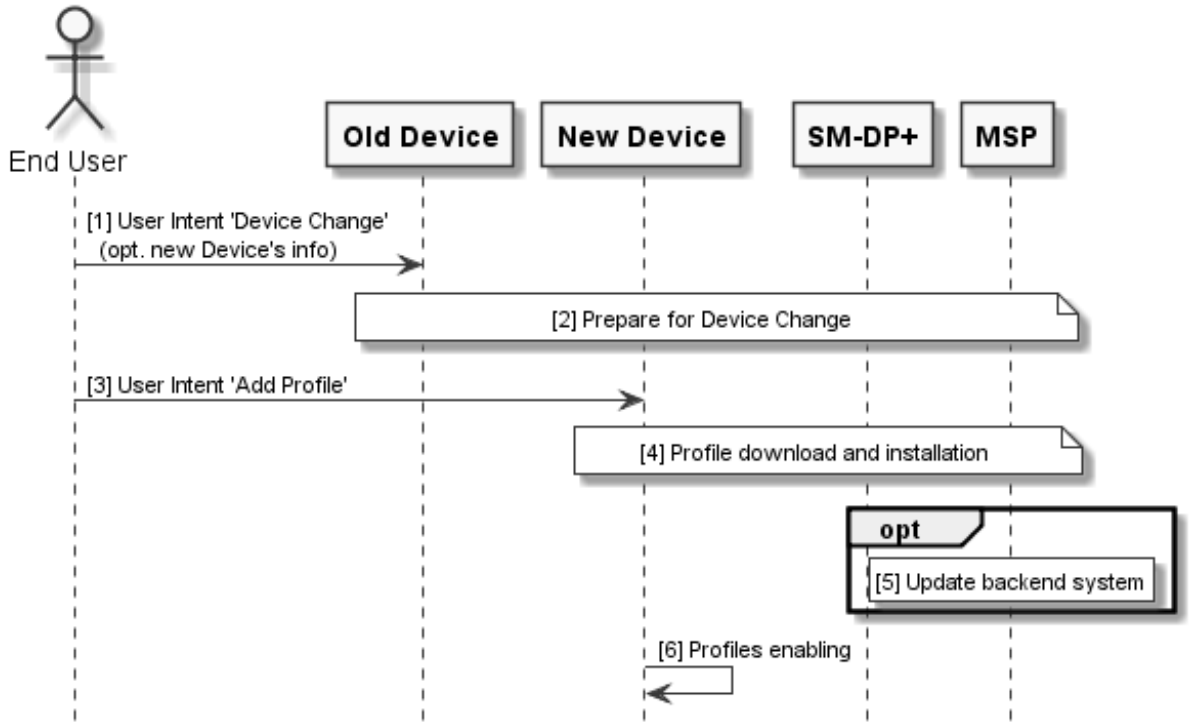

Figure 21: Device Change Procedure

Start Conditions:

a) The End User has an old Device containing one or more Profiles. The End User gets a new Device
b) The old Device still has connectivity.

Procedure:

1. The End User provides User Intent 'Device Change', indicates which Profiles they intend to move and optionally provides information (e.g. EID) of the new Device to the old Device.
2. The old Device prepares Device Change of the installed Profiles that the End User wants to move, and optionally deletes the installed Profiles based upon the Mobile Service Providers' configurations. This step can involve SM-DP+(s) and/or Mobile Service Providers servers. This may include an Eligibility Check for Device Change.
3. The End User provides User Intent 'Add Profile' to the new Device.
   Steps 4 to 5 are repeated for every Profile the End User wants to move in the new Device. If the installation of one of the Profile fails during the Device Change operation with more than one Profile, the End User has to confirm to continue the Device Change procedure with the other Profiles.
4. The new Device downloads and installs a Profile from the SM-DP+.
5. (Optional) The Mobile Service Provider updates the backend system such as HSS/AuC and BSS.
6. The Profiles can now be enabled using one of the mechanisms described in this specification.

4.18.3 Device Change Support Requirements

4.18.3.1 General Requirements

Req no.	Description
DC1	There SHALL be a means to ensure that the Profile prepared for the Device Change is only downloaded to the target Device/eUICC intended by the initiator (e.g. End User).
DC2	With regard to DC1, a Mobile Service Provider SHALL be able to enforce the means if it wants.

Table 43: General Device Change Support Requirements

4.18.3.2 LPA Requirements for the old Device

Req no.	Description
DC-LPA-X1	It is OPTIONAL for the LPA to support the Device Change requirements as defined in this section.
DC-LPA-X2	The LPA supporting Device Change SHALL support the Local Profile Management Operation 'Device Change'. This operation SHALL allow the End User to initiate Device Change for the selected Profile. Strong Confirmation SHALL be enforced.
DC-LPA-X3	The LPA supporting Device Change SHALL be able to request the Device Change to the SM-DP+ specified in the installed Profile.

Req no.	Description
	Note: This operation will be performed for every Profile that the End User wants to move.
DC-LPA-X4	With regard to DC-LPA-X3, the Device Change request SHALL identify the installed Profiles the End User wants to move.
DC-LPA-X5	The LPA supporting Device Change SHALL be able to process the Device Change response(s).
DC-LPA-X6	With regard to DC-LPA-X5, the LPA SHALL be able to provide the relevant information for the new Device to download the prepared Profile Package(s).
DC-LPA-X7	With regard to DC-LPA-X6, the LPA SHALL be able to provide the information via the LUI (e.g., in a text or QR code format). Additional mechanisms (e.g., via USB, Bluetooth, etc.) MAY be provided and are Device manufacturer specific.
DC-LPA-X8	If indicated by the SM-DP+ as per DC-SMDP-X8, if the deletion of an installed Profile is requested, the LPA SHALL delete this Profile. Strong Confirmation SHALL be enforced in such a case.
DC-LPA-X9	With regard to DC-LPA-X8 and DC-SMDP-X4, in consideration of the network connectivity lost due to the Profile deletion, there SHALL be a means for the LPA to deliver the Delete Notification of the deleted Profile to the SM-DP+ via the information provided to the new Device as per DC-LPA-X6.
DC-LPA-X10	The LPA SHOULD display the Mobile Service Provider Message, if it is included as per DC-SMDP-X9.
DC-LPA-X11	If the Profile has been deleted from the old Device as per DC-LPA-X8 and if it is allowed as per DC-SMDP-X10, the End User MAY request, via the LPA, the SM-DP+ to recover the deleted Profile on the old Device.
DC-LPA-X12	The LPA supporting Device Change SHALL be able to allow the End User to move one or more Profiles installed in the eUICC.

Table 44: LPA Requirements for the old Device

4.18.3.3 LPA Requirements for the new Device

Req no.	Description
DC-LPA-Y1	The LPA supporting Device Change SHALL be able to download the Profile prepared for the Device Change by using the information provided as per DC-LPA-X6.
DC-LPA-Y2	With respect to DC-LPA-X9, if the LPA is unable to immediately deliver the Delete Notification to the Notification Receivers, it SHALL be retained and sent before completing the Device Change procedure.
DC-LPA-Y3	If the installation of one Profile fails during the movement of more than one Profile from the old Device, the LPA SHOULD ask the End User if they want to continue the Device Change operation.

Table 45: LPA Requirements for the new Device

4.18.3.4 SM-DP+ Requirements

Req no.	Description
DC-SMDP-X1	It is OPTIONAL for the SM-DP+ to support the Device Change requirements as defined in this section.

Req no.	Description
DC-SMDP-X2	The SM-DP+ supporting Device Change SHALL be able to notify the Mobile Service Provider of the progress of the Device Change.
DC-SMDP-X3	On reception of the Device Change request, the SM-DP+ supporting Device Change SHALL be able to prepare a suitable Profile for the new Device.
DC-SMDP-X4	With regard to DC-SMDP-X3, if a Profile with the same Network Access Credentials is used, the SM-DP+ SHALL be able to ensure that the Profile in the old Device is deleted before the new Device downloads the prepared Profile Package.
DC-SMDP-X5	With regard to DC-SMDP-X3, if a Profile with the same Network Access Credentials is used, the SM-DP+ SHALL be able to ensure that the Profile in the old Device is deleted before the Profile in the new Device becomes usable.
DC-SMDP-X6	On reception of the Device Change request, the SM-DP+ SHALL respond with the processing result of the request on behalf of the Mobile Service Provider.
DC-SMDP-X7	With regard to DC-SMDP-X6, the response indicating success SHALL be able to provide information for the new Device to download the prepared Profile Package.
DC-SMDP-X8	With regard to DC-SMDP-X6, the response indicating success SHALL be able to indicate whether the old Device has to delete the Profile that was identified in the Device Change request.
DC-SMDP-X9	With regard to DC-SMDP-X6, the response indicating success SHALL be able to include a Mobile Service Provider Message to be displayed to the End User.
DC-SMDP-X10	With regard to DC-SMDP-X8, the response indicating that the old Device has to delete the Profile SHALL be able to additionally indicate whether the old Device is allowed to request the recovery of the deleted Profile, for the case where the Profile has been deleted but there is a permanent error in installing the prepared Profile on the new Device. NOTE: A permanent error indicates that Profile installation failed due to an error processing the prepared Profile in the eUICC except following temporary errors: • Insufficient memory for the Profile, or • Interruption during the Profile installation
DC-SMDP-X11	If the End User requests the recovery of the Profile on the old Device as per DC-LPA-X1 and if the SM-DP+ received a notification from the new Device indicating that there was a permanent error in installing the prepared Profile on the new Device, the SM-DP+ SHALL provide the old Device with a Profile for the recovery.

Table 46: SM-DP+ Requirements

5 Operational Procedures

5.1 LPA Initiated Download

5.1.1 LPA Initiated Download Requirements

Req no.	Description
LID1	[Void]
LID2	[Void]

Table 47: 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.

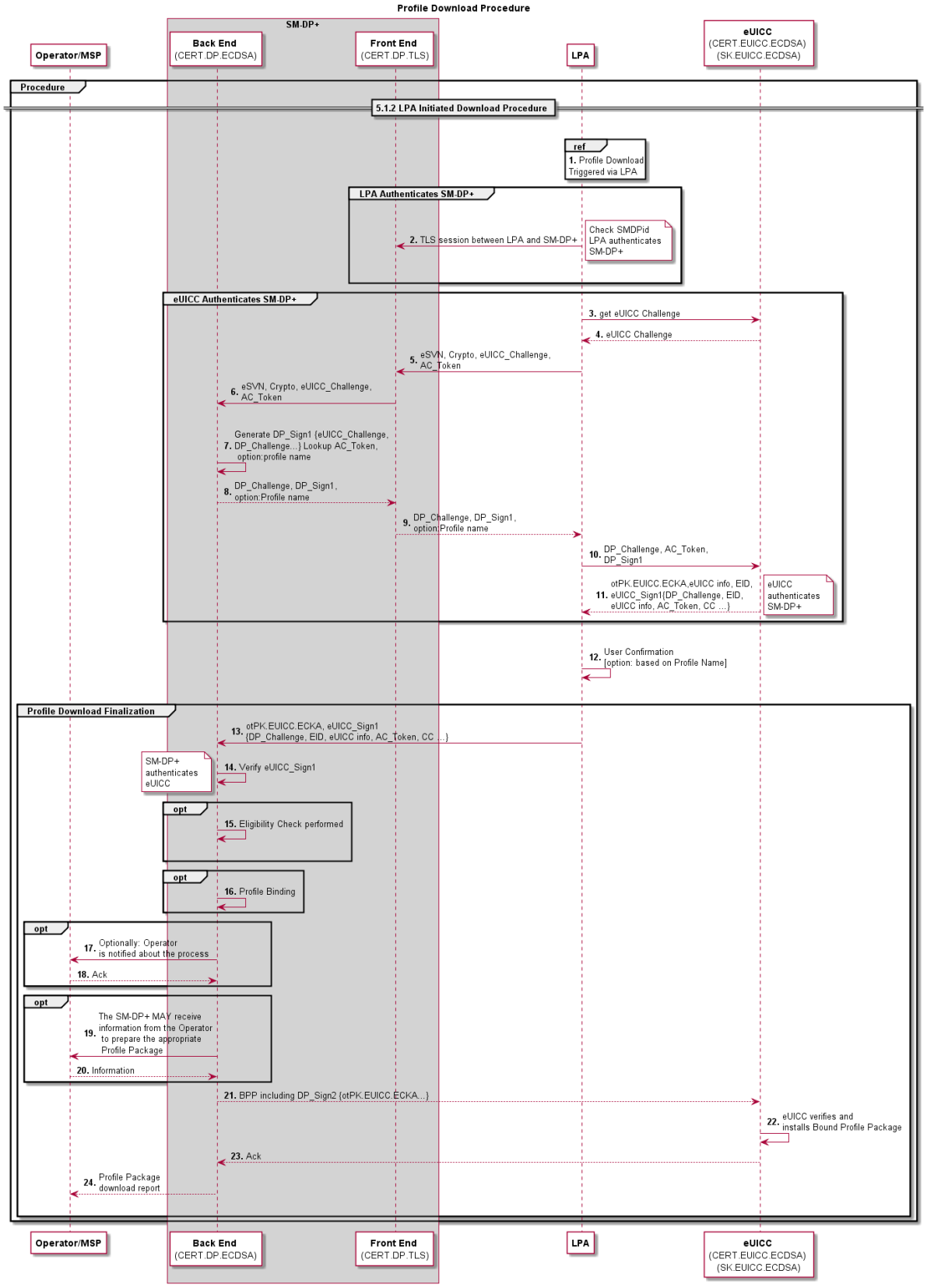

Figure 22: Profile Download Procedure

Start conditions:

a. The Subscriber has completed the Subscription process to the selected Mobile 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 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 Mobile Service Provider.
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 Eligibility Check and Profile binding functions are performed by the SM-DP+.

17. to 22. OPTIONAL

17. The Mobile Service Provider and Operator is notified about the Profile Package that is about to be downloaded.
18. If the Mobile Service Provider or Operator has been notified, it MAY request to stop the download process by indicating an error code to the SM-DP+.
19. If the Mobile Service Provider or 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 Mobile Service Provider and 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) • Reference to eSIM CA Certificate (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, if a camera is available on the Device, QR code scanning.
AC6	[Void]
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 SM-DP+. It SHALL be possible for the Activation Code to be uniquely linked to an individual Mobile Service Provider.
AC12	The Activation Code request to the SM-DP+ SHALL be extended by the eUICC with the EID after the specific SM-DP+ has been authenticated.

Table 48: 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.

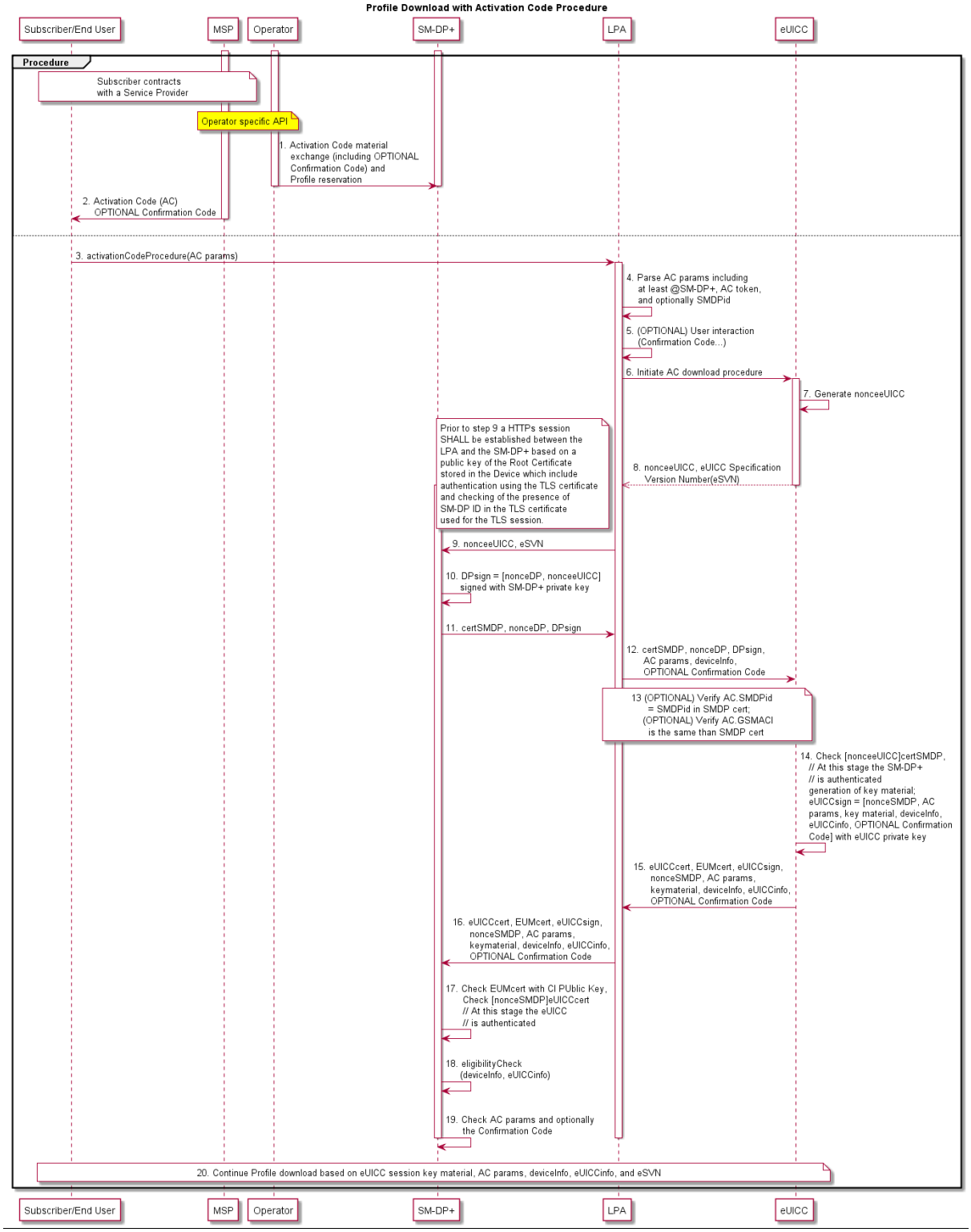

Figure 23: Profile Download with Activation Code Procedure

Start Conditions:

1. A Subscription has been established by the Subscriber.

2. 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 Mobile 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 step 9, 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 Check procedure and optionally the Confirmation Code and transmits them with the signed nonceeUICC and nonceSMDP to the eUICC.
13. If configured in the Activation Code, the eUICC and the LPA checks whether the SMDPid configured in the AC and the SMDPid within the SM-DP+ Certificate for the Profile installation (called CERT.DPauth in SGP.22 [24]) are the same (in case of failure, the download SHALL NOT proceed). If configured in the Activation Code, the eUICC and the LPA checks whether the eSIM CA Certificate, and the eSIM CA Certificate linked with the SM-DP+ for the Profile installation (called CERT.DPauth in SGP.22 [24]) are the same (in case of failure, the download SHALL NOT proceed).
14. The eUICC checks the signature attached to the nonceeUICC. 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
15. 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
16. The LPA sends the whole set of information received from the eUICC to the SM-DP+.
17. 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+.
18. The SM-DP+ proceeds with the eligibility check based on the transmitted information (EID, Device information, eUICC information, eSVN).
19. The SM-DP+ checks the Activation Code parameters and optionally the Confirmation Code to retrieve the referenced Profile Package.
20. 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 Mobile Service Provider and 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.

