



## SGP.31 eSIM IoT Architecture and Requirements

Version 1.0

19 April 2022

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

### **Copyright Notice**

Copyright © 2022 GSM Association

### **Disclaimer**

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

### **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.

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Overview	5
1.2	Scope	5
1.3	Intended Audience	5
1.4	Definition of Terms	5
1.5	Abbreviations	6
1.6	References	7
1.7	Conventions	8
<b>2</b>	<b>Principles</b>	<b>8</b>
2.1	Basic Principles	8
2.2	IoT Device principles	10
2.3	IoT Profile Principles	10
<b>3</b>	<b>Roles</b>	<b>11</b>
3.1	Mobile Service Provider, Operator	11
3.2	Subscriber, End User, eUICC Manufacturer, Device Manufacturer	11
<b>4</b>	<b>Architecture</b>	<b>11</b>
4.1	Architecture Diagram	12
4.1.2	IPA in the eUICC	13
4.2	Architecture Elements	13
4.2.1	eSIM IoT Remote Manager	13
4.2.2	IoT Profile Assistant	14
4.3	eUICC Architecture	15
4.3.1	eUICC Architecture Overview	15
4.4	Interfaces	15
4.4.1	Operator – SM-DP+ (ES2+)	15
4.4.2	Operator – eUICC (ES6)	15
4.4.3	SM-DP+ – eUICC (ES8+)	15
4.4.4	SM-DP+ – IPA (ES9+)	16
4.4.5	SM-DP+ – eIM (ES9+')	16
4.4.6	IPA – eUICC (ES10a)	16
4.4.7	IPA – eUICC (ES10b)	16
4.4.8	IPA – SM-DS (ES11)	16
4.4.9	eIM – SM-DS (ES11')	16
4.4.10	SM-DP+ – SM-DS (ES12)	16
4.4.11	eIM – eUICC (ESpsmo)	16
4.4.12	eIM – IPA (ESipa)	16
<b>5</b>	<b>Requirements</b>	<b>17</b>
5.1	Functional Requirements	17
5.1.1	General Functional Requirements	17
5.1.2	eUICC Functional Requirements	17
5.1.3	eIM Functional Requirements	18
5.1.4	IPA Functional Requirements	19

5.2	Security Requirements	20
5.2.1	eUICC Security Requirements	20
5.2.2	eIM Security Requirements	20
5.2.3	General Security Requirements	20
<b>6</b>	<b>Procedures</b>	<b>20</b>
6.1	Profile Download Procedures	20
6.1.1	Profile Download Triggered by eIM with Activation Code	20
6.1.2	eIM Initiated Direct Profile Download with SM-DS	22
6.1.3	eIM Assisted Profile Download Triggered by eIM with Activation Code	26
6.1.4	Profile Download with Default SM-DP+	28
6.1.5	eIM Assisted Profile Download Triggered by eIM with SM-DS	30
6.2	Profile Enabling	33
6.2.1	Profile Enabling via eIM	33
6.3	Profile Disabling	35
6.3.1	Profile Disabling via eIM	35
6.4	Profile Delete	37
6.4.1	Profile Delete via eIM	37
6.5	eIM Configuration	39
6.5.1	Add eIM Configuration Data via IPA	39
6.5.2	eIM Configuration via eIM	40
6.5.3	Complete Removal of eIM Configuration Data from the eUICC	41
<b>Annex A</b>	<b>Threats and Risks (Informative)</b>	<b>43</b>
A.1	Compromised IoT Device	43
A.2	Compromised eIM	43
A.3	Malicious eIM	43
A.4	Privacy Leakage	43
A.5	New Profile on New IoT Device	44
A.6	Profile Disabling / Profile Deletion	44
A.7	Profile Switch	44
A.8	Profile Swap	44
A.9	Cryptographic Related Risks	44
A.10	Quality of Service	45
A.11	Non-human or Unpredictable	45
A.12	New Profile during Subscriber Journey	45
A.13	Others	46
<b>Annex B</b>	<b>eIM Configuration Scenarios (Informative)</b>	<b>46</b>
B.1	eIM Configuration Performed by the EUM	46
B.2	eIM Configuration Performed in the IoT Device Production	46
B.3	eIM Configuration Performed in the Field by a Backend System	47
B.4	eIM Configuration Performed by an eIM	48
B.5	Removal of eIM Configuration	49
<b>Annex C</b>	<b>Profile Download Deployment Scenarios (Informative)</b>	<b>50</b>
C.1	Indirect Profile Download	50
C.1.1	Indirect Profile Download Assisted by eIM Using AC	50

## SGP.31 eSIM IoT Architecture and Requirements

C.1.2	Indirect Profile Download Assisted by eIM Using SM-DS	51
C.2	Direct Profile Download	52
C.2.1	Direct Profile Download Assisted by eIM Using Activation Code	52
C.2.2	Direct Profile Download Assisted by eIM Using SM-DS	53
C.2.3	Direct Profile Download Unassisted by eIM Using SM-DS	54
C.2.4	Direct Profile Download Unassisted by eIM Using Default SM -DP+	55
<b>Annex D</b>	<b>Document Management</b>	<b>56</b>
D.1	Document History	56
D.2	Other Information	59

# 1 Introduction

## 1.1 Overview

This document specifies an architecture and requirements for remote provisioning of eUICCs in Network Constrained and/or User Interface (UI) Constrained IoT Devices.

NOTE 1: The primary focus of this version of the document is to support IoT Devices that require the use of a remote Profile management entity. Permissive requirements are included to support energy and Network Constrained IoT Devices, and for IoT Devices that do not require the use of a remote Profile management entity. The document can be amended by additional requirements for these types of IoT Devices in future releases.

NOTE 2: A set of basic principles for support of eSIM in IoT Devices is also presented, though, as noted, these include items for which specific or complete requirements are not included in this version of the document.

## 1.2 Scope

This document defines requirements and architectures to enable the remote provisioning and management of the eUICC in IoT Devices which are Network Constrained and/or UI Constrained Devices based on the architecture described in SGP.21 [1]. This framework aims to provide the basis for global interoperability among actors in IoT deployment scenarios.

## 1.3 Intended Audience

Technical experts within Operators, eUICC solution providers, Subscription management providers, IoT Device vendors, standards organisations, solution providers, network infrastructure vendors, Mobile Service Providers and IoT service providers and other impacted industry bodies.

## 1.4 Definition of Terms

Term	Description
Activation Code	Information issued by an Operator to request the download and installation of a Profile.
Associated eIM	An eIM whose eIM Configuration Data is available within the eUICC and used by the eUICC for verification of an eIM Configuration Operation or PSMO.
Bound Profile Package	As defined in SGP.21 [1].
eIM Configuration Data	The data to be used by the eUICC to authenticate the eIM commands.
eIM Configuration Operation	An operation related to eIM Configuration Data (e.g. add eIM Configuration Data, remove eIM Configuration Data in the eUICC) through the IPA.
eUICC	As defined in SGP.21 [1]
Event	As defined in SGP.21 [1].
Event Record	As defined in SGP.21 [1].
IoT	As defined in TS.34[3].
IoT Device	As defined in TS.34 [3].

Term	Description
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.
Network Constrained Device (NCD)	An IoT Device where communications resources are limited in bandwidth and/or available protocol alternatives. E.g., the bandwidth is typically limited to relatively low data rates, and may allow asynchronous data exchange with a platform, and device may not support TCP (or even IP) protocols.
Notification	A report about a Profile Download or PSMO processed by the eUICC. NOTE: This also applies for implicit changes of a Profile status, e.g. as a result of enabling another Profile.
Notification Receivers	A list defined in the Profile containing SM-DP+s that are to receive Notifications concerning that Profile.
Operator	As defined in SGP.21 [1].
Profile	As defined in SGP.21 [1].
Profile Package	As defined in SGP.21 [1].
Profile State Management Operation (PSMO)	An operation related to the state update of a Profile in a dedicated ISD-P on the eUICC (e.g: enable Profile, disable Profile, delete Profile, list Profile information, and query Profile metadata, update Profile metadata). NOTE: in SGP.21 [1], the corresponding term is Profile Management.
Roll-Back Mechanism	Mechanism of enabling the previously enabled Profile in case no communication between the eIM and IPA can be established using the recently enabled Profile.
Root SM-DS	As defined in SGP.21 [1].
Subscriber	As defined in SGP.21 [1].
Subscription	As defined in SGP.21 [1].
Subscription Manager Data Preparation + (SM-DP+)	As defined in SGP.21 [1] with the difference that LPA is IPA in the context of this document.
Subscription Manager Discovery Server (SM-DS)	As defined in SGP.21 [1].
User Interface Constrained Device (UICD)	An IoT Device with limited, or without, a UI for RSP management functions.

## 1.5 Abbreviations

Term	Description
AC	Activation Code
CASD	Controlling Authority Security Domain
CoAP	Constrained Application Protocol
DTLS	Datagram Transport Layer Security
ECASD	eUICC Controlling Authority Security Domain

Term	Description
eDRX	Extended Discontinuous Reception
eIM	eSIM IoT Remote Manager
FFS	For Further Study
IoT	Internet of Things
IP	Internet Protocol
ISD-P	Issuer Security Domain – Profile
ISD-R	Issuer Security Domain – Root
IPA	IoT Profile Assistant
IP Ae	IoT Profile Assistant located in the eUICC
IP Ad	IoT Profile Assistant located in the IoT Device
LPWA	Low-Power Wide Area
MNO-SD	Mobile Network Operator – Security Domain
NAA	Network Access Application
NB-IoT	Narrow Band Internet of Things
NCD	Network Constrained Device
NIDD	Non-IP Data Delivery
PSM	Power Saving Mode
PSMO	Profile State Management Operation
RSP	Remote SIM Provisioning
SD	Security Domain
SM-DP+	Subscription Manager Data Preparation +
SM-DS	Subscription Manager Discovery Server
SSD	Supplementary Security Domain
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User Interface
UICD	UI Constrained Device

## 1.6 References

Ref	Doc Number	Title
[1]	SGP.21 V2.4	eSIM Architecture Specification
[2]	TCA eUICC Profile Package v3.1 or higher	eUICC Profile Package: Interoperable Format Technical Specification
[3]	TS.34 V7.1	IoT Device Connection Efficiency Guidelines
[4]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
[5]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words

Ref	Doc Number	Title
		<a href="https://www.rfc-editor.org/info/rfc8174">https://www.rfc-editor.org/info/rfc8174</a>

## 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 RFC 2119 [4] and clarified by RFC 8174 **¡Error! No se encuentra el origen de la referencia.¡Error! No se encuentra el origen de la referencia.**, when, and only when, they appear in all capitals, as shown here.”

## 2 Principles

This specification will be based on the SGP.21 [1] architecture and define features related to the scope of the current document. The specification will refer to SGP.21 [1] where appropriate. This implies that to cover the whole range of eSIM provisioning for IoT Devices SGP.31 MUST be used together with SGP.21 [1].

### 2.1 Basic Principles

This section describes basic principles on what is expected from the architecture.

Principle no.	Description
BP01	It should be possible to securely perform all supported Profile State Management Operations remotely on a given IoT Device containing an eUICC.
BP02	It should be possible for a IoT Device containing an eUICC to establish a secure connection with an entity performing Profile State Management Operations. NOTE: a secure connection is a connection that provides confidentiality, integrity and mutual authentication.
BP03	It should be possible to provision eUICCs in IoT Devices where SMS is not available.
BP04	It should be possible to provision eUICCs in IoT Devices where connection-oriented protocols (e.g: TCP/IP) are not supported.
BP05	It should be possible to use a lightweight protocol based on CoAP (e.g. LwM2M) for transfer of Profile download and Profile State Management Operation related messages (e.g. ES8+ messages) over LPWA networks in a secure way.
BP06	The architecture should support Profile download and Profile State Management Operations in an asynchronous way with execution on a IoT Device happening after an extended period of time (e.g. due to eDRX, PSM cycles). NOTE: It may be necessary to store the information about the request for a longer period of time until the IoT Device is connected.
BP07	The principle BP06 should also be applicable for automated Profile download and Profile State Management Operations on a large number of IoT Devices.
BP08	The architecture should allow push mechanism to the IoT Device to initiate a Profile provisioning or management transaction.

<b>BP09</b>	The architecture should allow polling by the IoT Device to check whether there is a Profile-provisioning or management transaction waiting, e.g. for when the IoT Device can no longer communicate with the network due to rejection of registration attempts. Such polling may use an alternative connectivity.
<b>BP10</b>	The architecture should avoid ongoing and frequent polling between the IoT Device and the RSP system.
<b>BP11</b>	The Notification mechanism should take into account the possibly limited availability of the IoT Device in the network as well as being adapted to the use in constrained networks, such as LPWA networks.
<b>BP12</b>	It should be possible for an entity managing a IoT Device (e.g. Mobile Service Provider, IoT Device owner/user, enterprise or IoT service provider) to remotely enable, disable and delete a Profile in a secure way.
<b>BP13</b>	It should be possible for an entity managing a fleet of IoT Devices (e.g. IoT Device owner/user, enterprise, Mobile Service Provider, or IoT service provider) to automate Profile download triggering and Profile State Management Operations for its IoT Devices.
<b>BP14</b>	It should be possible to leverage the IoT Device's existing protocol stack for IoT Device and data management (e.g. CoAP over DTLS) for secure transfer of Profile downloads and Profile State Management Operation related messages (e.g. ES8+ messages) to and from the IoT Device.
<b>BP15</b>	The secure download of Bound Profile Packages via a RSP mechanism for a certain production batch of modules/IoT Devices with eUICC by a dedicated production-line server/appliance should be possible.
<b>BP16</b>	The secure transfer of Bound Profile Packages from an SM-DP+ to a dedicated server in a manufacturing environment should be possible.
<b>BP17</b>	The secure download of the Bound Profile Package from the (off-line) production-line server to the IoT Device/eUICC should be possible.
<b>BP18</b>	The architecture should support a secure asynchronous mode for Profile provisioning and management.
<b>BP19</b>	The asynchronous procedure of BP18 should only allow a Bound Profile Package to be installed once on an eUICC.
<b>BP20</b>	The specification should provide a formula for the calculation of Profile Package sizes.
<b>BP21</b>	It should be possible to provision eUICCs in IoT Devices using an IP transport (e.g.: CoAP over UDP).
<b>BP22</b>	It should be possible to provision eUICCs in IoT Devices using a non-IP transport (e.g.: CoAP over NIDD).
<b>BP23</b>	The architecture should enable installation of Profiles during eUICC or IoT Device manufacture or distribution (online or offline) using end-to-end security equivalent to that provided for in-service (field) Profile download and installation.
<b>BP24</b>	The architecture should support a single-round trip key management protocol to establish the secure channel between the eUICC and the server.
<b>BP25</b>	The specifications should aim to describe protocols for the support and security of Profile download or Profile State Management Operation to minimise the number of transactions required over the lifetime of the IoT Device.

<b>BP26</b>	The architecture should support Profile State Management Operation and Profile download operations with minimal integration between different components and/or different entities.
<b>BP27</b>	The architecture should optimize the traffic (e.g. avoid excessive polling) between the network and the IoT Device to enable mass IoT deployment. “TS34 – IoT Device Connection Efficiency Guidelines” of the GSMA [3] should be followed.
<b>BP28</b>	The architecture should minimise the number of operations at IoT Device/eUICC side to avoid IoT Devices having very long operational lifetime wearing out sensitive memory.
<b>BP29</b>	The architecture should be able to cope with the IoT Device being unreachable for prolonged periods of time.
<b>BP30</b>	The transmission of Notifications should be highly reliable when connectivity is available and the IoT Device can process the task, taking into account limited memory to store Notifications until they can be sent.
<b>BP31</b>	It should be possible to remotely trigger the IoT Device, in a secure way, to start the download of a Profile.
<b>BP32</b>	It should be possible to perform remote operations described in BP31, BP15) and BP16 without requiring local interaction with a given IoT Device.
<b>BP33</b>	Wherever practical, the installation process described in BP23 should utilize the same protocols and encryption techniques as those used in field installation (e.g: to minimise code requirements in the eUICC/IoT Device).
<b>BP34</b>	Computational complexity of processes should be consistent with process transaction latency for IoT Devices having limited power and/or total lifetime energy resources, without impacting the security level.

NOTE 1: Requirements, or additional requirements, for some basic principles may be added in future versions of this document.

NOTE 2: The following basic principles have been highlighted as principles that require further study: BP09, BP10, BP13, BP15, BP16, BP17, BP18, BP19, BP20, BP23, BP24, BP25, BP27, BP29, BP33.

## 2.2 IoT Device principles

Principle no.	Description
<b>DEVP1</b>	Impact of Profile constraints on IoT Device functionality is out of scope of this specification.
<b>DEVP2</b>	Profile handling related code on the IoT Device SHOULD be kept to a minimum for memory constrained IoT Devices.

## 2.3 IoT Profile Principles

All Profile principles in SGP.21 [1] apply for this specification. The below are additional principles:

Principle no.	Description
<b>PROF1</b>	This document uses the term Profile as defined by SGP.21 [1].

<b>PROF2</b>	Profile description is defined by Trusted Connectivity Alliance (formerly SIMalliance) eUICC Profile Package: Interoperable Format Technical Specification [2].
<b>PROF3</b>	Description of a Profile intended for use with IoT services and Subscriptions will be done by the issuing Mobile Service Provider and is out of scope of this document.
<b>PROF4</b>	Profile package size SHOULD be kept to a minimum for Network Constrained Devices.

### 3 Roles

#### 3.1 Mobile Service Provider, Operator

This document adopts the definitions of SGP.21 [1] for the roles 'Mobile Service Provider' and 'Operator'.

