# RSP Architecture

# Version 1.0

# 23 December 2015

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

## Security Classification: Non-confidential

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

## Copyright Notice

## Disclaimer

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

## Antitrust Notice

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

# Table of Contents

# 1 Introduction

## 1.1 Overview

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

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

This version focuses on Devices for the consumer market.

## 1.2 Scope

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

## 1.3 Intended Audience

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

## 1.4 Definition of Terms

| Term | Description |
|---|---|
| Activation Code | Information issued by an Operator/Service Provider to an End User. It is used by the End User to request for the download and installation of a Profile. |
| Activation Code Token | A part of the Activation Code information provided by the Operator/Service Provider to reference a Profile. |
| Authenticated Confirmation | Describes a mechanism for which the End User is confirming their action through a method involving the input of personalised information (e.g. PIN, fingerprint). |
| Bound Profile Package | A Protected Profile Package which has been encrypted for a target eUICC. |
| Certificate | A certificate as defined in RFC.5280 [1] and GlobalPlatform specifications [11]. |
| Certified eUICC | An eUICC meeting the GSMA requirements for Remote SIM Provisioning and certified according to a GSMA eUICC protection Profile. |
| Companion Device | A Device that relies on the capabilities of a Primary Device for the purpose of Remote SIM Provisioning. |

| Term | Description |
|---|---|
| Confirmation Code | A code entered by an End User to authorise the usage of an Activation Code to confirm the download and installation of a Profile. For added security, the Operator MAY choose to communicate the Confirmation Code via a separate delivery channel. |
| Confirmation Code Required Flag | A parameter to indicate whether the Confirmation Code is required or not. |
| Data Subset | The Data Subset is a list of Elementary Files of the respective Profile whose content SHALL be stored in the Metadata of said 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 Factory Reset | A term generally understood in the industry to mean that the Device is returned to a state equivalent to a Factory State. Further definition is beyond the scope of this document. |
| Device Manufacturer | An entity responsible for manufacturing Devices. The Device Manufacturer MAY be responsible for the selection and insertion of eUICCs in Devices. |
| Disabled Profile | Profile, the files and/or applications (e.g. NAA) of which are not selectable over the UICC-Device interface. |
| Embedded UICC (eUICC) | UICC which enables the secure remote and/or local management of Profiles. |
| Enabled Profile | Profile, the files and/or applications (e.g. NAA) of which are selectable over the UICC-Device interface. [18] |
| End User | The person using the Device. |
| End User Data | Information that pertains to the identity of an End User such as personal details, name, address, biometric characteristics, assigned identification numbers, etc.<br>Note: In many jurisdictions (including EU and US), identifying data extends to indirect identifiers (such as ICCID, EID, MSISDN, cookies, etc) that are linkable to a person's real identity when considered in combination with other data sources. |
| eUICC Certificate | A Certificate issued by the EUM for a specific eUICC.<br>This Certificate can be verified using the EUM Certificate. |
| eUICC Eligibility Check Information | The information set sent from the eUICC to the SM-DP+ to allow eligibility checks. |
| eUICC Manufacturer | The eUICC Manufacturer provides eUICC products. |
| eUICC Memory Reset | An action that returns the eUICC to a state equivalent to a Factory State. |
| EUM Certificate | A Certificate issued to a GSMA accredited EUM which can be used to verify eUICC Certificates.<br>This Certificate can be verified using the Root Certificate. |
| Factory State | The configured state of the Device and/or the eUICC at the point it was distributed after manufacture. |

| Term | Description |
|---|---|
| Form Factor | Manifestation of the UICC as specified in ETSI TS 102 221 [2] and ETSI TS 102 671 [3]. |
| ICCID | Unique number to identify a Profile in an eUICC as defined by ITU-T E.118 [19].<br>*Note: the ICCID throughout this specification is used to identify the Profile.* |
| International Mobile Subscriber Identity | Refer to 3GPP 21.905 [4]. |
| 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.<br>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 Management | Local Profile Management are operations that are locally initiated on the ESeu interface. |
| Local Profile Management Operation | Local Profile Management Operations include enable Profile, disable Profile, delete Profile, query Profile Metadata, eUICC Memory Reset, edit nickname, and add Profile. |
| Metadata | The Metadata is a copy of the Data Subset of the respective Profile stored in the eUICC for informative displaying to the End User that contains the information listed in Section 4.6. |
| Mobile Network Operator | An entity providing access capability and communication services to its Subscribers through a mobile network infrastructure. |
| Mobile Virtual Network Operator | An entity providing access capability and communication services to its Subscribers through a mobile network infrastructure but does not have an allocation of spectrum. |
| Network Access Application | Refer to 3GPP 21.905 [4]. |
| Network Access Credentials | Data required to authenticate to an ITU E.212 [5] network. This MAY include data such as Ki/K and IMSI stored within a NAA. |
| Nonce | An arbitrary random number generated for one time use, employed for cryptographic communication. |
| Operator | A Mobile Network Operator or Mobile Virtual Network Operator; a company providing wireless cellular network services. |
| Operator Credentials | A set of credentials owned by the Operator, including Network Access Credentials, OTA Keys for remote Profile Management, and authentication algorithm parameters. |
| OTA Keys | The credentials included in the Profile used in conjunction with OTA Platforms. |
| OTA Platform | A platform used by an Operator for the remote management of enabled Operator Profiles on eUICCs, i.e. using OTA RAM or RFM. |
| 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 Operator data and applications to be provisioned on to an eUICC for the purposes of providing services by the Operator. The Profile SHALL be in support of a Subscription with the relevant Operator. Applications MAY be included to provide non-telecommunication services. |
| Profile Description | The description of a Profile in a format specific to the Operator; example formats could be an Excel table, xml format, or plain text. |
| Profile Management | A combination of local and remote management operations (enable, disable, delete, and query) |
| Profile Package | A personalised Profile using an interoperable description format that is transmitted to an eUICC to load and install a Profile [6]. |
| Protected Profile Package | A Profile Package which has been encrypted for storage but not to a specific eUICC. |
| Remote SIM Provisioning | The downloading, installing, enabling, disabling, switching, and deleting of a Profile on an eUICC. |
| Root Certificate | A Certificate used to authenticate other entities within the Remote SIM Provisioning framework. |
| Service Provider | The Service Provider provides Subscriptions to Subscribers either as part of an Operator or as a party with a wholesale agreement with an Operator. The Service Provider could also be the Operator. |
| Simple Confirmation | Describes a mechanism for which the End User is confirming their action through a confirmation (e.g yes or no). |
| SMDPid | Identifier of the SM-DP+ that is globally unique and is included as part of the SM-DP+ Certificate. |
| Subscriber | An entity (associated with one or more users) that is engaged in a Subscription with an Operator. The Subscriber is allowed to subscribe and unsubscribe to services, as well as register an End User or a list of End Users authorised to use these services. |
| Subscriber Data | Information that pertains to the identity of a Subscriber such as contract details, authentication credentials, cryptographic keys, etc.<br>Note: In many instances, the Subscriber is also the End User and therefore Subscriber Data is likely to include End User Data. |
| Subscription | A Subscription describes the commercial relationship between the Subscriber and the Service Provider. |
| Subscription Manager Data Preparation+ (SM-DP+) | This role prepares Profile Packages, secures them with a Profile protection key, stores Profile protection keys in a secure manner and the Protected Profile Packages in a Profile Package repository, and allocates the Protected Profile Packages to specified EIDs.<br>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. |
| User Intent | Describes the direct, real time acquisition and validation of the manual End User instruction by the LUI to trigger locally a Profile download or Profile Management operation. |

## 1.5 Abbreviations

| Abbreviation | Description |
|---|---|
| AC | Activation Code |
| AuC | Authentication Centre |
| BSS | Business Support Services |
| CI | Certificate Issuer |
| DNSCurve | Domain Name System Curve |
| DNSSEC | Domain Name System Security Extensions |
| ECASD | eUICC Certificate Authority Security Domain |
| EID | Embedded UICC Identifier |
| eSVN | embedded Specification Version Number |
| ETSI | European Telecommunications Standards Institute |
| eUICC | Embedded UICC |
| EUM | eUICC Manufacturer |
| GSMA | GSM Association |
| HLR | Home Location Register |
| HTTP | Hypertext Transfer Protocol |
| ICCID | Integrated Circuit Card Identifier |
| IMSI | International Mobile Subscriber Identity |
| ISD-P | Issuer Security Domain - Profile |
| ISD-R | Issuer Security Domain - Root |
| ISIM | IP Multimedia Services Identity Module |
| ITU | International Telecoms Union |
| LPA | Local Profile Assistant |
| LPD | Local Profile Download |
| LUI | Local User Interface |
| MNO | Mobile Network Operator |
| MNO-SD | Mobile Network Operator - Security Domain |
| MSISDN | Mobile Subscriber International Subscriber Directory Number |
| NAA | Network Access Application |
| OTA | Over The Air |
| RAM | Remote Application Management |
| RFM | Remote File Management |
| SAS | Security Accreditation Scheme |
| SD | Security Domain |
| SIM | Subscriber Identity Module |
| SM-DP+ | Subscription Manager - Data Preparation + |
| 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] | ETSI TS 102 671 | Smart cards; Machine to Machine UICC; Physical and logical characteristics |
| [4] | 3GPP 21.905 | Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications |
| [5] | ITU E.212 | The international identification plan for public networks and Subscriptions |
| [6] | SIMAPP | SIMalliance: eUICC Profile Package - Interoperable Format Technical Specification<br>http://simalliance.org/euicc/euicc-technical-releases/ |
| [7] | ETSI TS 102 226 | Remote APDU structure for UICC based applications |
| [8] | RFC 2119 | “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner<br>http://www.ietf.org/rfc/rfc2119.txt |
| [9] | 3GPP TS 21.133 | 3G security; Security threats and requirements |
| [10] | SGP.02 | GSMA Remote SIM Provisioning of Embedded UICC Technical specification |
| [11] | GPC_SPE_034 | GlobalPlatform Card Specification with its Amendments |
| [12] | 3GPP TS 35.231 | Specification of the TUAK Algorithm Set; Document 1: Algorithm Specification |
| [13] | 3GPP TS 35.205 | Specification of the MILENAGE Algorithm Set; Document 1: General |
| [14] | 3GPP TS 35.206 | Specification of the MILENAGE Algorithm Set; Document 2: Algorithm Specification |
| [15] | RFC 7469 | Public Key Pinning Extension for HTTP |
| [16] | EUM SAS | FS.04 - Security Accreditation Scheme for UICC Production – Standard |
| [17] | SM-DP SAS | FS.08 - GSMA SAS Standard for Subscription Manager Roles |
| [18] | ETSI TS 103 383 | Smart Cards; Embedded UICC; Requirements Specification |
| [19] | ITU-T E.118 | The International Telecommunication Charge Card |

## 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 [8].

# 2 Principles

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

## 2.1 Basic Principles

| Principle no. | Description |
|---|---|
| BAS1 | Existing standards and specifications SHALL be used where possible for the specification of the eUICC and related provisioning systems. |
| BAS2 | GlobalPlatform specifications SHALL be used as a framework of choice for the implementation of the eUICC. |
| BAS3 | The overall security of the eUICC in combination with the related management processes SHALL at all times and under all circumstances be at least equivalent to the current removable UICC and its provisioning processes. |
| BAS4 | The architecture of the eUICC and its Remote SIM Provisioning system SHALL comply with the requirements of 3GPP TS 21.133 [9]. |
| BAS5 | The architecture SHALL support a level of security with respect to the protection of Operator Credentials which is at least equal to the present levels of security. This applies in particular to:<br>• the confidentiality of cryptographic keys and authentication parameters;<br>• 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 equal 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 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 in compliance with local regulations e.g. the EID, ICCID, etc. |

**Table 1 Basic Principles**

## 2.2 Profile Principles

| Principle no. | Description |
|---|---|
| PRO1 | Profiles are the property of and SHALL be under the control of the issuing Operator. |
| PRO2 | A Profile does not exist outside of an eUICC. I.e. a Profile is always located on a particular eUICC. |
| PRO3 | A Profile SHALL be uniquely identified. |
| 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. |

| Principle no. | Description |
|---|---|
| PRO6 | It SHALL be possible to delete Profiles only when in a disabled state, with the exception of the eUICC Memory Reset function which deletes all Profiles. |

**Table 2 Profile Principles**

# 3 Roles

## 3.1 eUICC Manufacturer

| Role no. | Description |
|---|---|
| EUM1 | The eUICC Manufacturer is responsible for the initial cryptographic configuration and security architecture of the eUICC. |
| EUM2 | The eUICCs are delivered by the eUICC Manufacturer (EUM) to other parties (e.g. the Device Manufacturer). |
| EUM3 | Relevant parts of the eUICC Manufacturer's products and processes are certified by a GSMA-approved certification process. |
| EUM4 | The EUM SHALL issue the eUICC Certificate to allow:<br>• eUICC authentication and proof of certification to other entities;<br>• authenticated keyset establishment between a SM-DP+ and an eUICC. |
| EUM5 | Both storage and communication channels for the EUM Certificate and Root Certificate SHALL be reliable. |

**Table 3 eUICC Manufacturer Role**

## 3.2 Device Manufacturer

| Role no. | Description |
|---|---|
| DM1 | The Device Manufacturer SHALL be responsible for the implementation of any LPA elements that reside on the Device and the compliance of the LPA with the requirements in Section 4.8.2. |
| DM2 | The Device Manufacturer SHALL be responsible for the implementation of any application that resides on the Primary Device allowing User Interface access to the Companion Device. |

**Table 4 Device Manufacturer Role**

## 3.3 Operator and Service Provider

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

| Role no. | Description |
|---|---|
| OPE1 | The Operator SHALL have access to a SM-DP+. |
| OPE2 | In the event that a Subscriber has selected a Service Provider, that Service Provider will initiate the provisioning of a Profile. |
| OPE3 | The Operator, potentially on behalf of the Service Provider, specifies the Profile characteristics and any features and applications analogous to |

| Role no. | Description |
|---|---|
| | removable UICCs. |
| OPE4 | Operators SHALL be able to use an OTA Platform in order to manage the content of their Enabled Profile in the eUICC (RAM, RFM). |
| OPE5 | A Subscriber MAY have a relationship with any number of Service Providers simultaneously. |