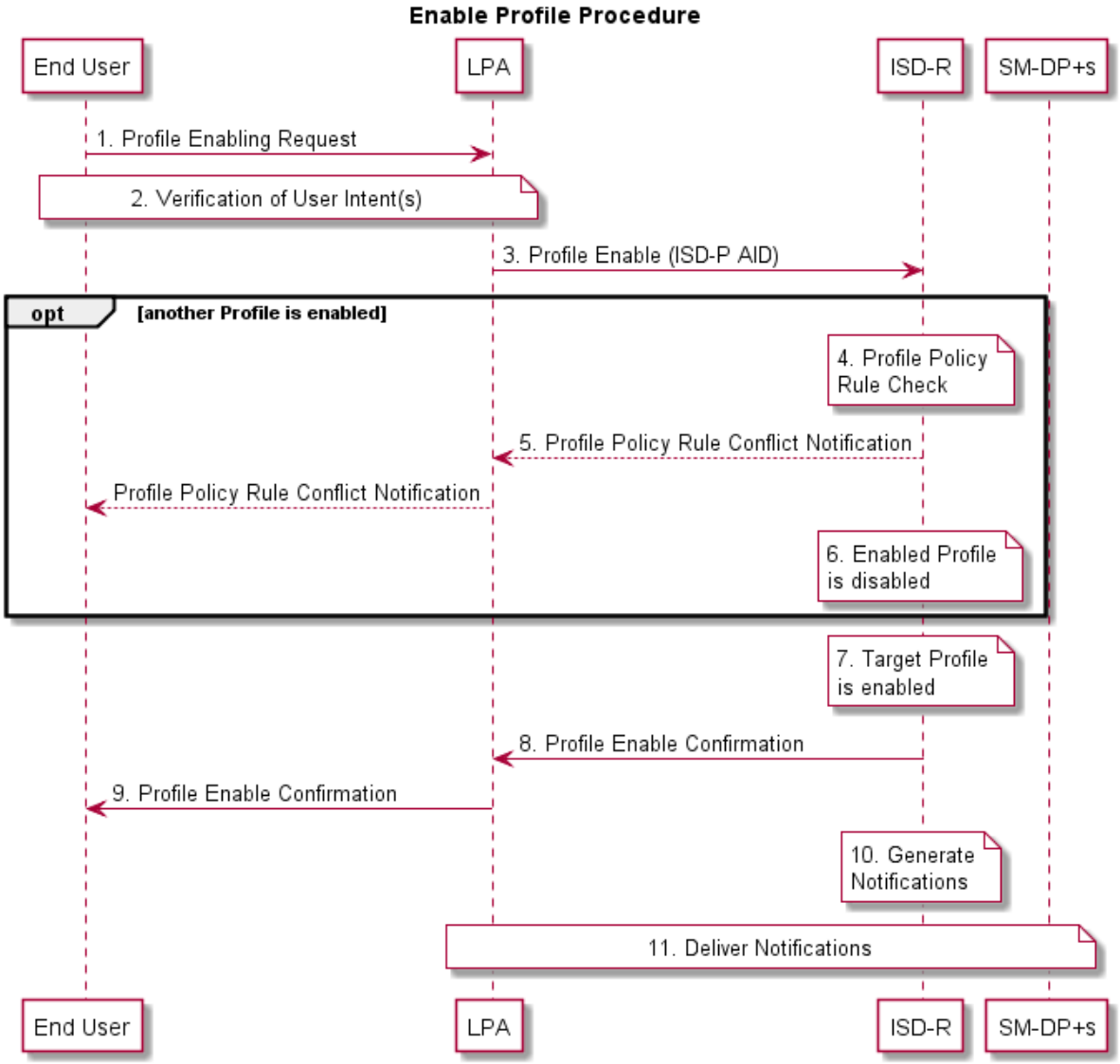

Figure 24: Enable Profile Procedure

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.

   If another Profile is currently enabled, then steps 4 through 6 are performed; otherwise, execution of the procedure continues at step 7.

4. The ISD-R checks if applied Profile Policy Rules on the currently Enabled Profile permit 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 currently Enabled Profile is disabled
7. The target Profile is enabled.
8. The ISD-R informs the LPA of the enabling of the Profile.
9. The End User is informed via the LPA.
10. The ISD-R generates and stores enable Notifications for all Notification Receivers configured in the Profile Metadata of the target Profile. If this procedure caused another Profile to be disabled, then the ISD-R also generates and stores disable Notifications for all Notification Receivers configured in that Profile.
11. All enable and disable Notifications on the eUICC are delivered.

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.

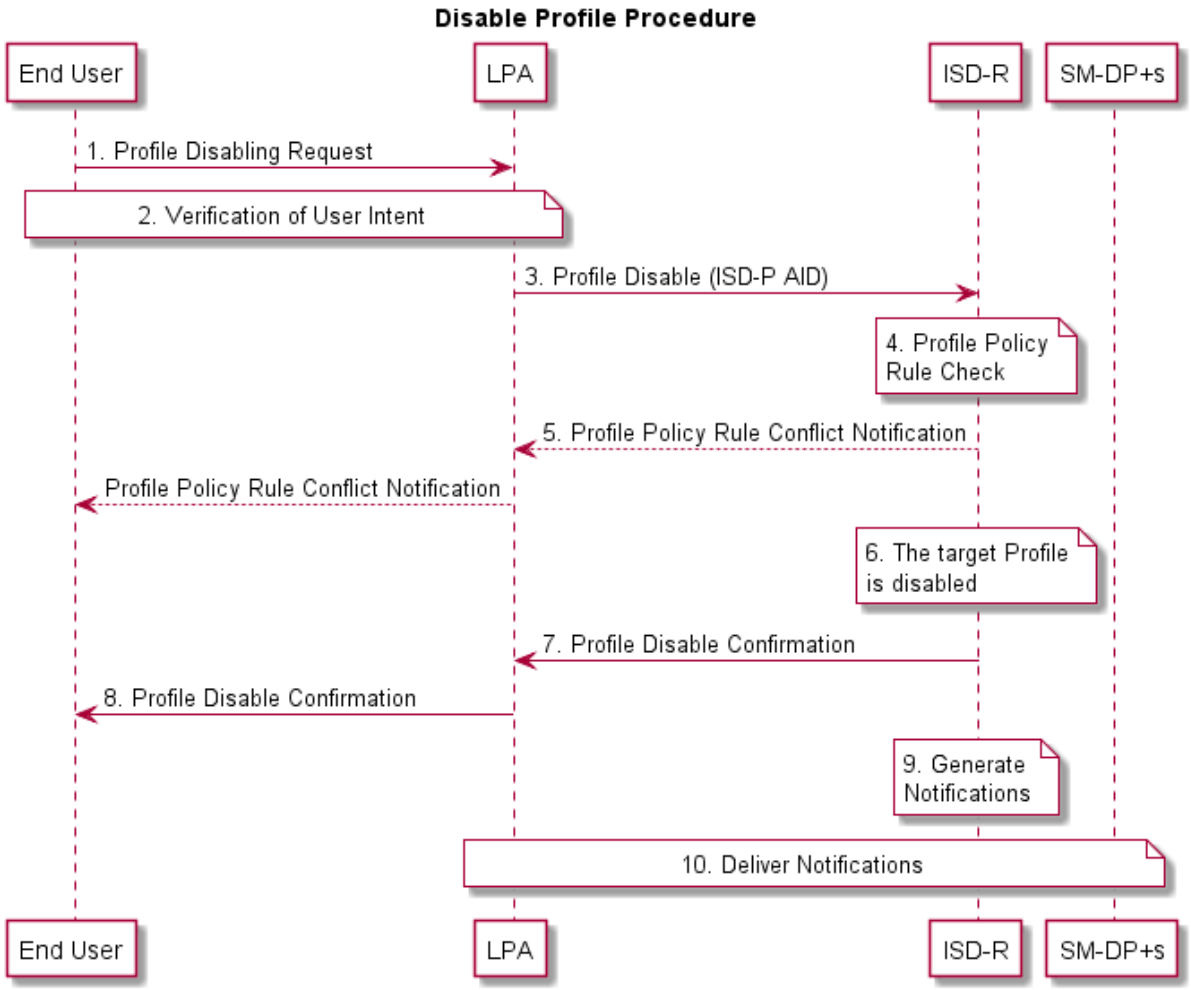

Figure 25: Disable Profile Procedure

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.
9. The ISD-R generates and stores disable Notifications for all Notification Receivers configured in the Profile Metadata.
10. All disable Notifications on the eUICC are delivered.

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.

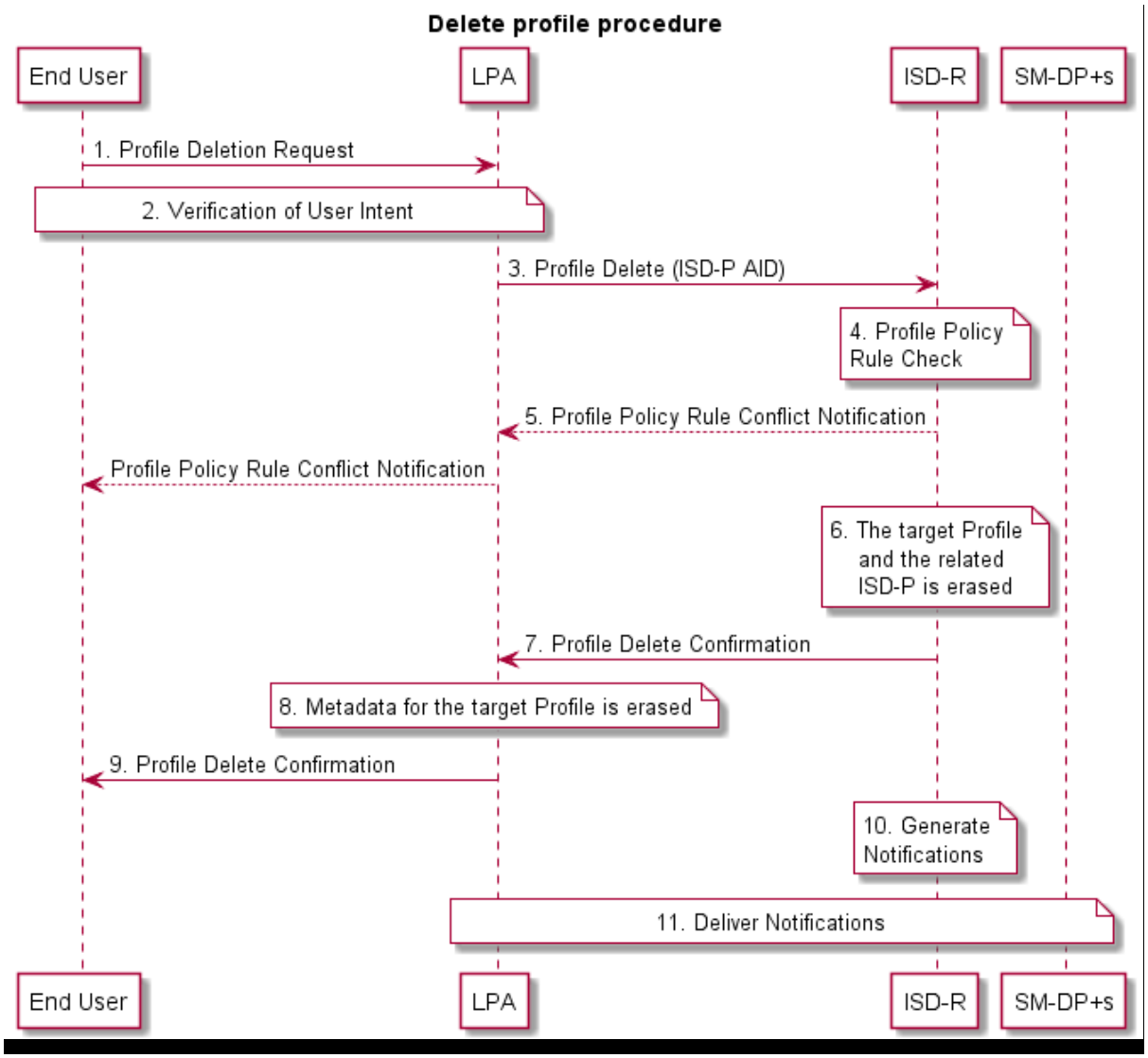

Figure 26: Delete Profile Procedure

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 ISD-R generates and stores delete Notifications for all Notification Receivers configured in the Profile Metadata.
11. All delete Notifications on the eUICC are delivered.

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.

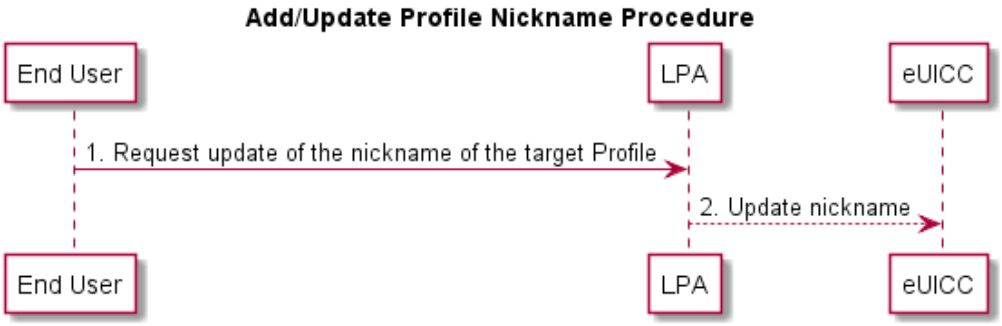

Figure 27: Add/Update Profile Nickname Procedure

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.

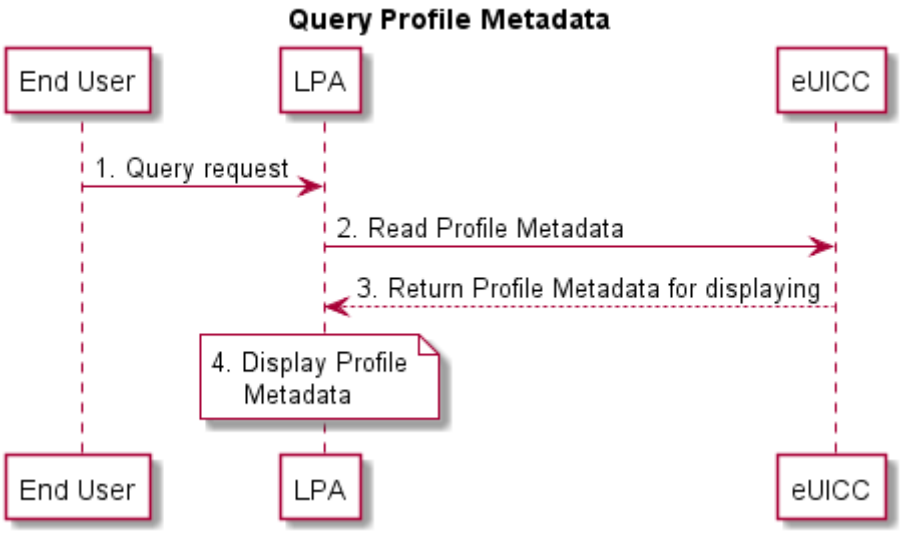

Figure 28: Query Profile Metadata Procedure

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**.**

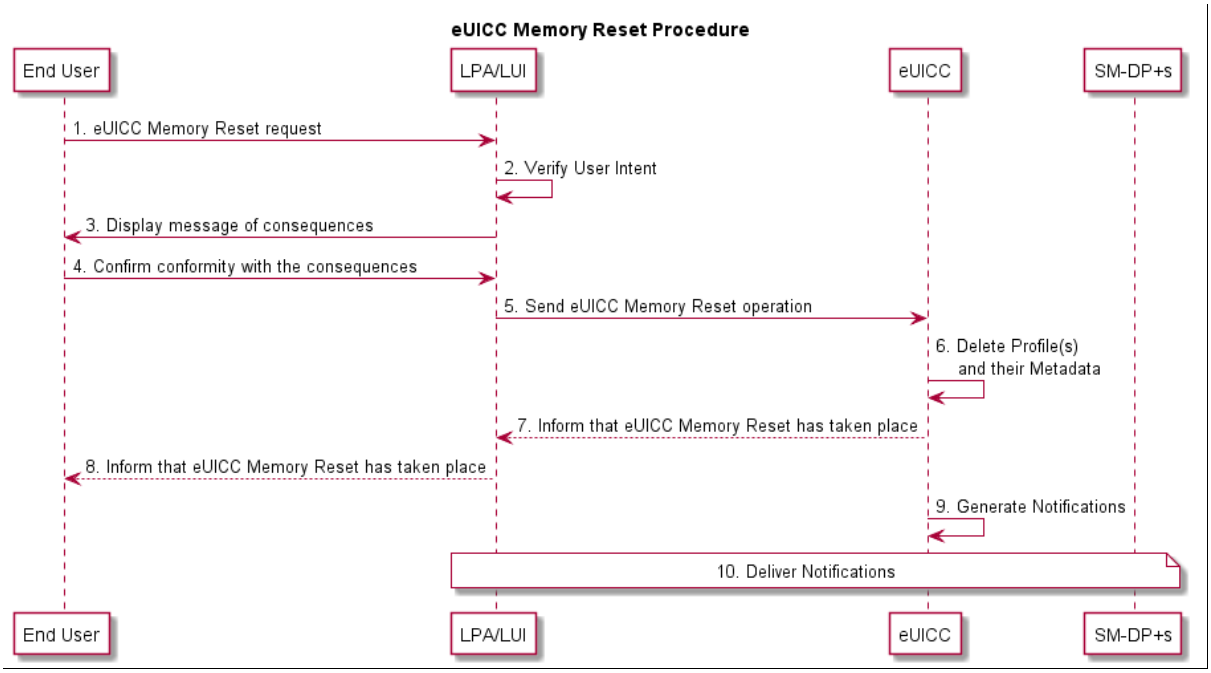

Figure 29: eUICC Memory Reset Procedure

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 Profiles on the eUICC even if one 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 eUICC generates and stores delete Notifications for all Notification Receivers configured in the Profile Metadata of every Profile.
10. All of the delete Notifications on the eUICC are delivered as soon as connectivity is available.