Subscriptions used by IoT Devices in the scope of solutions described by this document are defined through the Subscription products/contracts and eSIM Profiles supplied by the Mobile Service Provider and their description or usage are not in scope of this document.

NOTE: A Mobile Service Provider issues Subscription contracts for network access and has the commercial customer relationship. This document does not separate between service providers for specialised market segments. These are all considered as providers of Subscriptions for mobile network access.

#### 3.2 Subscriber, End User, eUICC Manufacturer, Device Manufacturer

The roles eUICC Manufacturer, Device Manufacturer, Subscriber and End User are used as defined in SGP.21 [1].

### 4 Architecture

This section contains the functional description of the system architecture for the eSIM IoT. Architecture elements include eUICC, SM-DP+, eIM, IPA, SM-DS and Operator. The IPA is located either in the IoT Device (IPAd) or in the eUICC (IP Ae).

NOTE: The interaction between a Subscriber and the Mobile Service Provider is not shown on this architecture but is expected to be similar to the interactions described in SGP.21 [1].

### 4.1 Architecture Diagram

The following architecture diagrams describe the roles and interfaces (Figure 1).

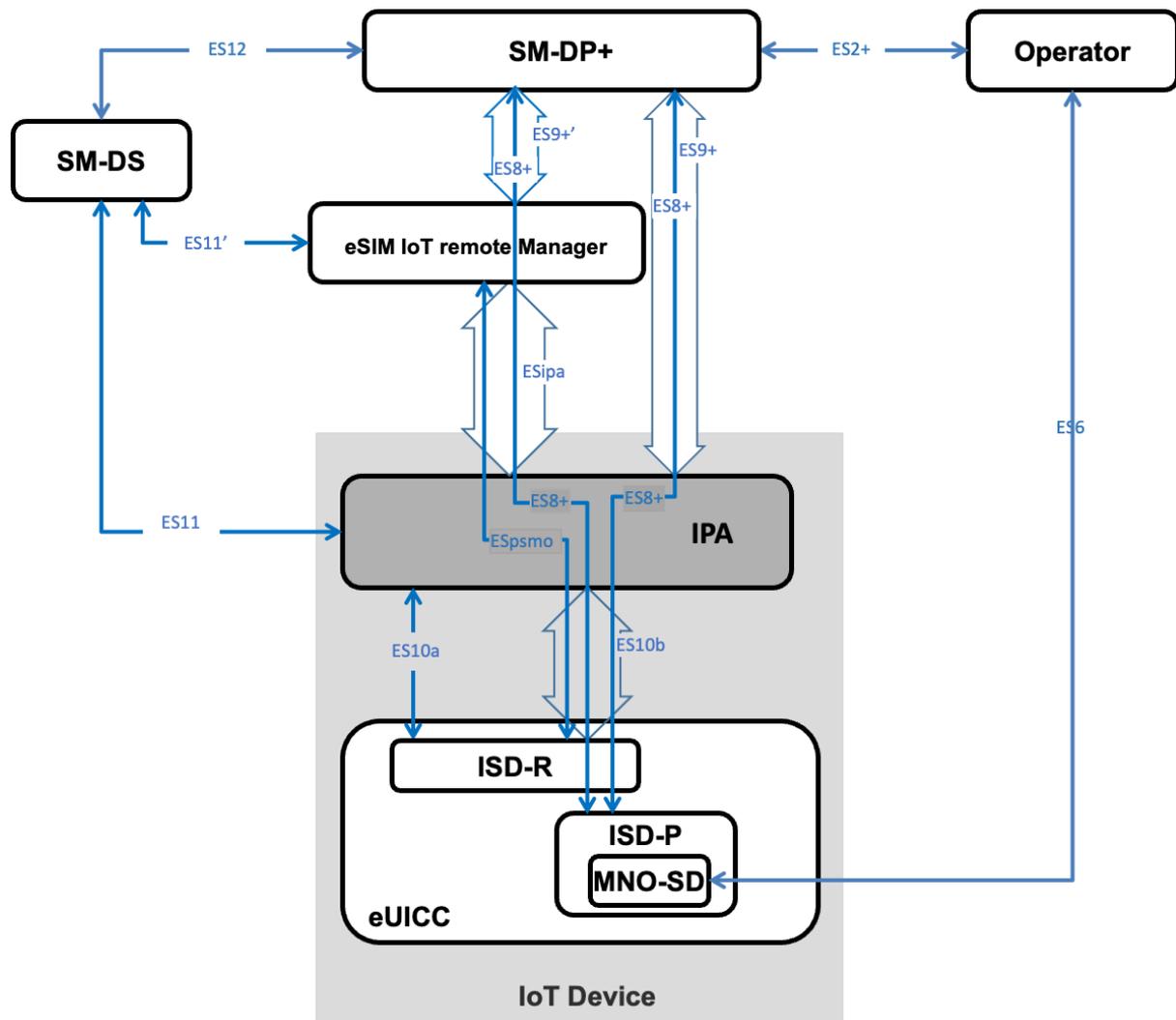


Figure 1: eSIM IoT Functional Architecture (IPA in the IoT Device)

### 4.1.2 IPA in the eUICC

The following architecture diagrams describe the architecture model (Figure 2) where the IPA is located in the eUICC.

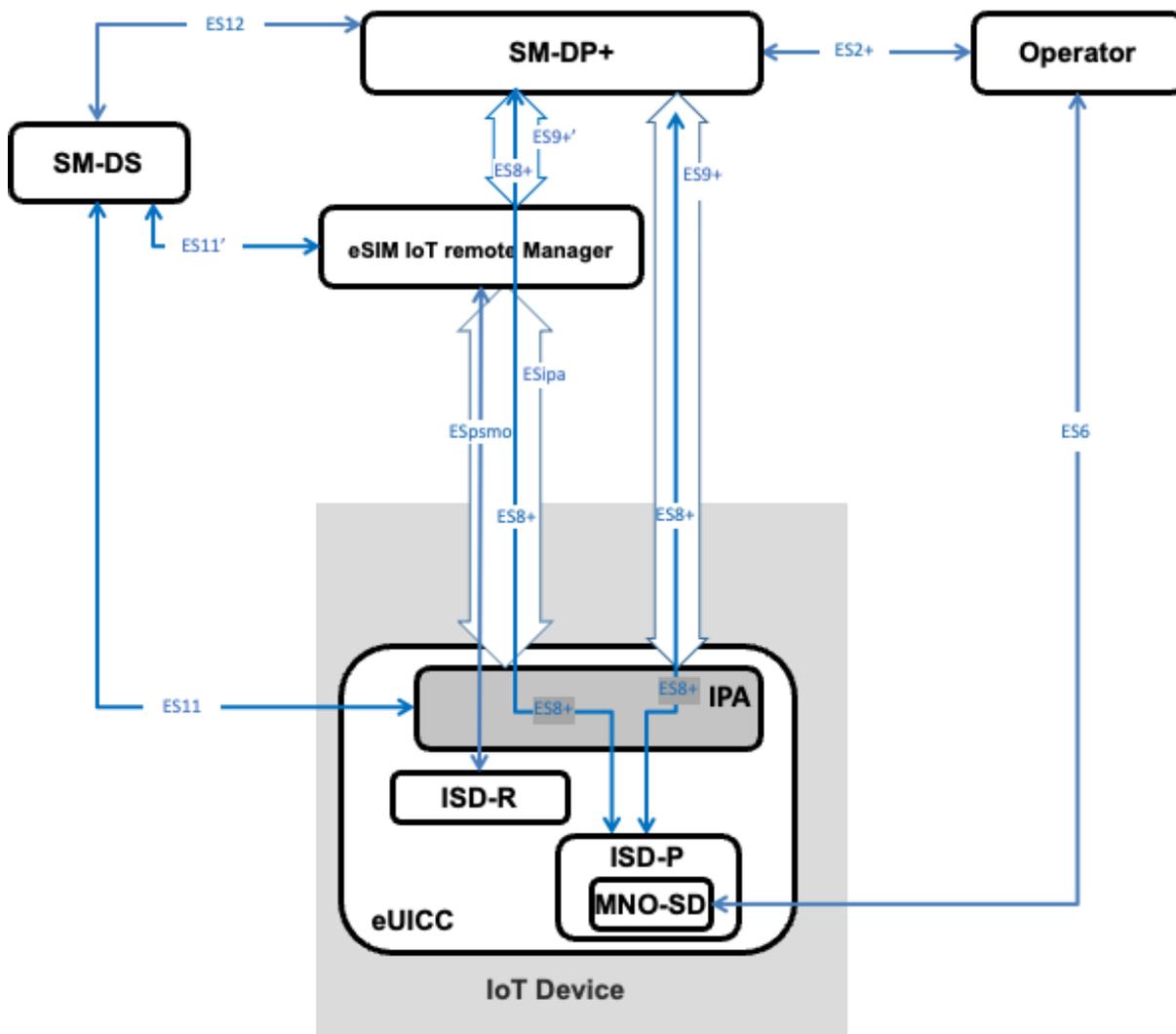


Figure 2: eSIM IoT Functional Architecture (IPA in the eUICC)

## 4.2 Architecture Elements

### 4.2.1 eSIM IoT Remote Manager

The eSIM IoT Remote Manager is responsible for remote Profile State Management Operations on a single IoT Device or a fleet of IoT Devices.

The eIM can either be a stand-alone component or a component of a higher-level functional system (e.g. device management platform).

NOTE: Apart from the necessary functional and security requirements, this specification will not further describe the implementation of the eIM, neither is the interaction between a

Subscriber and the Mobile Service Provider which is expected to be similar to the interactions described in SGP.21 [1].

#### 4.2.2 IoT Profile Assistant

The IoT Profile Assistant (IPA) provides functions that enable the eUICC in the IoT Device to be provisioned by the SM-DP+.

The IPA can either be a stand-alone component or a component of a higher-level functional software in the IoT Device (e.g. device management client).

The IPA provides multiple distinct functions, the Profile Download, the Discovery Service, the Notification Handling, Conveying PSMO and related results as described below.

Function name	Description
<b>Discovery Service</b>	When REQUIRED, this service is responsible for retrieving pending Event Records from the SM-DS.
<b>Profile Download</b>	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 IPA 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, IoT Device, and eUICC capabilities.
<b>PSMO Conveying</b>	This is responsible for conveying PSMOs and related results between eIM and eUICC.
<b>Notification Handling</b>	This is responsible for forwarding notifications to the eIM and/or the SM-DP+.

**Table 1 IPA Function Descriptions**

### 4.3 eUICC Architecture

#### 4.3.1 eUICC Architecture Overview

This section describes the internal high-level architecture of the eUICC. The eUICC architecture is similar to the one used in [1].

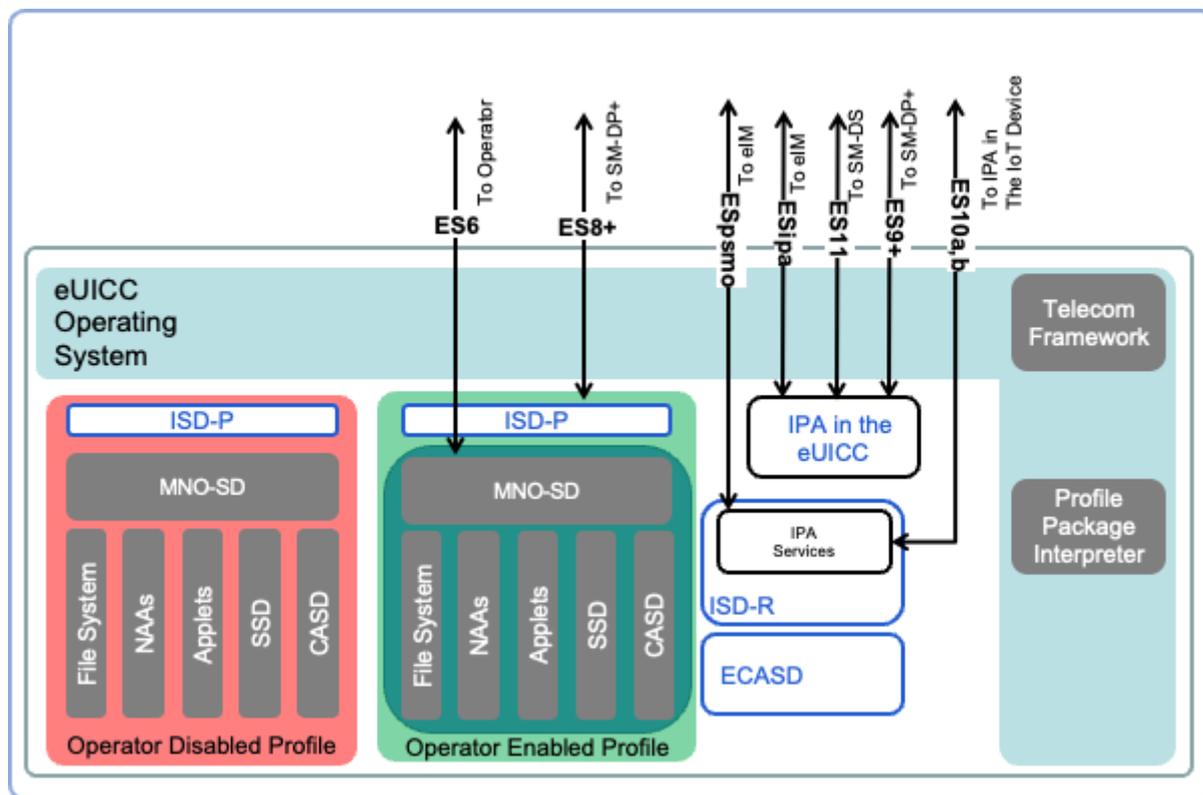


Figure 3: eUICC Architecture

#### 4.4 Interfaces

In this section we define the interfaces used in this specification. Interfaces as defined in SGP.21 [1] will be referenced as appropriate.

##### 4.4.1 Operator – SM-DP+ (ES2+)

The ES2+ interface is used by the Operator to order Profiles for specific eUICCs as well as other administrative functions as defined in SGP.21[1].

##### 4.4.2 Operator – eUICC (ES6)

The ES6 interface is used by the Operator for the management of Operator services via OTA services. It's used for Profile Content Management operations. This interface is defined in SGP.21[1].

##### 4.4.3 SM-DP+ – eUICC (ES8+)

The ES8+ is a logical interface which 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. This interface is defined in SGP.21 [1].

#### 4.4.4 SM-DP+ – IPA (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 IPA. This interface is defined in SGP.21 [1].

#### 4.4.5 SM-DP+ – eIM (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 eIM. The eIM is acting on behalf of the IPA. This interface implements the same procedures as ES9+ defined in SGP.21 [1].

#### 4.4.6 IPA – eUICC (ES10a)

The ES10a interface is used by the IPA in the IoT Device to get the configured addresses from the eUICC for Root SM-DS, and optionally the default SM-DP+. This interface is defined in SGP.21 [1].

#### 4.4.7 IPA – eUICC (ES10b)

The ES10b interface is used by the IPA in the IoT Device and the IPA services in the eUICC to transfer a Bound Profile Package to the eUICC as defined in SGP.21[1]. The ES10b is also used by the IPA to transfer PSMO to the eUICC.

#### 4.4.8 IPA – SM-DS (ES11)

The ES11 interface allows the IPA to retrieve Event Records for the respective eUICC. This interface is defined in SGP.21 [1].

#### 4.4.9 eIM – SM-DS (ES11')

The ES11' interface allows the eIM to retrieve Event Records for the respective eUICC. The eIM is acting on behalf of the IPA. This interface implements the same procedures as ES11 defined in SGP.21 [1].

#### 4.4.10 SM-DP+ – SM-DS (ES12)

The ES12 interface allows any SM-DP+ to issue or remove Event Registrations on the SM-DS. This interface is defined in SGP.21 [1].

#### 4.4.11 eIM – eUICC (ESpsmo)

The ESpsmo is a logical end-to-end interface between the eIM and the eUICC.

Req no.	Description
ESPSMO1	The PSMO SHALL be integrity protected over ESpsmo. NOTE: The solution shall not require associating at eUICC manufacturing the eUICC with a specific eIM.
ESPSMO2	The PSMO SHALL be protected against replay attacks.
ESPSMO3	The PSMO SHALL be protected in terms of integrity and authenticity.

**Table 2: eIM – eUICC (ESpsmo) Interface Requirements**

#### 4.4.12 eIM – IPA (ESipa)

The ESipa is a logical interface between an eIM and an IPA. It could be used to trigger a Profile download at the IPA. It is also used to provide a secure transport for the delivery of

PSMO between an eIM and an IPA, unless the underlying transport provides necessary security.

NOTE : The underlying transport layer can provide transport for other functions (e.g. device management) and should allow multiplexing of these functions in parallel with the ESipa.

Req no.	Description
ESipa1	ESipa SHALL support triggering of Profile download.
ESipa2	ESipa SHALL support delivery of PSMO between eIM and eUICC.
ESipa3	ESipa messages SHALL be protected in terms of confidentiality, integrity and authenticity.
ESipa4	ESipa message protection as per ESipa3 MAY be provided by the underlying transport.
ESipa5	An EID sent to the eIM via ESipa SHALL be privacy protected.

**Table 3: eIM – IPA (ESipa) Interface Requirements**

## 5 Requirements

### 5.1 Functional Requirements

#### 5.1.1 General Functional Requirements

Req no.	Description
GENF01	It is OPTIONAL for the IoT Device, eIM and the SM-DP+ to permit the use of an SM-DS.