**Table 5 Operator Role**

## 3.4 Subscriber and End User

| Role no. | Description |
|---|---|
| SEU1 | The Subscriber is the contract partner of the Service Provider for the Subscription.<br>*Note: The Subscriber MAY not be the End User.* |
| SEU2 | The End User is a human and uses the Device and/or the services related to the Enabled Profile. |
| SEU3 | There SHALL be a means for the End User to obtain the EID. |

**Table 6 Subscriber and End User Role**

## 3.5 Certificate Issuer

| Role no. | Description |
|---|---|
| CIS1 | The Certificate Issuer issues Certificates for Remote SIM Provisioning entities and acts as a trusted third party for the purpose of authenticating the entities of the system. |
| CIS2 | The Certificate Issuer communicates with the SM-DP+ and the EUM through interfaces that are out of scope of this specification. |

**Table 7 Certificate Issuer Role**

# 4 Remote SIM Provisioning System Architecture

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

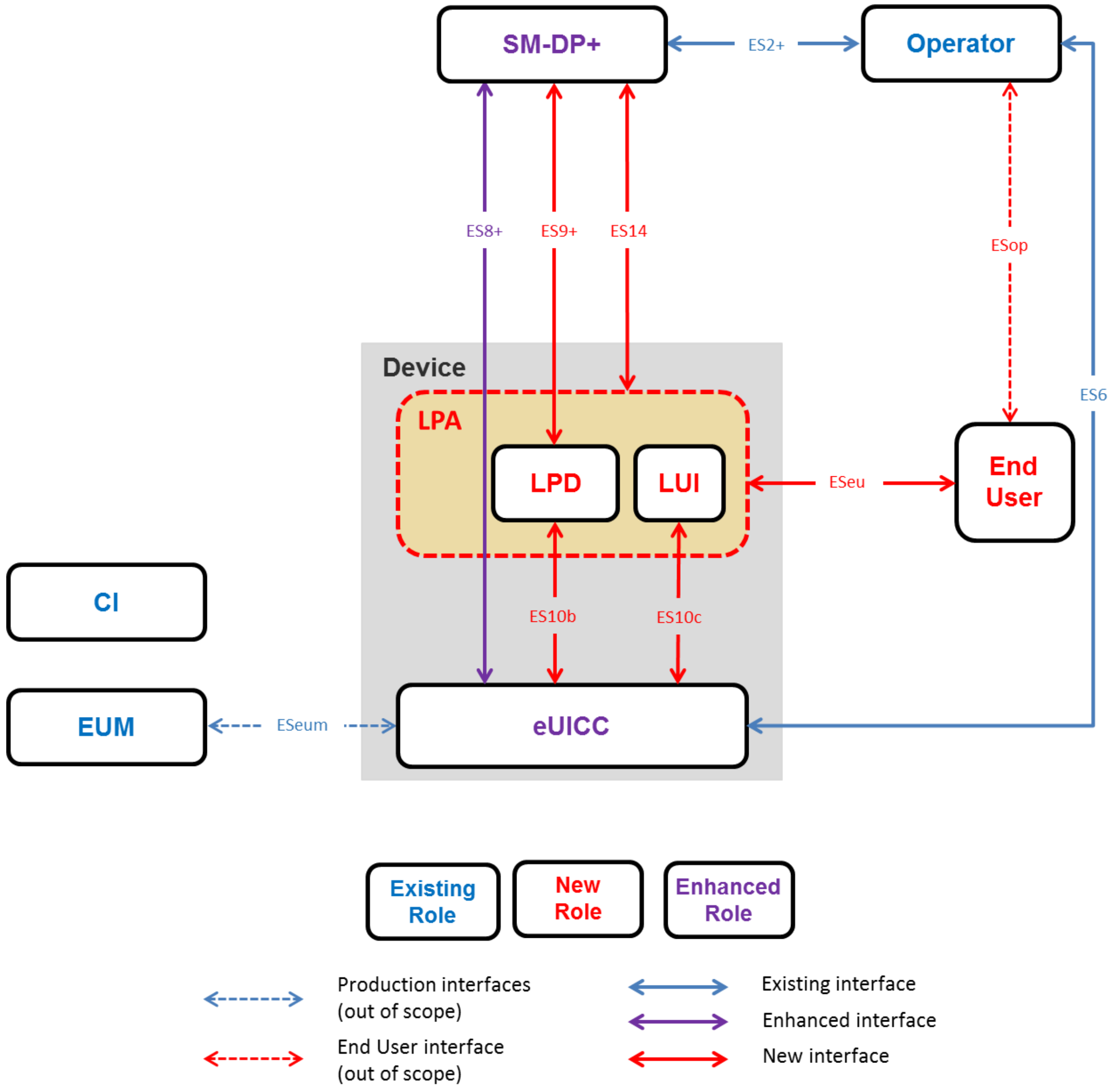

**Figure 1: Remote SIM Provisioning System Architecture**

## 4.1 eUICC Architecture

### 4.1.1 eUICC Architecture Overview

This section describes the internal high-level architecture of the eUICC. It SHOULD be noted that the eUICC architecture is similar to that used in the GSMA Remote SIM specification [10]. Profiles are provisioned based on the security framework defined in the GlobalPlatform Card Specification [11].

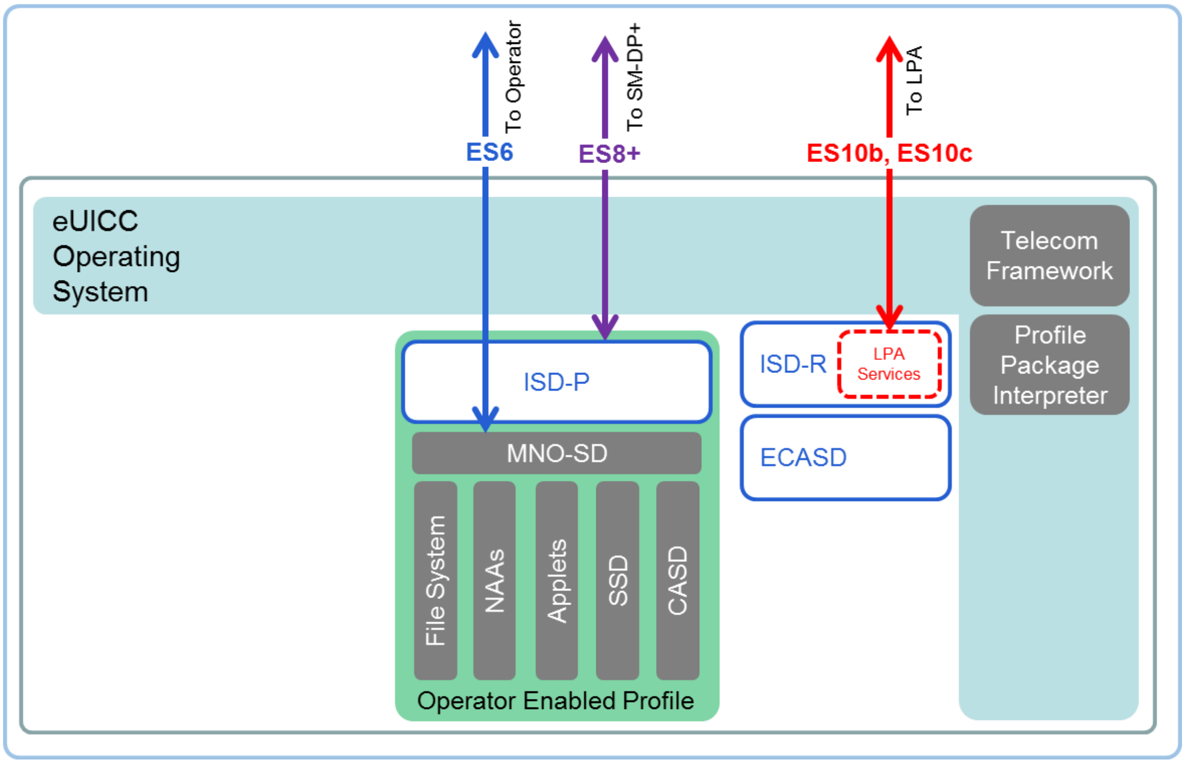

**Figure 2: Schematic Representation of the eUICC**

#### 4.1.1.1 ECASD

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

There SHALL be only one ECASD on an eUICC. The ECASD SHALL be installed and personalised by the EUM during the eUICC manufacturing as described in [11].

The ECASD SHALL have the following properties:

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

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

#### 4.1.1.2 ISD-R

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

#### 4.1.1.3 ISD-P

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

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

#### 4.1.1.4 MNO–SD

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

#### 4.1.1.5 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.

#### 4.1.1.6 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.

#### 4.1.1.7 LPA Services

The LPA services provide necessary access to the services and data required by the LPA functions.

## 4.2 eUICC Requirements

| Req no. | Description |
|---|---|
| EUICC1 | The eUICC is a discrete hardware component in a standardised ETSI Form Factor [2] [3]. |
| EUICC2 | The eUICC SHALL be either removable or non-removable. |
| EUICC3 | The behaviour of the eUICC with an Enabled Profile SHALL be similar to the UICC. |
| EUICC4 | The eUICC SHALL be able to contain zero or one Profile. |
| EUICC5 | At a maximum, only one Profile SHALL be enabled at any point in time. |
| EUICC6 | The behaviour of a NAA USIM or ISIM within a Profile on an eUICC SHALL be identical to a removable UICC NAAs USIM or ISIM.<br>*Note: No changes to existing 3GPP/3GPP2 USIM, CSIM and ISIM specifications are expected.* |
| EUICC7 | The eUICC MAY implement the TUAK algorithm [12] in addition to Milenage [13][14]. |
| EUICC8 | The ownership of the eUICC MAY change throughout its lifetime as can the Device. |
| EUICC9 | If any operation such as Profile enabling, Profile disabling, and Profile download and installation does not complete successfully, the eUICC SHALL maintain the state it was in before it received the request. |
| EUICC10 | The eUICC SHALL contain an ECASD and ISD-R security domains installed and personalised during manufacture. |
| EUICC11 | The ECASD cannot be deleted or modified after eUICC manufacture. |
| EUICC12 | The ISD-R SHALL be responsible for the creation of new ISD-Ps and the lifecycle management of all ISD-Ps. |

| Req no. | Description |
|---|---|
| EUICC13 | The ISD-R SHALL be installed and personalised by the EUM during eUICC manufacturing as described in [11]. |
| EUICC14 | The eUICC SHALL be able to support an eUICC Memory Reset. This can only be requested by the End User. |
| EUICC15 | The eUICC SHALL support the eUICC Profile Package Interoperable format as defined by SIMalliance [6]. |
| EUICC16 | An ISD-R SHALL:<br>• be created within an eUICC at the time of manufacture;<br>• NOT be deleted or disabled;<br>• NOT be able to perform any operations inside an ISD-P. |
| EUICC17 | An ISD-P SHALL be created by the ISD-R at the request of the SM-DP+. |
| EUICC18 | If a Profile download and installation does not terminate successfully, the Profile and the ISD-P SHALL be securely deleted. |
| EUICC19 | The eUICC SHALL ensure that the communication between the eUICC and the SM-DP+ participating in the Profile creation is protected in authenticity, integrity, and confidentiality. |
| EUICC20 | The eUICC SHALL NOT export Profiles installed on the eUICC. |
| EUICC21 | 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. |
| EUICC22 | The integrity of the Bound Profile Package SHALL be ensured during its installation on the eUICC. |
| EUICC23 | The eUICC SHALL be tamper resistant (physically and logically). |
| EUICC24 | Profile keys and algorithm parameters SHALL NOT be extractable from the eUICC. |
| EUICC25 | All cryptographic functions SHALL be implemented in a robust tamper-resistant way and be resistant to side-channel attacks. |
| EUICC26 | The Operator SHALL be able to update the OTA Keys in its Profile on the eUICC in a secure and confidential way, reusing existing OTA Platform mechanisms. |
| EUICC27 | A downloaded Profile Package SHALL be installed on the eUICC in a disabled state. |
| EUICC28 | The eUICC SHALL enforce a mechanism to ensure that there is not more than one Profile installed.<br>*Note: This mechanism enforcement is dedicated for phase 1.* |
| EUICC29 | The eUICC SHALL always report its specification version number in the first communication during the commencement of each session. |
| EUICC30 | The EUM SHALL install an eUICC Certificate in the eUICC used to verify the eUICC Certification. |
| EUICC31 | The EUM SHALL install an EUM Certificate in the eUICC used to verify the eUICC Certificate. |

**Table 8 eUICC Requirements**

## 4.3 eUICC Eligibility Check

The eUICC eligibility check enables a SM-DP+ to validate the eligibility of an eUICC for the installation of a Profile using information sent by the eUICC. The set of information sent by the eUICC to the SM-DP+ for eligibility checking purposes is referenced herein as the eUICC Eligibility Check Information.