End conditions:

a. The Profiles are 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.

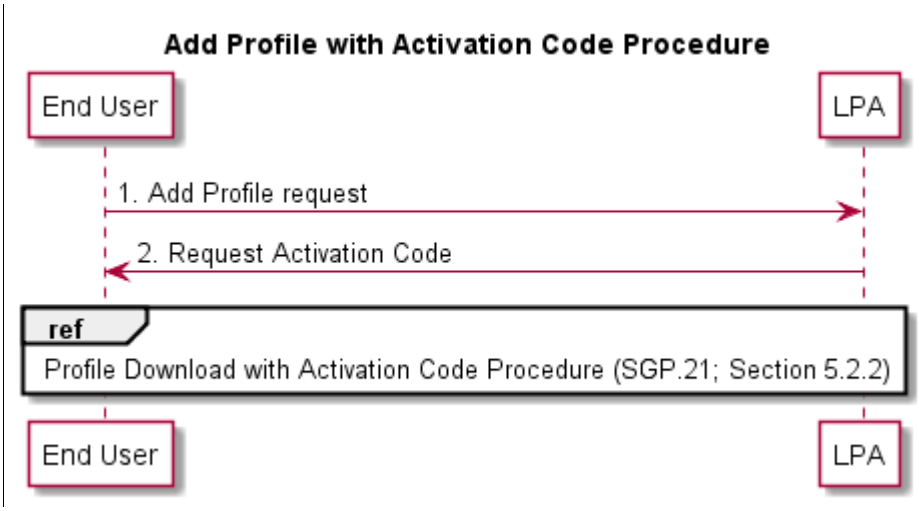

Figure 30: Add Profile with Activation Code Procedure

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 the eUICC or Device.

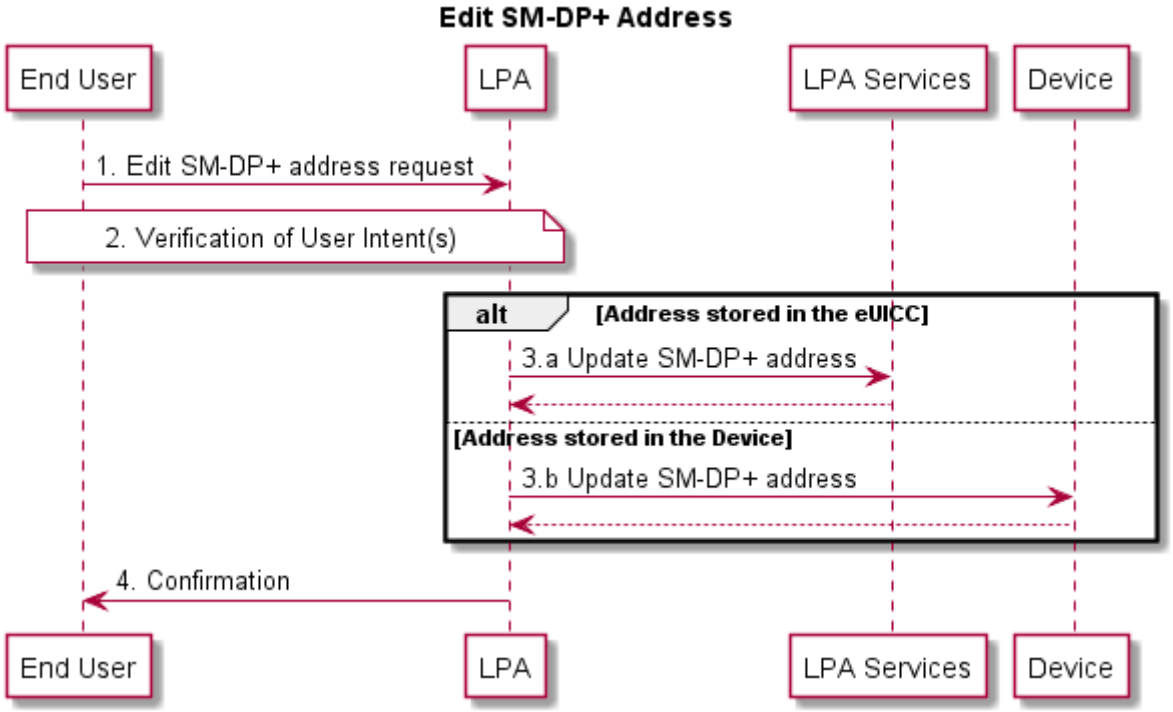

Figure 31: Edit SM-DP+ Address

Start conditions:

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

Procedure:

1. The End User edits an SM-DP+ Address via the LPA.
2. Simple Confirmation from the End User is required.
3. Depending on the storage location of the selected SM-DP+ Address:
   a. If the address is stored in the eUICC, the LPA sends the default SM-DP+ address for storage in the LPA Services.
   b. If the address is stored in the Device, the LPA updates the default SM-DP+ address for storage in the Device.
4. The End User is informed via the LPA.

End conditions:

c. The target default SM-DP+ Address is edited in the LPA Services or the Device.

5.4 Remote Profile Management

This section describes the overall mechanisms, requirements and flow diagrams for Remote Profile Management operations. Remote Profile Management operations are actions performed by Managing SM-DP+(s) at the request of the Profile Owner. These operations include enabling, disabling, and deleting Profiles as well as listing Profile information and

updating specific Profile Metadata. Profile Owners will also be able to update the list of Managing SM-DP+(s) that are authorised to perform Remote Profile Management operations.

5.4.1 Overview on RPM commands retrieval

Different mechanisms are defined to retrieve the RPM commands:

Option 1: The Root SM-DS is reached.

Option 2: An Alternative SM-DS is reached.

Option 3: One Managing SM-DP+ configured in the Profile is reached.

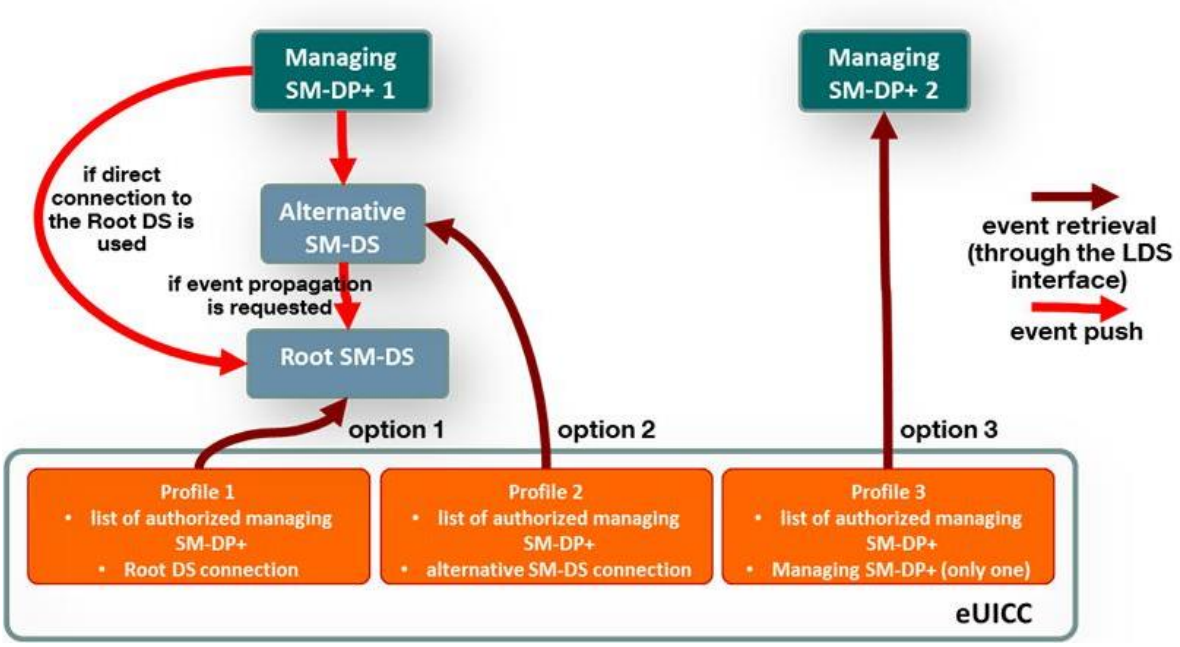

Figure 32: The different options to achieve RPM command retrieval

5.4.2 Remote Profile Management Requirements

Req no.	Description
RPM1	It is OPTIONAL for the Device, the eUICC, and the SM-DP+ to support the RPM requirements defined in this document.
RPM2	The Profile SHALL be able to include information of zero, one or several Managing SM-DP+(s) (META19) that are authorised to perform RPM operations on the Profile.
RPM3	Only the Profile Owner, or another Profile Owner explicitly pre-authorised, SHALL be able to request the SM-DP+ to perform RPM operations for this specific Profile.
RPM4	The eUICC SHALL only accept RPM operations on a Profile from a Managing SM-DP+ configured in the Profile.
RPM5	A Profile Owner SHALL be able to replace, add and remove Managing SM-DP+(s) to/from its Profile.

Req no.	Description
RPM6	RPM SHALL support the Profile Management operations ‘enable’, ‘delete’, ‘list Profile information’, ‘disable’, ‘update Metadata’, ‘Contact PCMP’, and unset Profile Policy Rules.
RPM7	The RPM ‘Enable’ command SHALL only be executed if the Profile can be enabled without implicitly disabling a currently Enabled Profile. (See RPM13 for chaining an RPM ‘Disable’ and an RPM ‘Enable’ command.)
RPM8	With regard to RPM7, if an RPM 'Enable' command is issued to an MEP-Capable Device, the LPA MAY provide the eUICC with information which of the available Logical Interface(s) to be used for executing the RPM 'Enable'.
RPM9	RPM operations SHALL be applicable to Enabled as well as Disabled Profiles, with the exception of RPM operation ‘Delete’ which only applies to Disabled Profiles and RPM operation ‘Contact PCMP’ which only applies to Enabled Profiles.
RPM10	The execution of an RPM operation SHALL at least require the following level of End User confirmation: • No user confirmation: List Profile Information, Update Metadata, unset Profile Policy Rules, Contact PCMP • Simple Confirmation: Disable Profile, Enable Profile • Strong Confirmation: Delete Profile Note: It is up to the Device to inform the End User about the consequences of deleting a Profile.
RPM11	It SHALL be possible to store and configure a Polling Address in each Profile to check for RPM operations. The Polling Address, if configured, SHALL be one of the following: • A reference to a Root SM-DS • A single Managing SM-DP+ configured in this Profile • An Alternative SM-DS
RPM12	The eUICC SHALL support operations for an Operator to list Profile(s) information on the eUICC. The following parameter SHALL be returned: List of own Profiles including state and Profile Metadata
RPM13	A mechanism SHALL be supported to allow the execution of a set of RPM operations together originating from a single Managing SM-DP+, with a particular ordering of the RPM operations attached to this set of operations. E.g. a set of RPM operations constituted by an RPM disable operation followed by an RPM delete operation or an RPM disable operation followed by an RPM enable operation.
RPM14	If the mechanism in RPM13**RPM18** is used, the set of RPM operations SHALL NOT start before the complete reception of the set of RPM operations.
RPM15	There SHALL be a mechanism to configure the continuation upon the result of each operation in the set of RPM operations.

Req no.	Description
RPM16	Remote Profile Management operations ‘enable’, ‘disable’, and ‘delete’ and ‘unset Profile Policy Rules’ 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
RPM17	The eUICC SHALL support the operation ‘update Metadata’ to update Profile Metadata via a Managing SM-DP+ on request of the Profile Owner. Only the Profile Metadata listed in META13 SHALL be able to be modified. The content of the respective Profile SHALL reflect the updated Metadata.
RPM18	The Profile Owner SHALL be able to configure, per RPM operation, any Managing SM-DP+ configured in the Profile as authorised to execute that operation. Note: e.g. If the Profile Owner configures an Enterprise SM-DP+ as a Managing SM-DP+, then the Enterprise can perform the authorised RPM operations.
RPM19	The mechanism RPM18 SHALL be able to be configured within the setting of the Profile Package or after the issuance of the Profile through the ES6 interface (Operator-eUICC interface).
RPM20	RPM SHALL support a command ‘Contact PCMP’ sent from a Managing SM-DP+ to the LPA to initiate a connection to the Profile Content Management Platform address configured in the Enabled Profile.
RPM21	While the LPR is executing an RPM command as identified in RPM20, the LPA SHALL suspend any other RPM commands until the proxy session is complete.
RPM22	The RPM command described in RPM20 SHALL be able to configure a DPI to request a redirection to a Delegated Profile Content Management Platform
RPM23	RPM SHALL be authorised only by the Profile Owner. This MAY be at the request of another party (e.g., MVNO, enterprise, etc.).

Table 49: Remote Profile Management Requirements

5.4.3 Remote Profile Management Procedures (Informative)

5.4.3.1 Common RPM Procedure - Command Independent

The following sequence diagram shows the common part of the overall RPM procedure. The sequence is focused on pure functional requirements and intentionally leaves out technical aspects like security and authentication. Security measures are assumed for any communication as required - these should be incorporated during technical elaboration as a cross-cutting concern.

For the avoidance of doubt, Notifications and Policy rules also apply to Remote Profile Management operations.

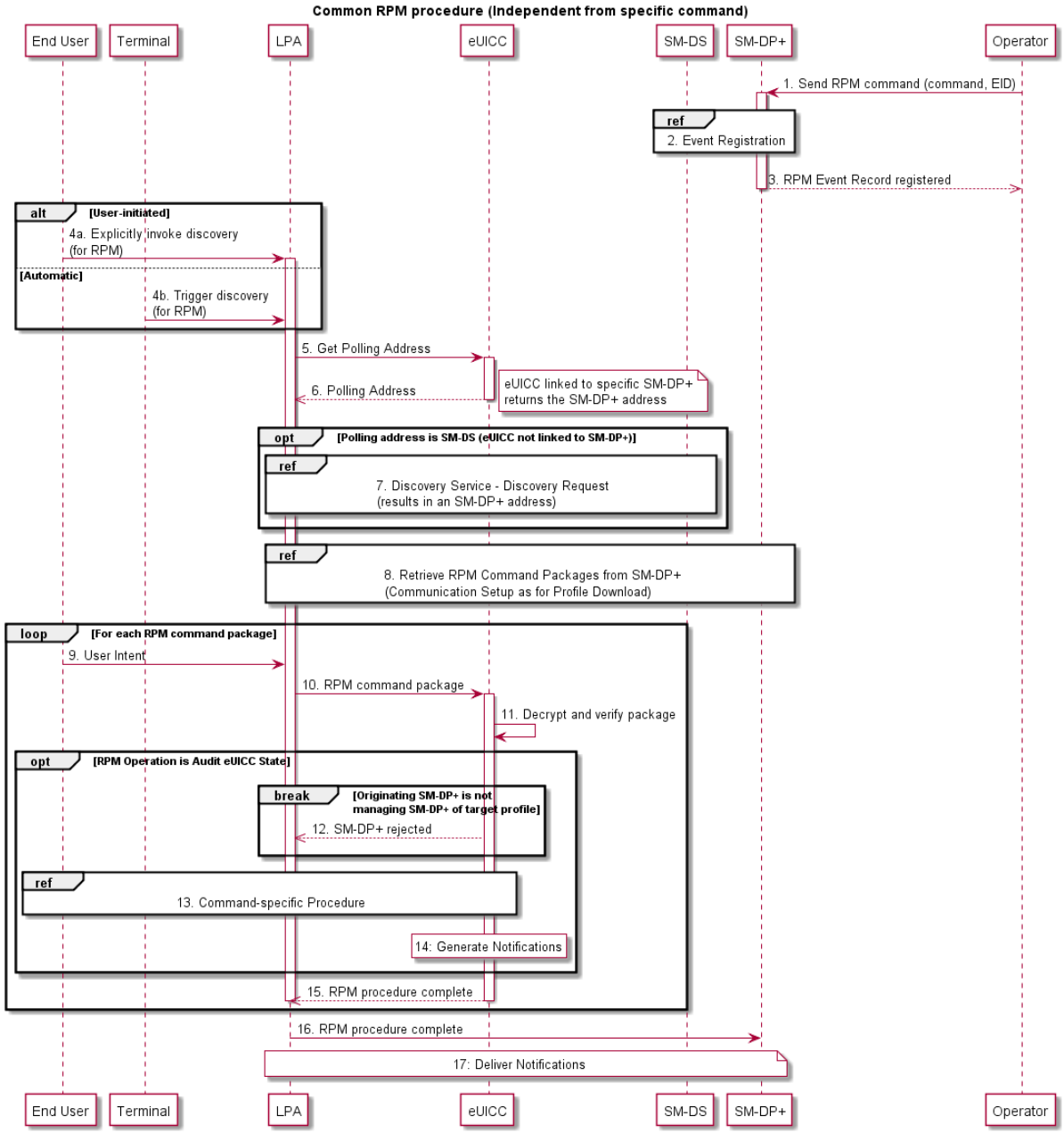

Figure 33: Common RPM Procedure

Procedure:

1. The Operator sends the RPM command to the connected SM-DP+.
2. The SM-DP+ registers the Event Record on the SM-DS to be retrieved by the LDS.
3. The SM-DP+ informs the Operator that the RPM Event Record has been registered on the SM-DS.

