eSIM IoT Architecture and Requirements
Version 1.2
26 April 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA 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 GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

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].
Connectivity Parameters	A set of data required by the eUICC to open a communication channel (for example HTTPS) on a dedicated network.
eIM Configuration Data	The data to be used by the eUICC to authenticate the eIM commands.
eIM Configuration Operation (eCO)	An operation related to eIM Configuration Data (e.g. add eIM Configuration Data, read/remove eIM Configuration Data in the eUICC) through the IPA.
Eligibility Check Information	As defined in SGP.21 [1].
Emergency Profile	An Operational Profile with an attribute indicating that this Profile is to be enabled for Emergency Calls.

Term	Description
	An Emergency Profile complies with regulatory requirements and only provides the capability to make Emergency Calls and receive calls from an Emergency centre (e.g. Public Safety Answering Point). It only applies for voice capable IoT Devices.
Emergency Mechanism	eUICC-based mechanism, triggered by the IPA, which enables and disables the Emergency Profile.
eUICC	As defined in SGP.21 [1]
eUICC Package	A signed package prepared by the eIM that contains either PSMO(s) or eCO(s). The package is verified and executed by the eUICC.
Event	As defined in SGP.21 [1].
Event Record	As defined in SGP.21 [1].
Event Registration	As defined in SGP.21 [1].
Event Retrieval	A process for the IPA or eIM to retrieve Event Records for an eUICC from an SM-DS.
Fallback Attribute	This is an attribute of a Profile which, when set, identifies the Profile to be enabled by the Fallback Mechanism.
Fallback Mechanism	eUICC-based mechanism, triggered by the IPA, which enables the Profile with Fallback Attribute set when the Enabled Profile loses network connectivity.
Fallback Profile	An Operational Profile having the Fallback Attribute set.
IoT	As defined in TS.34[3].
IoT Device	As defined in TS.34 [3].
IPA Capabilities	List of functionalities supported by the IPA.
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.

Term	Description
Rollback 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
eCO	eIM Configuration Operation
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
IPAe	IoT Profile Assistant located in the eUICC
IPAd	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

Term	Description
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 V2.5	eSIM Architecture Specification
[2]	TCA eUICC Profile Package	eUICC Profile Package: Interoperable Format Technical Specification
[3]	TS.34	IoT Device Connection Efficiency Guidelines
[4]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner
[5]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words
[6]	ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[7]	SGP.24	eSIM Compliance Process
[8]	SGP.33-1	eSIM IoT eUICC Test Specification

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! Reference source not found.Error! Reference source not found.**, when, and only when, they appear in all capitals, as shown here.”

1.8 References to SGP.21

The present document contains several references to SGP.21 [1].

The following list maps the terms used by SGP.21 [1] to the terms used in the present document:

- LPA (Local Profile Assistant) refers to IPA.

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. They are used to create the adequate normative requirements in this document.

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 at least confidentiality, integrity and authenticity.
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.
BP09	The architecture should allow polling by the IoT Device to check whether there is a Profile-provisioning or management transaction waiting.
BP10	The architecture should avoid ongoing and frequent polling between the IoT Device and the RSP system.
BP11	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.

BP12	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.
BP13	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.
BP14	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.
BP15	Void
BP16	Void
BP17	Void
BP18	Void
BP19	Void
BP20	The specification should provide a formula for the calculation of Profile Package sizes.
BP21	It should be possible to provision eUICCs in IoT Devices using an IP transport (e.g.: CoAP over UDP).
BP22	It should be possible to provision eUICCs in IoT Devices using a non-IP transport (e.g.: CoAP over NIDD).
BP23	Void
BP24	The architecture should support a single-round trip key management protocol to establish the secure channel between the eUICC and the server.
BP25	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.
BP26	The architecture should support Profile State Management Operation and Profile download operations with minimal integration between different components and/or different entities.
BP27	The architecture should optimize the traffic (e.g. avoid excessive polling) between the network and the IoT Device to enable mass IoT deployment. "TS.34 – IoT Device Connection Efficiency Guidelines" of the GSMA [3] should be followed.
BP28	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.
BP29	The architecture should be able to cope with the IoT Device being unreachable for prolonged periods of time.
BP30	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.
BP31	It should be possible to remotely trigger the IoT Device, in a secure way, to start the download of a Profile.

BP32	It should be possible to perform remote operations described in BP31, BP15 and BP16 without requiring local interaction with a given IoT Device.
BP33	Void
BP34	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: The following basic principles have been highlighted as principles that require further study in the future: BP09, BP10, BP13, BP20, BP23, BP24, BP25, BP27, BP29.

2.2 IoT Device principles

Principle no.	Description
DEVP1	Impact of Profile constraints on IoT Device functionality is out of scope of this specification.
DEVP2	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
PROF1	This document uses the term Profile as defined by SGP.21 [1].
PROF2	Profile description is defined by Trusted Connectivity Alliance (formerly SIMalliance) eUICC Profile Package: Interoperable Format Technical Specification [2].
PROF3	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.
PROF4	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 (IPAe).

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).