### 4.3.1 eUICC Eligibility Check Requirements

| Req no. | Description |
|---|---|
| ELG1 | The eUICC SHALL include the eSVN in the eUICC Eligibility Check Information. |
| ELG2 | The eUICC SHALL include the available memory in the eUICC Eligibility Check Information. |
| ELG3 | The eUICC SHALL declare whether a Profile is currently installed in the Eligibility Check Information. |
| ELG4 | Eligibility Check Information SHALL be integrity and authenticity protected by the eUICC for its sending to the SM-DP+. |

**Table 9 eUICC Eligibility Check Requirements**

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

## 4.4 Device Requirements

| Req no. | Description |
|---|---|
| DEV1 | The Device SHALL conform to the terminal requirements within ETSI TS 102 221 [2] or ETSI TS 102 671 [3]. |
| DEV2 | There SHALL be a means for the End User to obtain the EID from the Device. |
| DEV3 | If an eUICC is within the Device packaging, then the EID SHALL be printed in machine readable form on the Device packaging. |
| DEV4 | Bearer connection of the Companion Device to the SM-DP+ SHALL only be determined by the bearer availability.<br>*Note: The Companion Device MAY use any connectivity method available to connect to the SM-DP+.* |

**Table 10 Device Requirements**

## 4.5 Device Initiated Requirements

### 4.5.1 Device Factory Reset

| Req no. | Description |
|---|---|
| FAC1 | Invocation of Device Factory Reset SHALL NOT impact the eUICC. |

**Table 11 Device Factory Reset Requirements**

### 4.5.2 eUICC Memory Reset

| Req no. | Description |
|---|---|
| MEM1 | eUICC Memory Reset SHALL delete all Profiles on the eUICC including the Enabled Profile if any. |
| MEM2 | A secured means SHALL be provided to enable eUICC Memory Reset. |
| MEM3 | Such means as described in MEM2, SHALL include an item in the LUI menu of the Device. |
| MEM4 | In addition to MEM3, other secure means MAY be provided to perform the eUICC Memory Reset function. The same level of security and User Intent as is offered by the LUI based reset function SHALL apply. |

**Table 12 eUICC Memory Reset Requirements**

## 4.6 Metadata Requirements

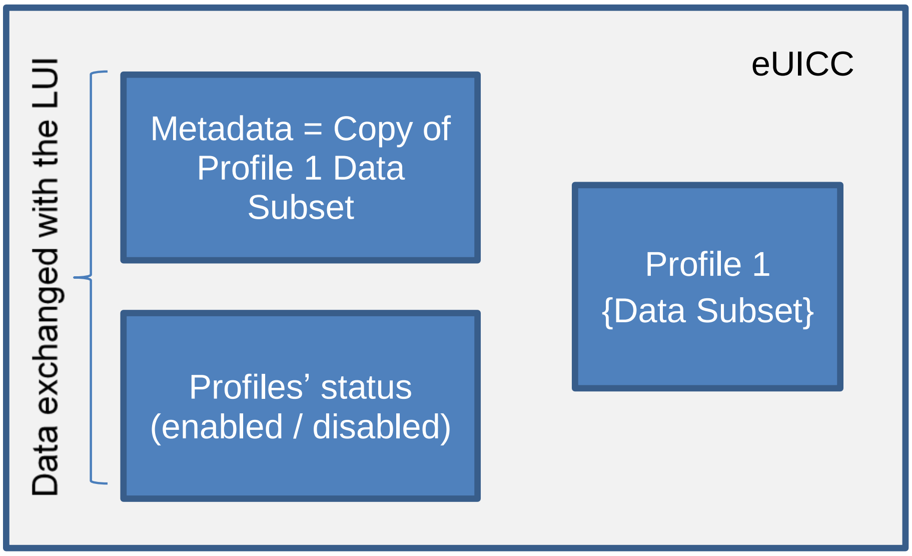
eUICC
Data exchanged with the LUI
Metadata = Copy of Profile 1 Data Subset
Profiles' status (enabled / disabled)
Profile 1
{Data Subset}

**Figure 3: eUICC Metadata Representation**

| Req no. | Description |
|---|---|
| META1 | All Profiles SHALL have a Data Subset which will be included in the associated Metadata. |
| META2 | When a Profile is installed, the Metadata SHALL be automatically copied by the eUICC operating system from the Profile Data Subset during Profile installation. |
| META3 | The Metadata SHALL at all times reflect the respective data in the Profile with the exception of the nickname which can be edited by the End User. |
| META4 | The Metadata SHALL be exclusively stored in the eUICC. |
| META5 | The Metadata SHALL be accessible irrespective of the state of the Profile. |
| META6 | The Metadata SHALL include a field for the Service Provider name. The Elementary File of the Profile associated with this data SHALL be EFmetservice (a new EF TBD).<br>*Note: EFSPN is already used in a different context outside of this specification and could be blank.* |

| Req no. | Description |
|---|---|
| META7 | The Metadata SHALL include a field for the ICCID of the Profile. The Elementary File of the Profile associated with this data SHALL be EFiccid. |
| META8 | The Metadata SHALL include a field for the End User nickname of the Profile. The Elementary File of the Profile associated with this data SHALL be EFmetnick (a new EF TBD). |
| META9 | The Metadata SHALL include a field for containing a short description of the Profile defined by the Operator/Service Provider. The Elementary File of the Profile associated with this data SHALL be EFmettxt (a new EF TBD). |
| META10 | The nickname SHALL be End User editable. |
| META11 | The Metadata SHALL always be available to the LUI to allow the End User to be informed of installed Profiles in the eUICC. |
| META12 | The Metadata SHALL include a field to allow the display of an icon defined by the Operator/Service Provider for the respective Profile. |

**Table 13 Metadata Requirements**

## 4.7 Subscription Manager Data Preparation + (SM-DP+)

### 4.7.1 SM-DP+ Overview

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

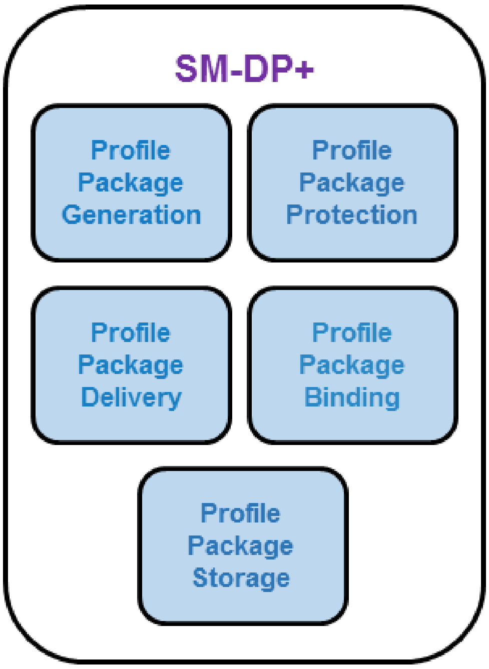

**Figure 4: SM-DP+ Functions**

| 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 or directly to the eUICC. |

**Table 14 SM-DP+ Function Descriptions**

### 4.7.2 SM-DP+ Requirements

| Req no. | Description |
|---|---|
| SMDP1 | The SM-DP+ SHALL act on behalf of the Operator. |
| SMDP2 | The SM-DP+ SHALL be able to initiate the request for ISD-P creation as part of the Bound Profile Package delivery. |
| SMDP3 | The SM-DP+ SHALL establish an end-to-end secure channel to the eUICC to download and install Bound Profile Packages via the LPA. |
| SMDP4 | The SM-DP+ SHALL allocate 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 allocated 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 | Once the Bound Profile Package is downloaded, the SM-DP+ SHALL NOT retain a network connection to the LPA/eUICC. |
| 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 | The SM-DP+ SHALL accept “Certificate pinning” operations up to server granularity (refer to [15]). |
| SMDP13 | 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). |
| SMDP14 | Past communications associated with Bound Profile Package download and |

| Req no. | Description |
|---|---|
| | installation between the SM-DP+ and the eUICC whenever intercepted by a third party, SHALL NOT be recoverable due to the compromise of a single long-term key (i.e. Perfect Forward Secrecy). |
| SMDP15 | The transport used for the Bound Profile Package SHALL implement anti-replay mechanisms between the SM-DP+ and the eUICC. |
| SMDP16 | Connectivity to the SM-DP+ SHALL be aborted and an explicit error message SHALL be triggered by the SM-DP+ upon failure to verify authenticity of the connecting party. (No message SHALL be sent to the connecting party) |
| SMDP17 | After a configurable number of failed attempts to download a Bound Profile Package, the transport encryption procedure SHALL be renewed.<br>If subsequent attempts to download the Bound Profile Package fail more than a configurable number of times, the provisioning transaction SHALL be terminated and the Operator SHALL be notified. |
| SMDP18 | The SM-DP+ SHALL use a secure version of Internet protocols whenever available (e.g. DNSSEC, DNSCurve, etc.). |
| SMDP19 | The SM-DP+ SHALL implement rate-limiting mechanisms to avoid DoS attacks. |
| SMDP20 | The SM-DP+ SHALL log all Certificate authentication failures. |
| SMDP21 | The SM-DP+ SHALL prepare Profile Packages following the eUICC Profile Package Interoperable Format Specification as defined by SIMalliance [6]. |
| SMDP22 | The SM-DP+ SHALL be able to create Bound Profile Packages on demand. |
| SMDP23 | It SHALL be possible for the SM-DP+ to create Profile Packages in bulk. |
| SMDP24 | The SM-DP+ SHALL send a confirmation of the successfully completed download and installation of a Profile to the Operator. |
| SMDP25 | There SHALL be a mechanism to remove any relationship between the 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. |
| SMDP26 | The SM-DP+ SHALL be globally uniquely identified by its SMDPid. |
| SMDP27 | The SM-DP+ Certificate SHALL include the SMDPid. |

**Table 15 SM-DP+ Requirements**

## 4.8 Local Profile Assistant (LPA)

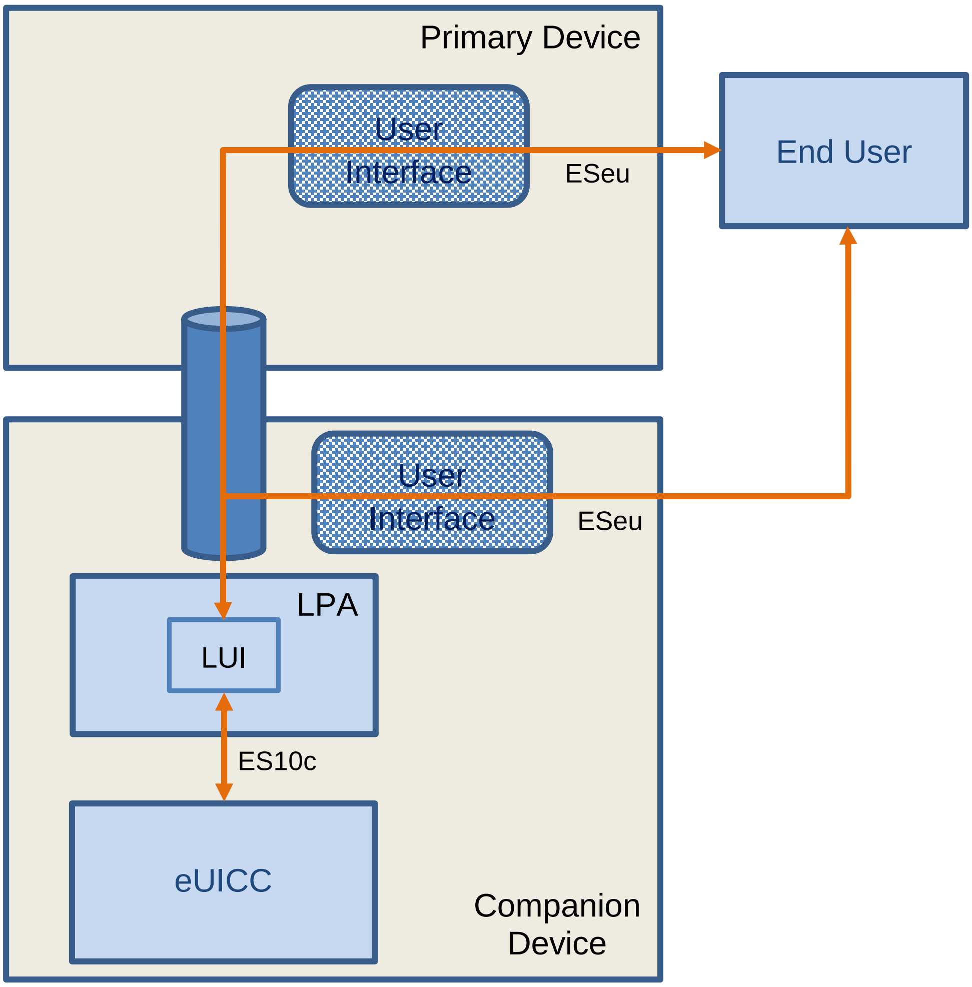

**Figure 5: End User Interaction and Interfaces between a Primary and Companion Device, where the Companion Device MAY have a UI**

### 4.8.1 LPA Overview

This role exists within the Device and in conjunction with LPA Services provided by the eUICC. It provides two distinct functions 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. Therefore, the functions of the LPA will be undertaken within the Device. The way this variability is implemented across different Devices and Device types is for further study.