4a. With Discovery Service (SM-DS): An End User triggered request via the LPA to establish if there is an Event Record for RPM waiting on an SM-DS.

Without Discovery Service: An End User triggered request via the LPA to establish if there is an Event for RPM waiting on an SM-DP+.

4b. Alternatively, it can be started on specific events detected by the Device

5. The LPA requests a Polling Address for pending operations from the eUICC.
6. The Polling Address is sent from the eUICC to the LPA.
7. The LPA sends a query with its EID to the Polling Address. If the contacted peer is an SM-DS, the SM-DS returns the Event-ID for that EID.
8. The SM-DP+ looks up the pending operations for the specific EID, and sends them to the LPA.
   For each received package, the LPA SHALL do the following:
9. Based upon the operation type the LPA obtains the appropriate level of End User confirmation.
10. The LPA then sends the received RPM command package to the eUICC.
11. The package is decrypted and verified by the eUICC.
12. The eUICC verifies whether the command package originates from one of the target Profile's Managing SM-DP+s.
13. The command is executed according to its operation-specific sequence (see sections 5.4.3.2, 5.4.3.3, 5.4.3.4, 5.4.3.5, 5.4.3.6, 5.4.3.7).
14. For each command, the eUICC generates and stores Notifications for all configured Notification Receivers for the command.
15. The eUICC informs the LPA that the RPM procedure is complete and if appropriate the response information.
16. The LPA informs the SM-DP+ that the RPM procedure is complete and if appropriate the response information.
17. All pending Notifications on the eUICC are delivered.

5.4.3.2 RPM Operation: Enable Profile

The command "Enable Profile" results in an Enabled (active) Profile comparable to the insertion of a removable SIM card. Prior to execution of this command by the eUICC, a check is performed to ensure that no Profile from another Mobile Service Provider is currently enabled.

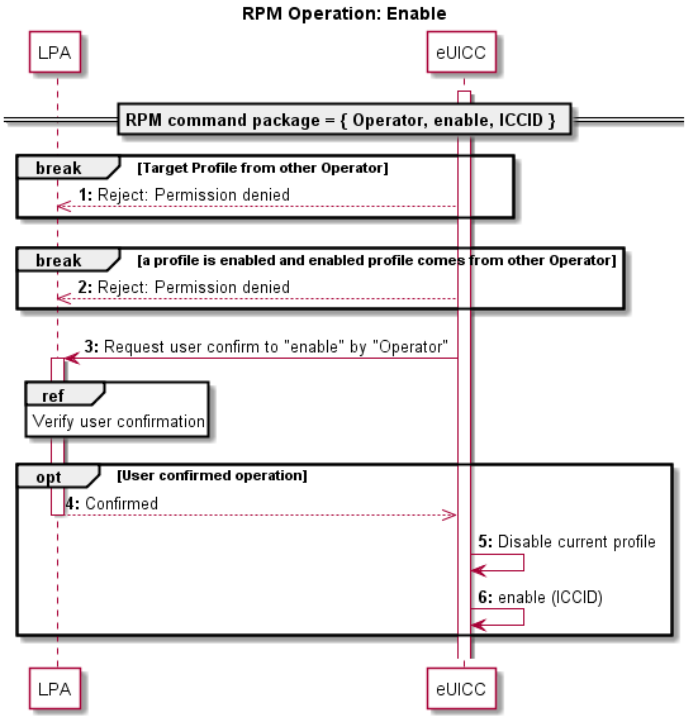

Figure 34: RPM Operation – Enable Profile

5.4.3.3 RPM Operation: Disable Profile

The command “Disable Profile” results in a Disabled (inactive) Profile comparable to the removal of a removable SIM card.

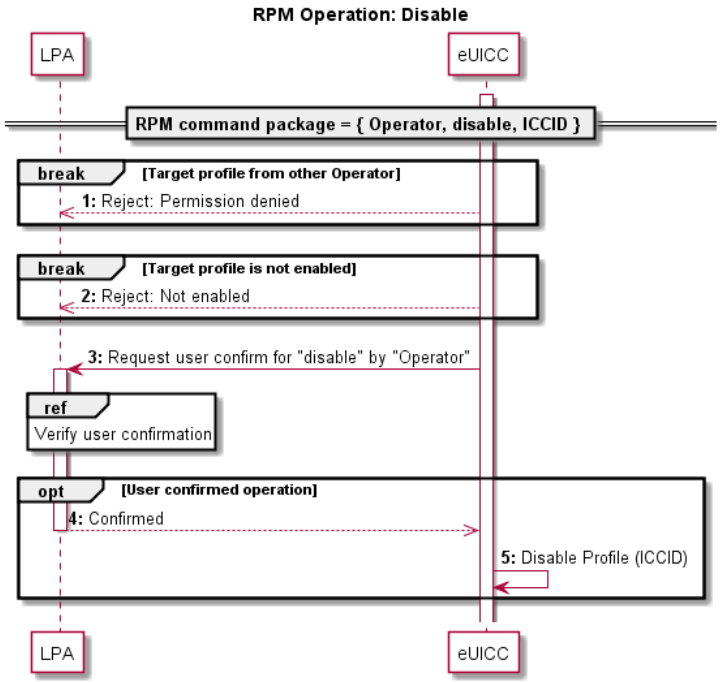

Figure 35: RPM Operation – Disable Profile

5.4.3.4 RPM Operation: Delete Profile

The command “Delete Profile” results in the deletion/removal of a Disabled Profile comparable to the destruction of a removable SIM card.

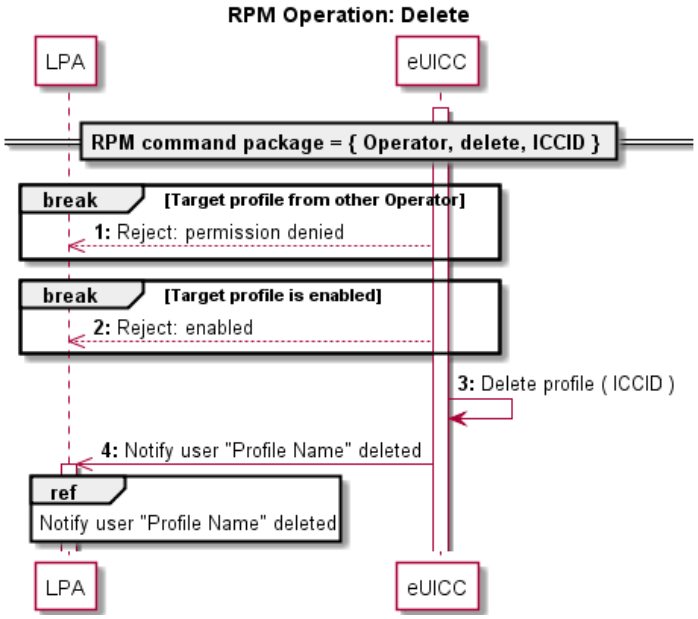

Figure 36: RPM Operation – Delete Profile

5.4.3.5 RPM Operation: List Profile Information

The command "List Profile Information" returns a list of Profiles owned by the Operator/Mobile Service Provider including state and Profile Metadata to the Managing SM-DP+ that issued the command. This command does not require local End User confirmation.

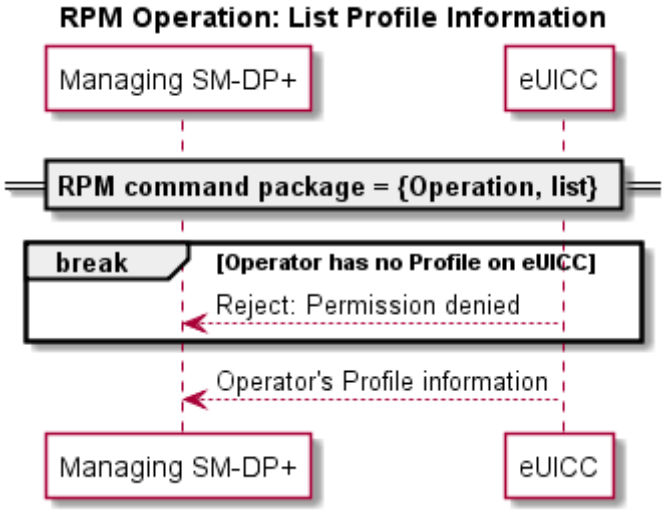

Figure 37: RPM Operation – List Profile Information

5.4.3.6 RPM Operation: Unset Profile Policy Rule

The command “unset Profile Policy Rule” results in the unsetting of a Profile Policy Rule from a Disabled or Enabled Profile. This command does not require a local End User confirmation.

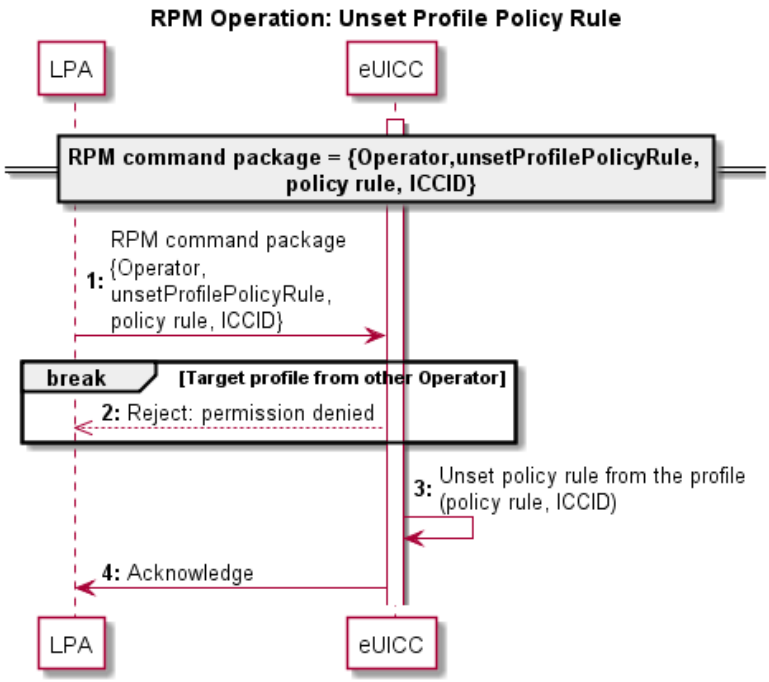

Figure 38: RPM Operation – Unset Profile Policy Rule

5.4.3.7 RPM Operation: Contact PCMP

The command “contact PCMP” results in the initialisation for a connection to the PCMP server configured in the Enabled Profile. If an optional parameter DPI is provided in the RPM command and/or configured in the Enabled Profile, they will be attached during the connection to the PCMP to signify an expected connection to a Delegated PCMP.

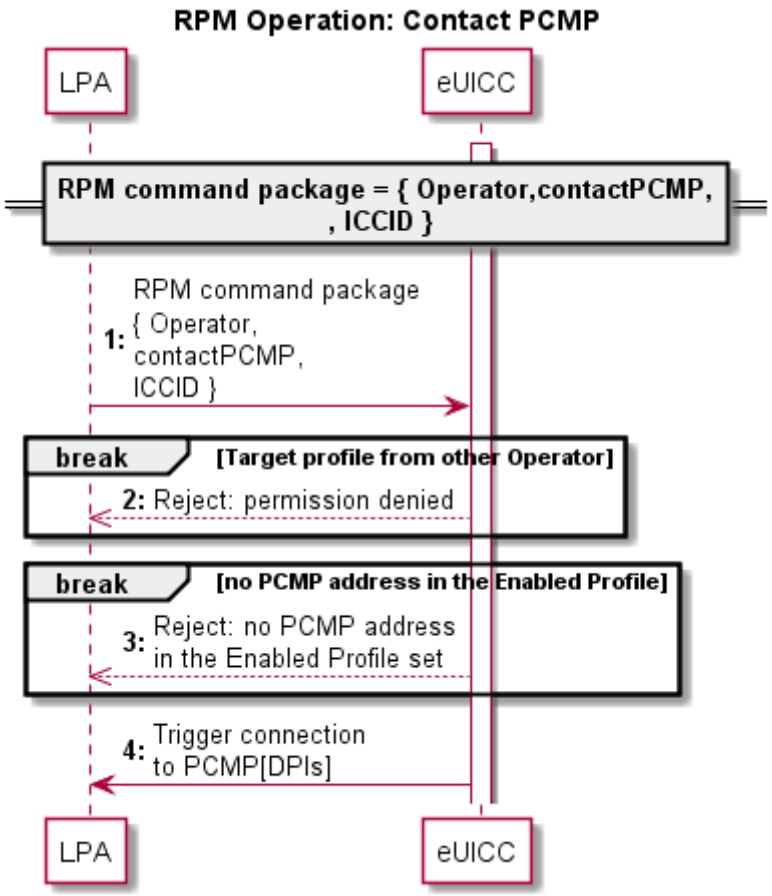

Figure 39: RPM Operation – Contact PCMP

Annex A [Void]

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.

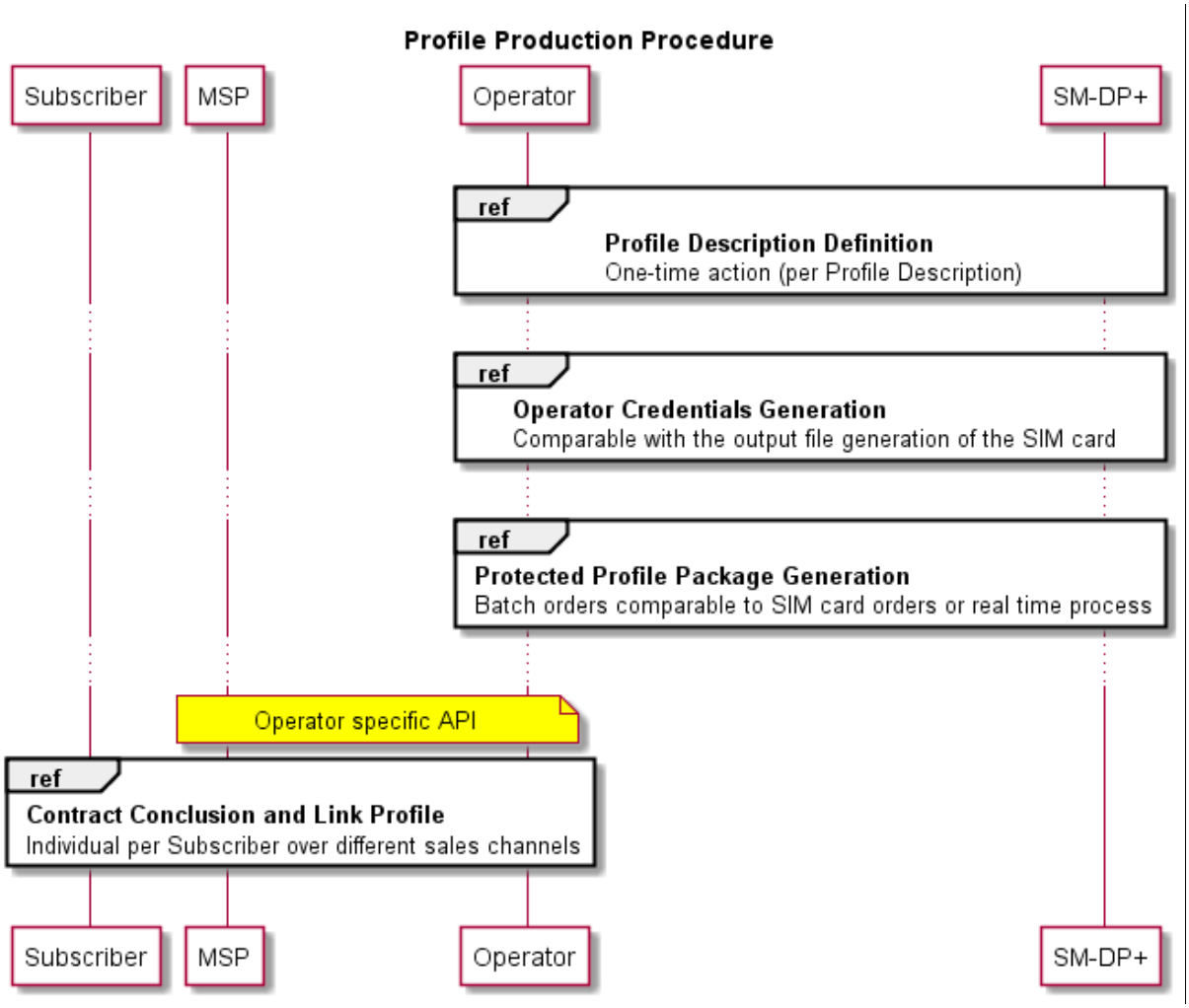

Figure 40: Profile Production Procedure

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:

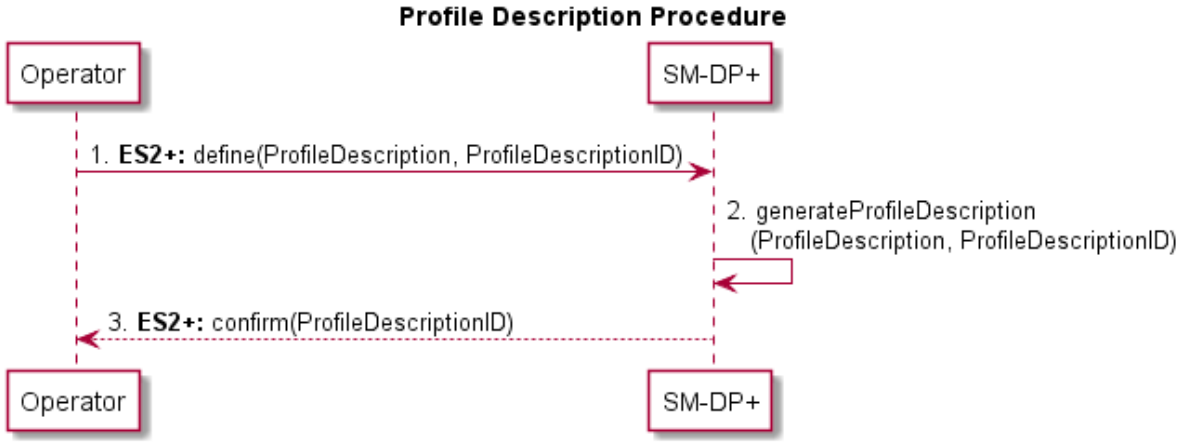

Figure 41: Profile Description Procedure

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:

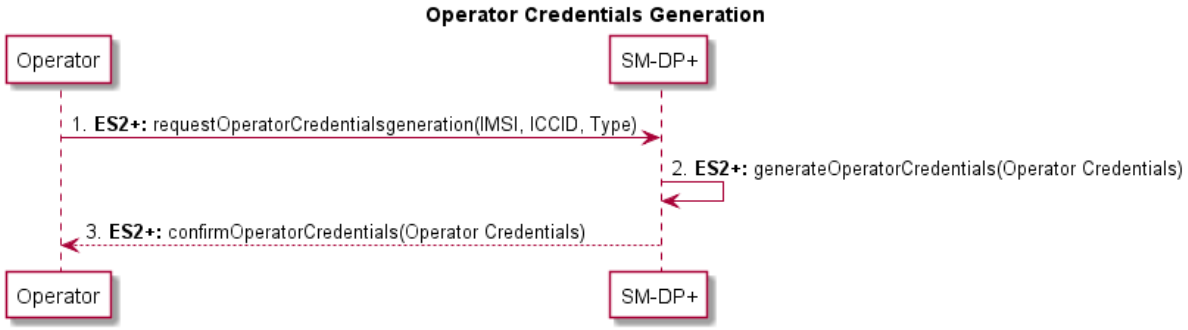

Figure 42: Operator Credentials Generation

Start Condition:

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

Procedure:

18. 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.
19. 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.
20. 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.