#### 5.1.2 eUICC Functional Requirements

Req no.	Description
EUICCF1	The eIM Configuration Data SHALL include credentials (e.g. eIM public key) to allow the eUICC to authenticate the commands from the eIM.
EUICCF2	It SHALL be possible to transfer eIM Configuration Data to the eUICC at the stage of eUICC production.  NOTE: The mechanism and security applied are left to the implementation and may be EUM specific.
EUICCF3	The eUICC SHALL provide an interface to the IPA to perform eIM Configuration Operations. NOTE: Whether IPA/device uses this interface is an implementation specific decision.
EUICCF4	When the eUICC is not associated to any eIM, the eUICC SHALL accept adding any eIM Configuration Data provided through the interface defined in EUICCF3.  NOTE: This interface can be disabled by configuring any (even non-existing) eIM.
EUICCF5	Once an eIM is associated with the eUICC, the eUICC SHALL only accept further eIM Configuration Operations signed by the Associated eIM, except EUICCF6.  The processing of this signed eIM Configuration Operations SHALL be handled as a signed PSMO.

<b>EUICCF6</b>	The eUICC MAY provide an interface to the IPA to allow the complete removal of all eIM Configuration Data from the eUICC. NOTE: The mechanism has to be protected against misuse and could be realised by a kind of reset functionality.
<b>EUICCF7</b>	The eUICC SHALL support the Roll-Back Mechanism.
<b>EUICCF8</b>	If the eIM has requested use of the Roll-Back Mechanism (see EIMF8), and if the IPA informs the eUICC that Roll-Back is required (see IPAF1), the eUICC SHALL execute the Roll-Back Mechanism. NOTE: In this version only the requesting eIM is notified about the result.
<b>EUICCF9</b>	The eUICC SHALL provide a signed result of a requested PSMO or Profile installation to the IPA. NOTE: This signed result is included by the IPA within its responses to requests from the eIM.
<b>EUICCF10</b>	The eUICC SHALL be able to provide Notifications to the IPA for IPA to send to Notification Receivers. This mechanism SHALL be in accordance with SGP.21[1].
<b>EUICCF11</b>	The eUICC SHALL be able to accept SM-DS or default SM-DP+ triggered Profile download and automatic activation without signed PSMO from any potentially Associated eIM.
<b>EUICCF12</b>	The behavior in EUICCF11 SHALL be configurable in the eUICC.
<b>EUICCF13</b>	Changing the configuration in the eUICC (see EUICCF12) SHALL not require a signed PSMO, if there is no eIM associated. If an eIM is associated, only the Associated eIM can change the configuration in the eUICC.  An EUM MAY lock the behavior in eUICC manufacturing.

### 5.1.3 eIM Functional Requirements

Req no.	Description
<b>EIMF1</b>	The eIM SHALL be able to trigger the IPA to initiate a Profile Download from the SM-DP+. Depending on the technical capabilities of the IoT Device (see IPAF12), at least one of the following three Profile Download mechanisms SHALL be supported: <ul style="list-style-type: none"> <li>• Profile Download from default SM-DP+</li> <li>• Profile Download with Activation Code</li> <li>• Profile Download via SM-DS</li> </ul> NOTE: Impact of this optionality on Profile Provisioning procedures is FFS.
<b>EIMF2</b>	The eIM SHALL be able to trigger a PSMO to be executed by the eUICC.
<b>EIMF3</b>	An eIM MAY support eIM Configuration Operations.
<b>EIMF4</b>	The eIM MAY support the transfer of the Bound Profile Package and related communication between the SM-DP+ and IPA/eUICC.
<b>EIMF5</b>	An eIM which is designed for use with IoT Devices that do not require to support the establishment of a direct ES9+ interface to the SM-DP+, SHALL be able to support the transfer of the Bound Profile Package and related communication between the SM-DP+ and the IPA.
<b>EIMF6</b>	The eIM MAY support the transfer of the Event Records and related communication between the SM-DS and IPA/eUICC.
<b>EIMF7</b>	An eIM which is designed for use with IoT Devices that do not require to support the establishment of a direct ES11 interface to the SM-DS, SHALL be able to support the transfer of the Event Records and related communication between the SM-DS and the IPA.

<b>EIMF8</b>	The eIM SHALL be able to request of the eUICC the activation of the Roll-Back Mechanism.
<b>EIMF9</b>	The eIM MAY support the transfer of Notifications and related communication between the SM-DP+ and IPA/eUICC.
<b>EIMF10</b>	An eIM which is designed for use with IoT Devices that do not require to support the establishment of a direct ES9+ interface to the SM-DP+, SHALL be able to support the transfer of Notifications between the SM-DP+ and the IPA.

#### 5.1.4 IPA Functional Requirements

<b>Req no.</b>	<b>Description</b>
<b>IPAF1</b>	If the eIM has requested activation of the Roll-Back Mechanism, then following a Profile Enabling request from an eIM and its execution by the eUICC, the IPA SHALL (a) determine if communications with that eIM can be established; and (b) inform the eUICC that Roll-Back is required if no communication with the eIM is possible.
<b>IPAF2</b>	If the eIM request contains a signed PSMO, or a signed eIM Configuration Operation, or triggers a Profile installation that returns a signed result from the eUICC, the IPA SHALL retrieve the signed result from the eUICC and SHALL include it in a response to the eIM.
<b>IPAF3</b>	The IPA SHALL retrieve pending Notifications from the eUICC and SHALL send the Notifications to the Notification Receivers.
<b>IPAF4</b>	An IPA which is designed for use with IoT Devices that do not require to support the establishment of a direct ES9+ interface to the SM-DP+, SHALL be able to include Notifications into responses between the IPA and the eIM.
<b>IPAF5</b>	As per EIMF10, there SHALL be a means for the IPA to identify Notifications to be transferred by a specific eIM to a designated SM-DP+.
<b>IPAF6</b>	The IPA SHALL send Notifications on a best-effort basis when connectivity is available.
<b>IPAF7</b>	The IPA SHALL retain signed eUICC results until they can be sent in a response to the eIM.
<b>IPAF8</b>	IPA MAY support direct Profile download via ES9+.
<b>IPAF9</b>	IPA MAY support indirect Profile download via ESipa.
<b>IPAF10</b>	The IPA MAY support eIM Configuration Operations.
<b>IPAF11</b>	As per EIMF1, the IPA SHALL be able to accept a Profile Download trigger from the eIM.
<b>IPAF12</b>	The IPA SHALL support at least one of the following three mechanisms for Profile Download: <ul style="list-style-type: none"> <li>• Profile Download from default SM-DP+</li> <li>• Profile Download with Activation Code</li> <li>• Profile Download via SM-DS</li> </ul>
<b>IPAF13</b>	IPA MAY support Profile download and automatic activation through SM-DS or default SM-DP+ without eIM involvement.

## 5.2 Security Requirements

### 5.2.1 eUICC Security Requirements

Req no.	Description
EUICCS1	The eUICC SHALL only accept PSMO triggered from an Associated eIM as per EUICCF1.
EUICCS2	Prior to processing any PSMO in the eUICC, the eUICC SHALL verify that the PSMO is signed by an Associated eIM.
EUICCS3	With regards to EUICCF5, the eUICC SHALL verify that the eIM Configuration Operation is signed by an Associated eIM prior to its processing.
EUICCS4	The eUICC SHALL support an asymmetric cryptographic scheme for verifying an eIM signature.
EUICCS5	The eUICC SHALL have means to verify that Profile download and automatic activation through default SM-DP+ or SM-DS is authorised.

### 5.2.2 eIM Security Requirements

Req no.	Description
EIMS1	Any PSMO sent to the eUICC SHALL be signed by the eIM.
EIMS2	If supported by the eIM, the eIM SHALL sign eIM Configuration Operations.
EIMS3	The eIM SHALL support an asymmetric cryptographic scheme for signing PSMO.

### 5.2.3 General Security Requirements

Req no.	Description
GS1	The mechanism to modify the eIM Configuration Data within the eUICC SHALL be protected in terms of integrity and authenticity. NOTE: The security and the mechanisms other than the signed eIM request is left to the implementation.

## 6 Procedures

This section contains the high level description of the procedures.

### 6.1 Profile Download Procedures

#### 6.1.1 Profile Download Triggered by eIM with Activation Code

The following procedure describes the direct Profile Download procedure between the SM-DP+ and the eUICC when it's triggered by the eIM, using an Activation Code.

#### Start Conditions:

1. The ordering process related to this Profile has been completed.
2. Activation Code is generated by the Operator and made available to the eIM.

#### Procedure:

1. The eIM sends the AC, containing the SM-DP+ identifier, to the IPA.
2. The IPA parses the Activation Code parameters to identify the SM-DP+ address.
3. The IPA establishes a secure connection with the SM-DP+.

4. Mutual Authentication between eUICC and SM-DP+ is performed. Additional information from eUICC is provided to the SM-DP+ to proceed with the Profile preparation.
  5. The SM-DP+ proceeds with the Profile preparation:
    - a. Performs the eligibility check based on the provided information by the eUICC.
    - b. Prepare the Bound Profile Package.
- NOTE: The Operator owning the Profile SHALL be able to stop the Profile download at this stage.
6. The Bound Profile Package is downloaded to the eUICC through the IPA using the secure connection with SM-DP+.
  7. The Profile is installed by the eUICC.
  8. Successful installation of the Profile on the eUICC is acknowledged and the eIM and the SM-DP+ are notified.
  9. The Operator is notified by the SM-DP+ about the Profile Installation

#### End Conditions:

- a) A Bound Profile Package has been downloaded and installed on the eUICC in a Disabled state.

NOTE: the automatic enabling for an installed profile is FFS.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OPE
participant "<b>SM-DP+" as DP
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

EIM -> IPA: [1] Sends AC

rnote over IPA #FFFFFF
[2]
Identify SM-DP+
endrnote

rnote over IPA, DP #FFFFFF
[3]
Secure Connection establishment
endrnote

rnote over E, DP #FFFFFF
[4]
Mutual Authentication Procedure
Additional information for Profile Generation is provided
endrnote

rnote over DP #FFFFFF
[5]
a. Eligibility check
b. Profile generation and protection
endrnote

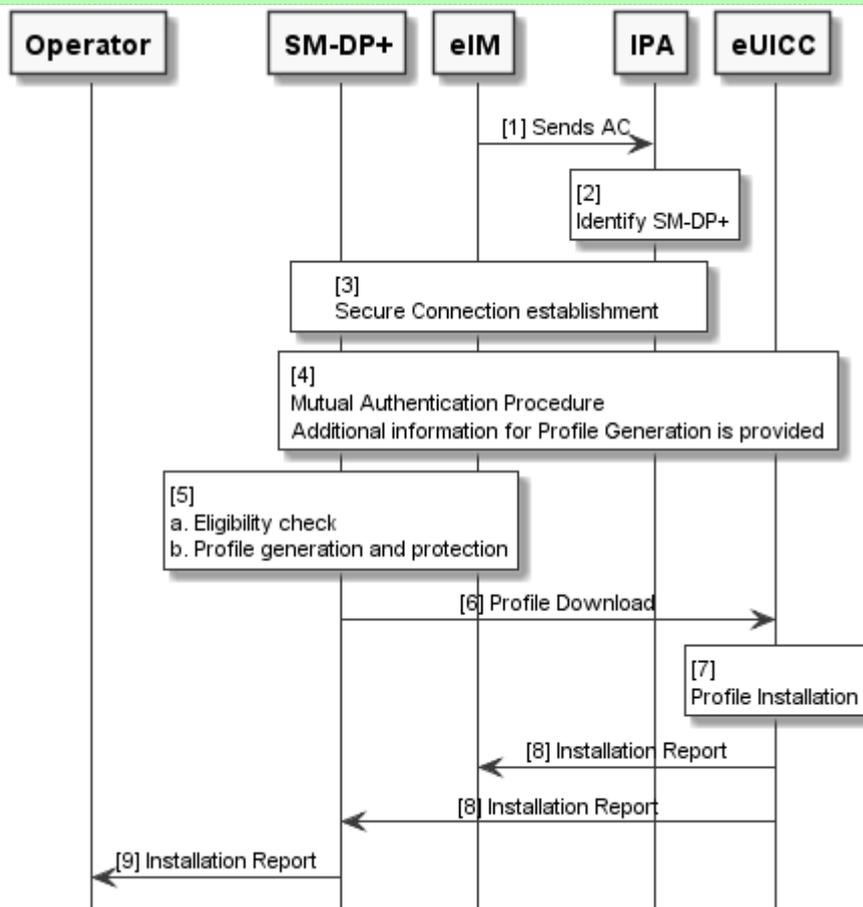
DP -> E: [6] Profile Download

rnote over E #FFFFFF
```

```
[7]
Profile Installation
endnote

E -> EIM: [8] Installation Report
E -> DP: [8] Installation Report
DP -> OPE: [9] Installation Report

@enduml
```



### 6.1.2 eIM Initiated Direct Profile Download with SM-DS

The following procedure describes two options for the direct Profile Download between the SM-DP+ and the eUICC.

Option a) with the IPA being triggered by the eIM in order to download the corresponding Event Record from the SM-DS and

Option b) with the eIM retrieving the corresponding Event Record from the SM-DS and forwarding it to the IPA for further processing.

#### Start Conditions:

1. The ordering process to this Profile has been completed and a respective Event Record for a Profile Download has been created via ES12.
2. Option a) IPA is configured with the SM-DS address.  
 Option b) eIM is configured with the SM-DS address.

**Procedure:**

Option a)

1. A secure connection between IPA and eIM is established via ESipa.
2. The IPA is triggered to initiate a connection to the configured SM-DS for Event Record retrieval, requests and receives information from eUICC REQUIRED to perform mutual authentication with SM-DS.
3. The IPA establishes a secure connection to the SM-DS via ES11
4. Mutual Authentication between the SM-DS and the eUICC is performed. The mutual authentication is initiated and driven by the IPA and involves relaying authentication messages between the IoT Device and SM-DS.
5. The IPA downloads the Event Record to process.

Option b)

1. A secure connection between IPA and eIM is established via ESipa.
2. The eIM requests the IPA to get information from the eUICC REQUIRED to perform mutual authentication between the eUICC and the SM-DS.
3. The eIM establishes a secure connection to the configured SM-DS via ES11'
4. Mutual authentication between the SM-DS and the eUICC is performed. The mutual authentication is initiated and driven by the eIM on behalf of the IPA and involves relaying authentication messages between the IoT Device and SM-DS including re-encoding of the messages for the two secure connections ESipa and ES11'.
5. The eIM downloads the Event Record via ES11', connects to the IPA and forwards the Event Record to process to the IPA.

NOTE: Unrequested Profile download is to be prevented by the detailed version of this procedure.

For both Option a) and Option b) the procedure continues as follows:

6. The IPA identifies the address of the SM-DP+ where the Profile is stored.
7. The IPA establishes a secure connection with the SM-DP+.
8. Mutual Authentication between eUICC and SM-DP+ is performed. Additional information from eUICC is provided to the SM-DP+ to proceed with the Profile preparation.
9. The SM-DP+ proceeds with the Profile preparation:
  - a. Perform the eligibility check based on the provided information by the eUICC.
  - b. Prepare the Bound Profile Package.

NOTE: The Operator owning the Profile is able to stop the Profile download at this stage.

10. The Bound Profile Package is downloaded to the eUICC through the IPA using the secure connection with SM-DP+.
11. The Profile is installed by the eUICC.
12. Successful installation of the Profile on the eUICC is acknowledged and both the eIM and the Notification Receivers are informed.

## End Conditions:

- a) A Bound Profile Package has been downloaded and installed on the eUICC in a Disabled state.

NOTE: the automatic enabling for an installed profile is FFS.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OPE
participant "<b>SM-DP+" as DP
participant "<b>SM-DS" as DS
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

Group Option a)
  rnote over EIM, IPA #FFFFFF
    [1] Secure Connection establishment via ESipa
  endrnote

  EIM -> IPA: [2] trigger connection establishment to DS
  IPA -> E: [2a] request information for mutual authentication
  E -> IPA: [2b] information for mutual authentication

  rnote over IPA, DS #FFFFFF
    [3] Establish secure Connection via ES11
  endrnote

  rnote over DS, E #FFFFFF
    [4] Mutual Authentication
  endrnote

  DS -> IPA: [5] Event Record
end

Group Option b)
  rnote over EIM, IPA #FFFFFF
    [1] Secure Connection establishment via ESipa
  endrnote

  EIM -> IPA: [2] request information for mutual authentication
  IPA -> E: [2a] request information for mutual authentication
  E -> IPA: [2b] information for mutual authentication
  IPA -> EIM: [2c] information for mutual authentication

  rnote over EIM, DS #FFFFFF
    [3] Establish secure Connection via ES11'
  endrnote

  rnote over DS, E #FFFFFF
    [4] Mutual Authentication
  endrnote

  DS -> EIM: [5] Download Event Record
  EIM -> IPA: [5] Event Record
end

rnote over IPA #FFFFFF
[6] Identify SM-DP
endrnote
```

```

rnote over IPA, DP #FFFFFF
[7] Secure Connection establishment
endrnote

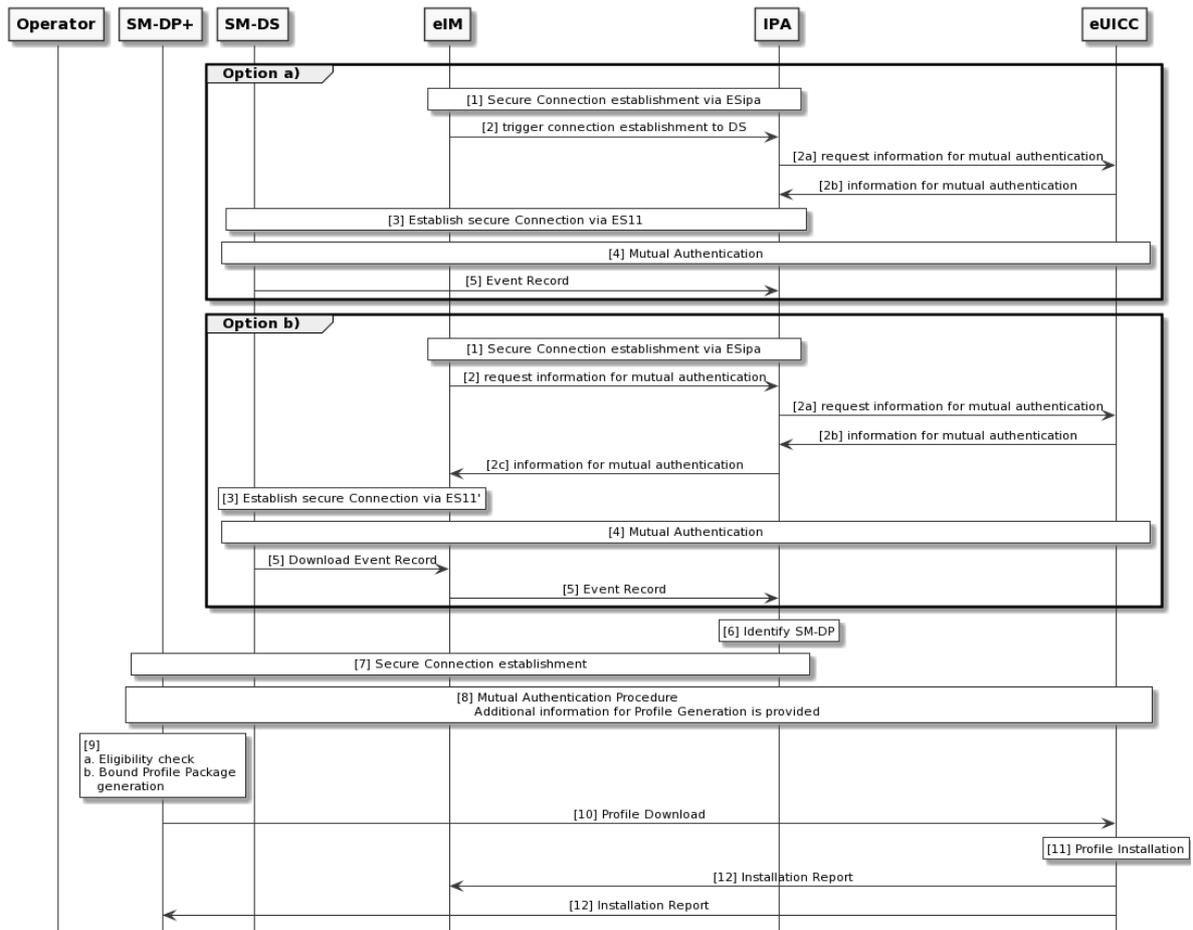
rnote over E, DP #FFFFFF
[8] Mutual Authentication Procedure
  Additional information for Profile Generation is provided
endrnote

rnote over DP #FFFFFF
[9]
a. Eligibility check
b. Bound Profile Package
  generation
endrnote

DP -> E: [10] Profile Download

rnote over E #FFFFFF
[11] Profile Installation
endrnote

E -> EIM: [12] Installation Report
E -> DP: [12] Installation Report
@enduml
  