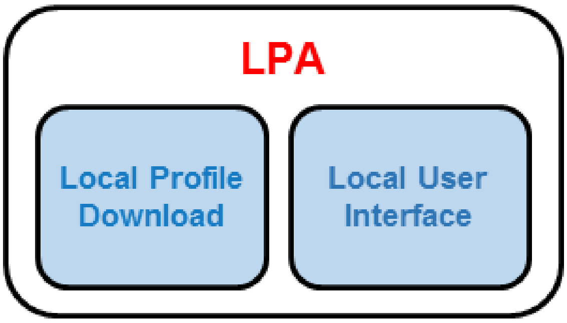

**Figure 6: LPA Functions**

| Function name | Description |
|---|---|
| Local Profile Download<br>(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.<br>This function will depend on network, Device, and eUICC capabilities. |
| Local User Interface<br>(LUI) | This function allows Local Profile Management on the Device by the End User. User Intent has to be enforced as required. |

**Table 16 LPA Function Descriptions**

### 4.8.2 LPA Requirements

| Req no. | Description |
|---|---|
| LPA1 | The LPA SHALL be responsible for instructing the eUICC to perform Local Profile Management functions as per End User request. |
| LPA2 | A mechanism SHALL be implemented between any LPA elements outside the eUICC, and the eUICC to ensure that the communication is not compromised. |
| LPA3 | A secure mechanism SHALL be implemented between the LUI and the associated display or input applications on the Device. |
| LPA4 | Access to the LUI application(s) SHALL be protected according to current best practices. This SHALL be enforced by the Device OS. |
| LPA5 | All Local Profile Management Operations SHALL require User Intent (no automation). |
| LPA6 | LUI access SHALL require User Intent (no automation). |
| LPA7 | The End User SHALL be able to easily access the list of installed Profiles. |
| LPA8 | Profile Metadata SHALL be protected from unauthorised access. |
| LPA9 | The Local Profile Management Operation, 'enable' SHALL be supported. This operation SHALL allow the End User to select the Profile. |
| LPA10 | The Local Profile Management Operation, 'disable' SHALL be supported. This operation SHALL allow the End User to disable the Enabled Profile. |
| 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. Authenticated 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 Profiles on the eUICC and relevant associated information through the Metadata. |
| LPA13 | The Local Profile Management Operation 'eUICC Memory Reset' SHALL be supported. This operation SHALL execute the eUICC Memory Reset as described in Section 4.5.2. The End User SHALL acknowledge the message of consequences of 'eUICC Memory Reset'. Authenticated Confirmation SHALL be enforced. |
| LPA14 | The Local Profile Management Operation 'edit nickname' SHALL be supported. This operation SHALL allow the End User to add or modify a nickname for the selected Profile. The operation SHALL NOT modify the Service Provider name. |
| LPA15 | The Local Profile Management Operation "add Profile" SHALL be supported. This |

| | |
|---|---|
| | operation SHALL allow the LPA to request an Activation Code in order to download and install a new Profile to the eUICC. Authenticated Confirmation SHALL be enforced. |
| LPA16 | The LPA SHALL NOT be accessible by any applications other than that developed by the provider of the LPA for the sole purpose of enabling the services and functions of the LPA. |
| LPA17 | The LPA provider SHALL enforce a secure and non-interceptable Authenticated Confirmation. |
| LPA18 | The LPA provider SHALL enforce a secure and non-interceptable Simple Confirmation located on the Device. |
| LPA19 | Access to the LUI SHALL be protected by an Authenticated Confirmation. |
| LPA20 | The mechanism in LPA19 SHALL be selectable/unselectable by the End User. |
| LPA21 | The mechanisms in LPA19 SHALL be prompted to be enabled by default but this can be skipped by the End User. |
| LPA22 | The Device SHALL implement a mechanism to protect the LPA access through an Authenticated Confirmation. This Authenticated Confirmation MAY be implemented by using the mechanisms implemented in the Device such as phone lock code, fingerprint input, etc. |
| LPA23 | The End User SHALL be able to define dedicated personalised information to access the LPA. |
| LPA24 | If the End User selects the protection of access to the LUI (LPA21), then the subsequent Authenticated Confirmation at operation level MAY be replaced with a Simple Confirmation. |
| LPA25 | When enforced, any User Intent SHALL allow the End User to cancel the Local Profile Management Operation. |
| LPA26 | It SHALL be possible to expose the LUI of a Companion Device allowing input from an End User interface on the Primary Device. |
| LPA27 | When a Companion Device LUI allows input from a Primary Device, the Companion Device LUI SHALL be able to restrict the actions that can be applied. For example:<br>• not offer the eUICC Memory Reset;<br>• only ‘enable’ and ‘disable’ operation are exposed.<br>• Profile enabling is exposed only if no Profile is already enabled on the Companion Device. |
| LPA28 | The LUI of the Companion Device SHALL be able to request an End User initiated action on the Companion Device before the establishment of any proximity secure link (used for inputs into the LUI from another Device). |
| LPA29 | A point-to-point proximity secure link initiated by the End User and offering confidentiality and integrity SHALL be established between the Companion and Primary Device for any input executed from the Primary Device. |
| LPA30 | Any required User Intent SHALL only be executed by the LPA on the Companion Device. A User Intent input MAY be done in either the Primary or the Companion Device. |
| LPA31 | The Device Manufacturer of the Companion Device SHALL implement a secure measure to ensure integrity and eligibility of any application accessing the LUI. |
| LPA32 | The End User Data used for the User Intent protection (e.g. PIN code, fingerprint) |

| | |
|---|---|
| | SHALL be stored in a secure environment. |
| LPA33 | 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+ can be established. |
| LPA34 | 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+ can be established. |
| LPA35 | The LPA SHALL be able to determine if a connection to the internet and or SM-DP+ is available. |
| LPA36 | The LPA SHALL be able to prompt the End User that there is no connection to internet and or no connection to the SM-DP+, in order to allow the End User to enable or troubleshoot required connectivity. |
| LPA37 | The LPA SHALL only be able to access the eUICC if it has assigned privileges. |
| LPA38 | There SHALL only be one LPA on the Device. |
| LPA39 | Any action where the End User MAY be unaware of the consequences about the result of the operation, the LUI SHALL offer additional explanation prior to user acceptance. |
| LPA40 | The LPA SHALL only handle actions that are described in this specification. |
| LPA41 | The LPA SHALL have no part in or trigger the subscription selection process. |
| LPA42 | LPA procedures SHALL always be initiated by the LPA itself. |
| LPA43 | LPA procedures SHALL not be called by any external (non-LPA) processes. |

**Table 17 LPA Requirements**

## 4.9 Interfaces

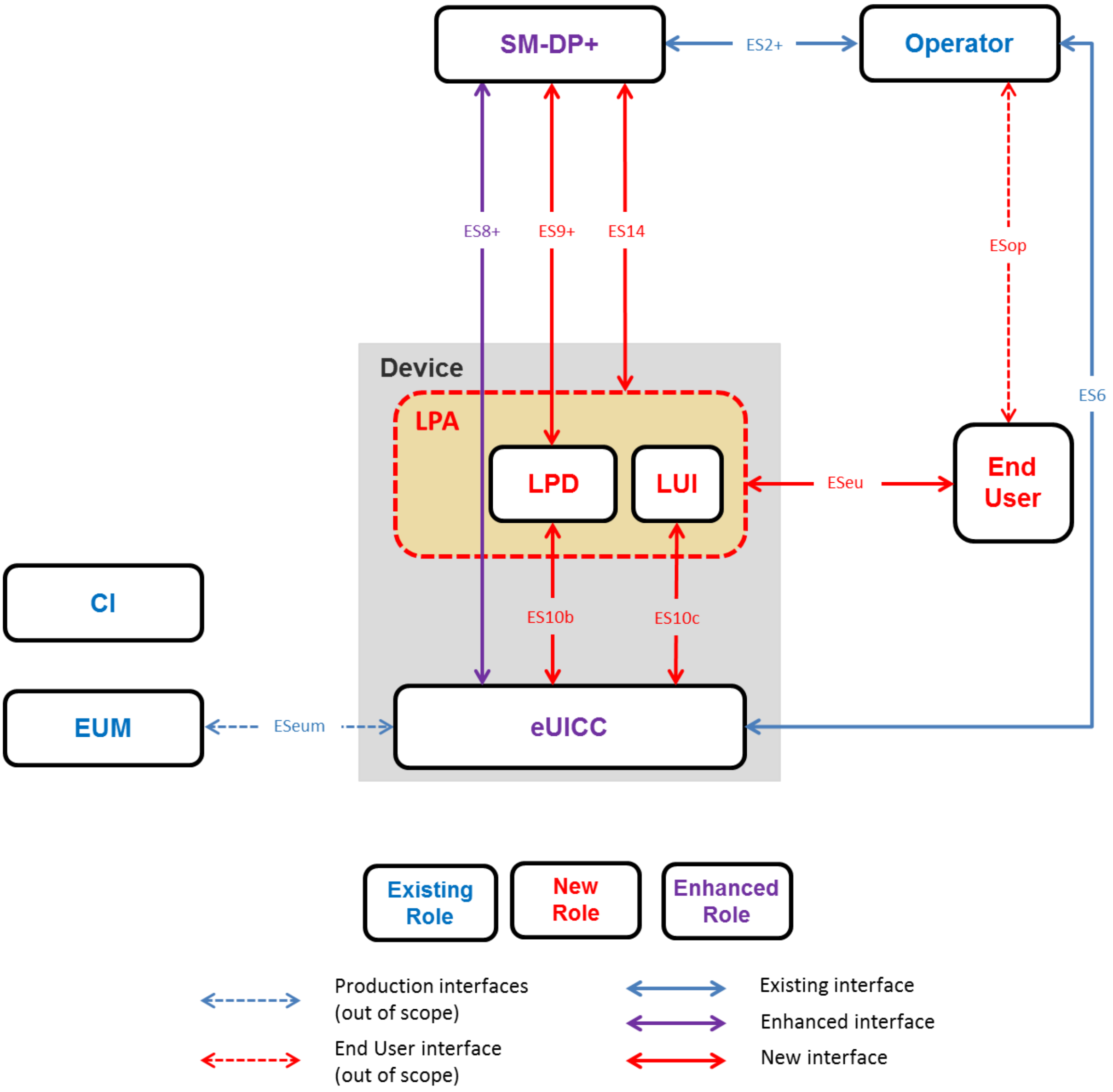

**Figure 7: Interfaces on the eUICC Architecture with the LPA in the Device Configuration**

### 4.9.1 Operator – SM-DP+ (ES2+)

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

### 4.9.2 Operator – End User (ESop)

Out of scope of this document.

### 4.9.3 End User - LUI (ESeu)

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

In a Primary/Companion Device scenario the LUI used SHALL only reside on the Companion Device.

The ESeu interface is used to support the following requirements:

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

**Table 18 End User to LUI (ESeu) Interface Requirements**

### 4.9.4 Operator – eUICC (ES6)

Used by the Operator for the management of Operator services via OTA services.

### 4.9.5 LPA – SM-DP+ (ES14)

This interface 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

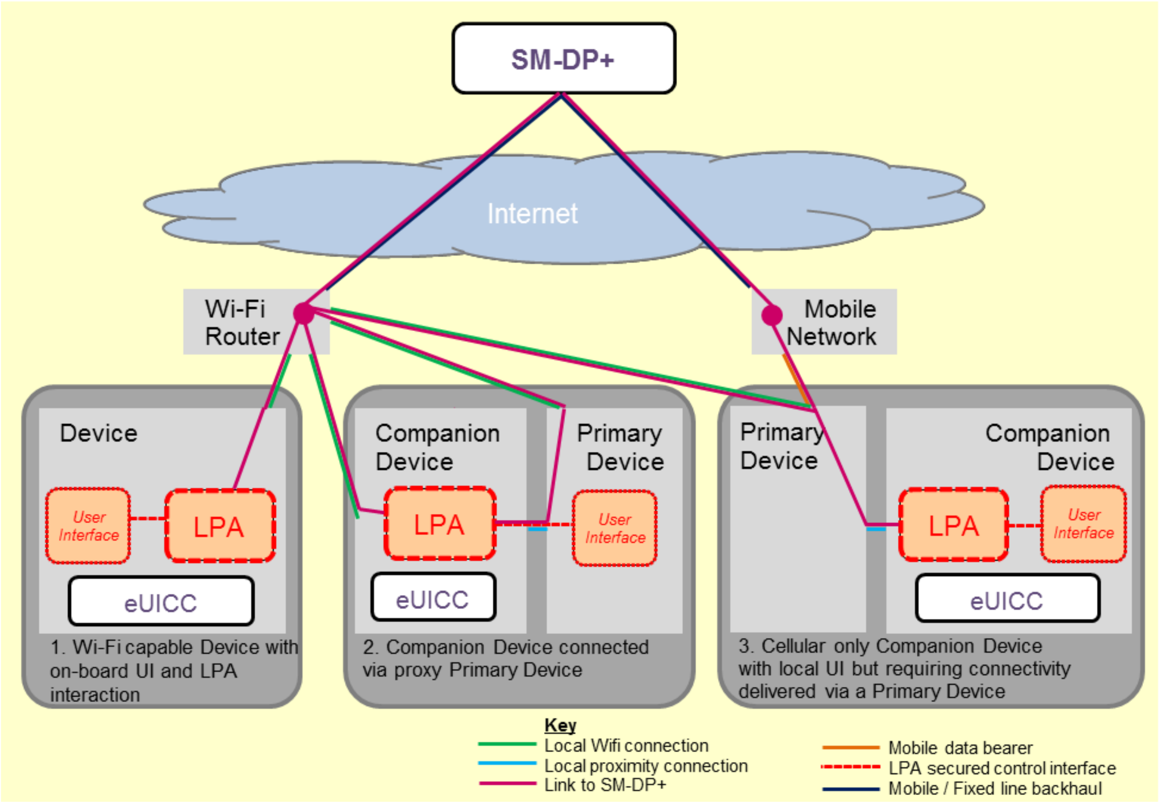
SM-DP+
Internet
Wi-Fi Router
Mobile Network
Device
User Interface
LPA
eUICC
1. Wi-Fi capable Device with on-board UI and LPA interaction
Companion Device
Primary Device
LPA
User Interface
eUICC
2. Companion Device connected via proxy Primary Device
Primary Device
Companion Device
LPA
User Interface
eUICC
3. Cellular only Companion Device with local UI but requiring connectivity delivered via a Primary Device
Key
Local Wifi connection
Local proximity connection
Link to SM-DP+
Mobile data bearer
LPA secured control interface
Mobile / Fixed line backhaul

**Figure 8: Example Connection Methods for Companion Devices to reach out to the SM-DP+**

### 4.9.6 SM-DP+ – LPD (ES9+)

For Devices with an LPA, this interface is used to provide a secure transport for the delivery of the Bound Profile Package between the SM-DP+ and the LPD.

### 4.9.7 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. It is an enhanced version of the existing ES8 interface, providing Perfect Forward Secrecy.

### 4.9.8 EUM – eUICC (ESeum)

Out of scope of this document.

### 4.9.9 LPD – eUICC (ES10b)

The ES10b interface is used by the LPA to transfer a Bound Profile Package to the eUICC.

### 4.9.10 LUI – eUICC (ES10c)

The ES10c interface is used for Local Profile Management by the End User.