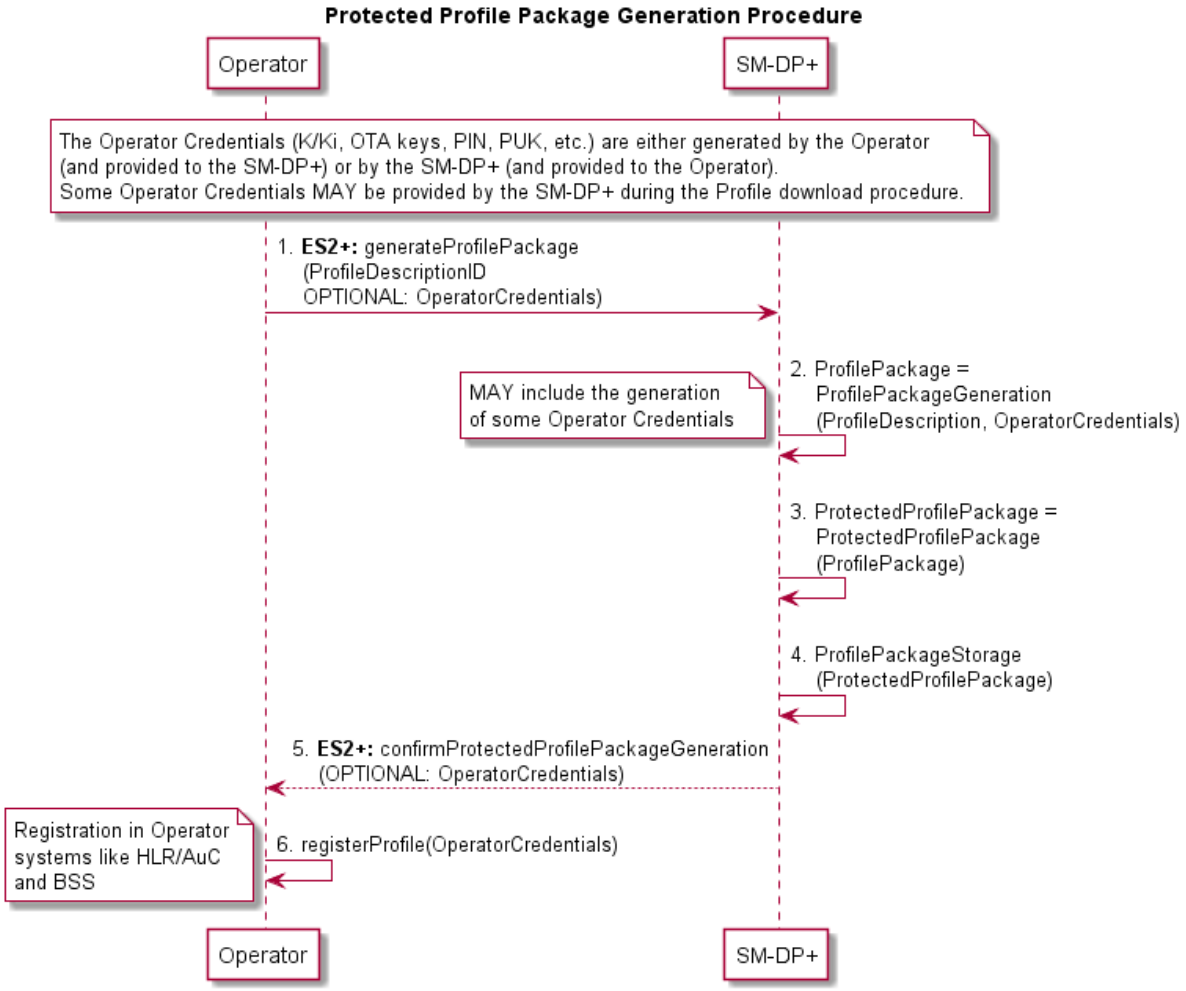

Figure 43: Protected Profile Package Generation Procedure

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 Mobile Service Provider during the conclusion of the contract.
- **Activation Code with unknown EID:** The EID is not given by the Subscriber to the Mobile Service Provider 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 Mobile Service Provider.
- **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 Mobile Service Provider.

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

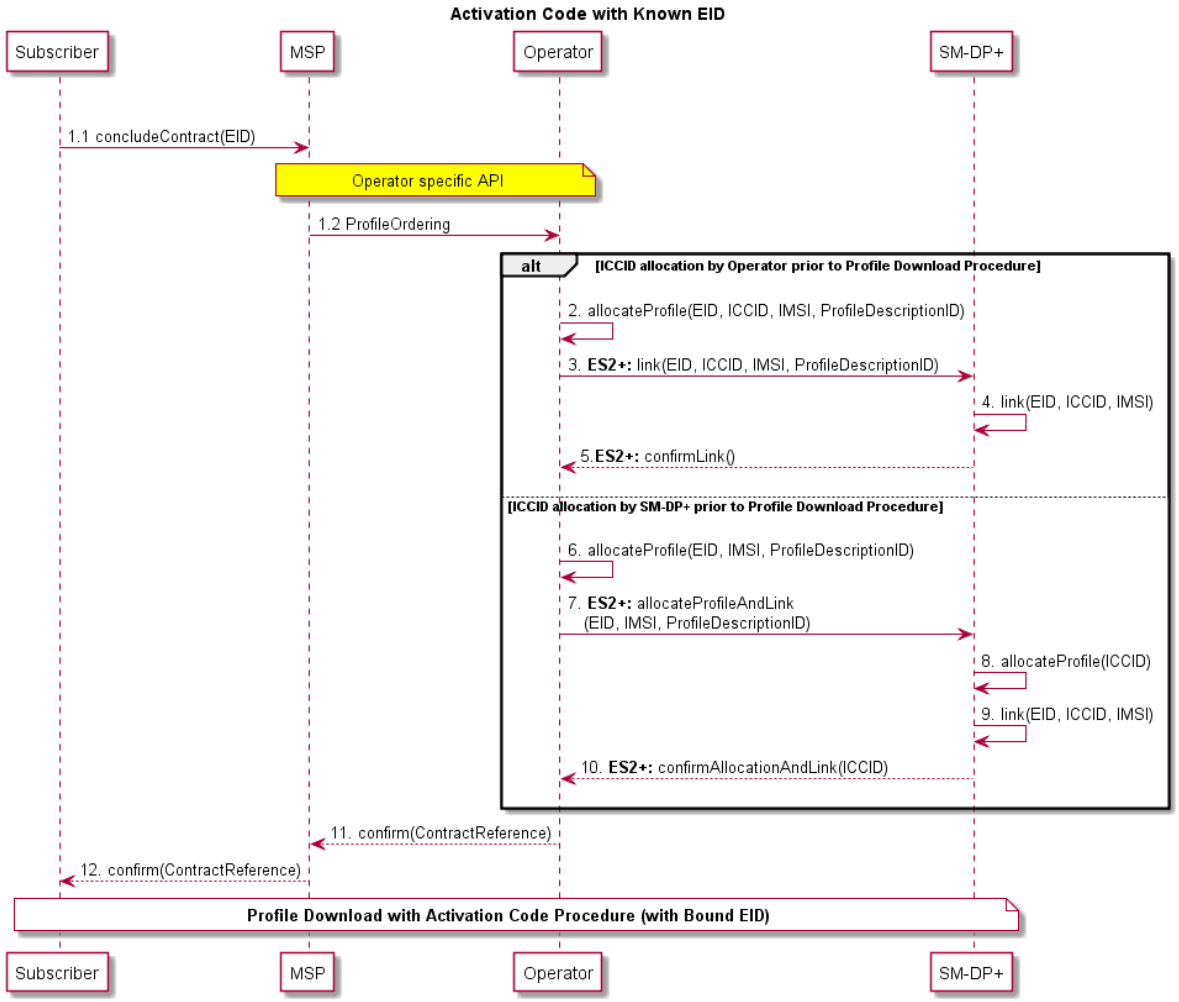

Figure 44: Activation Code with Known EID Procedure

Procedure:

Steps 1-12 in Figure 44: Contract conclusion with known EID

1. The Subscriber concludes a contract with the Mobile Service Provider 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. to 12. The Mobile Service Provider 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 Mobile Service Provider.
b. The SM-DP+ is informed about a future Profile download procedure request.

B.1.4.2 Activation Code with Unknown EID

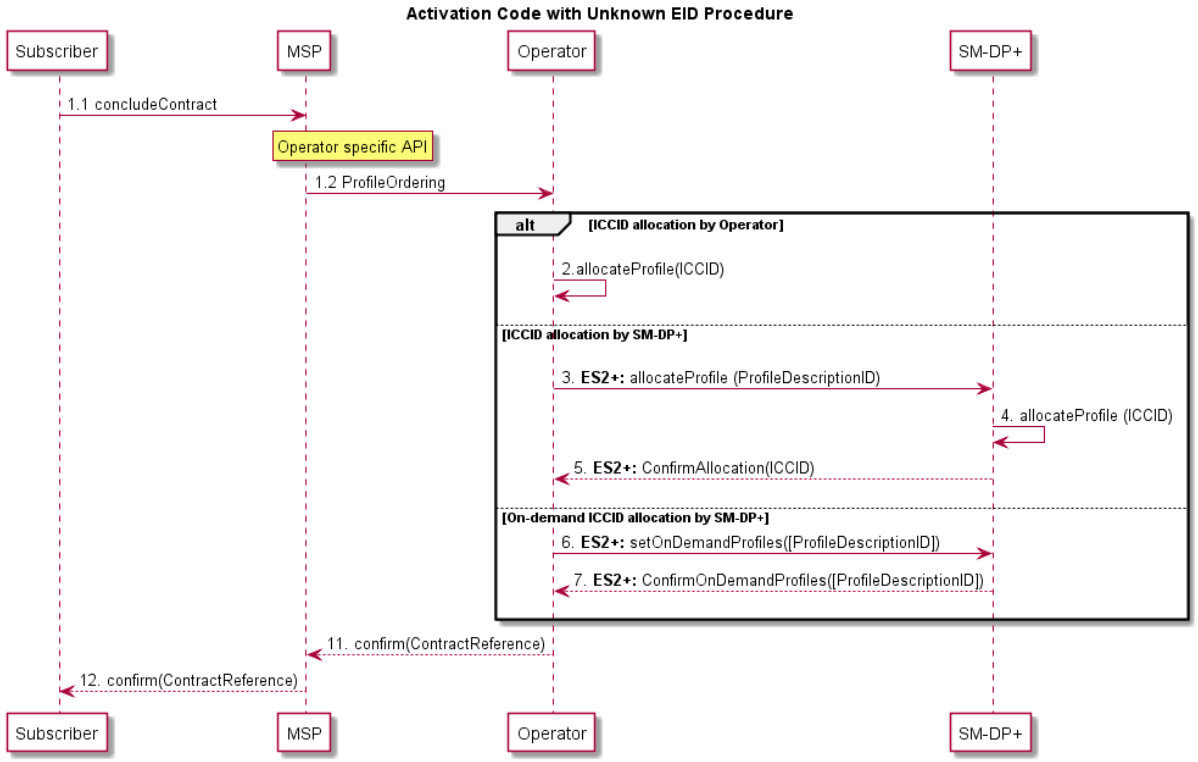

Figure 45: Activation Code with Unknown EID Procedure

Procedure:

Steps 1-9 in Figure 45: Contract conclusion without EID

1. The Subscriber concludes a contract with the Mobile Service Provider 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. to 7. **Alternatively 'On-demand ICCID allocation by SM-DP+':** The operator sends the Profile templates (IDs) allowed for this Activation Code. When the LPA starts the Profile download process, the SM-DP+ will allocate the ICCID of the most convenient Profile ID type for the Device and eUICC features.
8. to 9. The Mobile Service Provider 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 Mobile Service Provider.
b. The SM-DP+ is informed about a future Profile download procedure request.

B.1.4.3 Activation Code with EID Provided to the Mobile Service Provider

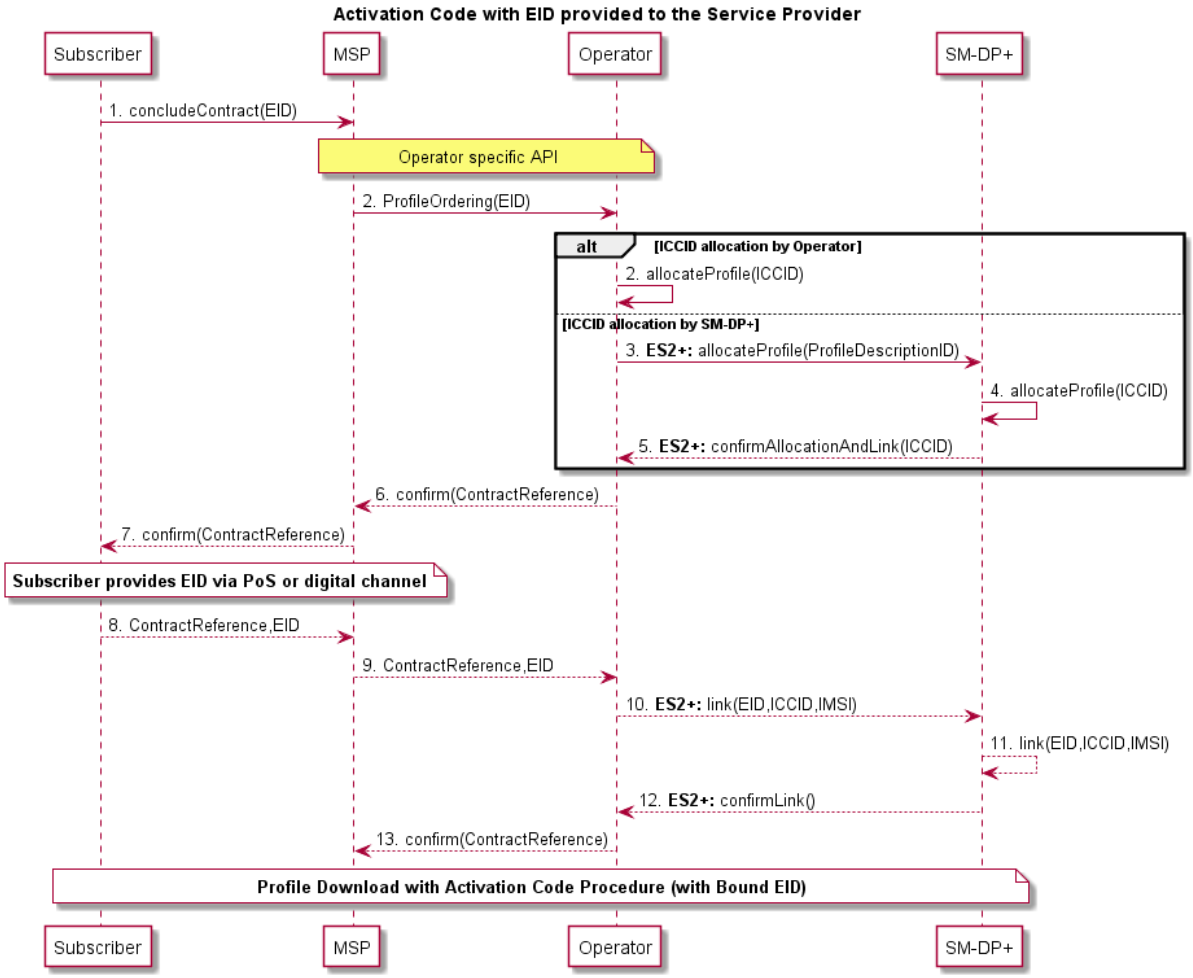

Figure 46: Activation Code with EID Provided to the Mobile Service Provider

Procedure:

Steps 1-14 in Figure 46: Activation Code with EID provided to the Mobile Service Provider

1. The Subscriber concludes a contract with the Mobile Service Provider 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. to 7. The Mobile Service Provider confirms the contract conclusion to the Subscriber with the corresponding information (contract reference).

8. to 9**.** After the Subscriber has chosen the Device/eUICC, the EID is provided together with the contract reference to the Mobile Service Provider.
10. to 12. 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.
13. to 14**.** The Mobile Service Provider 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 Mobile Service Provider.
b. The SM-DP+ is informed about a future Profile download procedure request.