```



### 6.1.3 eIM Assisted Profile Download Triggered by eIM with Activation Code

The following procedure describes the indirect Profile Download procedure between the SM-DP+ and the eUICC where the eIM assists with the Profile download. The Profile download is triggered by the eIM using an Activation Code.

#### Start Conditions:

1. The ordering process related to this Profile has been completed.
2. The Activation Code is available at the eIM.

#### Procedure:

1. The secure connection between the IPA and the eIM is established via ESipa.
2. The eIM parses the Activation Code (AC) to identify the SM-DP+ address.
3. The eIM establishes a secure connection with the SM-DP+.
4. Mutual Authentication between eUICC and SM-DP+ is performed. The mutual authentication is initiated and driven by the eIM on behalf of the IPA and involves relaying authentication messages between the IoT Device and SM-DP+ including re-encoding of the messages for the two different secure connections.

NOTE: The Matching Id from the AC is provided by the eIM to IPA as part of the mutual authentication exchange.

5. The SM-DP+ proceeds with the Profile preparation:
  - a. Performs the eligibility check based on the provided eUICC and IoT Device information.
  - b. Prepare the Bound Profile Package.  
NOTE: The Operator owning the Profile SHALL be able to stop the Profile download at this stage.
6. The eIM receives the Bound Profile Package from the SM-DP+ using the secure connection with SM-DP+.
7. The Bound Profile Package is loaded to the eUICC:
  - a. The eIM sends a request to IPA to load the Bound Profile Package to the eUICC. The request contains the Bound Profile Package and is sent using the secure connection with the IoT Device/IPA.
  - b. IPA loads the Bound Profile Package to the eUICC.
8. The Profile contained in the Bound Profile Package is installed by the eUICC.
9. Successful installation of the Profile is reported back to the eIM in the response to the request from the eIM. The response contains a Profile installation result Notification signed by the eUICC.
10. The eIM delivers the Notification to the SM-DP+ using the secure connection with SM-DP+.
11. The Operator is notified by the SM-DP+ about the Profile Installation

#### End Conditions:

- a) A Bound Profile Package has been downloaded and the Profile contained in the Bound Profile Package is installed on the eUICC. The Profile is in Disabled state.

NOTE: the automatic enabling for an installed profile is FFS.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
```

```
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "operator" as operator #white
participant "SM-DP+" as smdp #white
participant eIM as eim #white
participant "device/IPA" as ipa #white
participant eUICC as euicc #white

'title eIM Assisted Profile Download triggered by eIM with Activation Code

group Procedure

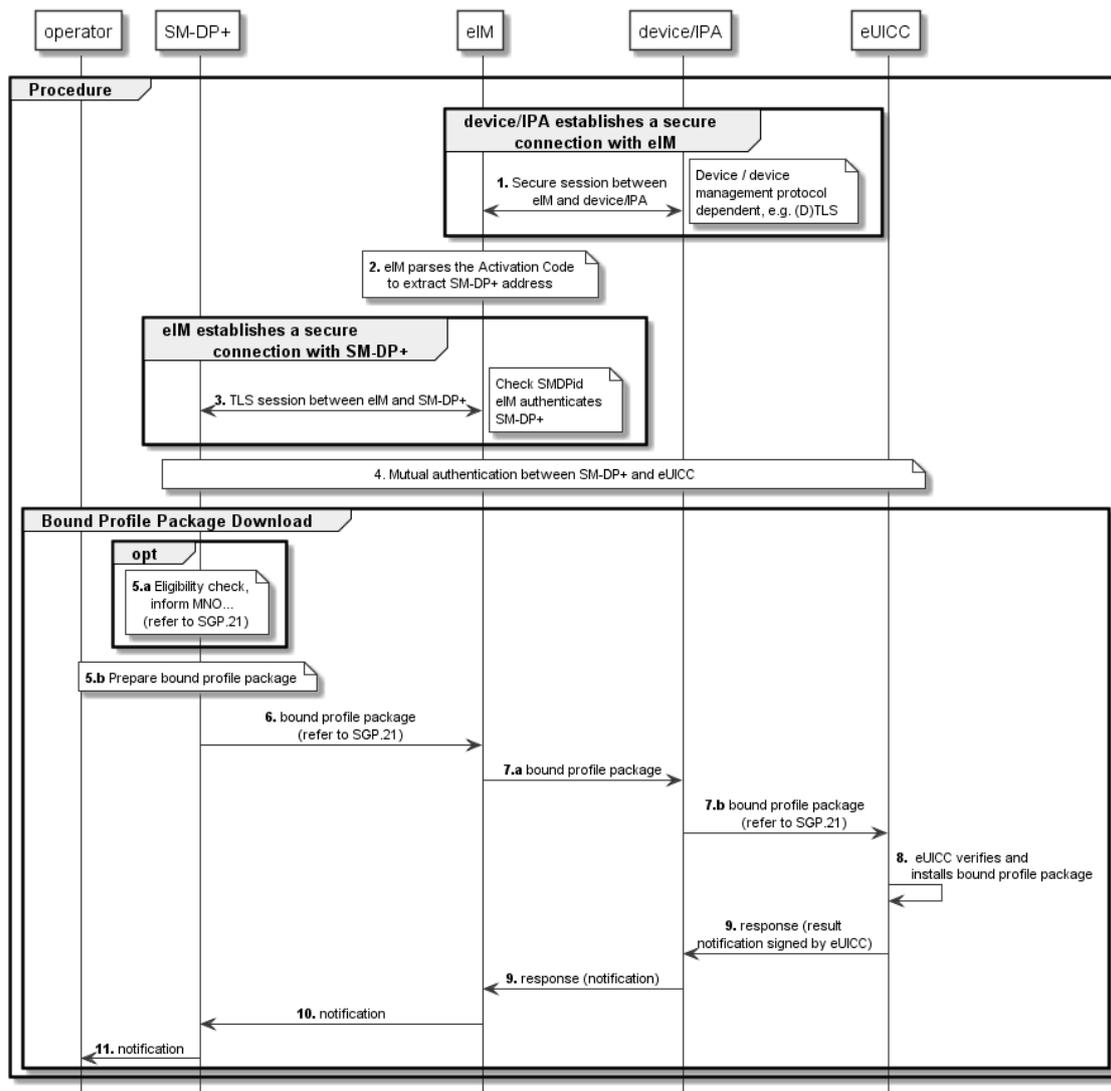
group device/IPA establishes a secure \n          connection with eIM
eim <-> ipa : <b>1. </b>Secure session between\n          eIM and device/IPA
note right #white
Device / device
management protocol
dependent, e.g. (D)TLS
end note
end

note over eim #white: <b>2. </b>eIM parses the Activation Code \n          to extract
SM-DP+ address

group eIM establishes a secure \n          connection with SM-DP+
eim <-> smdp : <b>3. </b>TLS session between eIM and SM-DP+
note right #white
Check SMDPid
eIM authenticates
SM-DP+
end note
end

'group Mutual authentication between eUICC and SM-DP+
'smdp <-> euicc : <b>4 </b>Mutual authentication between eUICC and SM-DP+
note over smdp, euicc #white
4. Mutual authentication between SM-DP+ and eUICC
end note
'end

group Bound Profile Package Download
group opt
note over smdp #white : <b>5.a </b>Eligibility check,\n          inform Operator...\n          (refer to SGP.21)
end
note over smdp #white : <b>5.b </b>Prepare bound profile package
eim <- smdp : <b>6. </b>bound profile package\n          (refer to SGP.21)
eim -> ipa : <b>7.a </b>bound profile package
ipa -> euicc : <b>7.b </b>bound profile package\n          (refer to SGP.21)
euicc -> euicc : <b>8. </b> eUICC verifies and\n          installs bound profile package
ipa <- euicc : <b>9. </b>response (result \nnotification signed by eUICC)
eim <- ipa : <b>9. </b>response (notification)
eim -> smdp : <b>10. </b>notification
operator <- smdp : <b>11. </b>notification
end
end
@enduml
```



### 6.1.4 Profile Download with Default SM-DP+

The following procedure describes the direct Profile Download procedure between the SM-DP+ and the eUICC using Default SM-DP+ address.

#### Start Conditions:

1. The ordering process related to this Profile has been completed.
2. At least one default SM-DP+ address is configured in the eUICC or IPA.

#### Procedure:

1. The IPA is triggered to initiate a Profile Download from the configured default SM-DP+ address.
2. The IPA establishes a secure connection to the SM-DP+.
3. Mutual Authentication between eUICC and SM-DP+ is performed. Additional information from eUICC is provided to the SM-DP+ to proceed with the Profile preparation.
4. The SM-DP+ proceeds with the Profile preparation:
  - a. Performs the eligibility check based on the provided information by the eUICC.
  - b. Prepare the Bound Profile Package.

NOTE: The Operator owning the Profile SHALL be able to stop the Profile download at this stage.

5. The Bound Profile Package is downloaded to the eUICC through the IPA using the secure connection with SM-DP+.
6. The Profile is installed by the eUICC.
7. Successful installation of the Profile on the eUICC is acknowledged and the eIM and the SM-DP+ are notified.
8. The Operator is notified by the SM-DP+ about the Profile Installation

NOTE: it is the responsibility of the Operator to notify the Mobile Service Provider.

#### End Conditions:

- a) A Bound Profile Package has been downloaded and installed on the eUICC in a Disabled state.

NOTE: the automatic enabling for an installed profile is FFS.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OPE
participant "<b>Default SM-DP+" as DP
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

rnote over IPA #FFFFFF
[0] Default SM-DP+ address
is configured
endrnote

IPA -> DP: [1] Profile Download Request

rnote over DP, IPA #FFFFFF
[2] Secure connection establishment
endrnote

rnote over DP, E #FFFFFF
[3] Mutual authentication procedure
Additional information for Profile generation is provided
endrnote

rnote over DP #FFFFFF
[4]
a. Eligibility check
b. Bound Profile Package
generation
endrnote

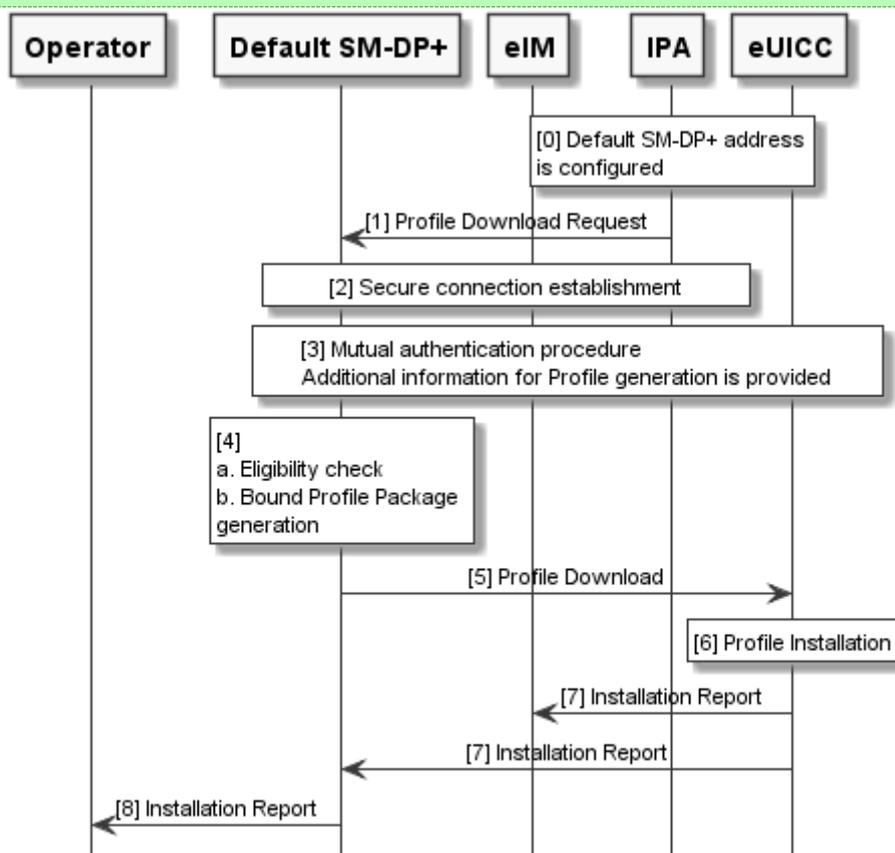
DP -> E: [5] Profile Download

rnote over E #FFFFFF
[6] Profile Installation
endrnote

E -> EIM: [7] Installation Report
E -> DP: [7] Installation Report

DP -> OPE: [8] Installation Report
```

@endum1



### 6.1.5 eIM Assisted Profile Download Triggered by eIM with SM-DS

The following procedure describes the indirect Profile Download procedure between the SM-DP+ and the eUICC using the SM-DS where the eIM assists with both the retrieval of the Event Record and the Profile Download.

#### Start Conditions:

1. The ordering process to this Profile has been completed and a respective Event Record for a Profile Download has been created via ES12.
2. The SM-DS address is available at the eIM.

#### Procedure:

1. The secure connection between IPA and eIM is established via ESipa.
2. The eIM requests the IPA to get information from the eUICC REQUIRED to perform mutual authentication between the eUICC and the SM-DS.
3. The eIM establishes a secure connection to the configured SM-DS
4. Mutual authentication between the SM-DS and the eUICC is performed. The mutual authentication is initiated and driven by the eIM on behalf of the IPA and involves relaying authentication messages between the IoT Device and SM-DS including re-encoding of the messages for the two secure connections ESipa and ES11'.
5. The eIM downloads the Event Record via ES11'.
6. The eIM identifies the address of the SM-DP+ where the Profile is stored.

7. The eIM establishes a secure connection with the SM-DP+ and establishes a secure connection to the IPA.
8. Mutual authentication between eUICC and SM-DP+ is performed. The mutual authentication is initiated and driven by the eIM on behalf of the IPA and involves relaying authentication messages between the IoT Device and SM-DP+ including re-encoding of the messages for the two secure connections ESipa and ES9+'. Additional information from eUICC is provided to the SM-DP+ to proceed with the Profile preparation.
9. The SM-DP+ proceeds with the Profile preparation:
  - a. Perform the eligibility check based on the provided information by the eUICC.
  - b. Prepare the Bound Profile Package.

NOTE: The Operator owning the Profile is able to stop the Profile download at this stage.

10. The eIM receives the Bound Profile Package from the SM-DP+ via ES9+'.
11. The Bound Profile Package is loaded to the eUICC:
  - a. The eIM sends a request to IPA to load the Bound Profile Package to the eUICC. The request contains the Bound Profile Package and is sent using the secure connection with the IoT Device/IPA.
  - b. IPA loads the Bound Profile Package to the eUICC.
12. The Profile contained in the Bound Profile Package is installed by the eUICC.
13. Successful installation of the Profile on the eUICC is reported back to the eIM in the response to the request from the eIM. The response contains a Profile installation result Notification signed by the eUICC.
14. The eIM delivers the Notification to the SM-DP+ using the secure connection with SM-DP+.
15. The Operator is notified by the SM-DP+ about the Profile Installation.