### 4.9.11 General Interface Requirements

| Req no. | Description |
|---|---|
| INT1 | All interfaces from the eUICC SHALL indicate the specification version number. |
| INT2 | The behaviour of all interfaces SHALL support the indicated specification version number. |
| INT3 | During the indication of the supported specification version number from the eUICC to the SM-DP+, the eUICC version SHALL be used or the procedure SHALL fail. See table below. |
| INT4 | All communicating entities involved in remote Profile Management SHALL be mutually authenticated. |

**Table 19 General Interface Requirements**

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

**Table 20 eUICC Version vs Platform**

## 4.10 Certification

### 4.10.1 eUICC Certification

| Req no. | Description |
|---|---|
| CERTEU1 | The EUM SHALL be GSMA SAS certified [16]. |
| CERTEU2 | The EUM SHALL be required to declare eUICC product compliance with GSMA SGP.22 V1.0. |
| CERTEU3 | The eUICC Certificate SHALL be signed by the EUM. |

**Table 21 eUICC Certification Requirements**

### 4.10.2 SM-DP+ Certification

| Req no. | Description |
|---|---|
| CERTDP1 | The SM-DP+ provider SHALL be required to declare product (SM-DP+) compliance with GSMA SGP.22 V1.0. |
| CERTDP2 | The SM-DP+ SHALL be GSMA SAS SM-DP part certified [17] excluding the communication with the SM-SR. |
| CERTDP3 | The SM-DP+ Certificate SHALL be signed by the GSMA CI. |

**Table 22 SM-DP+ Certification Requirements**

# 5 Operational Procedures

## 5.1 Profile Download with Activation Code

### 5.1.1 Activation Code Requirements

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

**Table 23 Activation Code Requirements**

### 5.1.2 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 Operator Profile from the Device itself.

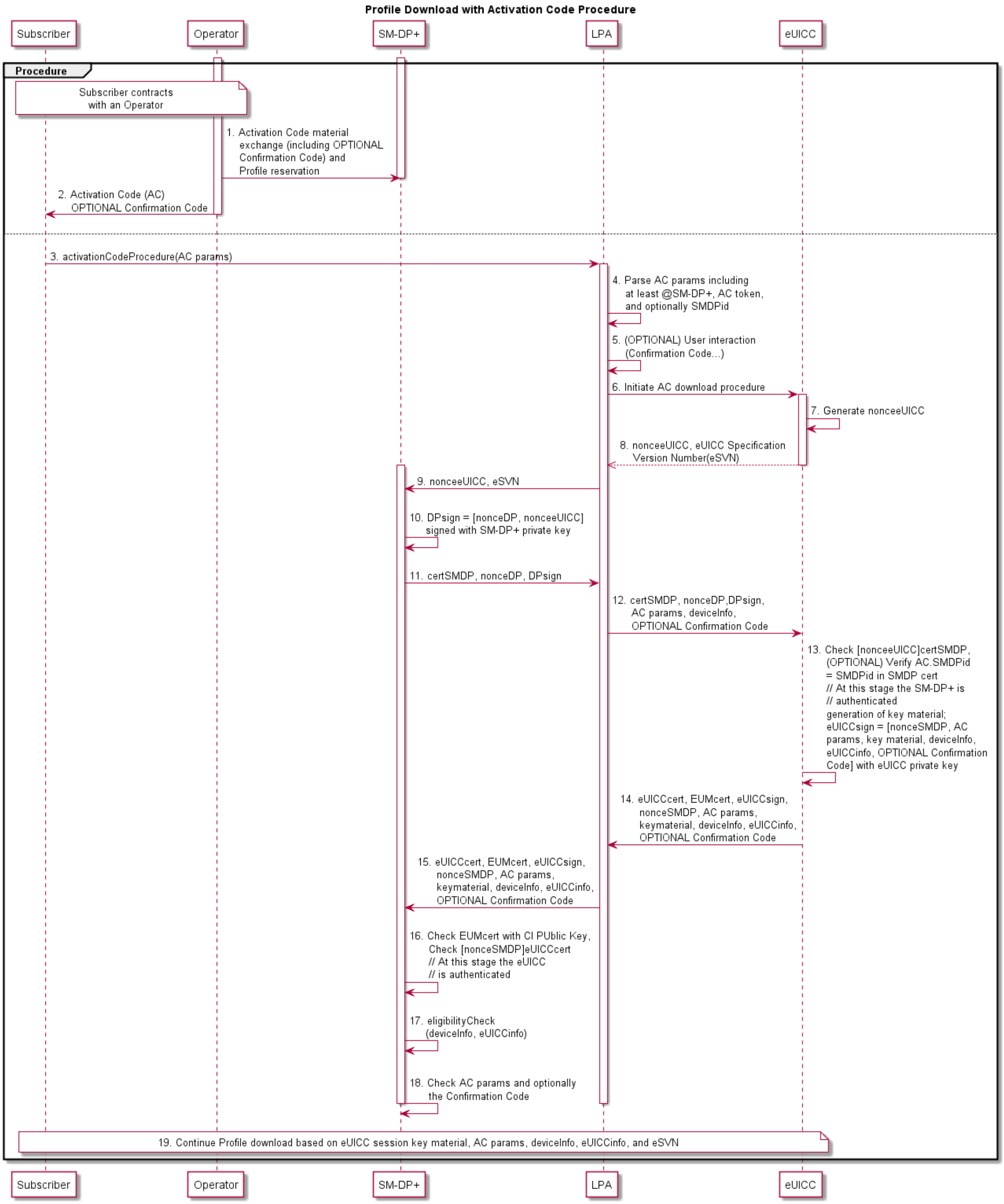
Profile Download with Activation Code Procedure
Subscriber
Operator
SM-DP+
LPA
eUICC
Procedure
Subscriber contracts with an Operator
1. Activation Code material exchange (including OPTIONAL Confirmation Code) and Profile reservation
2. Activation Code (AC) OPTIONAL Confirmation Code
3. activationCodeProcedure(AC params)
4. Parse AC params including at least @SM-DP+, AC token, and optionally SMDPid
5. (OPTIONAL) User interaction (Confirmation Code...)
6. Initiate AC download procedure
7. Generate nonceeUICC
8. nonceUICC, eUICC Specification Version Number(eSVN)
9. nonceeUICC, eSVN
10. DPsign = [nonceDP, nonceeUICC] signed with SM-DP+ private key
11. certSMDP, nonceDP, DPsign
12. certSMDP, nonceDP,DPsign, AC params, deviceInfo, OPTIONAL Confirmation Code
13. Check [nonceeUICC]certSMDP, (OPTIONAL) Verify AC.SMDPid = SMDPid in SMDP cert // At this stage the SM-DP+ is // authenticated generation of key material; eUICCsign = [nonceSMDP, AC params, key material, deviceInfo, eUICCinfo, OPTIONAL Confirmation Code] with eUICC private key
14. eUICCcert, EUMcert, eUICCsign, nonceSMDP, AC params, keymaterial, deviceInfo, eUICCinfo, OPTIONAL Confirmation Code
15. eUICCcert, EUMcert, eUICCsign, nonceSMDP, AC params, keymaterial, deviceInfo, eUICCinfo, OPTIONAL Confirmation Code
16. Check EUMcert with CI PUblic Key, Check [nonceSMDP]eUICCcert // At this stage the eUICC // is authenticated
17. eligibilityCheck (deviceInfo, eUICCinfo)
18. Check AC params and optionally the Confirmation Code
19. Continue Profile download based on eUICC session key material, AC params, deviceInfo, eUICCinfo, and eSVN
Subscriber
Operator
SM-DP+
LPA
eUICC

**Figure 9: Profile Download with Activation Code Procedure**

**Start Conditions:**

a. A Subscription has been established by the Subscriber.
b. An Activation Code has been provided to the End User and optionally a Confirmation Code (side channel).

**Procedure:**

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

Note: Prior to this step a HTTPs session SHALL be established between the LPA and the SM-DP+ based on a public key of the Root certificate stored in the Device used for the TLS session.

8. Upon receiving the nonceeUICC and the associated eSVN, the SM-DP+ creates nonceSMDP and signs both the nonceSMDP and the nonceeUICC.
9. The SM-DP+ sends the signed nonceeUICC and nonceSMDP to the LPA.
10. The LPA collects the Activation Code parameters as well as the Device information needed for the eligibility procedure and optionally the Confirmation Code and transmits them with the signed nonceeUICC and nonceSMDP to the eUICC.
11. The eUICC checks the signature attached to the nonceeUICC. If the SMDPid is configured in the AC, the eUICC checks that the SMDPid provided by the LPA and the SMDPid in the SM-DP+ Certificate correspond. The SM-DP+ is at this stage authenticated by the eUICC. The eUICC generates key material that will be used for the session key establishment.The eUICC signs a set of information with the eUICC private key which includes:
    a. The nonceSMDP
    b. Key material created by the eUICC to calculate session keys for the preparation of the Bound Profile Package
    c. Activation Code parameters
    d. The Device and eUICC information
    e. Optionally the Confirmation Code
12. 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
13. The LPA sends the whole set of information received from the eUICC to the SM-DP+.
14. 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+.
15. The SM-DP+ proceeds with the eligibility check based on the transmitted information (EID, Device information, eUICC information, eSVN).
16. The SM-DP+ checks the Activation Code parameters and optionally the Confirmation Code to retrieve the referenced Profile Package.
17. The Profile Package is downloaded to the eUICC:
   a. The SM-DP+ establishes session keys with the eUICC.
   b. A Bound Profile Package is prepared on the basis of the eUICC session key material and is downloaded and installed on the eUICC.
   c. Successful installation of the Profile on the eUICC is acknowledged and the Operator is notified by the SM-DP+.
   d. Successful installation of the Profile on the eUICC is acknowledged by the eUICC to the LPA which notifies the End User of the status.

**End Conditions:**

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

## 5.2 Local Profile Management Procedures

### 5.2.1 Enable Profile

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

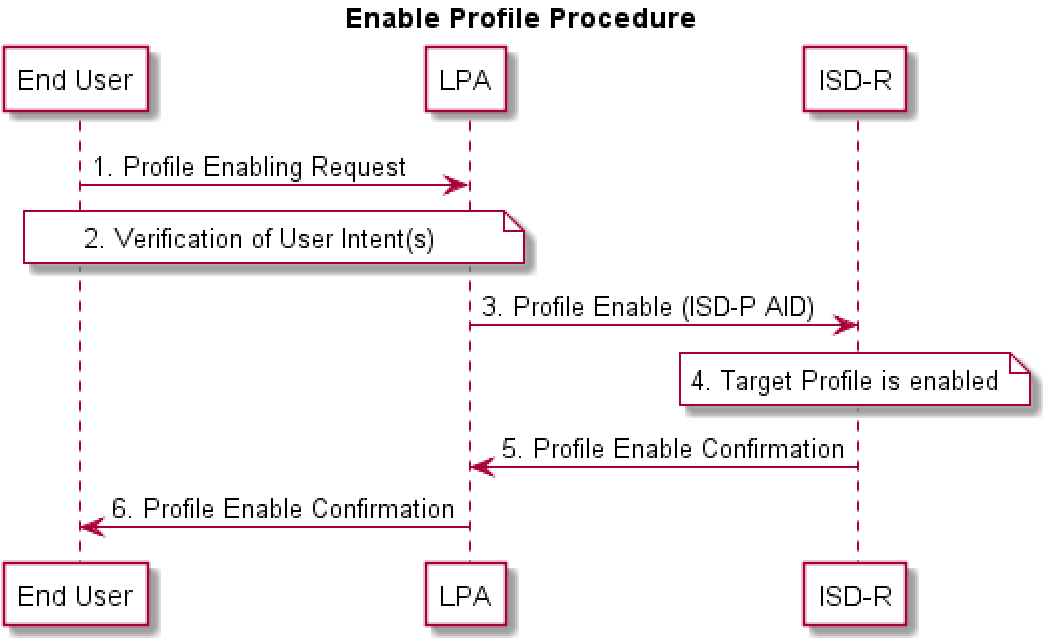
Enable Profile Procedure
End User
LPA
ISD-R
1. Profile Enabling Request
2. Verification of User Intent(s)
3. Profile Enable (ISD-P AID)
4. Target Profile is enabled
5. Profile Enable Confirmation
6. Profile Enable Confirmation
End User
LPA
ISD-R

**Figure 10: Enable Profile Procedure**

**Start conditions:**

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

**Procedure**:

1. The End User makes a Profile enable request on the LPA.
2. User Intent is verified.
3. The LPA sends a Profile enable operation for the target Profile to the ISD-R on the eUICC.
4. The target Profile is enabled.
5. The ISD-R informs the LPA of the enabling of the Profile.
6. The End User is informed via the LPA.

**End conditions:**

a. The target Profile is enabled.

### 5.2.2 Disable Profile

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

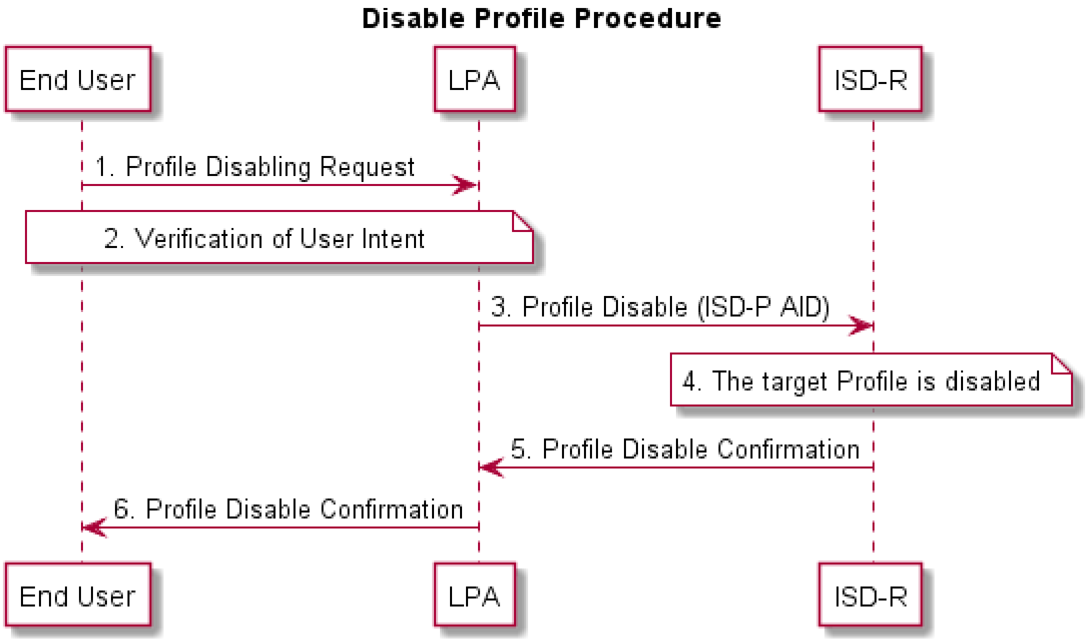
Disable Profile Procedure
End User
LPA
ISD-R
1. Profile Disabling Request
2. Verification of User Intent
3. Profile Disable (ISD-P AID)
4. The target Profile is disabled
5. Profile Disable Confirmation
6. Profile Disable Confirmation
End User
LPA
ISD-R

**Figure 11: 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 disables the target Profile.
5. The ISD-R informs the LPA of the disabling of the Profile.
6. The End User is informed via the LPA.