B.2 Profile preparation with dynamic interaction between the SM-DP+ and the Operator

This section describes a process which might be used to prepare a Profile with dynamic interaction between the SM-DP+ and the Operator through the ES2+ interface. This function could be used by the SM-DP+ for activation decisions when conditions are required from the Operator side.

The dynamic interaction is described in the following procedure:

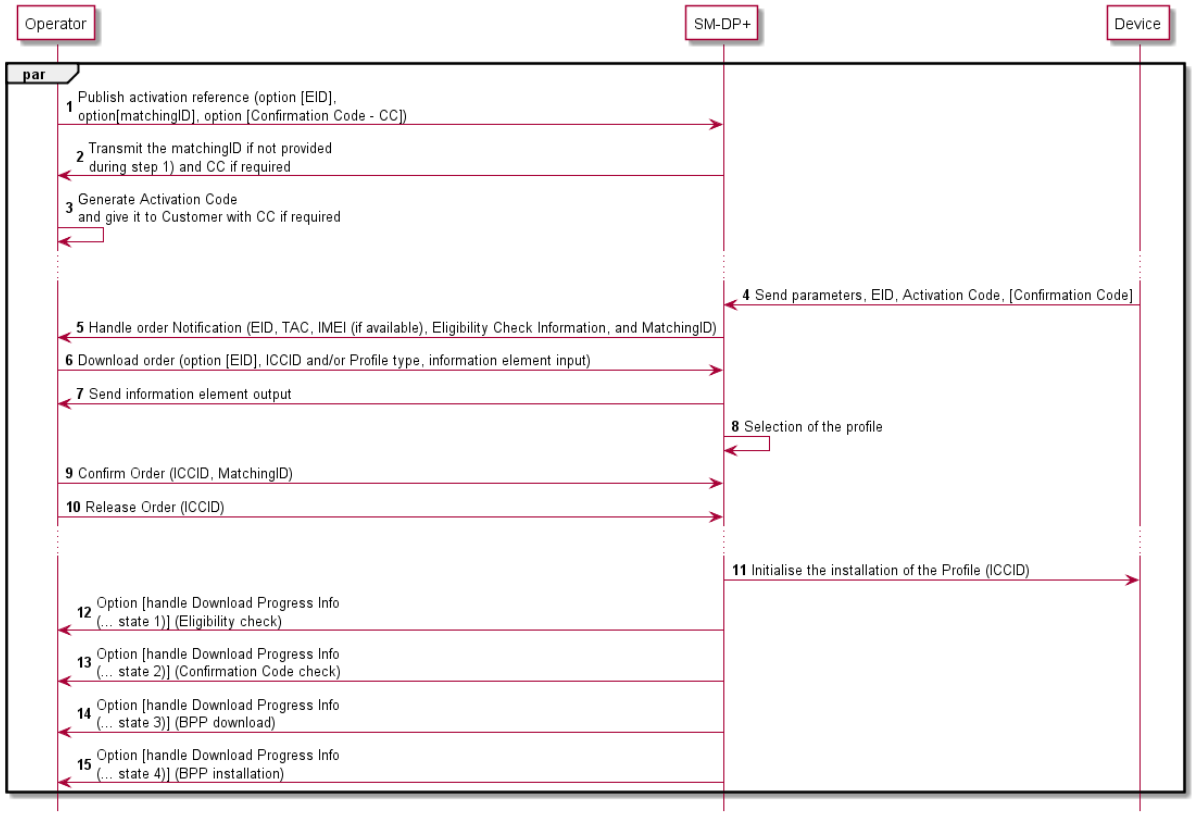

Figure 47: Profile preparation with dynamic interaction between the SM-DP+ and the operator

Procedure:

1. The Operator initialises an activation reference or request for its creation by the SM-DP+, called MatchingID. This MatchingID may be optionally linked to a specific EID and associated in addition to a Confirmation Code (CC).
2. The SM-DP+ acknowledges the generate order, and may send back a MatchingID if not provided by the Operator during the initialisation phase.
3. The Mobile Service Provider is able to generate an Activation Code associated to the MatchingID, and communicate it to the End User with in addition a Confirmation Code if desired.
4. At some point of time, the End User requests the installation of a Profile based on the Activation Code and eventually the Confirmation Code received from the Mobile Service Provider.

5. Handle order Notification is used by the SM-DP+ for activation decisions when conditions can't be taken by the SM-DP+. EID, TAC, IMEI (if available), Eligibility Check Information and MatchingID are transferred to the Operator and Mobile Service Provider.
6. The Operator is able to select a particular ICCID and/or a Profile type, sent back to the SM-DP+ through a DownloadOrder. Additional information elements may be exchanged between the Operator and the SM-DP+ through the DownloadOrder.
7. The SM-DP+ may respond with information elements to the Operator and Mobile Service Provider.
8. The SM-DP+ selects the adequate Profile.
9. The Operator confirms the download order by calling the ConfirmOrder function of the SM-DP+ with its relevant input data. MatchingID and ICCID are provided back to the SM-DP+.
10. After the Operator performs a relevant operation on its back-end (e.g. provisioning of HLR), the releaseProfile function is used to release the Profile in order to allow the End User to start the download and installation procedure.
11. The SM-DP+ initialises the download of the Profile.
12. to 15. Different Notifications to the Operator and Mobile Service Provider of the progress of a pending Profile download process may be provided at several points.

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.

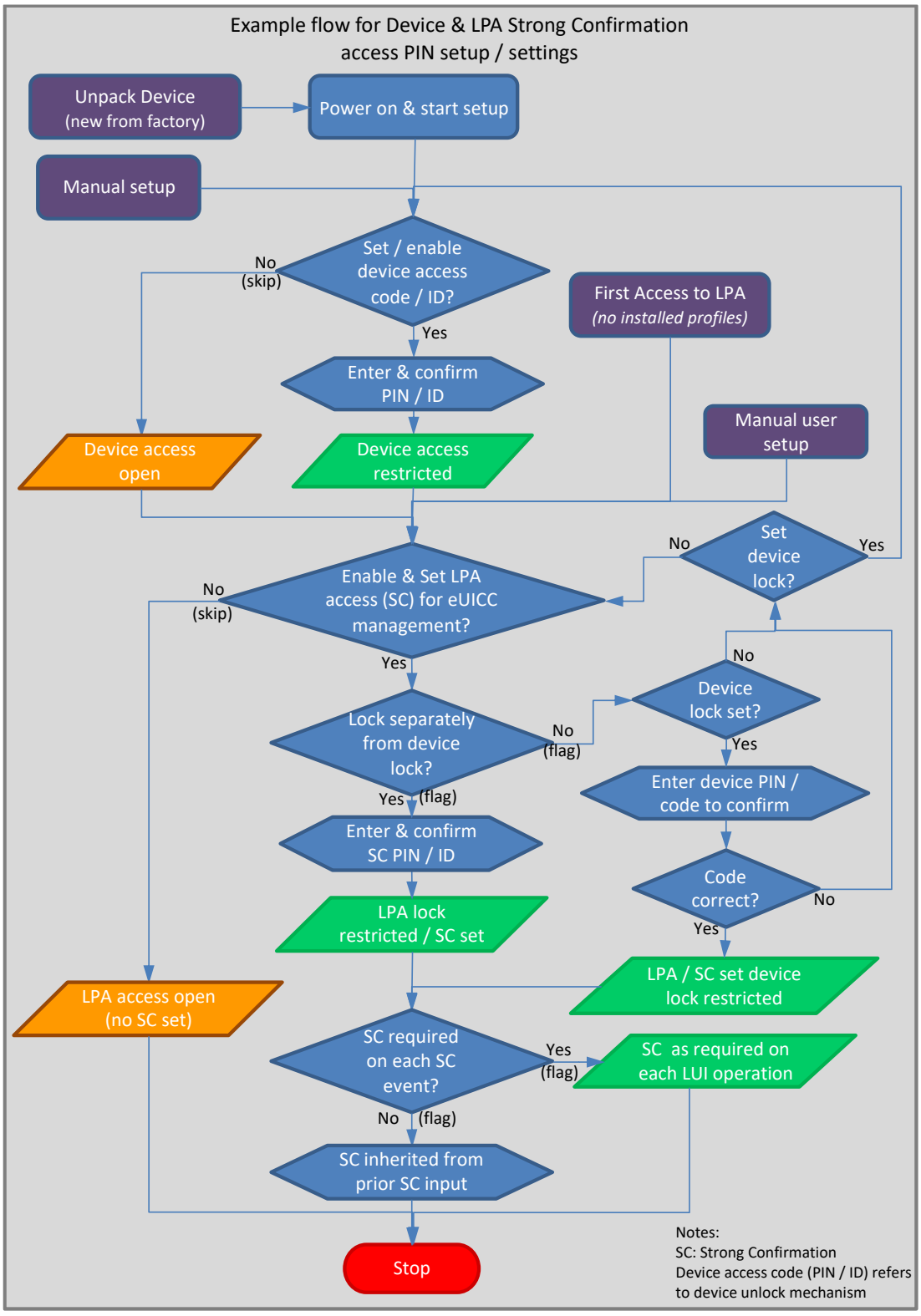

Figure 48: Example Flow for Device & LPA Strong Confirmation Access PIN Setup / Settings

Annex D [Void]

Annex E LPA Settings (Informative)

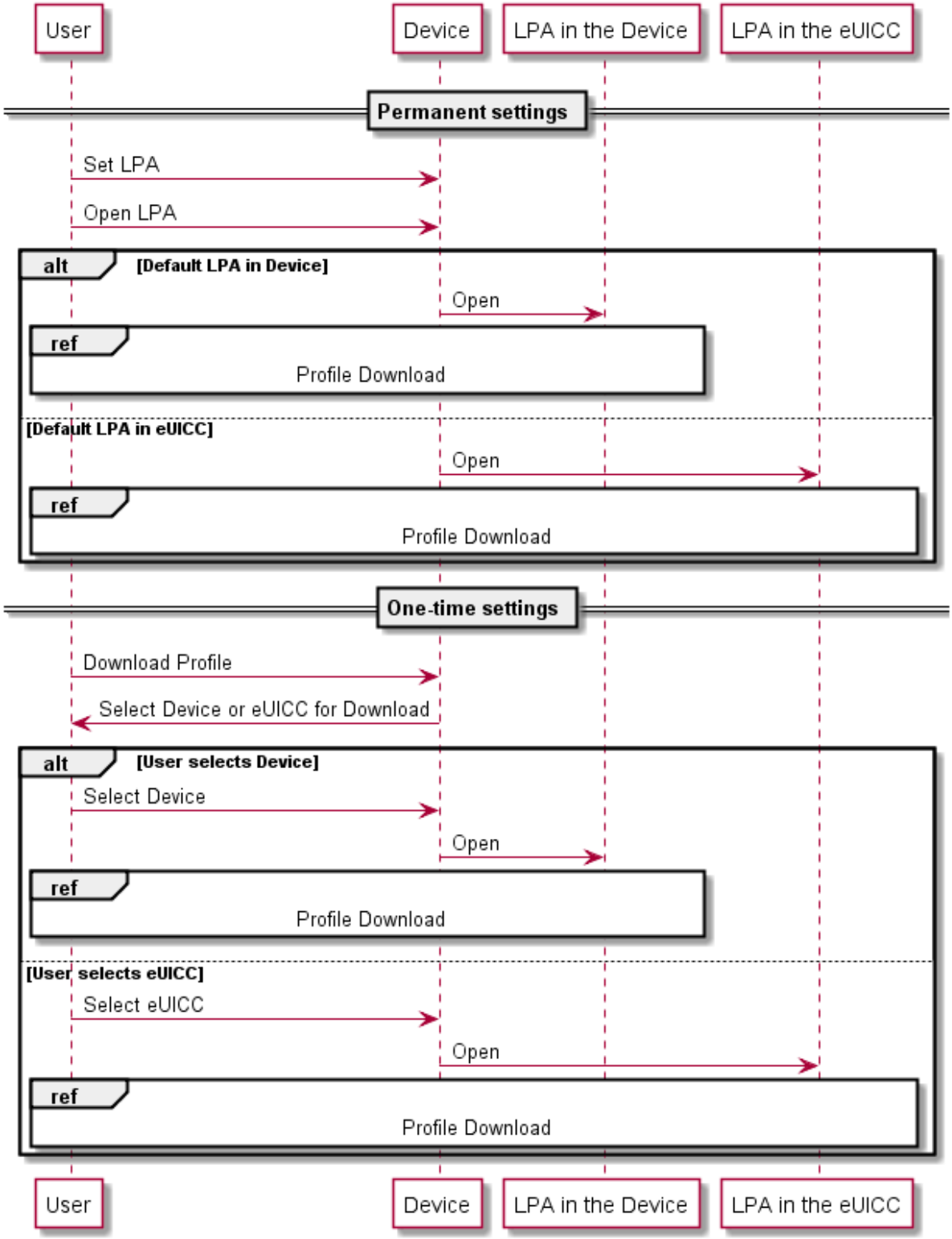

Figure 49: LPA Settings

Annex F Certifications Chain and Security Model (Normative)

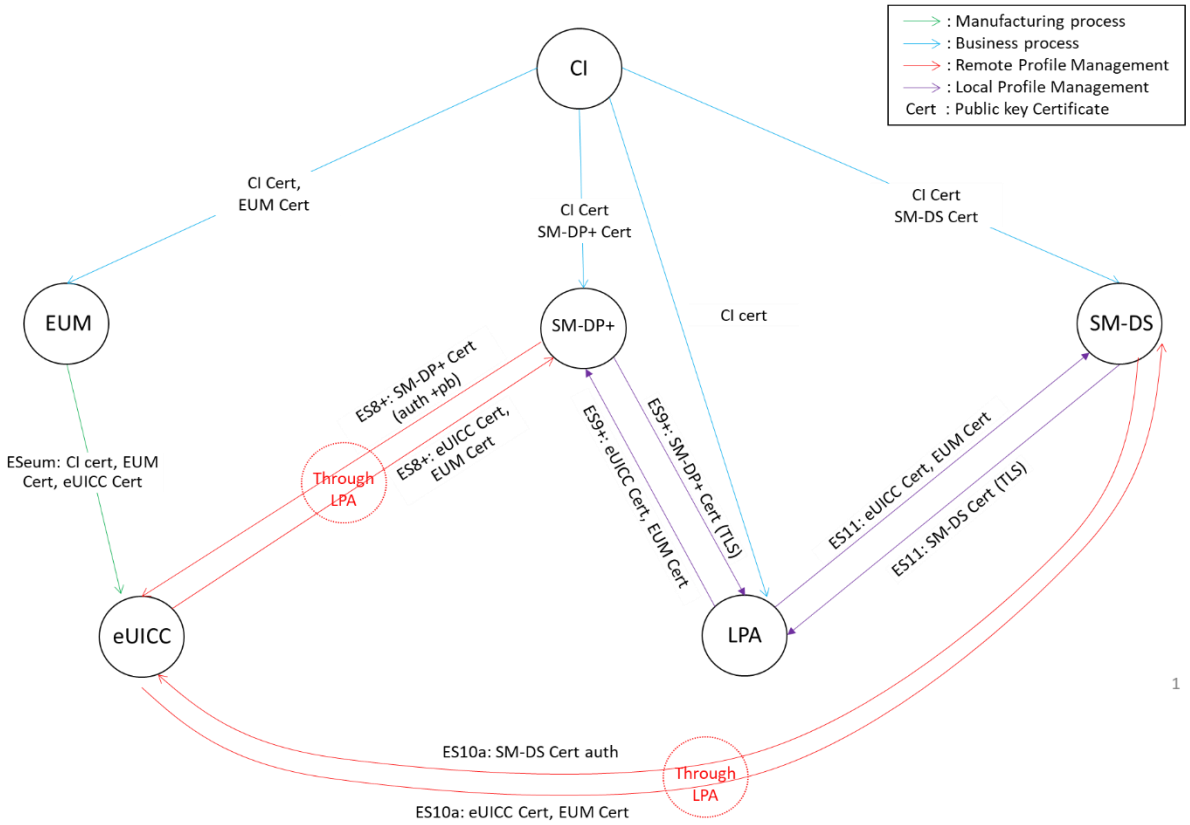

Figure 50: Certificate Exchange

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.