#### End Conditions:

- a) A Bound Profile Package has been downloaded and installed on the eUICC in a Disabled state.

NOTE: the automatic enabling for an installed profile is FFS.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OPE
participant "<b>SM-DP+" as DP
participant "<b>SM-DS" as DS
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

rnote over EIM, IPA #FFFFFF
[1] Secure connection
endrnote

EIM -> E: [2] Request eUICC information
E -> EIM: [2] Provide eUICC information

rnote over EIM, DS #FFFFFF
[3] Secure connection establishment
endrnote
```

```
rnote over DS, E #FFFFFF
[4] Mutual authentication procedure
endrnote

DS -> EIM: [5] Download Event Record via ES11'

rnote over EIM #FFFFFF
[6] Identify SM-DP+
endrnote

rnote over EIM, DP #FFFFFF
[7] Secure connection establishment
endrnote

rnote over E, DP #FFFFFF
[8]
Mutual authentication Procedure
Additional information for Profile generation is provided
endrnote

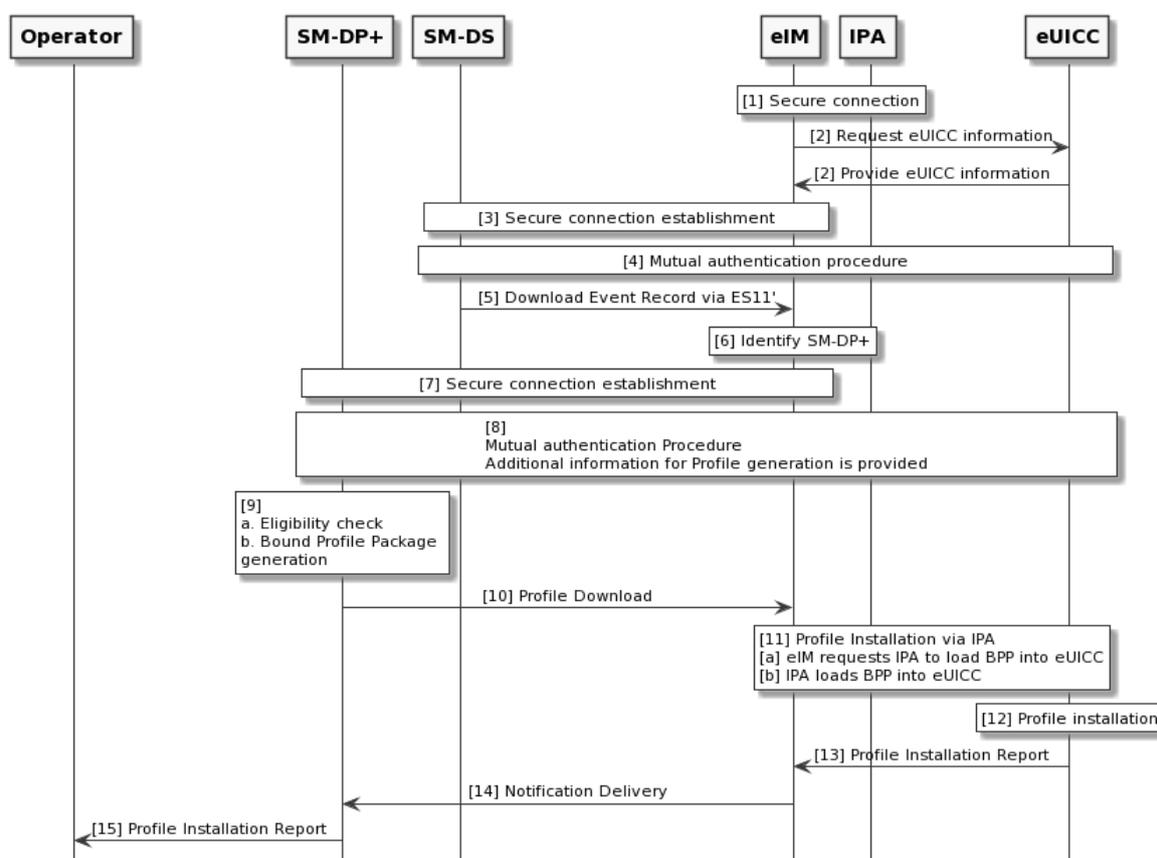
rnote over DP #FFFFFF
[9]
a. Eligibility check
b. Bound Profile Package
generation
endrnote

DP -> EIM: [10] Profile Download

rnote over EIM, E #FFFFFF
[11] Profile Installation via IPA
[a] eIM requests IPA to load BPP into eUICC
[b] IPA loads BPP into eUICC
endrnote

rnote over E #FFFFFF
[12] Profile installation
endrnote

E -> EIM: [13] Profile Installation Report
EIM -> DP: [14] Notification Delivery
DP -> OPE: [15] Profile Installation Report
@enduml
```



## 6.2 Profile Enabling

### 6.2.1 Profile Enabling via eIM

The following procedure describes the Profile Enabling procedure via the eIM.

#### Start Conditions:

1. The eIM and the eUICC are associated.
2. The target Profile has been selected by the eIM.

#### Procedure:

1. The eIM prepares and signs the Profile Enabling request for the target Profile and sends it to the IPA.
2. The IPA sends the signed Profile Enabling request for the target Profile to the eUICC.
3. The eUICC verifies that the Profile Enabling request is signed by an eIM that is configured in the eUICC as an Associated eIM.
4. If the verification fails, the eUICC aborts the procedure.
5. If the verification is successful, the eUICC disables the currently enabled Profile, if any, and enables the target Profile.
  - a. If the Profile is already enabled, no error SHOULD be generated.
6. The IPA retrieves the signed result of the enabling of the target Profile from the eUICC.
7. The IPA includes the signed result from the eUICC into a response to the eIM to notify about the result of the Profile Enabling execution.

- a. If the eIM cannot be notified and if the Roll-Back Mechanism has been requested by the eIM, the IPA informs the eUICC to execute the Roll-Back Mechanism. The eUICC informs the IPA, and the IPA informs the eIM of the enabling of the previously enabled Profile. The procedure stops here.
8. The IPA retrieves the pending Notifications from the eUICC and sends the Notifications to the Notification Receivers.

#### End Conditions:

- a) If the Roll-Back Mechanism has been executed, the previously enabled Profile is enabled.
- b) Otherwise, the target Profile is enabled and the previously enabled Profile, if any, is disabled.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>SM-DP+" as DP
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

EIM -> IPA: [1] Signed Profile Enable Request

IPA -> E: [2] Signed Profile Enable Request

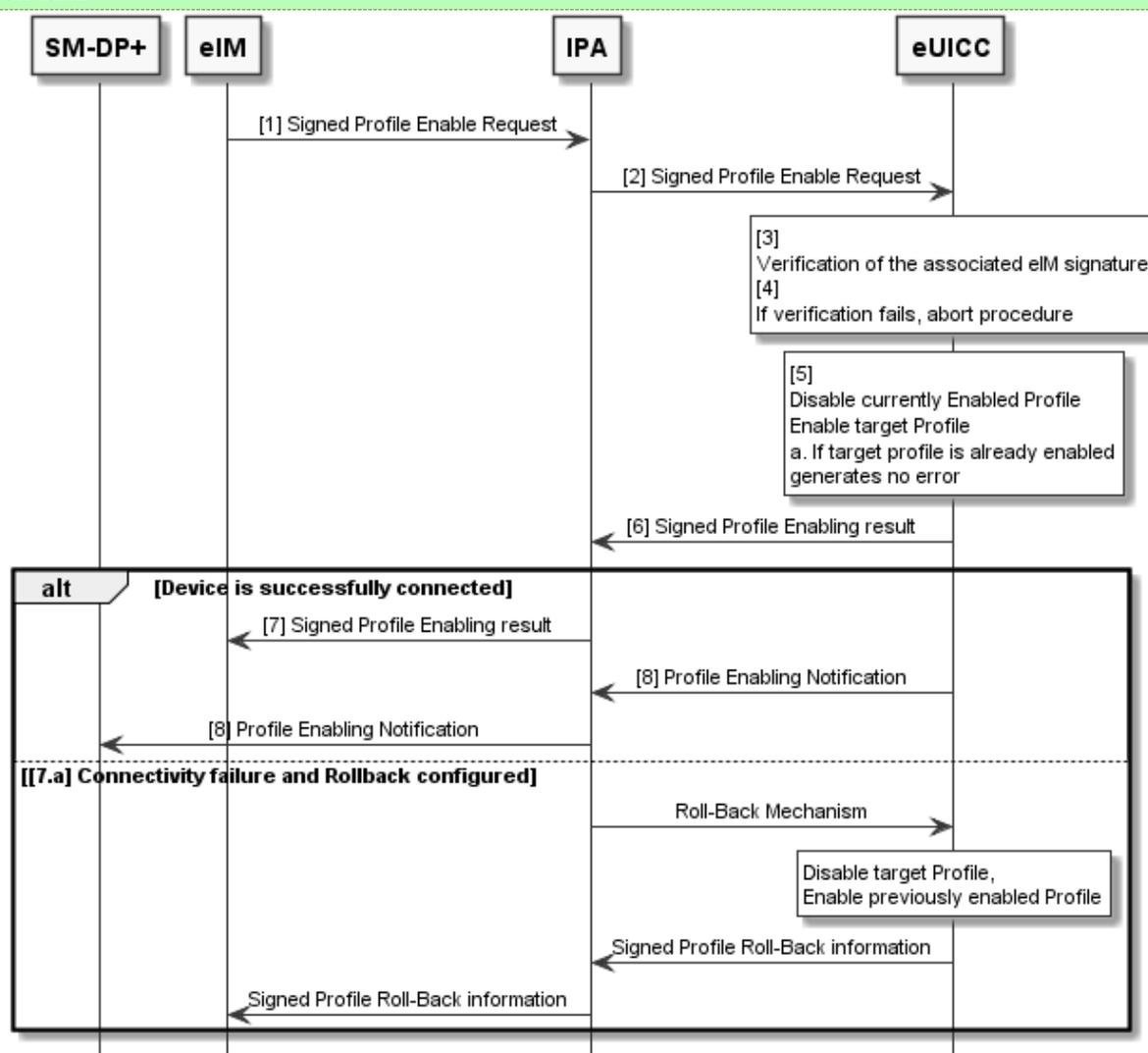
rnote over E #FFFFFF
[3]
Verification of the associated eIM signature
[4]
If verification fails, abort procedure
endrnote

rnote over E #FFFFFF
[5]
Disable currently Enabled Profile
Enable target Profile
a. If target profile is already enabled
generates no error
endrnote

E -> IPA: [6] Signed Profile Enabling result

alt Device is successfully connected
IPA -> EIM: [7] Signed Profile Enabling result
E -> IPA: [8] Profile Enabling Notification
IPA -> DP: [8] Profile Enabling Notification
else [7.a] Connectivity failure and Rollback configured
IPA -> E: Roll-Back Mechanism
rnote over E #FFFFFF
Disable target Profile,
Enable previously enabled Profile
endrnote
E -> IPA: Signed Profile Roll-Back information
IPA -> EIM: Signed Profile Roll-Back information
end
```

@endum1



## 6.3 Profile Disabling

### 6.3.1 Profile Disabling via eIM

The following procedure describes the Profile Disabling procedure via the eIM.

#### Start Conditions:

1. The eIM is configured in the eUICC as an Associated eIM.
2. The target Profile has been selected by the eIM.

#### Procedure:

1. The eIM prepares and signs a Profile Disabling request for the target Profile and sends it to the IPA
2. The IPA sends the signed Profile Disable request for the target Profile to the eUICC
3. The eUICC verifies that the Profile Disable request is signed by an eIM that is configured in the eUICC as an Associated eIM.
4. If the verification fails, the eUICC aborts the procedure.
5. If the verification is successful, the eUICC disables the target enabled Profile.

- a. If the Profile is already disabled, no error SHOULD be generated.
6. The IPA retrieves the signed result IPA of the disabling of the target Profile from the eUICC
7. The IPA includes the signed result from the eUICC into a response to the eIM.
8. The IPA retrieves the pending Notifications from the eUICC and sends the Notifications to the Notification Receivers.

**End Conditions:**

- a) The target Profile is disabled.
- b) Mobile connectivity not available

NOTE: the automatic enabling for an installed Profile and Profile Switch is FFS.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>SM-DP+" as DP
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

EIM -> IPA: [1] Signed Profile Disable request

IPA -> E: [2] Signed Profile Disable Request

rnote over E #FFFFFF
[3]
Verification of the associated eIM signature
[4]
If verification fails, abort procedure
endrnote

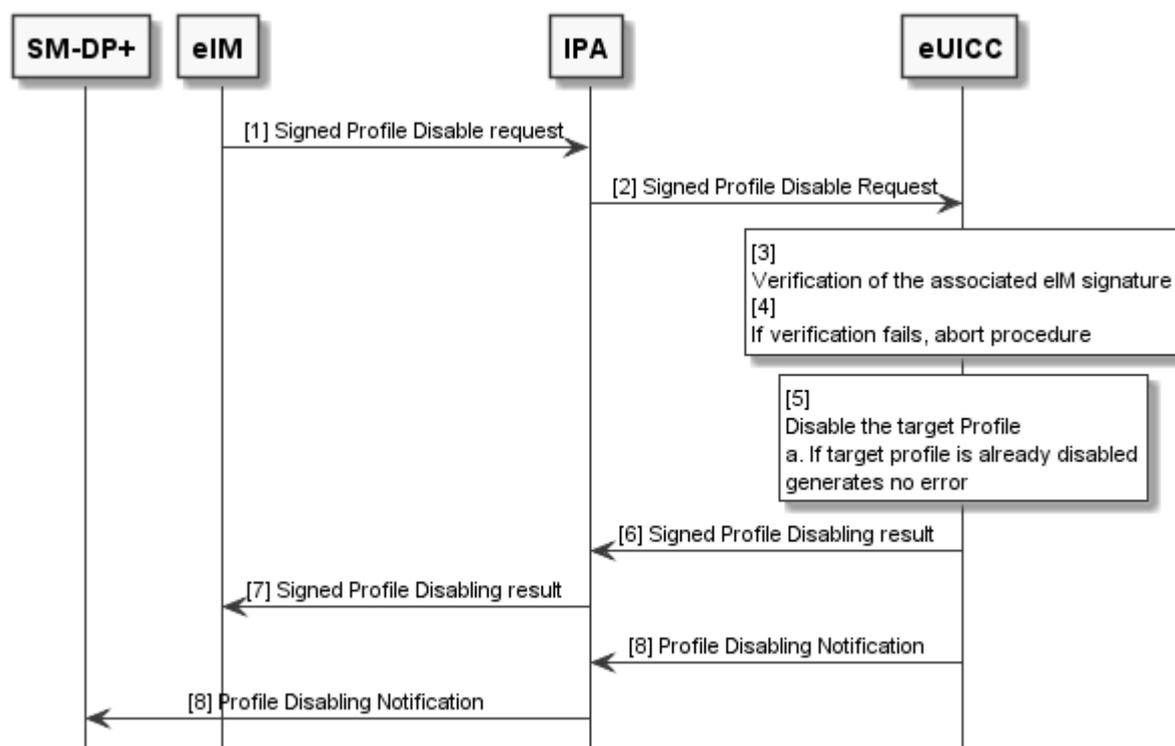
rnote over E #FFFFFF
[5]
Disable the target Profile
a. If target profile is already disabled
generates no error
endrnote

E -> IPA: [6] Signed Profile Disabling result

IPA -> EIM: [7] Signed Profile Disabling result

E -> IPA: [8] Profile Disabling Notification
IPA -> DP: [8] Profile Disabling Notification