**End conditions:**

a. The target Profile is disabled.

### 5.2.3 Delete Profile

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

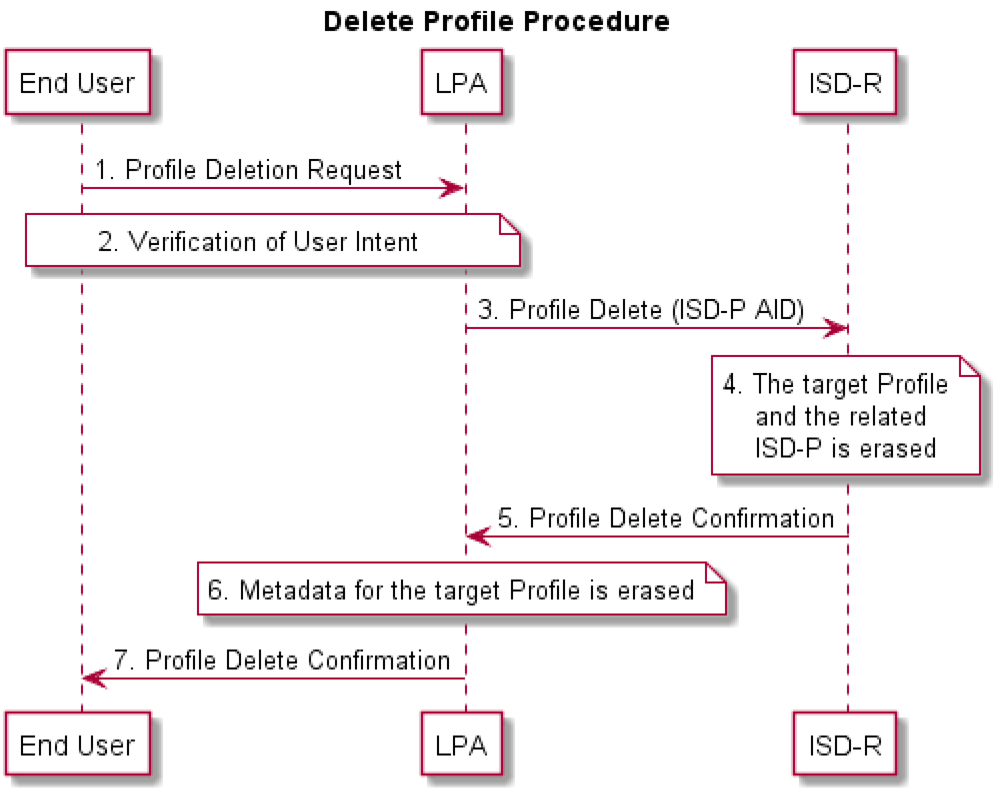
Delete Profile Procedure
End User
LPA
ISD-R
1. Profile Deletion Request
2. Verification of User Intent
3. Profile Delete (ISD-P AID)
4. The target Profile and the related ISD-P is erased
5. Profile Delete Confirmation
6. Metadata for the target Profile is erased
7. Profile Delete Confirmation
End User
LPA
ISD-R

**Figure 12: 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 erases the target Profile and the related ISD-P.
5. The ISD-R informs the LPA of the Profile deletion.
6. The Metadata for the target Profile is erased.
7. The End User is informed via the LPA.

**End conditions:**

a. The target Profile is deleted.

### 5.2.4 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 Metadata for that Profile.

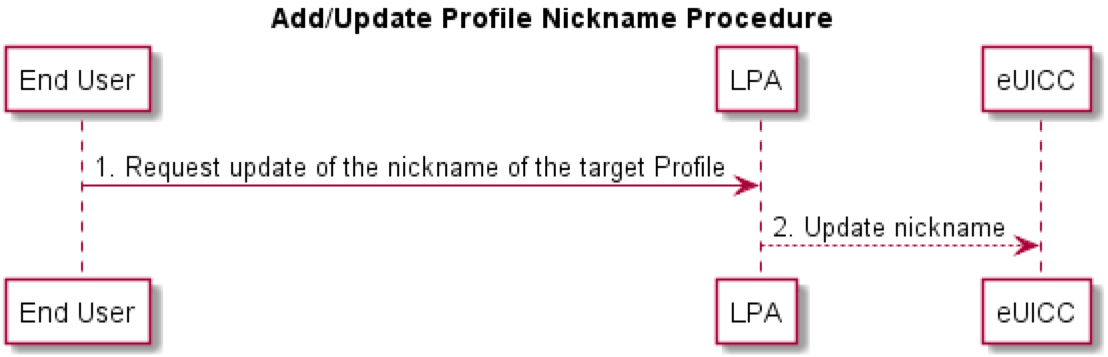
Add/Update Profile Nickname Procedure
End User
LPA
eUICC
1. Request update of the nickname of the target Profile
2. Update nickname
End User
LPA
eUICC

**Figure 13: 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 Metadata of the target Profile with the user’s choice of nickname in the eUICC.

**End conditions:**

a. Metadata of the target Profile has been updated with the user’s choice of nickname.

### 5.2.5 Query Profile Metadata

This procedure will allow the End User to query the metadata of the Profiles accessible to the End User. The result SHALL display all (or parts of) the 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.

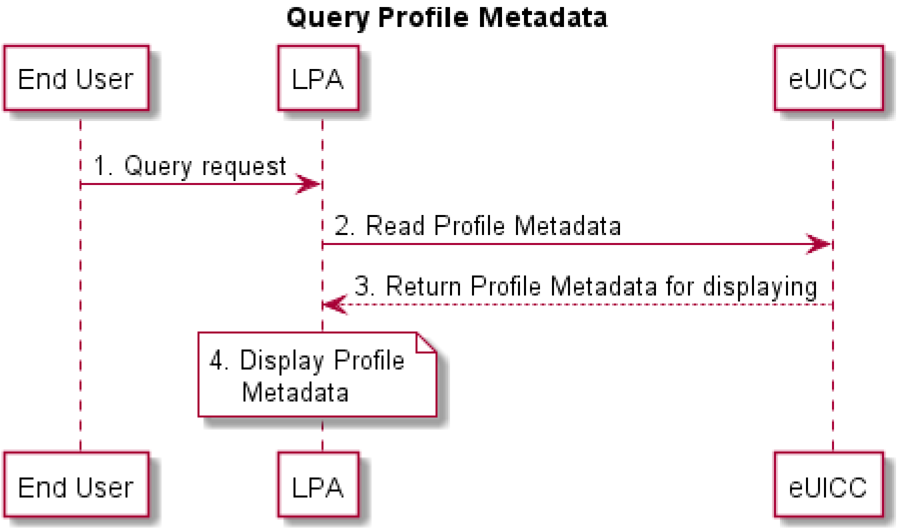

**Figure 14: Query Profile Metadata Procedure**

**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. LPA receives a query request from the User.

3. LPA requests Profile Metadata from the eUICC.
4. LPA displays Profile Metadata to the User on the LUI.

**End conditions:**

a. No change to Profile Metadata.

### 5.2.6 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.

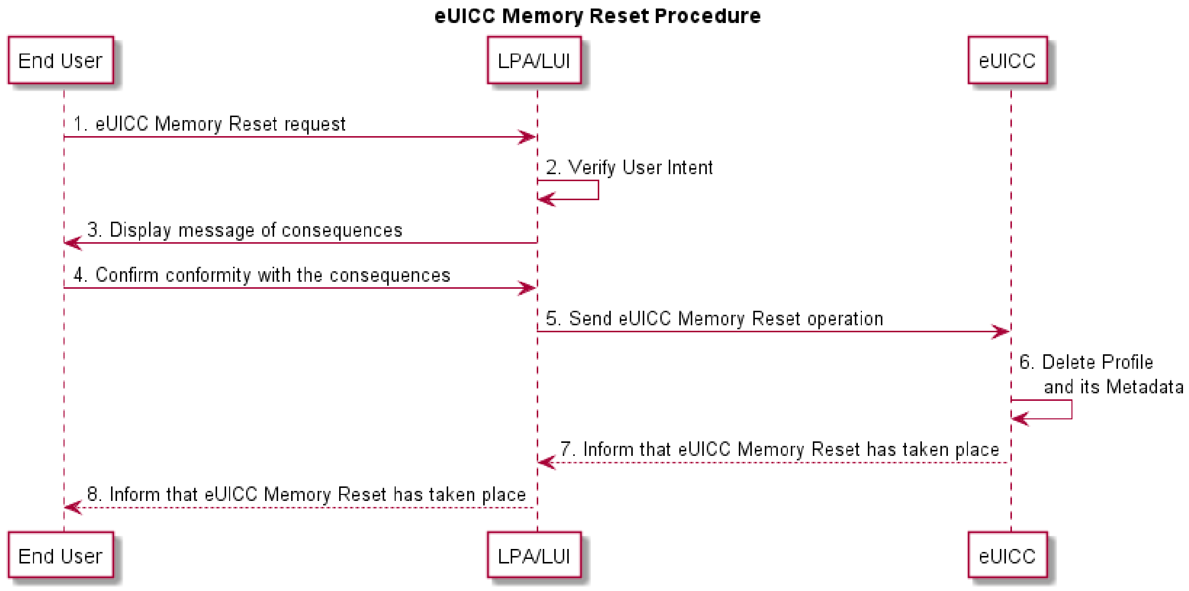
eUICC Memory Reset Procedure
End User
LPA/LUI
eUICC
1. eUICC Memory Reset request
2. Verify User Intent
3. Display message of consequences
4. Confirm conformity with the consequences
5. Send eUICC Memory Reset operation
6. Delete Profile and its Metadata
7. Inform that eUICC Memory Reset has taken place
8. Inform that eUICC Memory Reset has taken place
End User
LPA/LUI
eUICC

**Figure 15 eUICC Memory Reset Procedure**

**Start conditions:**

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

**Procedure**:

1. The End User makes an eUICC Memory Reset request on the LPA (LUI).
2. User Intent is verified.
3. The LPA (LUI) displays a message of consequences of ‘eUICC Memory Reset’ to the End User.
4. The End User confirms the conformity with the consequences to the LPA.
5. The LPA sends an eUICC Memory Reset operation to the eUICC.
6. The eUICC deletes the Profile on the eUICC even if it is an Enabled Profile including the 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).

**End conditions:**

a. The Profile is deleted from the eUICC.

### 5.2.7 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.

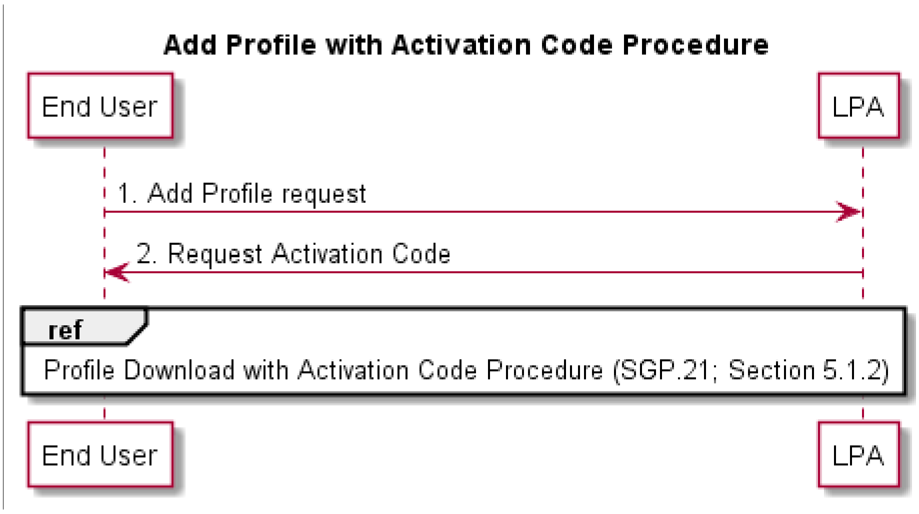
Add Profile with Activation Code Procedure
End User
LPA
1. Add Profile request
2. Request Activation Code
ref
Profile Download with Activation Code Procedure (SGP.21; Section 5.1.2)
End User
LPA

**Figure 16: 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 eUICC as legitimate for performing Profile download.

**Procedure:**

1. The End User obtains an Activation Code to add a Profile to his Device.
2. The LPA requests the End User to enter the Activation Code.
3. Profile Download with Activation Code Procedure as described in Section 5.1.2 starts.