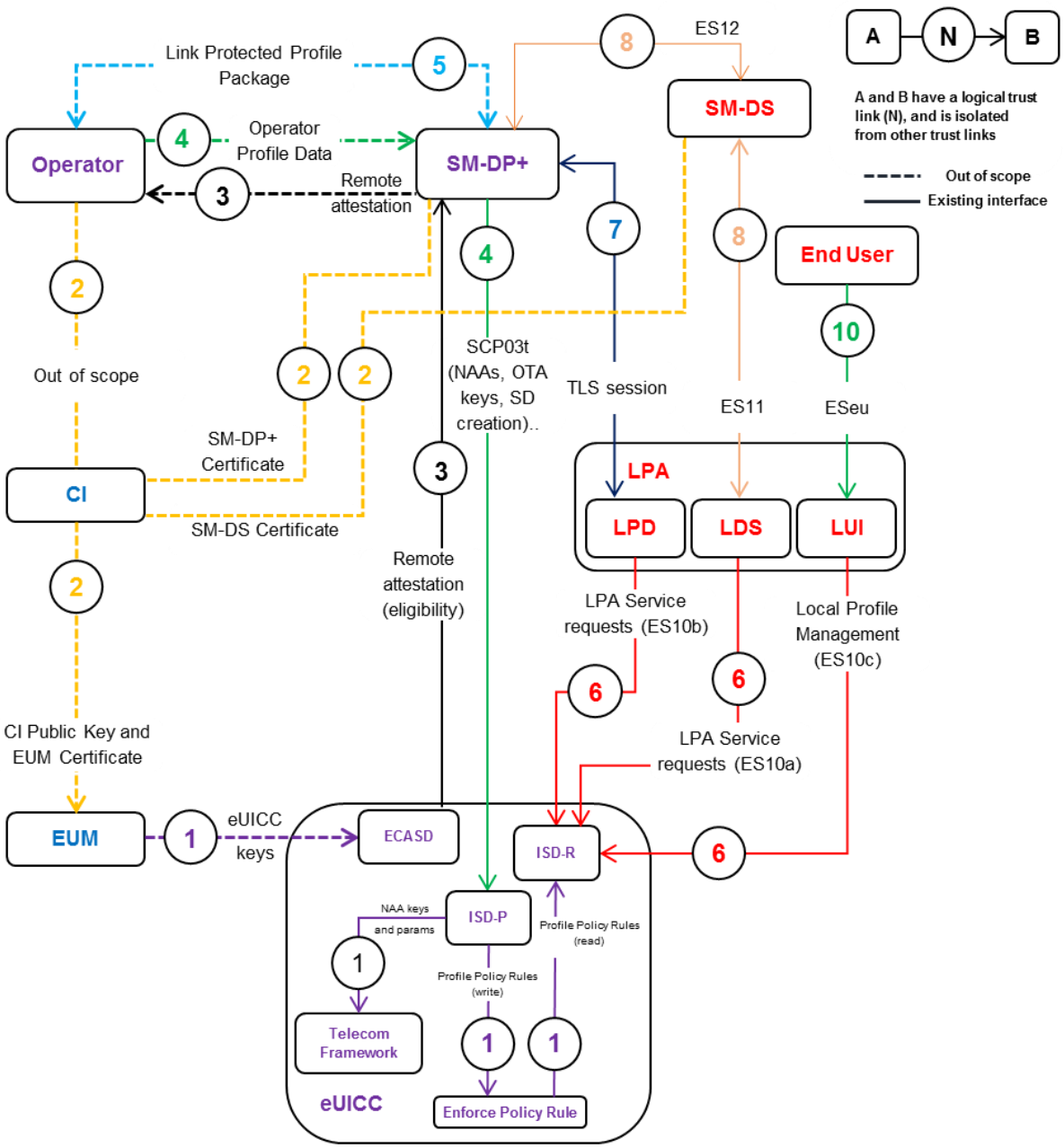

Figure 51: Trusted Link with LPA in the Device

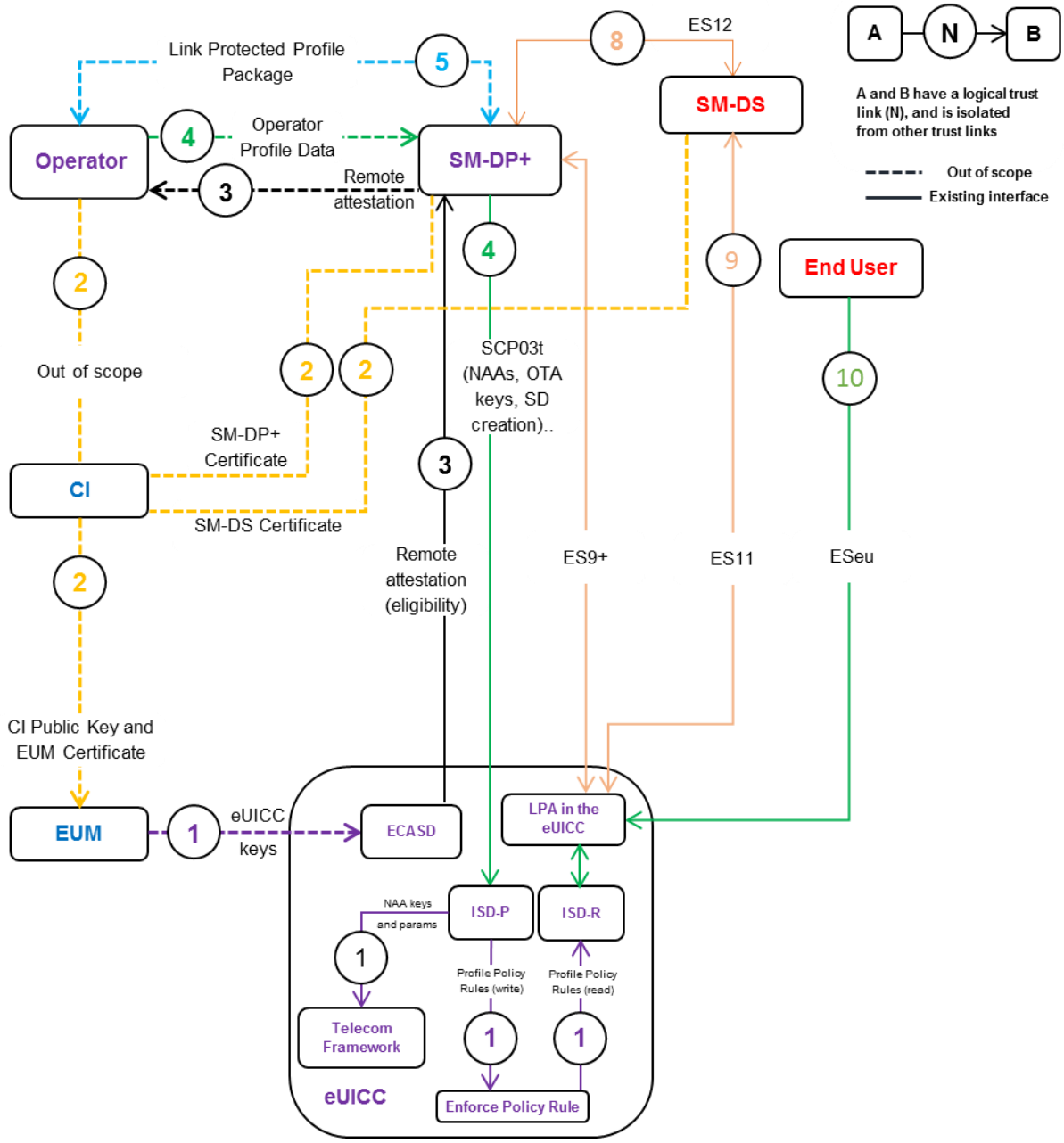

Figure 52: Trusted Link with LPA in the eUICC

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 (EUM & CI keyset eUICC Certificates).	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
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 Management Operations	ESeu	LPA security	eUICC loss of trust on LPA.

Trust link	Description	Interfaces involved	Possible compromises	Impact of loss of trust link
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 50: Trusted Link Descriptions

Compromised element	Impacted Links	Description	Impact of loss of trust	Countermeasures
eUICC	TL1, TL3, TL4, TL9, TL10	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.
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.

Compromised element	Impacted Links	Description	Impact of loss of trust	Countermeasures
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	TL11	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 51: 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 an eSIM CA 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 an eSIM CA upon achievement of the GSMA SAS or CI repair.
CERT3	The new EUM Certificate(s) SHALL be issued to the EUM by an eSIM CA 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.
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. Refer to 'SGP.14 Section 5.9.1 Circumstances for Revocation [26]' for details).

Req no.	Description
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. Refer to 'SGP.14 Section 5.9.1 Circumstances for Revocation [26]' for details).
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. Refer to 'SGP.14 Section 5.9.1 Circumstances for Revocation [26]' for details).

Table 52: Certificate Requirements

Annex G LPA Integrity (Normative)

The LPA and its interfaces with the eUICC SHALL be protected using industry best security practices.

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 53: Device Classes

Annex H [Void]

Annex I [Void]

Annex J Integrated eUICC Security Requirements (Normative)

J.1 General Security Requirements

Req no.	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 [40].
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**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

Req no.	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 54: General Security Requirements

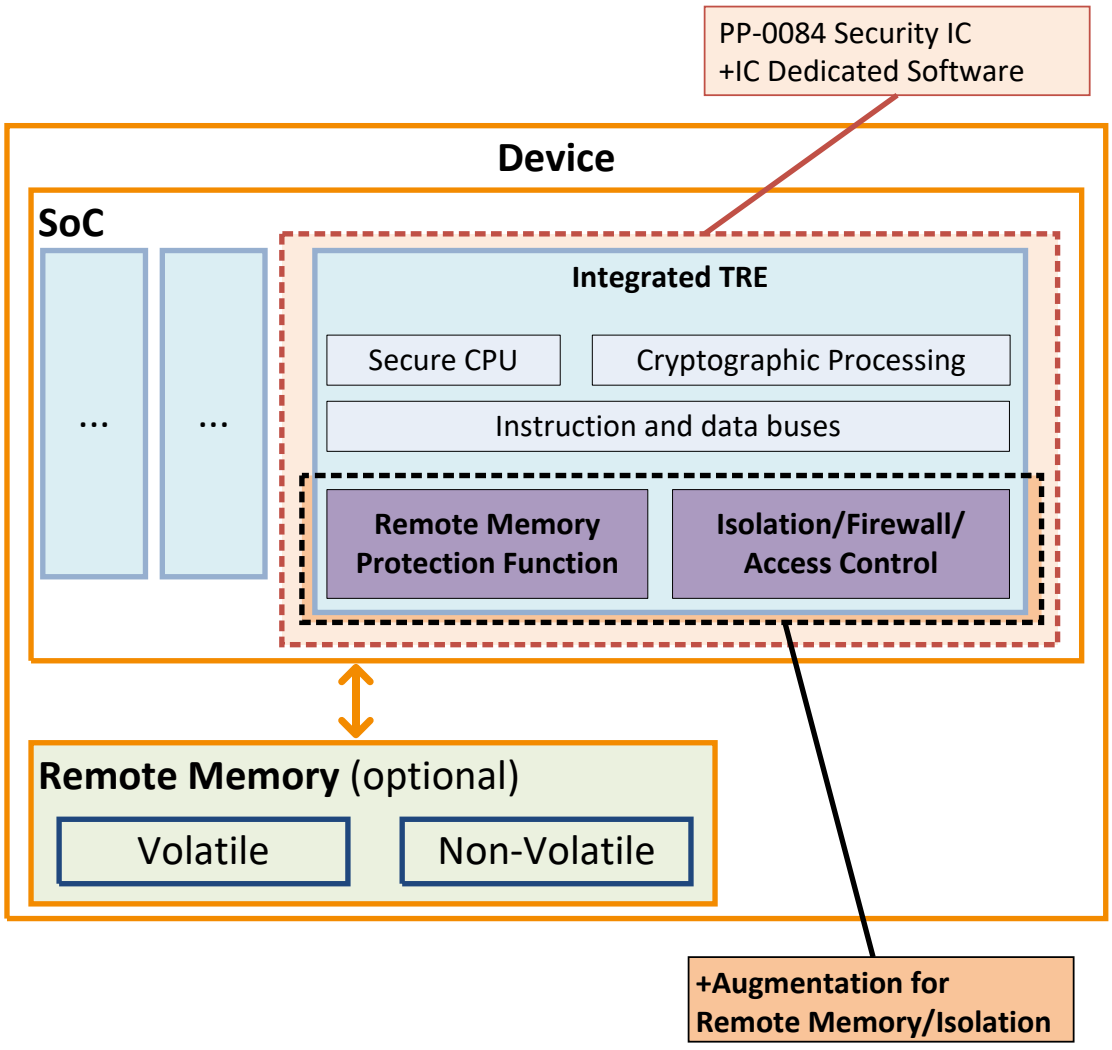

Figure 53: Example of Optional Remote Memory Usage

Note: IC Dedicated Software including its authentication by the TRE, is covered by BSI-CC-PP-0084 [40] and is not required to be augmented by this annex.

J.2 Security Certification Requirements

Req no.	Description
SC01	An Integrated TRE together with the RMPF SHALL be evaluated according to BSI-CC-PP-0084 [40] augmented with the requirements defined in this annex. Note: The requirements relating to Remote Memory and to RMPF 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 55: Security Certification Requirements

J.3 Conformance Claims

Req no.	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 [40] 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 [44].
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 [46].

Table 56: Conformance Claims

J.4 Security Objectives

BSI-CC-PP-0084 [40] defines security problems related to the Security IC being evaluated and corresponding security objectives. Within BSI-CC-PP-0084 [40], 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:

Req no.	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

Req no.	Description
	• manipulation

Table 57: Security Objectives

J.5 Security Functional Requirements

Req no.	Description
IESFR01	An Integrated TRE that uses Remote Memory SHALL implement 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 [40].
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 [41][41] 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 [45][18] or recommended by BSI in BSI TR-02102-1 [42] or recommended by ANSSI RGS v2 B1 [43].
Integrity and Authenticity	
IESFR13	The RMPF SHALL use a cryptographic integrity mechanism with security strength equivalent to, or greater than SHA-256.

Req no.	Description
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 • 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 [45] or recommended by BSI in BSI TR-02102-1 [42] or recommended by ANSSI RGS v2 B1 [43][43].
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 58: Security Functional Requirements

J.6 Identification Requirement

Req no.	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 59: Identification Requirement

Annex K Use Cases (Informative)

K.1 Device Change Support

K.1.1 Use Case 1 – Device Change normal case

The End User has an old Device containing one Profile and wants to install a Profile pertaining to the same Subscription in a new Device they bought. The old Device is working correctly and still has connectivity, perhaps through a Wi-Fi connection.

The End User starts the Device Change procedure on the old Device, inserting all the needed informations to perform the change. After that, the End User configures the new Device, preparing it for the Profile installation in the context of the Device Change. The Profile is downloaded and installed in the new Device and the Mobile Service Provider may perform the update of its backend system such as HSS/AuC and BSS with respect to the Profile installed in the new Device. The Mobile Service Provider or the End User may delete the Profile on the old Device.

The Profile downloaded and installed in the new Device can be a new Profile or the same Profile previously downloaded in the old Device.

At the end of the Device Change procedure the End User has their new Device configured with the Profile associated to the Subscription, and the old Device is no longer able to access the mobile service provided by using the old Profile.

K.1.2 Use Case 2 – Device Change normal case multiple Profiles

The End User has an old Device containing several Profiles and wants to install these Profiles pertaining to different Subscriptions in a new Device they have bought. The old Device is working correctly and still has connectivity, perhaps through a Wi-Fi connection.

The End User starts the Device Change procedure on the old Device, inserting all the needed information to perform the change. After that, the End User configures the new Device, preparing it for the Profile's installation in the context of the Device Change. The Profiles are downloaded and installed in the new Device and the Mobile Service Providers may perform the update of their backend system such as HSS/AuC and BSS with respect to the Profiles installed in the new Device. The Mobile Service Providers or the End User may delete the Profiles on the old Device.

The Profiles downloaded and installed in the new Device can be new Profiles or the same Profiles previously downloaded in the old Device.

At the end of the Device Change procedure, the End User has its new Device configured with the Profiles associated to their Subscriptions, and the old Device is no longer able to access the mobile service provided by using the old Profiles.

K.2 Multiple Enabled Profiles

The present section describes use cases wherein the Embedded UICC has a number profiles which are simultaneously used by the Device to provide connectivity to the End User.

K.2.1 Use Case 1 – Using installed Profiles in Dual-SIM mode

The End User has two mobile subscriptions: one for personal use and one for business use. Each subscription offers incoming/outgoing voice calls, incoming/outgoing text messages and mobile data.

The End User owns an eUICC-capable Device supporting two simultaneous device cellular connections e.g., Dual-SIM Dual Standby or Dual-SIM Dual Active modes. These Operational Modes are defined in GSMA TS.37 [48].

The End User installs two profiles onto the same eUICC from the LUI:

- Profile #1 is associated with the personal subscription, and
- Profile #2 is associated with the business subscription.

Once successfully installed onto the eUICC, the End User activates from the device settings menu Profile #1 and Profile #2.

The End User is able to receive voice calls and text messages simultaneously (and within the limits set by the Operational Modes as defined in GSMA TS.37 [48]) and has chosen which mobile line will be providing the active mobile data connection to the Device.

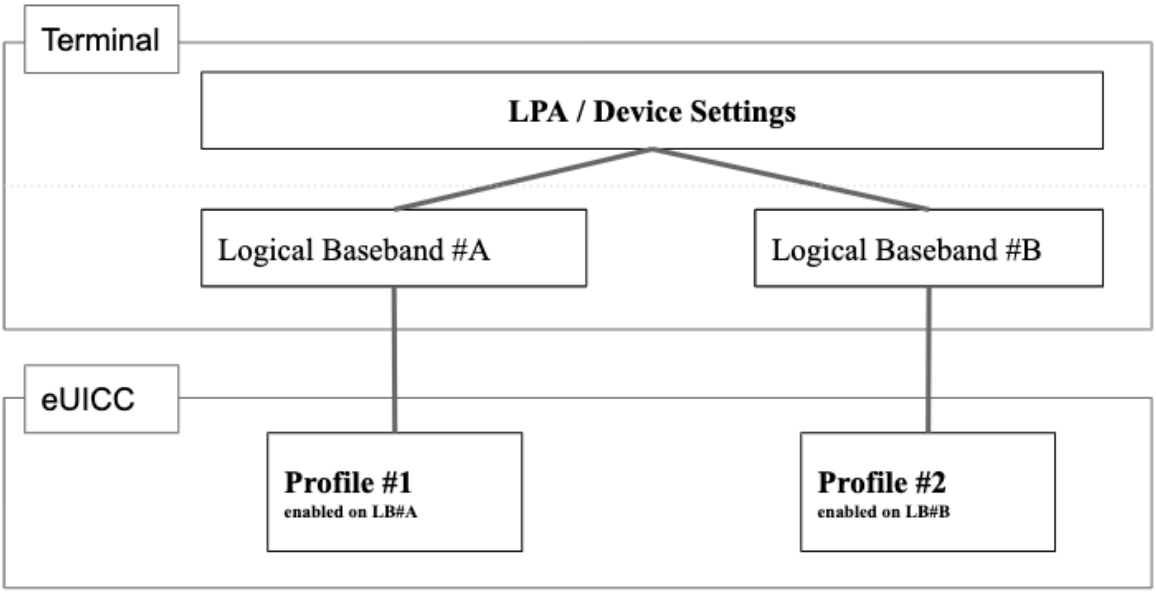

Figure 54: High Level Diagram of Multi-SIM Device with two Enabled Profiles

K.2.2 Use Case 2 – Activating another Profile on an existing logical baseband

The eUICC comprises three profiles, of which:

- Profile #1 and Profile #2 are enabled from the eUICC perspective and active on respectively logical baseband #A and #B.
- Profile #3 is disabled from the eUICC perspective

The User decides to enable Profile #3. The device interface indicates to the User that either Profile #1 or Profile #2 has to be disabled to allow this connectivity configuration change.