@enduml
```



## 6.4 Profile Delete

### 6.4.1 Profile Delete via eIM

The following procedure describes the Profile Delete procedure via the eIM.

#### Start Conditions:

1. The target Profile is present in the eUICC in disable state
2. The eIM is configured in the eUICC as an Associated eIM.
3. The target Profile has been selected by the eIM.

#### Procedure:

1. The eIM prepares and signs a Profile Delete request for the target Profile and sends it to the IPA.
2. The IPA sends and signs Profile Delete request for the target Profile to the eUICC.
3. The eUICC verifies that the Profile Delete operation is signed by an eIM that is configured in the eUICC as an Associated eIM.
4. If the verification fails, the eUICC aborts the procedure.
5. The eUICC verifies that the target Profile is disabled.
6. If the verification fails, the eUICC aborts the procedure and informs the eIM.  
NOTE: How the eIM is informed is left to the technical realisation.
7. If the verification is successful, the eUICC deletes the target Profile and all the data associated to this Profile.
8. The IPA retrieves the signed result of the deletion of the target Profile from the eUICC.
9. The IPA includes the signed result from the eUICC into a response to the eIM.
10. The IPA retrieves the pending Notifications from the eUICC and sends the Notifications to the Notification Receivers

**End Conditions:**

- a) The target Profile is deleted.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>SM-DP+" as DP
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

EIM -> IPA: [1] Signed Profile Delete request

IPA -> E: [2] Signed Profile Delete Request

rnote over E #FFFFFF
[3]
Verification of the associated eIM signature
[4]
If verification fails, abort procedure
endrnote

rnote over E #FFFFFF
[5]
Verification of the target Profile is disabled
endrnote

E -> IPA: [6] Error
IPA -> EIM: [6] Error

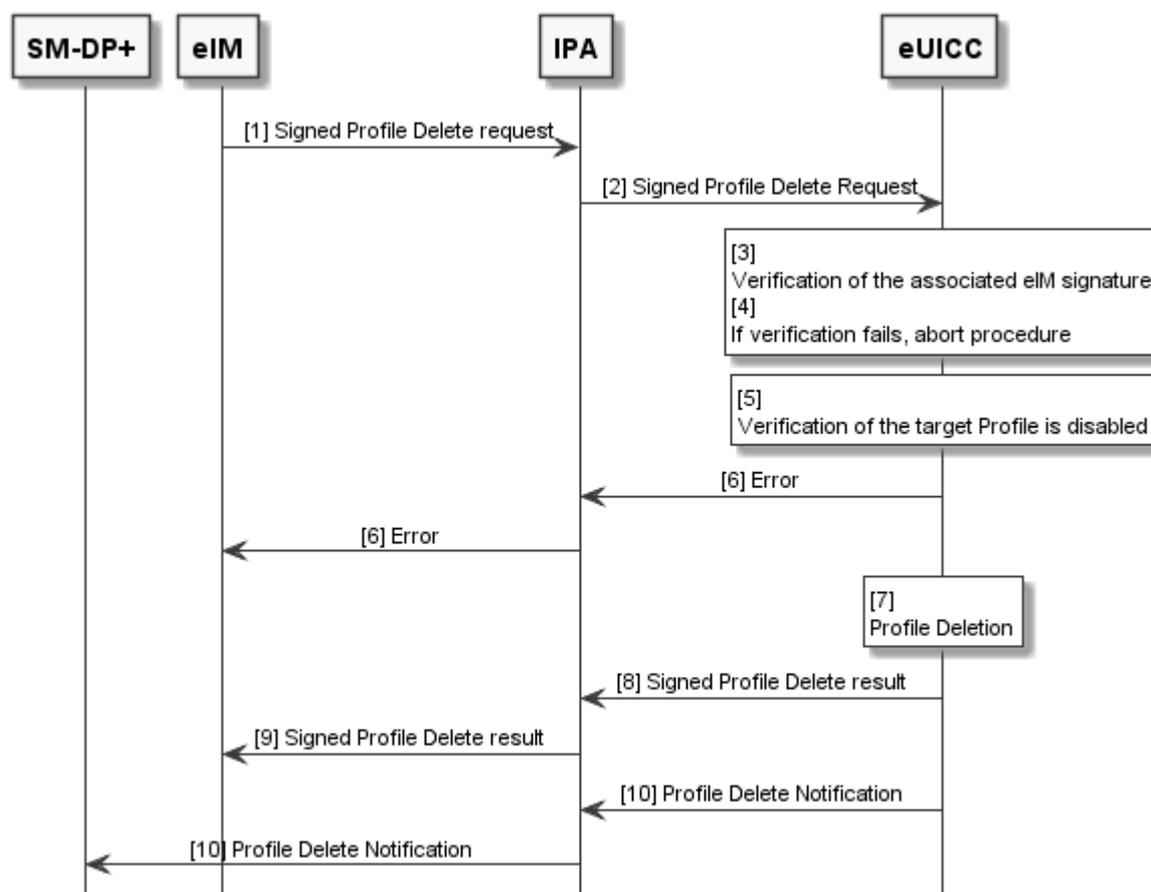
rnote over E #FFFFFF
[7]
Profile Deletion
endrnote

E -> IPA: [8] Signed Profile Delete result

IPA -> EIM: [9] Signed Profile Delete result

E -> IPA: [10] Profile Delete Notification
IPA -> DP: [10] Profile Delete Notification

@enduml
```



## 6.5 eIM Configuration

### 6.5.1 Add eIM Configuration Data via IPA

The following procedure describes adding eIM Configuration Data to the eUICC when no eIM is associated within the eUICC.

#### Start Conditions:

1. No eIM is associated within the eUICC

#### Procedure:

1. The IPA sends the eIM Configuration Operation, including the eIM Configuration Data to the eUICC.
2. The eUICC checks if an Associated eIM exists.
  - a. If no eIM is associated, the eUICC executes the eIM Configuration Operation, else
  - b. the eUICC aborts the procedure.
3. The IPA retrieves the result of the eIM Configuration Operation from the eUICC

#### End Conditions:

- a) The eIM Configuration Data of the Associated eIM is stored in the eUICC.

```

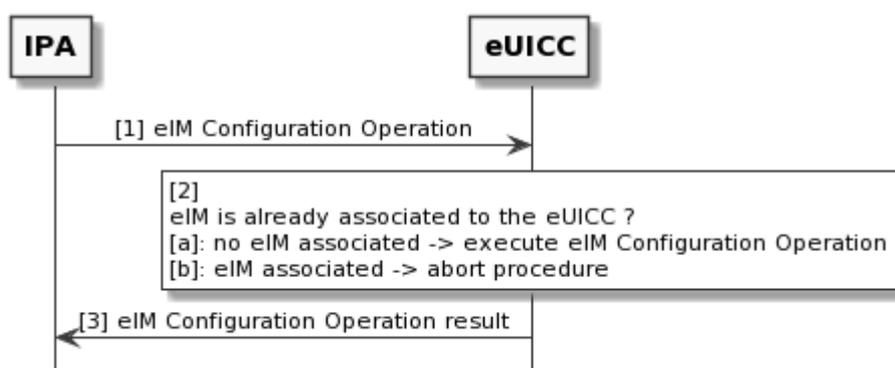
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>IPA" as IPA
participant "<b>eUICC" as E

IPA -> E: [1] eIM Configuration Operation
note over E #FFFFFF
[2]
eIM is already associated to the eUICC ?
[a]: no eIM associated -> execute eIM Configuration Operation
[b]: eIM associated -> abort procedure
endnote

E -> IPA: [3] eIM Configuration Operation result
@enduml

```



### 6.5.2 eIM Configuration via eIM

The following procedure describes the eIM Configuration Operation process when an eIM is associated within the eUICC.

#### Start Conditions:

1. An eIM is associated with an eUICC.

#### Procedure:

1. The eIM prepares and signs an eIM Configuration Operation and sends it to the IPA.
2. The IPA sends the signed eIM Configuration Operation to the eUICC.
3. The eUICC verifies that the eIM Configuration Operation is signed by an eIM that is configured in the eUICC as an Associated eIM.
  - a. If the verification is successful, the eUICC processes the eIM Configuration Operation else
  - b. the eUICC aborts the procedure.
4. The IPA retrieves the signed result from the eUICC.
5. The IPA includes the signed result from the eUICC into a response to the eIM.

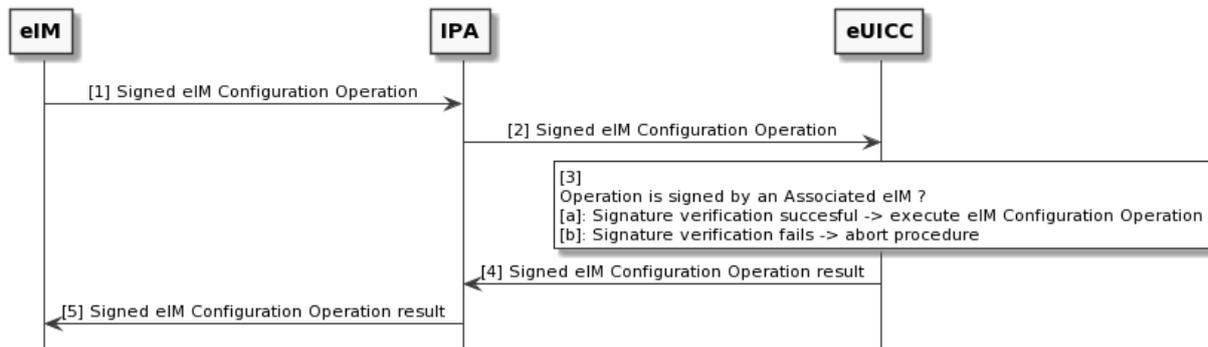
**End Conditions:**

- a) The requested eIM Configuration Data is stored in or removed from the eUICC.

```

@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid
participant "<b>eIM" as EIM
participant "<b>IPA" as IPA
participant "<b>eUICC" as E

EIM -> IPA: [1] Signed eIM Configuration Operation
IPA -> E: [2] Signed eIM Configuration Operation
note over E #FFFFFF
[3]
Operation is signed by an Associated eIM ?
[a]: Signature verification succesful -> execute eIM Configuration Operation
[b]: Signature verification fails -> abort procedure
Endrnote
E -> IPA: [4] Signed eIM Configuration Operation result
IPA -> EIM: [5] Signed eIM Configuration Operation result
@enduml
  
```



**6.5.3 Complete Removal of eIM Configuration Data from the eUICC**

The following procedure describes how to completely remove all eIM Configuration Data from the eUICC.

**Start Conditions:**

- 1. An eIM is associated within the eUICC

**Procedure:**

- 1. The IPA sends the eIM Configuration Data removal operation to the eUICC.
- 2. The eUICC executes the operation and removes all available eIM Configuration Data stored in it.
- 3. The IPA retrieves the result of the operation from the eUICC.

**End Conditions:**

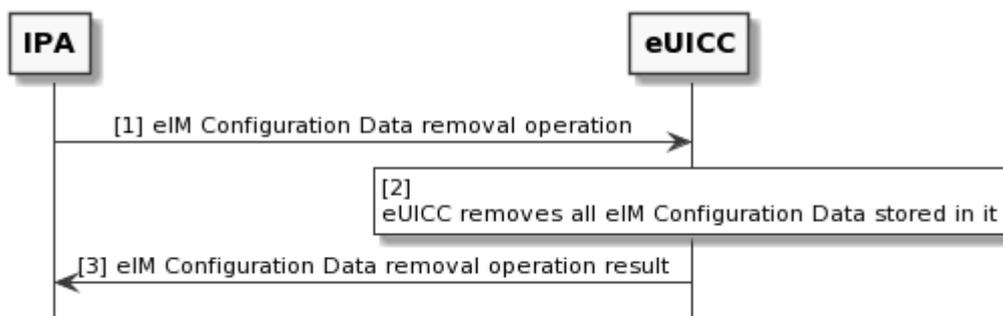
- a) The eIM Configuration Data is completely removed from the eUICC.
- b) The eUICC is not associated with any eIM anymore.

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>IPA" as IPA
participant "<b>eUICC" as E

IPA -> E: [1] eIM Configuration Data removal operation
note over E #FFFFFF
[2]
eUICC removes all eIM Configuration Data stored in it
endnote