**End conditions:**

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

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

New Profile on New Primary Device (Off Device Activation)

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

**Table 24 New Profile on New Primary Device Risks**

Profile Deletion

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

**Table 25 Profile Deletion Risks**

Profile Switch

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

**Table 26 Profile Switching Risks**

Profile Swap

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

**Table 27 Profile Swapping Risks**

Cryptographic Related Risks

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

**Table 28 Cryptographic Related Risks**

Quality of Service

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

**Table 29 Quality of Service Risks**

Non-human or Unpredictable

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

**Table 30 Non-human or Unpredictable Risks**

New Profile during Subscriber Journey

| Risk no. | Risk description |
|---|---|
| **EXN1** | Malicious pairing of new Device using unattended Primary or Companion Device. |
| **EXN2** | Use of public Wi-Fi for internet connectivity leading to the loss of confidentiality during the provisioning of Profile operations. |
| **EXN3** | Use of public Wi-Fi for internet connectivity leading to the tampering of registration information during provisioning of Profile operations. |

| Risk no. | Risk description |
|---|---|
| **EXN4** | Social engineering leading to the communication of OTP materials to attackers. |
| **EXN5** | Man-in-the-middle or eavesdropping during Profile provisioning leading to the loss of confidentiality. |
| **EXN6** | "Implicit authentication" (e.g. HTTP MSISDN enrichment) leading to the loss of authentication or Profile material. |

**Table 31 New Profile during Subscriber Journey Risks**

Device Swap

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

**Table 32 Device Swapping Risks**

Loss of Privacy

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

**Table 33 Loss of Privacy Risks**

Others

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

**Table 34 Other Risks**

Creation Process

| Req no. | Requirement description |
|---|---|
| **CRE1** | Profiles failing to be created SHALL be securely deleted or at least purged of authentication vectors. |
| **CRE2** | Communication between systems participating in the Profile creation SHALL be protected in integrity and confidentiality. |

**Table 35 Creation Process Requirements**

# Annex B Profile Production Procedure (Informative)

## B.1 Profile Production Procedure

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 the 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.

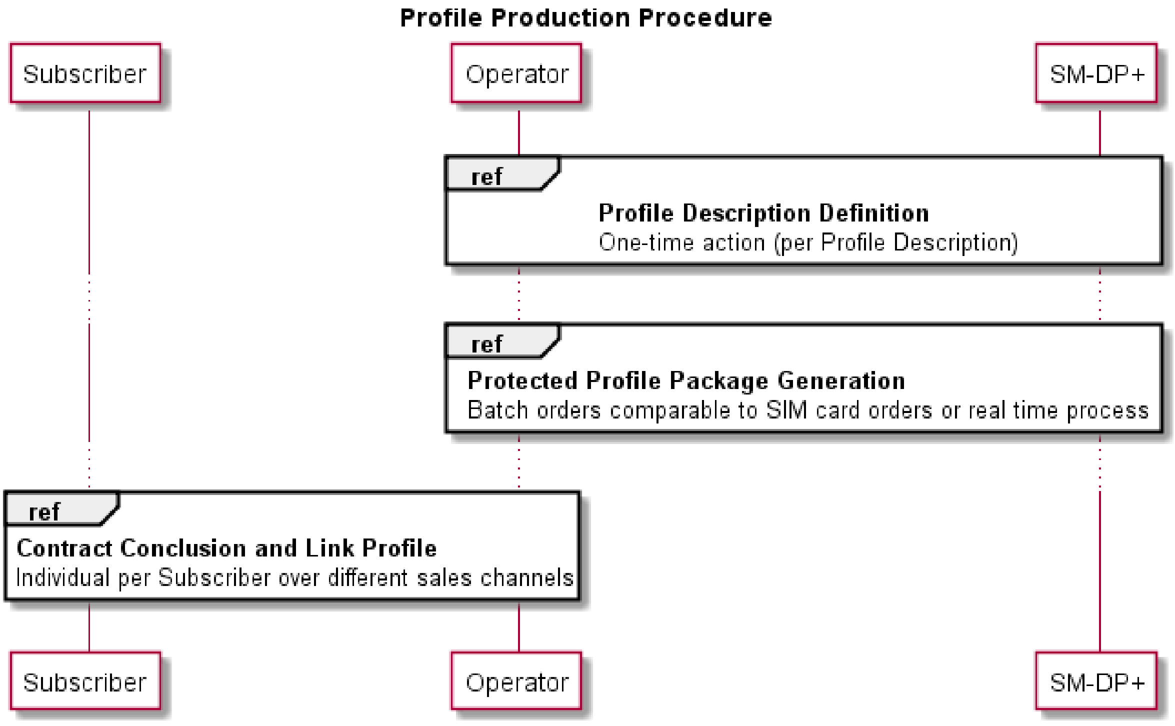
Profile Production Procedure
Subscriber
Operator
SM-DP+
ref
Profile Description Definition
One-time action (per Profile Description)
ref
Protected Profile Package Generation
Batch orders comparable to SIM card orders or real time process
ref
Contract Conclusion and Link Profile
Individual per Subscriber over different sales channels
Subscriber
Operator
SM-DP+

**Figure 17: Profile Production Procedure**

The Profile Production consists of three steps:

1. **Profile Description definition:** The SM-DP+ creates and registers a Profile Description based on the Operator Profile Description.

2. **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 of the respective Operator.

3. **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 5.1.2.

### B.1.1 Profile Description Definition

The Profile Description definition MAY comprise of the following sequences:

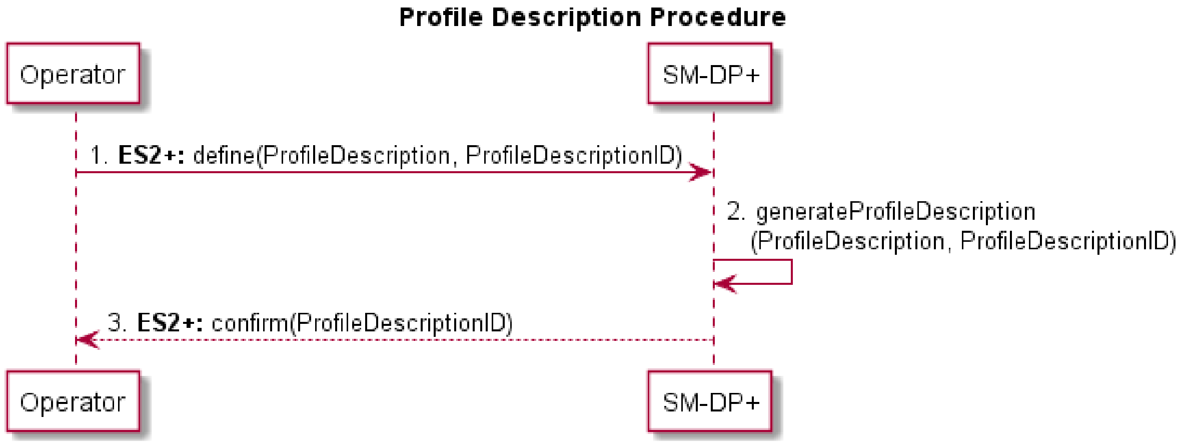
Profile Description Procedure
Operator
SM-DP+
1. ES2+: define(ProfileDescription, ProfileDescriptionID)
2. generateProfileDescription
(ProfileDescription, ProfileDescriptionID)
3. ES2+: confirm(ProfileDescriptionID)
Operator
SM-DP+

**Figure 18: Profile Description Procedure**

**Start Conditions:**

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 Protected Profile Package Generation

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

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.

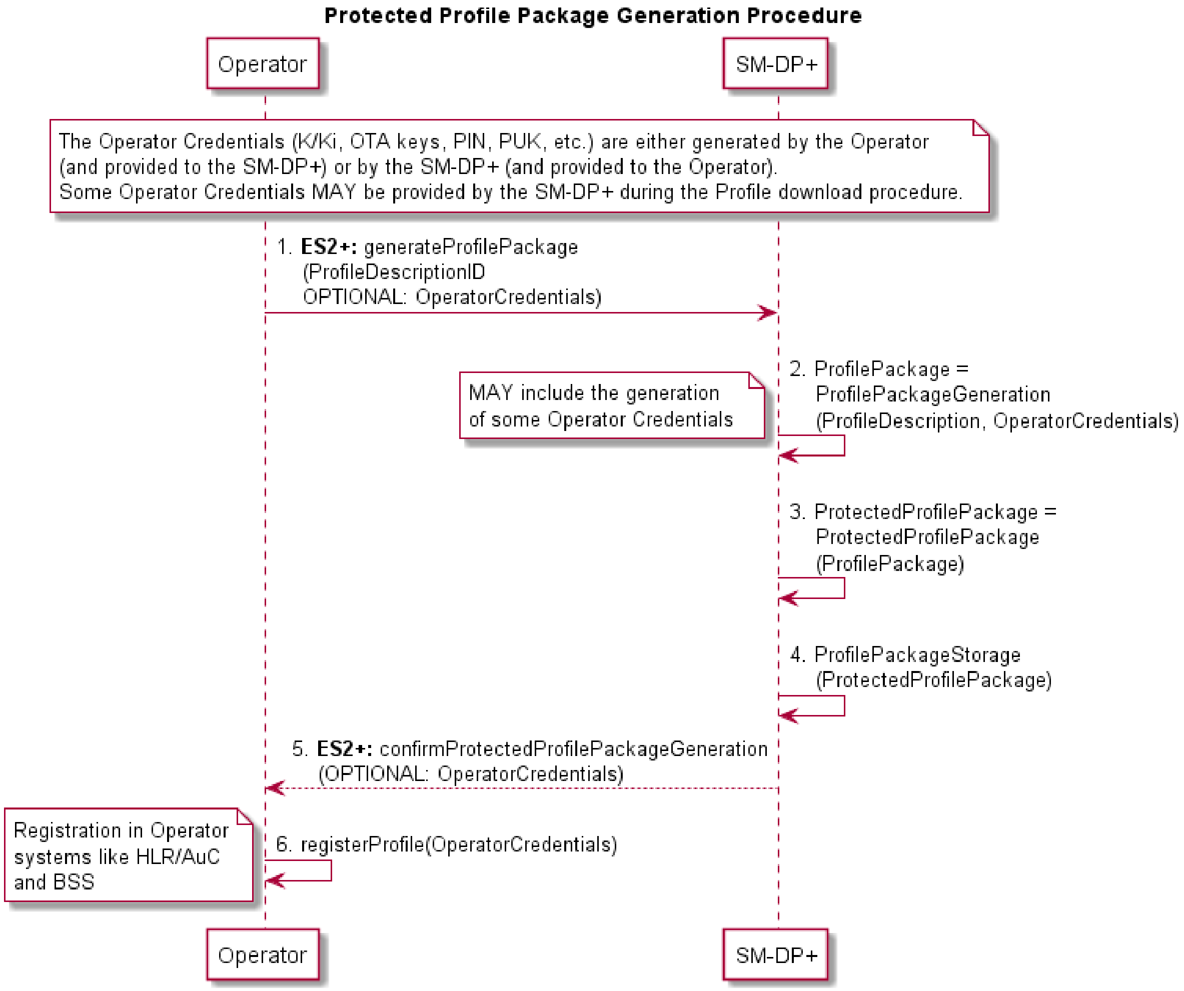
Protected Profile Package Generation Procedure
Operator
SM-DP+
The Operator Credentials (K/Ki, OTA keys, PIN, PUK, etc.) are either generated by the Operator (and provided to the SM-DP+) or by the SM-DP+ (and provided to the Operator).
Some Operator Credentials MAY be provided by the SM-DP+ during the Profile download procedure.
1. ES2+: generateProfilePackage (ProfileDescriptionID OPTIONAL: OperatorCredentials)
MAY include the generation of some Operator Credentials
2. ProfilePackage = ProfilePackageGeneration (ProfileDescription, OperatorCredentials)
3. ProtectedProfilePackage = ProtectedProfilePackage (ProfilePackage)
4. ProfilePackageStorage (ProtectedProfilePackage)
5. ES2+: confirmProtectedProfilePackageGeneration (OPTIONAL: OperatorCredentials)
Registration in Operator systems like HLR/AuC and BSS
6. registerProfile(OperatorCredentials)
Operator
SM-DP+

**Figure 19: 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.1.3 Contract Conclusion and Link Profile

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

- **Activation Code with known EID:** The EID is given by the Subscriber to the Operator during the conclusion of the contract.

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

- **Activation code with EID provided to the Operator in step 2 of Figure 22:** The EID is not immediately given by the Subscriber during the contract conclusion, but provided in step 2 to the Operator.