The User selects Profile #1 for disabling.

The Device disables Profile #1. The Device enables Profile #3 on logical baseband A.

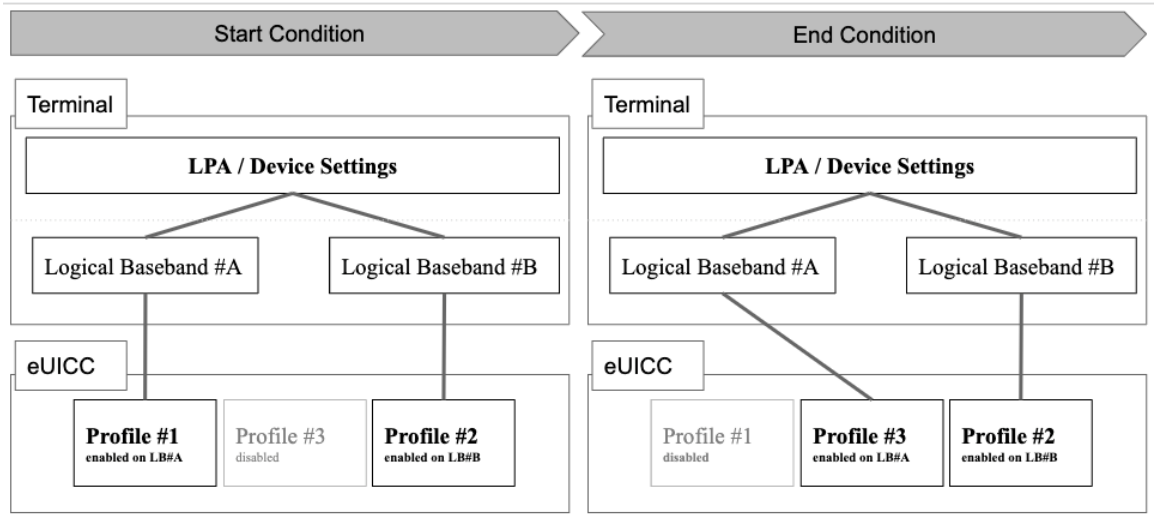

Figure 55: High Level Diagram of Multi-SIM Device with two Enabled Profiles

K.3 eUICC OS Update Interface

Device Manufacturers may have several eUICC providers for their Devices.

When an update of an eUICC OS is available and there is a decision to deploy this update into eUICCs present in the field, the Device Manufacturers obtains the secured eUICC OS update to be sent to the eUICC, from the relevant EUM.

Different types of update could be available depending on their impacts to the services and the End User. In some cases there is no impact at all for the services and for the End User, in some other cases there may be temporary impact on some services which may not be available during the update process, and finally in some cases the impact may be permanent.

In all these cases, the Device Manufacturer needs some information about the eUICC OS update in order to properly schedule the update and to inform the End User about what may happen during the update.

A typical use case for the eUICC OS Update may consist of several actions that rely on the information provided to the Device Application (e.g. the LPA or an eUICC OS Update agent) in charge of the eUICC OS Update.

- The Device needs to know if an eUICC OS update is available (or not) for its eUICC. In case of the same Device with multisource eUICC supplier, it is important to know which supplier is providing the eUICC OS Update.
- Before the eUICC OS update is applied to the eUICC, the Device needs to know if the eUICC OS update will impact or not the services, and whether the eUICC needs to be rebooted.
- At the end of the eUICC OS update, the Device needs to have a confirmation that the eUICC OS update is finished and a status to know if it was successful or not.

With this information, the Device will be able to schedule the eUICC OS update and to build a consistent user experience to avoid service issues to the End User.

In addition to the above field use case, Device Manufacturers may also use the eUICC OS update mechanism for refurbishment in production line or for repair center use cases. In such cases, the Device Application will need the same information as those needed for a field eUICC OS update. However this information may be used in a different way to take into account the specifics of a production/repair center environment (e.g. no End User involved).

K.4 Multiple Root Discovery Services

K.4.1 Use Case 1 – Resolving the Discovery Server address followed by Profile download process.

Basic flow:

- The Device is manufactured for a particular region of the world and wherein a number of Root Discovery Servers are available and supported by these regional Mobile Service Providers.
- The Device is shipped to this region.
- The Device is sold via a non-operator channel to the End User.
- The End User brings the Device to their Mobile Service Provider for activation (either physical location or online).
- The End User provides to the Mobile Service Provider the necessary information to determine the target Root SM-DS(s) to which the Device is connected.
- Upon successful verification of the provided information, the Mobile Service Provider performs the Profile download preparation and subscription activation process with their SM-DP+, wherein the Mobile Service Provider will transmit the relevant information for contacting the target Discovery Server (e.g. SM-DS address, etc.) and the Device-specific information for the download process (e.g. EID).

K.5 Enhanced SM-DS function SM-DS Event detection

In the SM-DS mechanism defined in version 2, the Device is unaware of when and whether an Event is registered at the SM-DS, so the Device needs to periodically perform the entire Event Retrieval procedure with the SM-DS without any advance information. Due to this situation, the following problems may be incurred.

1. The Device is not notified about the exact timing of an Event Registration. Therefore, the Device cannot contact the SM-DS right after an Event is registered. This may lead to a significant delay on the timing between the Event Registration and the Event Retrieval.

2. Some Root SM-DS may need to support billions of Devices in the field, thus suffering from a significant computational overhead to perform a lot of mutual authentications involving HSM. Each Device performs the full mutual authentication with the SM-DS even if there is no Event that has been registered for that Device.

K.5.1 Use Case 1 – Immediate process of Event with Push Service

If a Mobile Service Provider or SM-DP+ wants to perform a time-critical remote management (e.g. run-time consumer care service), the SM-DS can notify the LDS of an Event Registration by sending a push notification to the Device.

When the LDS receives a push notification, the Device performs the Event Retrieval procedure with the SM-DS that sent the push notification. In this way, the Event Record can be delivered to the Device as soon as the the Event is registered at the SM-DS.

K.5.2 Use Case 2 – Reducing unnecessary Event Retrieval transactions by Event Checking

The Device can perform the Event Checking procedure with the SM-DS to check the presence of any Event that has been registered for that Device. As a response to the Device's inquiry, the SM-DS returns to the Device the response indicating the presence of any registered Event(s) for the eUICC. If the Device receives the response containing the presence of registered Event, the eUICC starts to perform the Event Retrieval procedure with the SM-DS. By doing so, the Device always receives the Event Record(s) as a result of the Event Retrieval procedure, and hence any unnecessary Event Retrieval procedure can be avoided.

Annex L Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	03/12/15	First Release with amendments from Security review.	PSMC	Carmen Kwok, GSMA
V2.0	15/07/16	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	24/03/21	Phase 2 maintenance release	ISAG	Carmen Kwok, GSMA
V2.4	03/08/21	Phase 2 maintenance release	ISAG	Carmen Kwok, GSMA
V3.0	28/03/22	Includes Phase 3 content	ISAG	Carmen Kwok, GSMA

Detailed Document History

Version	Additions
V3.0	eSIMWG1 SGP.21 CR0047r1 Profile Principles
	eSIMWG1 SGP.21 CR0048r1 Roles eUICC manufacturer
	eSIMWG1 SGP.21 CR0049r1 Roles Device manufacturer
	eSIMWG1 SGP.21 CR0050r1 Roles Operator and Service Provider Editorial
	eSIMWG1 SGP.21 CR0051r1 Roles Subscriber and End User
	eSIMWG1 SGP.21 CR0054r1 General Interface requirements
	Agreed parts of eSIMWG1 SGP.21 CR0055r1 Eligibility check (Part 1)
	eSIMWG1 SGP.21 CR0056r1 eUICC OS update feature
	eSIMWG1 SGP.21 CR0010r2 Integrated eUICC
	eSIMWG1 SGP.21 CR0041r1 RMPF_Conditional
	eSIMWG1 SGP.21 CR0059r1 Test Profile Requirements
	eSIMWG1 SGP.21 CR0061r1 HR icon Requirements
	eSIMWG1 SGP.21 CR0108r1 SM-DS - pt1
	eSIMWG1 SGP.21 CR0097r1 Java Card support
	eSIMWG1 SGP.21 CR0107r3 Different Root SM-DS
	eSIMWG1 SGP.21 CR0117r1 Root SM-DS address location
	eSIMWG1 SGP.21 CR0120 EUICC40
	eSIMWG1 SGP.21 CR0135r3 Multiple SM-DS requirements
	eSIMWG1 SGP.21 CR0128r3 Device Change Overview
	eSIMWG1 SGP.21 CR0130r5 Device Change High Level Procedure

	Editorial - Removed yellow highlight from EUICC1 as per eSIMWG1 SGP.21 CR0010r2
	eSIMWG1 SGP.21 CR0131R01 - Terms and Requirements for Device Change
	eSIMWG1 SGP.21 CR0089r1 SM-DP+ Note: SMDP48 voided in CR, however requirement was not in SGP.21 V2.2 so no change has been made.
	eSIMWG1 SGP.21 CR0152r1 Device Change use cases
	eSIMWG1 SGP.21 CR0155r1 Profile package status query
	eSIMWG1 SGP.21 CR0132r05 - Requirements for Device Change request
	eSIMWG1 SGP.21 CR0133r05 - Requirements for Device Change response
	eSIMWG1 SGP.21 CR0137r05 - MEP-related Requirements
	eSIMWG1 SGP.21 CR0015r2 Adding Profile size indication in Profile metadata
	eSIMWG1 SGP.21 CR0148r3 Get current size of installed profile
	eSIMWG1 SGP.21 CR00162 Align META11a with SGP.22 V3.0
	eSIMWG1 SGP.21 CR0136r5 MEP Use Cases
	eSIMWG1 SGP.21 CR0166r1 Default SM-DP+ Address on the eUICC requirements - GREEN
	eSIMWG1 SGP.21 CR0168 NFC requirements - GREEN
	eSIMWG1 SGP.21 CR0170 AC requirements - GREEN
	eSIMWG1 SGP.21 CR0171r1 Editorial CR pt 1 - GREEN
	eSIMWG1 SGP.21 CR0172r1 Editorial CR pt 2 - GREEN
	eSIMWG1 SGP.21 CR0159r4 Requirements for Device Change response pt 2
	Withdrawn CR0087r2 LPAe pt1 – Voided DEV8
	Withdrawn CR0104 SMDS2 Requirement – Voided SMDS2
	Withdrawn CR0018r1 Allow extensibility and innovation pt2 – Voided ESeu1, LPA1. LPA45 voided in Draft 13 (missed this).
	eSIMWG1 SGP.21 CR0181 Certification Requirements - GREEN
	eSIMWG1 SGP.21 CR0092R01 Set Nickname
	eSIMWG1 SGP.21 CR0145 Cleanup of SM-DS wording
	eSIMWG1 SGP.21 CR0126R01 Operator vs SP cleanup in diagrams
	eSIMWG1 SGP.21 CR0156r5 ES12 Enhancements
	eSIMWG1 SGP.21 CR0063R06 Default SM-DP+ Address on the eUICC Requirements
	eSIMWG1 SGP.21 CR0072r2 AAC
	eSIMWG1 SGP.21 CR0077r7 RPM part 1
	eSIMWG1 SGP.21 CR0174r2 LPAe pt 2
	eSIMWG1 SGP.21 CR0190r2 Editorial change of GS02
	eSIMWG1 SGP.21 CR0197r1 Default SM-DP+ Address Updated Figure
	eSIMWG1 SGP.21 CR0139 Remote Primary Device
	eSIMWG1 SGP.21 CR0140r2 Internet Proxy at Remote Primary Device
	eSIMWG1 SGP.21 CR0074r4 Enterprise
	eSIMWG1 SGP.21 CR0065r1 Explain IESFR19
	eSIMWG1 SGP.21 CR0083r7 Device Requirements

	eSIMWG1 SGP.21 CR0093r2 LPA15
	eSIMWG1 SGP.21 CR0090r4 Editorial pt 2
	eSIMWG1 SGP.21 CR0080r2 Policy Rules
	eSIMWG1 SGP.21 CR0201 Align v3 to v2.3 on ieUICC
	eSIMWG1 SGP.21 CR0200 LPA61
	eSIMWG1 SGP.21 CR0195r2 RPM - Implicit disabling
	eSIMWG1 SGP.21 CR0196r2 RPM - LUI requirements
	eSIMWG1 SGP.21 CR0209r1 Editorial clean-up PPR4 references
	eSIMWG1 SGP.21 CR0138R03 - MEP Requirements - PPR1 handling
	eSIMWG1 SGP.21 CR0016r6 Clarify Profile Metadata extensibility
	eSIMWG1 SGP.21 CR0198r2 Requirements on Profile recovery for Device Change
	eSIMWG1 SGP.21 CR0194r3 Authorisation of RPM operations
	eSIMWG1 SGP.21 CR0202r2 Device Change for multiple Profiles - use case
	eSIMWG1 SGP.21 CR0203r3 Device Change for multiple Profiles - requirements
	eSIMWG1 SGP.21 CR0158r4 eUICC OS Update interface Use Cases
	eSIMWG1 SGP.21 CR0225r1 Enterprise MEP Requirement
	eSIMWG1 SGP.21 CR0226r1 Device Change clarification
	eSIMWG1 SGP.21 CR0134r5 Routing Discovery event to correct DS endpoint
	eSIMWG1 SGP.21 CR0176r9 Requirements for enhanced Discovery Service
	eSIMWG1 SGP.21 CR0229r1 Added abbreviations
	eSIMWG1 SGP.21 CR0219r3 Align EUICC55 with SGP.22
	eSIMWG1 SGP.21 CR0237r00 - Device Change procedure figure update
	eSIMWG1 SGP.21 CR0221r4 Device Information Code
	eSIMWG1 SGP.21 CR0079r4 Certification Requirements
	eSIMWG1 SGP.21 CR0241r1 eUICC Testing Requirements
	eSIMWG1 SGP.21 CR0238 Multiple Enabled Profiles for Removable eUICC is FFS
	eSIMWG1 SGP.21 CR0240 Changes from v2.3 CRs
	eSIMWG1 SGP.21 CR0084r4 Activation Code
	eSIMWG1 SGP.21 CR0182r2 Certification Requirements pt2
	eSIMWG1 SGP.21 CR0220r5 Certification Requirements
	eSIMWG1 SGP.21 CR0246 Enterprise Principles
	eSIMWG1 SGP.21 CR0039R01 Rename SP to MSP (Includes minor fixes to Figures in 4.12.2.1, 4.12.2.2 and 4.17.1 – MSP added between End User and Operator)
	eSIMWG1 SGP.21 CR0075r3 eUICC Requirements
	eSIMWG1 SGP.21 CR0260 eUICC Requirement - EUICC47
	eSIMWG1 SGP.21 CR0253r1 Comments on Basic Principles
	eSIMWG1 SGP.21 CR0210r2 eUICC Memory Reset - part 2
	eSIMWG1 SGP.21 CR0082r2 APDU API

	eSIMWG1 SGP.21 CR0081r5 LPA Proxy
	eSIMWG1 SGP.21 CR0235 Alignment of Strong Confirmation definition with SGP.21 v2.3
	eSIMWG1 SGP.21 CR0261 Fix Profile Metadata extensibility
	eSIMWG1 SGP.21 CR0071r7 NFC eUICC def
	eSIMWG1 SGP.21 CR0164r11 eUICC OS Update Interface description
	eSIMWG1 SGP.21 CR0146r2 Revisit of PK certificates definitions
	eSIMWG1 SGP.21 CR0257r1 Comments on Added abbreviations
	eSIMWG1 SGP.21 CR0266r1 eUICC OS Update Figure 3 update
	eSIMWG1 SGP.21 CR0267 Removal of AAC from SGP.21
	eSIMWG1 SGP.21 CR0085r5 eUICC Memory Reset
	eSIMWG1 SGP.21 CR0234r5 Requirements for Local Device Change
	eSIMWG1 SGP.21 CR0091r1 Primary and Companion Device Feature – Ignored LPA72 in this CR as it no longer exists in this draft.
	eSIMWG1 SGP.21 CR0232r2 Comments on RPM
	eSIMWG1 SGP.21 CR0228r8 Comments on Certificate Issuer role
	eSIMWG1 SGP.21 CR0153R05 Discrete eUICC definition
	eSIMWG1 SGP.21 CR0263r2 Comments on APDU Access API
	eSIMWG1 SGP.21 CR0272 Editor’s note resolution on Device Change reqs in Section 4.18.3
	eSIMWG1 SGP.21 CR0273 Editor’s note resolution on Device Change use cases in Annex K
	eSIMWG1 SGP.21 CR0279r1 Alternative - Optional support of the Device Change requirements
	eSIMWG1 SGP.21 CR0276r1 Remove editor’s note from DEV17
	eSIMWG1 SGP.21 CR0204 Editorial Clean-up - Removing ReM references
	eSIMWG1 SGP.21 CR0239r1 Additional Enterprise MEP requirement
	eSIMWG1 SGP.21 CR0259r2 Comments on References
	eSIMWG1 SGP.21 CR0258r3 Comments on Added terms
	eSIMWG1 SGP.21 CR0192r2 ES12 Enhancements – SMDPX5
	eSIMWG1 SGP.21 CR0121r2 ESapp Inclusion
	eSIMWG1 SGP.21 CR0280r1 Definitions clean up
	eSIMWG1 SGP.21 CR0281r1 Remove TBD in SMDP27c
	eSIMWG1 SGP.21 CR0122r11 eUICC Interoperable Running Environment
	eSIMWG1 SGP.21 CR0283 Profile state persistency requirements
	eSIMWG1 SGP.21 CR0183r1 ELG25
	eSIMWG1 SGP.21 CR0275r7 RPM with SEP and MEP - simplified alternative
	eSIMWG1 SGP.21 CR0264r4 Comments on LPA API Access Control
	eSIMWG1 SGP.21 CR0073r6 End User Intent
	eSIMWG1 SGP.21 CR0287 Fix ed note in ENT4

Other Information

Type	Description
Document Owner	Carmen Kwok
Editor / Company	Carmen Kwok, 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.