E -> IPA: [3] eIM Configuration Data removal operation result
@enduml
```



## Annex A Threats and Risks (Informative)

This section lists and describes different types of risks that are considered by the architecture as described within this specification.

### A.1 Compromised IoT Device

Risk no.	Risk description
DEV1	Malicious IoT Device SW/FW and/or malicious IPA is able to perform illegitimate PSMO on the eUICC.
DEV2	Malicious IoT Device SW/FW and/or malicious IPA is able to block all PSMO to eUICC.
DEV3	Malicious IoT Device SW/FW and/or malicious IPA is able to associate illegitimate eIM to eUICC.
DEV4	Malicious IoT Device SW/FW and/or malicious IPA is able to improperly deleting eIM associations on the eUICC.

**Table 4: Compromised IoT Device Risks**

### A.2 Compromised eIM

An authorized and legitimate eIM is manipulated and compromised.

Risk no.	Risk description
CeIM1	Attacker is able to perform illegitimate PSMO on a number of eUICCs.
CeIM2	Attacker is able to perform illegitimate eIM Configuration Operations on a number of eUICCs.

**Table 5: Compromised eIM Risks**

### A.3 Malicious eIM

A malicious eIM is both not authorized and illegitimate, e.g. malicious eIM acts as man-in-the-middle.

Risk no.	Risk description
MeIM1	Attacker is able to perform unauthorized, illegitimate PSMO on a number of IoT Devices / eUICCs.
MeIM2	Attacker is able to perform unauthorized, illegitimate eIM Configuration Operations on a number of eUICCs.

**Table 6: Malicious eIM Risks**

### A.4 Privacy Leakage

Leakage of privacy relevant data on the interface between the eIM and the IoT Device.

Risk no.	Risk description
PRI1	Attacker gets hold of privacy related information of the eUICC (e.g. EID) that may be used to track the location of the IoT Device.
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 IoT Devices or the Subscriber themselves.

**Table 7: Loss of Privacy Risks**

## A.5 New Profile on New IoT Device

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

**Table 8: New Profile on New IoT Device Risks**

## A.6 Profile Disabling / 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 / malicious entity launching coordinated or isolated disabling or deletion of one or several Profiles leading to a loss of connectivity to an IoT Device.
IND4	Malicious or compromised eIM launching coordinated or isolated disabling or deletion of one or several Profiles leading to a loss of connectivity to an IoT Device.
IND5	Accidental Profile disabling or deletion leading to a loss of connectivity to an IoT Device.
IND6	Malicious or compromised eIM repeatedly deleting Profiles and asking for them to be reloaded leading to surcharge of provisioning servers.
IND7	Malicious execution of PSMO leading to wrong enabled/disabled/deleted Profile.
IND8	Malicious execution of PSMO from an internal party leading to wrong Profile status reported to the eIM.

**Table 9: Profile Disabling or Deletion Risks**

## A.7 Profile Switch

Risk no.	Risk description
INP1	Malicious Profile switching originating from an internal party.
INP2	Malicious Profile switching originating from a malicious or compromised eIM.
INP3	Switching of alternate Profiles leading to a loss of connectivity.
INP4	Malware / malicious entity launching coordinated or isolated switching of one or several Profiles leading to a loss of connectivity.
INP5	Malware / malicious entity launching coordinated or isolated switching of one or several Profiles leading to major fraud scenarios.

**Table 10: Profile Switching Risks**

## A.8 Profile Swap

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

**Table 11: Profile Swapping Risks**

## A.9 Cryptographic Related Risks

Risk no.	Risk description
----------	------------------

<b>INO1</b>	Loss or theft of private keys in one or several Profile Management components leading to the loss of confidentiality on the whole chain.
<b>INO2</b>	Inability to revoke compromised Certificates leading to the loss of trust on the whole Certificate chain.
<b>INO3</b>	Local law enforcement requests leading to the forceful disclosure of key materials.
<b>INO4</b>	Local law enforcement requests leading to the forceful compromise of key components.
<b>INO5</b>	Malicious or accidental revocation of Certificates leading to the denial of service on the whole provisioning Certificate chain.
<b>INO6</b>	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 12: Cryptographic Related Risks**

### A.10 Quality of Service

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

**Table 13: Quality of Service Risks**

### A.11 Non-human or Unpredictable

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

**Table 14: Non-human or Unpredictable Risks**

### A.12 New Profile during Subscriber Journey

<b>Risk no.</b>	<b>Risk description</b>
<b>EXN1</b>	Malicious pairing of new IoT Device using unattended IoT Device.
<b>EXN2</b>	Use of public Wi-Fi for internet connectivity leading to the loss of confidentiality during the provisioning of Profile operations.
<b>EXN3</b>	Use of public Wi-Fi for internet connectivity leading to the tampering of registration information during provisioning of Profile operations.
<b>EXN5</b>	Man-in-the-middle or eavesdropping during Profile provisioning leading to the loss of confidentiality.
<b>EXN6</b>	“Implicit authentication” (e.g. HTTP MSISDN enrichment) leading to the loss of authentication or Profile material.

**Table 15: New Profile during Subscriber Journey Risks**

### A.13 Others

Risk no.	Risk description
EX01	Compromising of exchanges between Profile Management actors leading to the critical loss of private keys.
EX02	Profile cloning due to unpredicted implementation routines for specific scenarios.

Table 16: Other Risks

## Annex B eIM Configuration Scenarios (Informative)

This section describes different types of eIM configuration scenarios that are considered by the architecture described in this specification.

This section contains some examples and is not limited to them.

### B.1 eIM Configuration Performed by the EUM

The EUM performs the loading of the eIM Configuration Data into the eUICC the during eUICC manufacturing process.

The mechanisms are EUM specific and not described in this specification. The security of EUM production scenarios is covered by SAS UP.

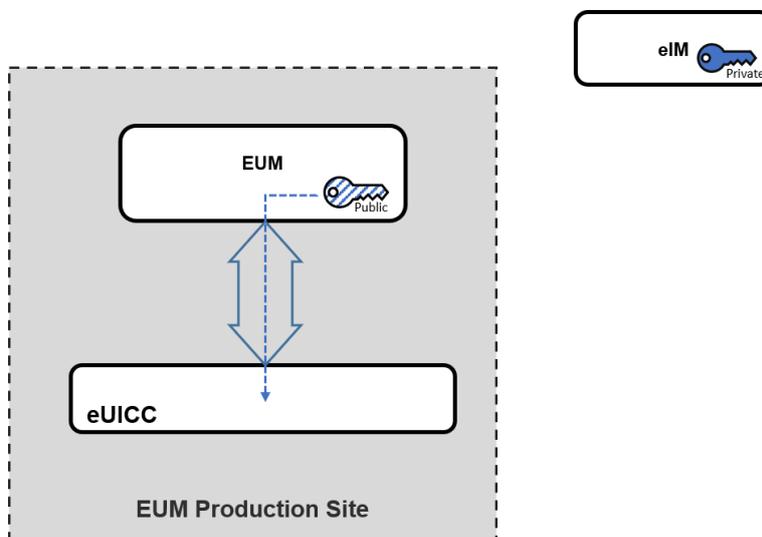


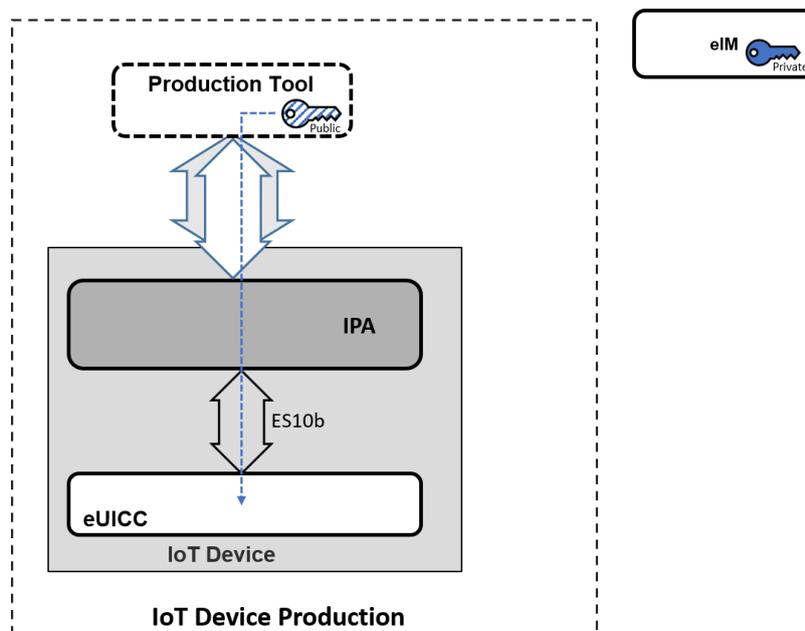
Figure 4: eIM Configuration performed by the EUM

### B.2 eIM Configuration Performed in the IoT Device Production

A production tool communicates with the IoT Device and establishes a secure link to the IPA to trigger eIM Configuration and to provide the eIM Configuration Data. The IPA transfers the eIM Configuration Operations and corresponding results to/from the eUICC.

NOTE: The mechanism and security applied between the production tool and the IPA are left to the implementation. Secure link between production tool and IPA can be provided by the underlying transport between production tool and IoT Device.

NOTE: IoT Device Production can be understood in a broader sense (e.g. module production, device production, warehouse, logistic partner, field technician etc.).



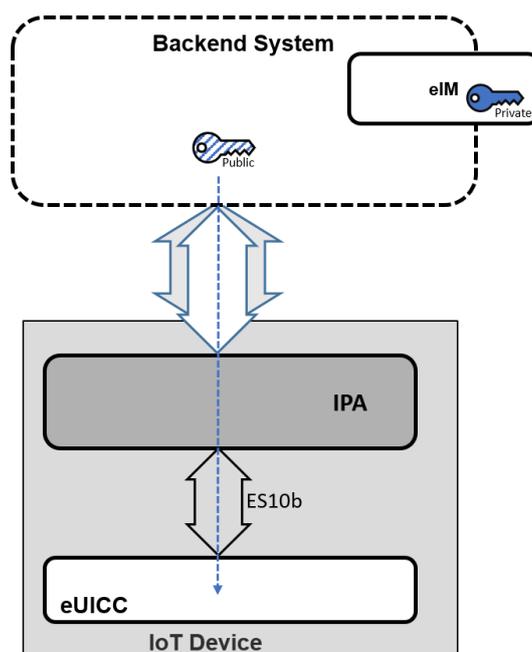
**Figure 5: eIM Configuration performed in IoT Device production**

### **B.3 eIM Configuration Performed in the Field by a Backend System**

A backend system (e.g. smart meter management platform or mobile application) has already a communication in place with the IoT Device. The backend system establishes a secure link to the IPA to trigger eIM Configuration and provides the eIM Configuration Data. The IPA transfers the eIM Configuration Operations and corresponding results to/from the eUICC.

NOTE: The mechanism and security applied between the backend system and the IPA are left to the implementation. Secure link between backend system and IPA can be provided by the underlying transport between backend system and IoT Device.

NOTE: General clarification and illustrated in Figure 6, the eIM can, but does not have to be part of the backend system.

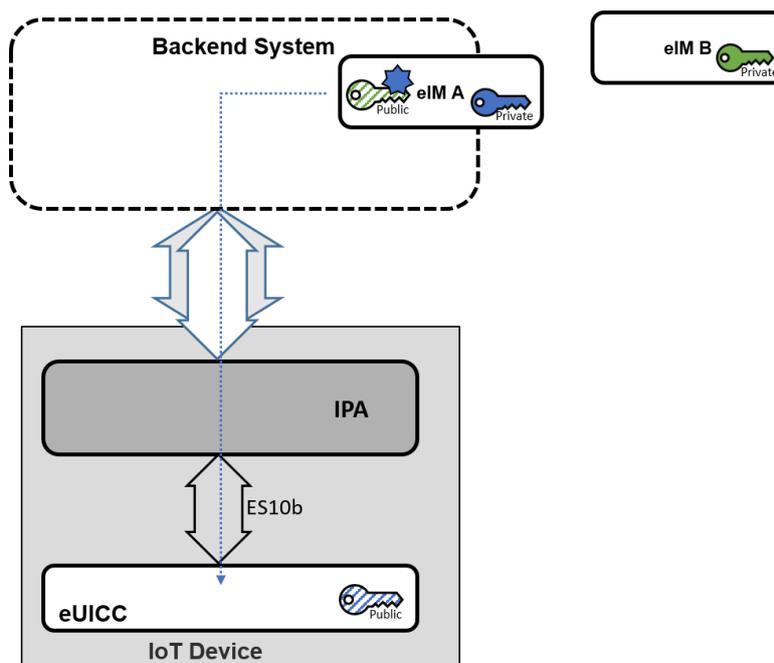


**Figure 6: eIM Configuration performed in the field by a backend system**

#### **B.4 eIM Configuration Performed by an eIM**

A backend system (e.g. smart meter management platform or mobile application) has already a communication in place with the IoT Device. In this example, the eIM\_A is considered as part of this backend system and is already associated to the eUICC.

To associate a new eIM\_B to the eUICC, the eIM\_A prepares an eIM Configuration Operation including the public key of eIM\_B and signs the Operation with its private eIM\_A key. The eIM\_A sends the signed eIM Configuration Operation to the IPA and the IPA forwards the operation to the eUICC, which proves the signature before executing the operation. After successful execution eIM\_B is associated to the eUICC.