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

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

### B.1.3.1 Activation Code with Known EID

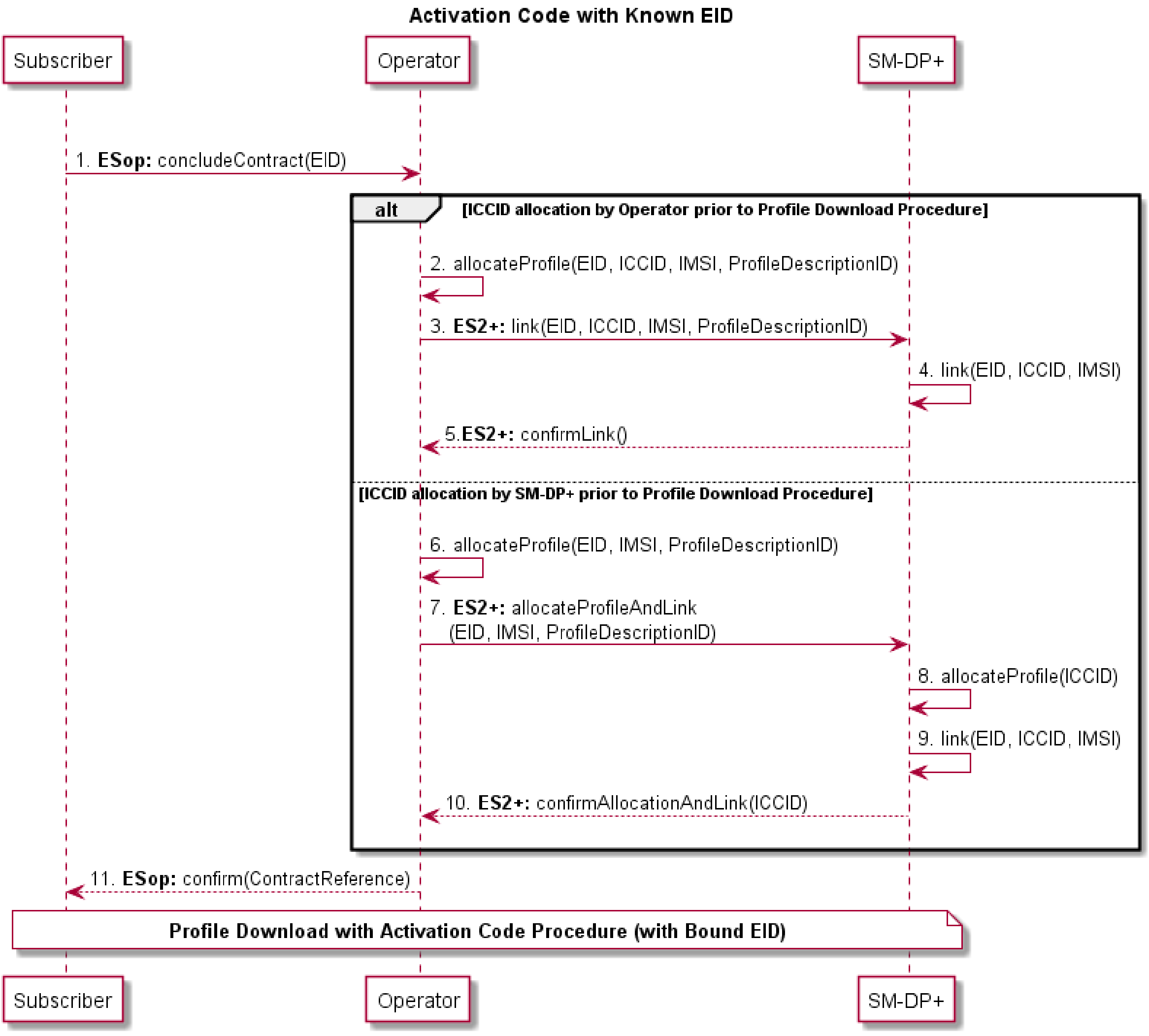
Activation Code with Known EID
Subscriber
Operator
SM-DP+
1. ESop: concludeContract(EID)
alt
[ICCID allocation by Operator prior to Profile Download Procedure]
2. allocateProfile(EID, ICCID, IMSI, ProfileDescriptionID)
3. ES2+: link(EID, ICCID, IMSI, ProfileDescriptionID)
4. link(EID, ICCID, IMSI)
5.ES2+: confirmLink()
[ICCID allocation by SM-DP+ prior to Profile Download Procedure]
6. allocateProfile(EID, IMSI, ProfileDescriptionID)
7. ES2+: allocateProfileAndLink
(EID, IMSI, ProfileDescriptionID)
8. allocateProfile(ICCID)
9. link(EID, ICCID, IMSI)
10. ES2+: confirmAllocationAndLink(ICCID)
11. ESop: confirm(ContractReference)
Profile Download with Activation Code Procedure (with Bound EID)
Subscriber
Operator
SM-DP+

**Figure 20: Activation Code with Known EID Procedure**

**Procedure:**

**Steps 1-11 in**Error! Reference source not found.**: Contract conclusion with known EID**

1. The Subscriber concludes a contract with the Operator and provides the EID during this process.

2. to 5. **Alternatively 'ICCID allocation by Operator prior to Profile download procedure':** The Operator allocates the Profile and sends the EID, IMSI and ICCID to the SM-DP+. The SM-DP+ links the different parameters and confirms this to the Operator.

6. to 10. **Alternatively 'ICCID allocation by SM-DP+ prior to Profile download procedure':** The Operator sends the EID, the IMSI and the Profile Description ID to the SM-DP+. The SM-DP+ allocates an ICCID to a corresponding Profile, links the different parameters and confirms the allocated ICCID and the link to the Operator.

11. The Operator confirms the contract conclusion to the Subscriber with the corresponding information (contract reference).

**End Condition:**

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

### B.1.3.2 Activation Code with Unknown EID

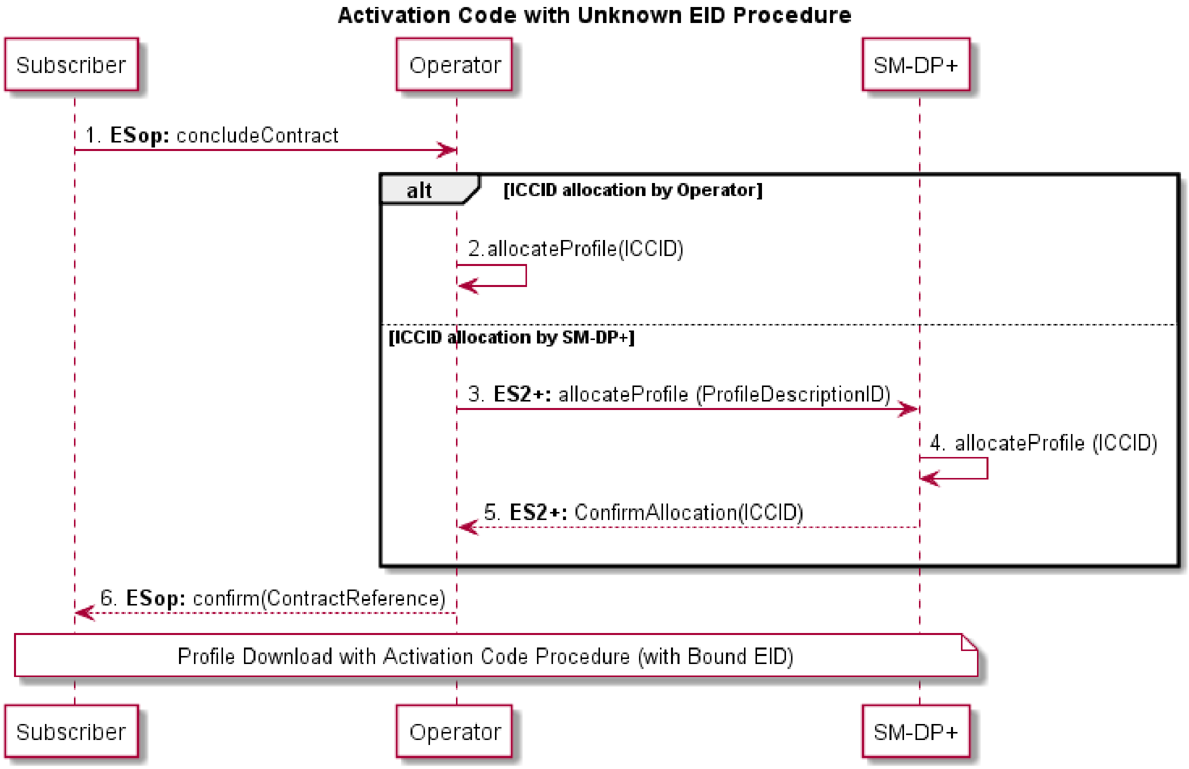
Activation Code with Unknown EID Procedure
Subscriber
Operator
SM-DP+
1. ESop: concludeContract
alt
[ICCID allocation by Operator]
2.allocateProfile(ICCID)
[ICCID allocation by SM-DP+]
3. ES2+: allocateProfile (ProfileDescriptionID)
4. allocateProfile (ICCID)
5. ES2+: ConfirmAllocation(ICCID)
6. ESop: confirm(ContractReference)
Profile Download with Activation Code Procedure (with Bound EID)
Subscriber
Operator
SM-DP+

**Figure 21: Activation Code with Unknown EID Procedure**

**Procedure:**

**Steps 1-6 in**Error! Reference source not found.**: Contract conclusion without EID**

1. The Subscriber concludes a contract with the Operator without knowledge about the target eUICC (EID).
2. **Alternatively 'ICCID allocation by Operator':** The Operator allocates the Profile (ICCID)

3. to 5. **Alternatively 'ICCID allocation by SM-DP+':** The Operator sends the Profile template (ID) to the SM-DP+. The SM-DP+ allocates a corresponding Profile (ICCID) and sends the allocated ICCID to the Operator.

6. The Operator confirms the contract conclusion to the Subscriber with the corresponding information (contract reference).

**End Condition**:

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

### B.1.3.3 Activation Code with EID Provided to the Operator in Step 2

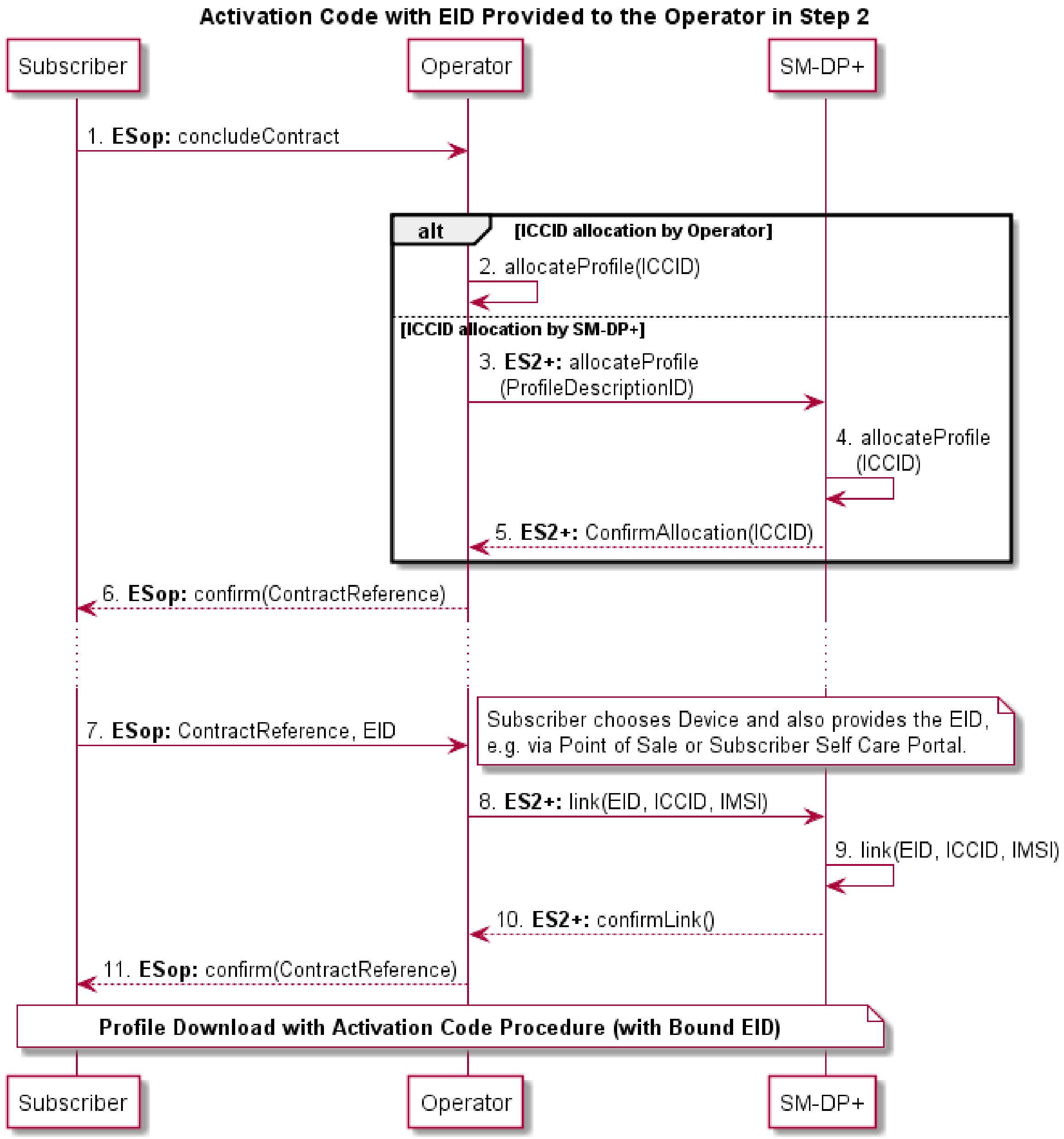
Activation Code with EID Provided to the Operator in Step 2
Subscriber
Operator
SM-DP+
1. ESop: concludeContract
alt
[ICCID allocation by Operator]
2. allocateProfile(ICCID)
[ICCID allocation by SM-DP+]
3. ES2+: allocateProfile (ProfileDescriptionID)
4. allocateProfile (ICCID)
5. ES2+: ConfirmAllocation(ICCID)
6. ESop: confirm(ContractReference)
7. ESop: ContractReference, EID
Subscriber chooses Device and also provides the EID, e.g. via Point of Sale or Subscriber Self Care Portal.
8. ES2+: link(EID, ICCID, IMSI)
9. link(EID, ICCID, IMSI)
10. ES2+: confirmLink()
11. ESop: confirm(ContractReference)
Profile Download with Activation Code Procedure (with Bound EID)
Subscriber
Operator
SM-DP+

**Figure 22: Activation Code with EID Provided to the Operator in Step 2**

**Procedure:**

**Steps 1-11 in**Error! Reference source not found.**: Activation code with EID provided to the Operator in Step 2**

1. The Subscriber concludes a contract with the Operator without knowledge about the target eUICC (EID).
2. **Alternatively ‘ICCID allocation by Operator’:** The Operator allocates the Profile (ICCID)

3. to 5**.** **Alternatively 'ICCID allocation by SM-DP+':** The Operator sends the Profile template (ID) to the SM-DP+. The SM-DP+ allocates a corresponding Profile (ICCID) and sends the allocated ICCID to the Operator.

6. The Operator confirms the contract conclusion to the Subscriber with the corresponding information (contract reference).

7. After the Subscriber has chosen the Device/eUICC, the EID is provided together with the contract reference to the Operator.

8. to 10. The Operator requests the linking of the eUICC (EID) and Profile (ICCID) by the SM-DP+. The SM-DP+ links the EID and the ICCID and confirm this to the Operator.

11. The Operator confirms the linking of the EID to the corresponding contract to the Subscriber.

**End Condition:**

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

# Annex C Document Management

## C.1 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 |

### Other Information

| Type | Description |
|---|---|
| Document Owner | Carmen Kwok |
| Editor / Company | GSMA |

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.