**Figure 7: eIM Configuration performed by an eIM**

## B.5 Removal of eIM Configuration

A backend system (e.g. smart meter management platform or mobile application) has already a communication in place with the IoT Device. The backend system establishes a secure link to the IPA to trigger the removal of the eIM Configuration. The IPA transfers the operations and corresponding results to/from the eUICC.

NOTE: The removal of the eIM association(s) might be realised by a kind of reset functionality by the IoT Device, protected against misuse.

NOTE: The mechanism and security applied between the backend system and the IPA are left to the implementation. Secure link between backend system and IPA can be provided by the underlying transport between backend system and IoT Device.

NOTE: General clarification and illustrated in Figure 8, the eIM can, but does not have to be part of the backend system.

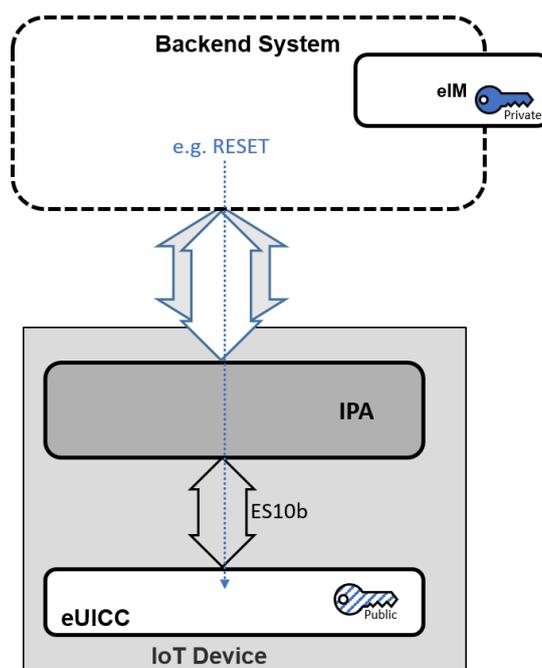


Figure 8: Removal of eIM Configuration

## Annex C Profile Download Deployment Scenarios (Informative)

This Annex gives some examples of deployment scenarios for the Profile download operations.

### C.1 Indirect Profile Download

In Indirect Profile download scenarios, the eIM is always involved in the Profile download operation. It is acting as a support between the SM-DP+ and the IPA. Hence, ES9+' and ESipa are used for Profile Download.

The transfer of the Profile from the SM-DP+ to the eIM is done using ES9+'. The transfer of the Profile from the eIM to the IPA is done using ESipa. ES8+ is always used between the SM-DP+ and the eUICC.

#### C.1.1 Indirect Profile Download Assisted by eIM Using AC

In this example (see Figure 9), the Profile download is triggered using the Activation Code.

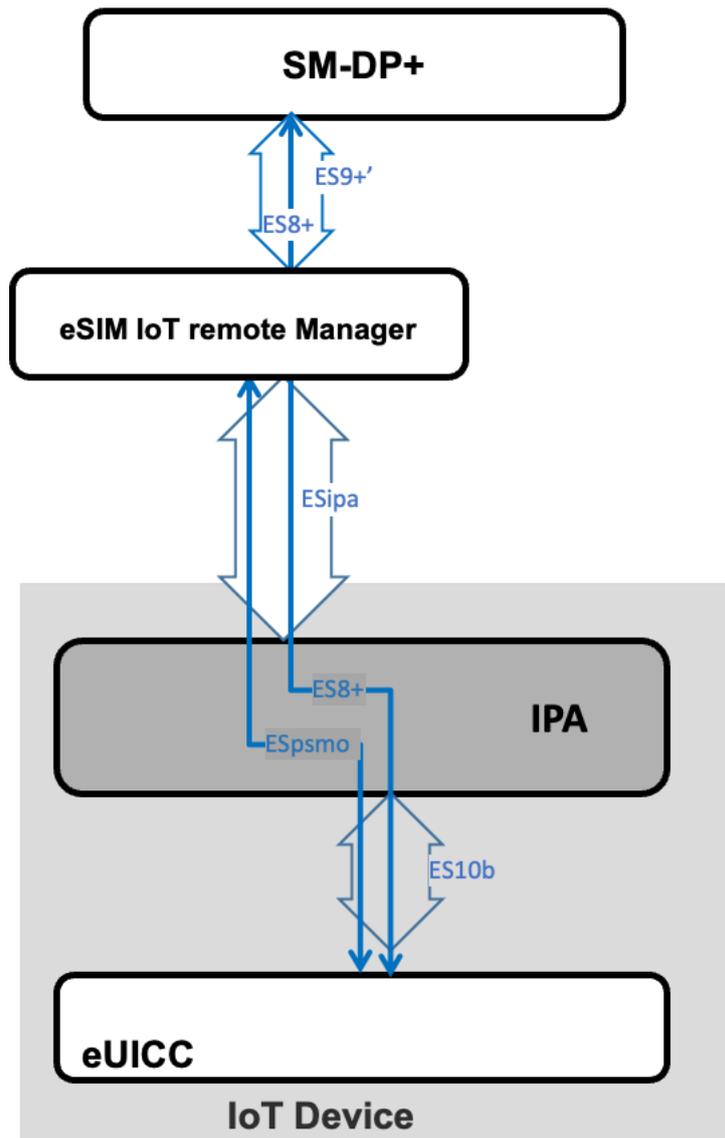
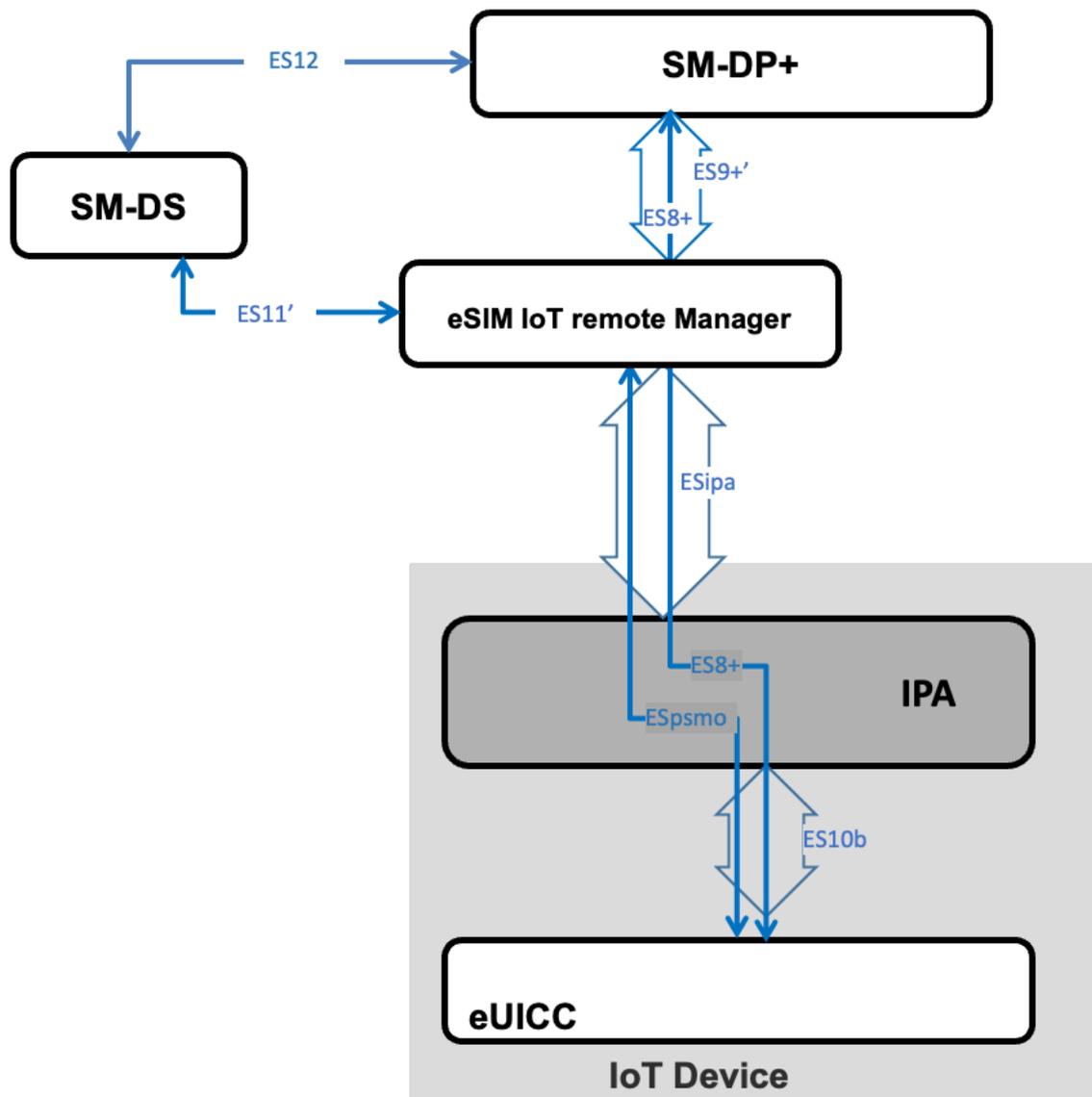


Figure 9: Indirect Profile download assisted by eIM using AC

### C.1.2 Indirect Profile Download Assisted by eIM Using SM-DS

In the example shown in Figure 10, the Profile download is triggered using SM-DS. The Profile download Event Record is retrieved by the eIM using ES11'.



**Figure 10: Indirect Profile download assisted by eIM using SM-DS**

## C.2 Direct Profile Download

In direct Profile download scenarios, ES9+' and ESipa are not used for Profile download. This means that the eIM doesn't use an ES9+' interface with the SM-DP+ for the Profile download.

The transfer of the Profile from the SM-DP+ to the IPA is always done via ES9+. The eIM may be involved to differing degrees (e.g. send the Activation Code,...).

### C.2.1 Direct Profile Download Assisted by eIM Using Activation Code

In this example (see Figure 11), the eIM instructs the IPA using an Activation Code.

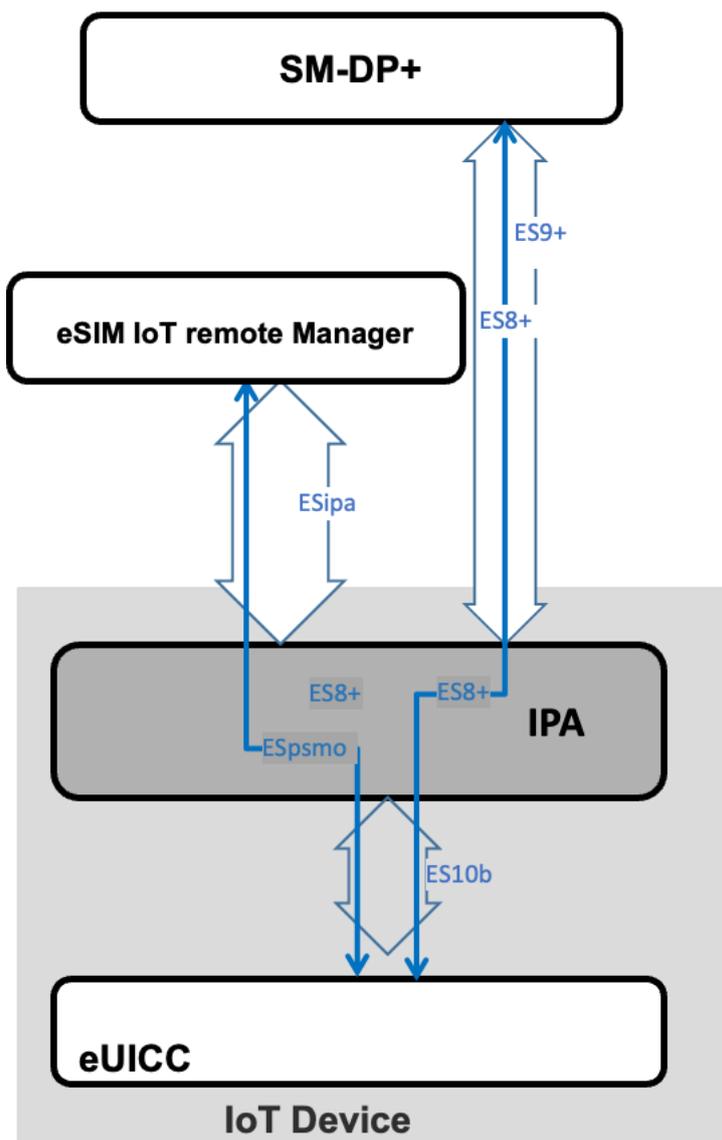


Figure 11: Direct Profile Download assisted by eIM using AC

### C.2.2 Direct Profile Download Assisted by eIM Using SM-DS

In this example (see Figure 12), the Profile download Event Record is retrieved by the eIM using ES11'. This Event is sent to the IPA using ESipa.

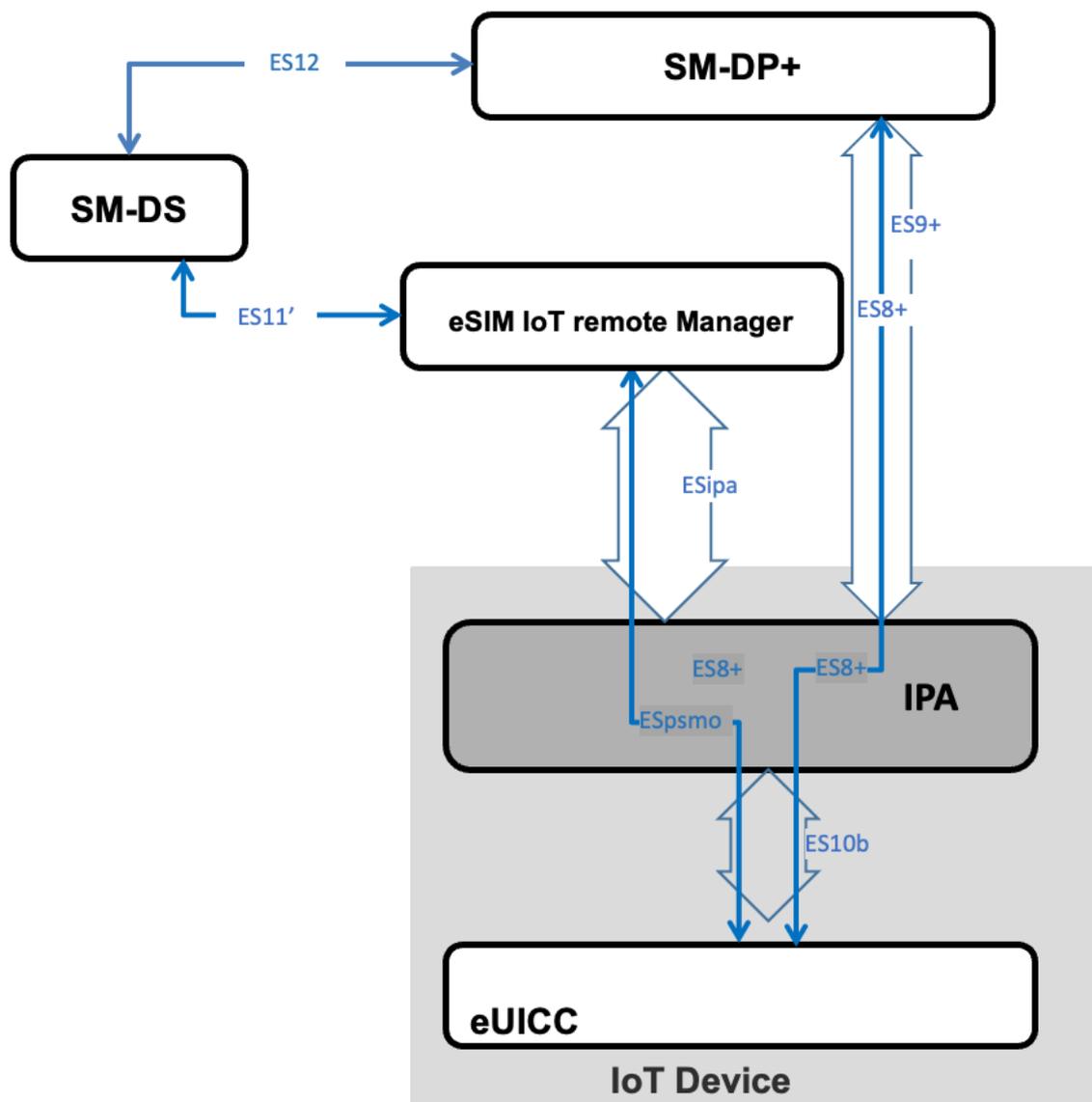


Figure 12: Direct Profile Download assisted by eIM using SM-DS

### C.2.3 Direct Profile Download Unassisted by eIM Using SM-DS

In this example (Figure 13), the IPA retrieves the Profile download Event Record from the SM-DS using ES11.

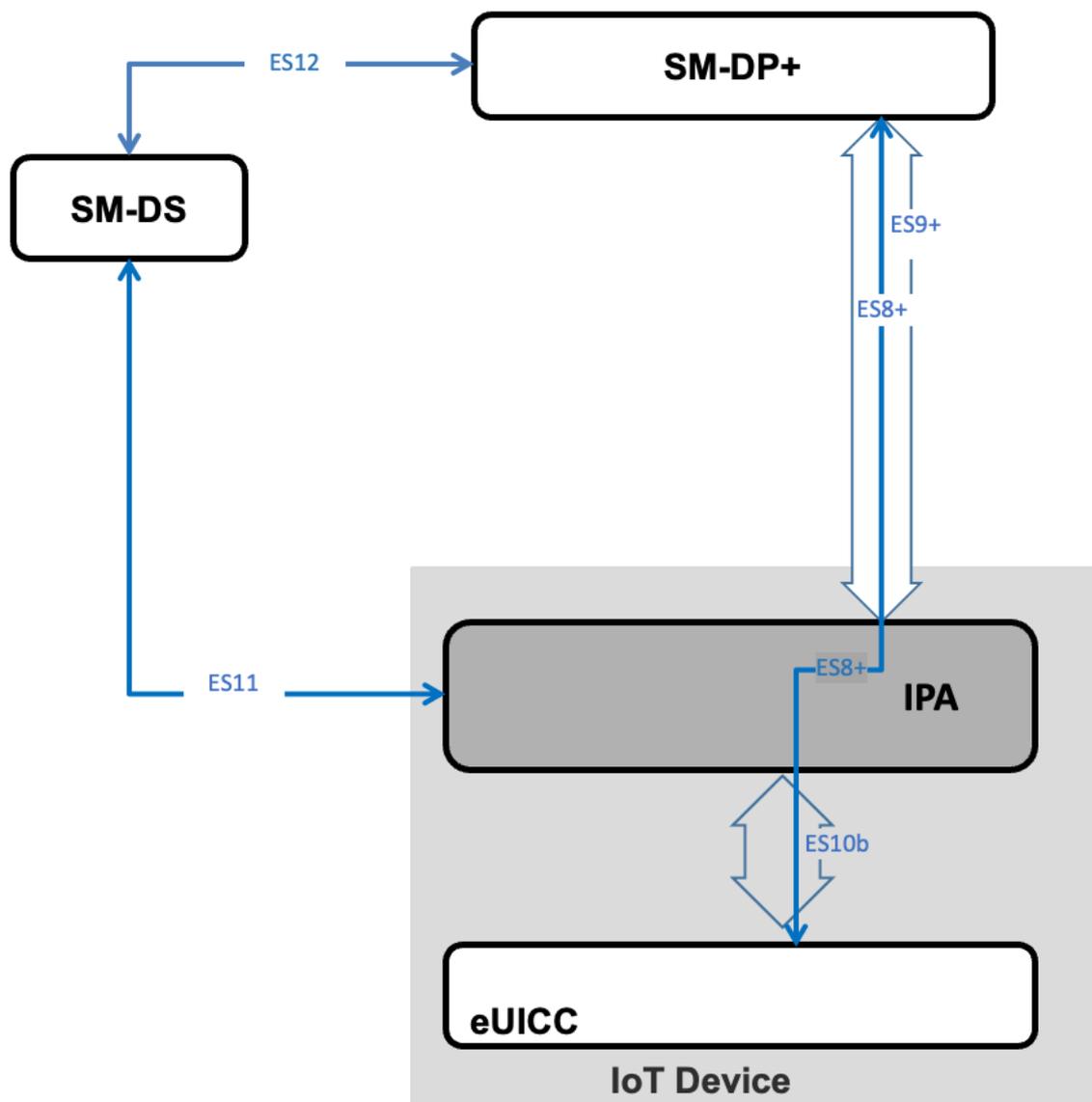


Figure 13: Direct Profile download unassisted by eIM using SM-DS

#### C.2.4 Direct Profile Download Unassisted by eIM Using Default SM -DP+

The Profile download is done using ES9+ between the IPA and the default SM-DP+.

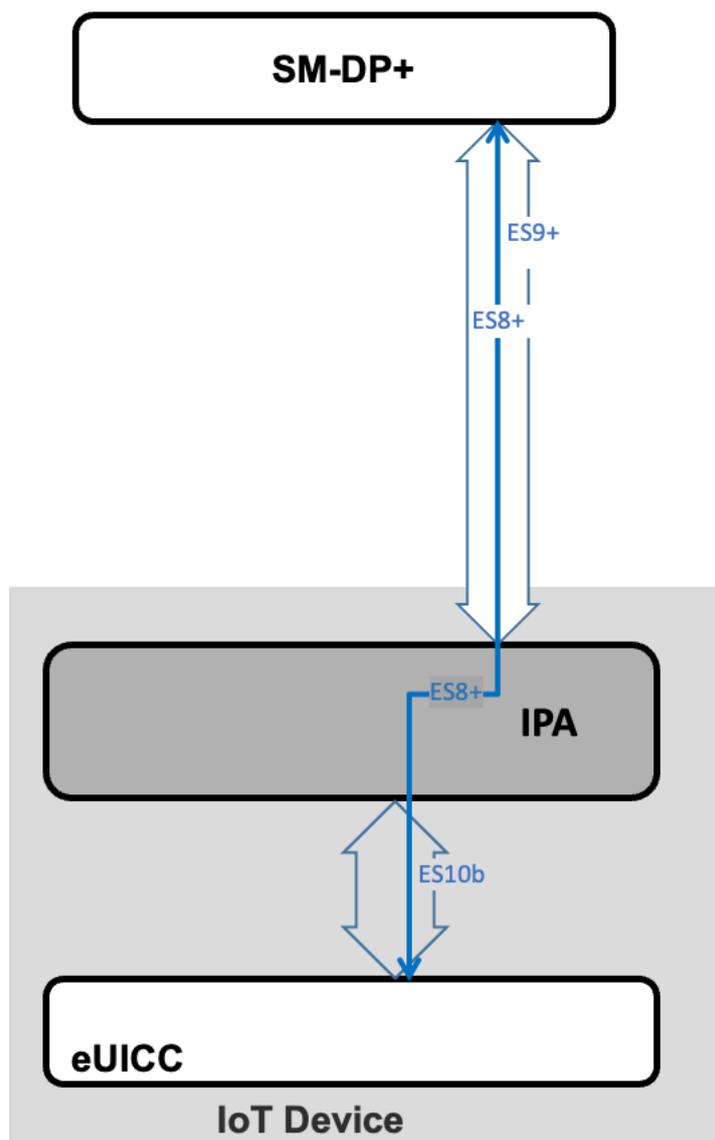


Figure 14: Direct Profile download unassisted by eIM using Default SM-DP+

## Annex D Document Management

### D.1 Document History

Version	Date	Additions
V1.0	19/04/2022	CR001R02 - Overview proposal
		CR002R01 - Intended audience proposal
		CR003R03 - Scope definition
		CR005R01 - Definition of network constrained device
		CR006R01 - Definition of User Interface constrained device
		CR008R01 - Draft Roles section
		CR009R03 - Draft Profile and Device principles
		CR011R05 - Basic Principles from IoT Working document

	<p>CR004R03 – Basic Principles          CR0016R02 - Additional Basic Principles from IoT Working document          CR0017R00 - Abbreviations and References addition</p>
	<p>CR0027R02 - eSIM for IoT Architecture - episode 1          CR0028R02 - eSIM IoT baseline architecture          CR0034R01 - Baseline Architecture CR</p>
	<p>CR0029R04 - eSIM for IoT Architecture - episode 2</p>
	<p>CR0035R01 - IPA functions descriptions          CR0036R01 - IoT Device definition          CR0037R00 - Major Threats</p>
	<p>CR0024R04 - eSIM IoT Security Risks          CR0040R02 - Functional requirements for eSIM IoT Remote Manager</p>
	<p>CR0026R06 - eSIM IoT Architecture          CR0038R01 - Missing definitions and abbreviations          CR0039R01 - Missing interfaces          CR0042R03 - eIM provisioning requirements          CR0043R03 - eIM-eUICC Interface Introduction</p>
	<p>CR0041R05 - Security Requirements          CR0045R02 - Introduction of ESipa interface          CR0046R00 - Resolution of editors note in EUICCS1</p>
	<p>CR0031R05 - eSIM for IoT Architecture - episode 4</p>
	<p>CR0051R02 - Add option for SM-DS to/from Device via eIM          CR0052R01 - Update of Arch diagram with SM-DP+ to Device via eIM          CR0053R01 - Update of Arch diagram with SM-DS to Device via eIM</p>
	<p>CR49R02 - Profile Download and Installation triggered by EIM          CR0055R02 - ES10b description update          CR0056R02 - Make the IPA simple</p>
	<p>CR0058R05 - Profile Enabling Triggered by eIM</p>
	<p>CR0023R03 - Architecture Procedure          CR0059R05 – Profile Delete Triggered by eIM          CR0060R04 - Profile Disabling Triggered by eIM</p>
	<p>CR0054R07 - SIM profile switch Roll-Back mechanism</p>
	<p>CR0064R02 - IPA requirements on Roll-Back          CR0065R00 - Editorial Change ES_PSM and PSMO</p>
	<p>CR0066R05 - Editorial Changes to Rollback Mechanism</p>
	<p>CR0075R01 - Changes to requirements IPAF1 / EUICCF5 / Roll-Back Definition          CR0067R01 - Changes to Enable Profile Procedure</p>
	<p>CR0071R00 - Editorial changes to draft 18          CR0073R00 - Editorial changes to draft 18 - Mobile Service Provider</p>
	<p>CR0070R04 – Notifications          CR0079R02 – Profile Download Procedure using default SM-DP+</p>

	CR0081R01 – Editorial Mobile Service Provider definition
	CR0076R04 – eIM assisted (indirect) Profile Download
	CR0069R05 - Enabling_ Disabling_ Delete diagrams CR0077R03 - Add indirect Profile Download with SM-DS procedure CR0082R00 - Editorial adding definitions for Operator, Subscriber and Subscriptions CR0083R00 - CR to remove redundant editor’s notes CR0084R01 - Notifications via eIM
	CR0086R00 - CR to remove editor’s notes agreed by delegates
	CR0072R02 - Adding optional encryption of PSMO messages CR0087R02 - Editorial clarification for NCD and UICD CR0088R01 - Editorial – Consistent Use of eIM in Section 4.4 (Interfaces)
	CR0078R04 - Add diagram and ES11’ based procedure to 6.1.2 CR0089R02 - SM-DS optionality for IoT Devices CR0090R01 - Detailing the eUICC architecture on the architecture diagram CR0091R01 - Detailing the eUICC architecture on the architecture diagram
	CR0093R04 - eIM Configuration Requirements CR0096R01 - Profile Download options CR0098R02 - eIM Configuration Procedures CR0105R02 - Deployment scenarios for profile download
	CR0094R02 - Update References CR0095R02 - Clarification of the term PSMO message CR0097R02 - Add asymmetric PSMO signing option CR0108R02 - Comprehensive device and profile management CR0113R01 - Support for SM-DS and default SM-DP+ triggered profile download and activation CR0116R01 – Resolve editor’s note in 6.1.2 and 6.1.3
	CR0018R00 - PR12 edit CR0092R04 - Introduction of IPA in the eUICC (“IPAE”) CR0100R00 - Removing editor's notes in 4.4.5 and 4.4.9 CR0101R00 - Change Editor's note in EUICCF5 CR0102R00 - Removing editor's notes in EIMF8 and EIMF10 CR0103R00 - Removing editor's note in IPAF4 CR0109R00 - Removal of Editor’s Notes related to automatic enabling CR0111R00 - Removal of Editor’s Notes within requirements CR0112R00 - Add eUICC abbreviations CR0114R00 – Remove MEP editor’s note in 6.2.1 CR0115R00 – Diagram for profile download via Def. DP+
	CR0014R03 – Definitions CR0104R01 – editor’s notes in 6.1.1- Telenor CR0119R01 – Resolution of comments

		CR0110R01 – CR Removal of Editor’s Notes
		CR121R01 - Update Reference of SGP.21 (2.2 to 2.4)
		CR0122R01 – Final Editorial Corrections
		CR0123R01 – Scope of SGP.31 V1.0 and notes on principles
		CR0124R00 – Ultimate Editorials Telenor
		CR0125R01 – clarifying start conditions of Profile Download procedure with AC
		CR0126R01 – Additional Editorial Corrections

## D.2 Other Information

Type	Description
Document Owner	eSIM
Editor / Company	Gloria Trujillo, 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](mailto:prd@gsma.com)

Your comments or suggestions & questions are always welcome.