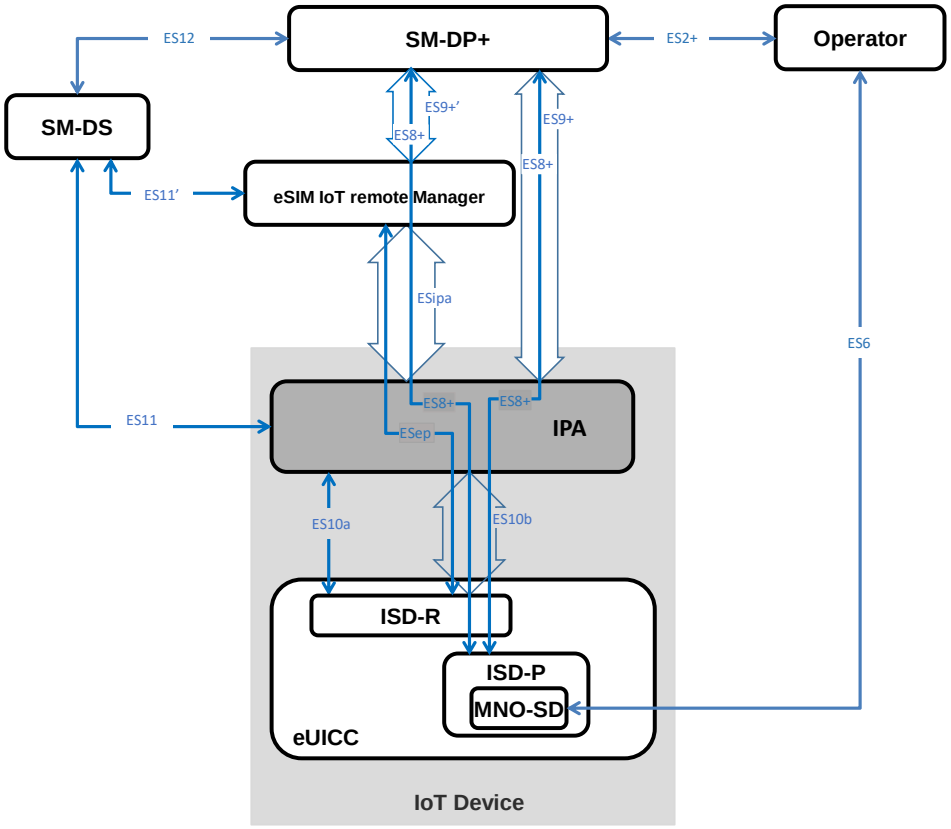

Figure 1 eSIM IoT Functional Architecture (IPA in the IoT Device)

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.

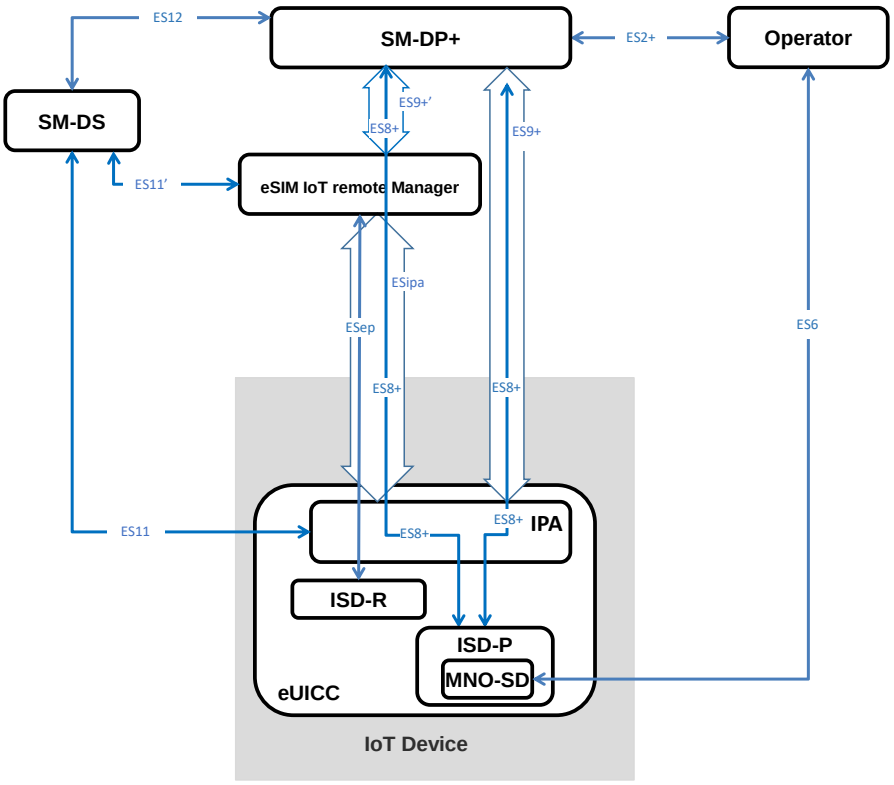

Figure 2 eSIM IoT Functional Architecture (IPA in the eUICC)

4.2 Architecture Elements

4.2.1 eSIM IoT Remote Manager

The eSIM IoT Remote Manager is responsible for remote Profile State Management Operations (PSMO) on a single IoT Device or a fleet of IoT Devices. . If supported by the eIM, the eIM can also be used to perform eIM Configuration Operations (eCO) on the eUICC when it is associated with the eUICC.

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, eCO and related results as described below.

Function name	Description
Discovery Service	When REQUIRED, this service is responsible for retrieving pending Event Records from the SM-DS.
Profile Download	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.
PSMO / eCO Conveying	This is responsible for conveying PSMOs, eCO and related results between eIM and eUICC.
Notification Handling	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].

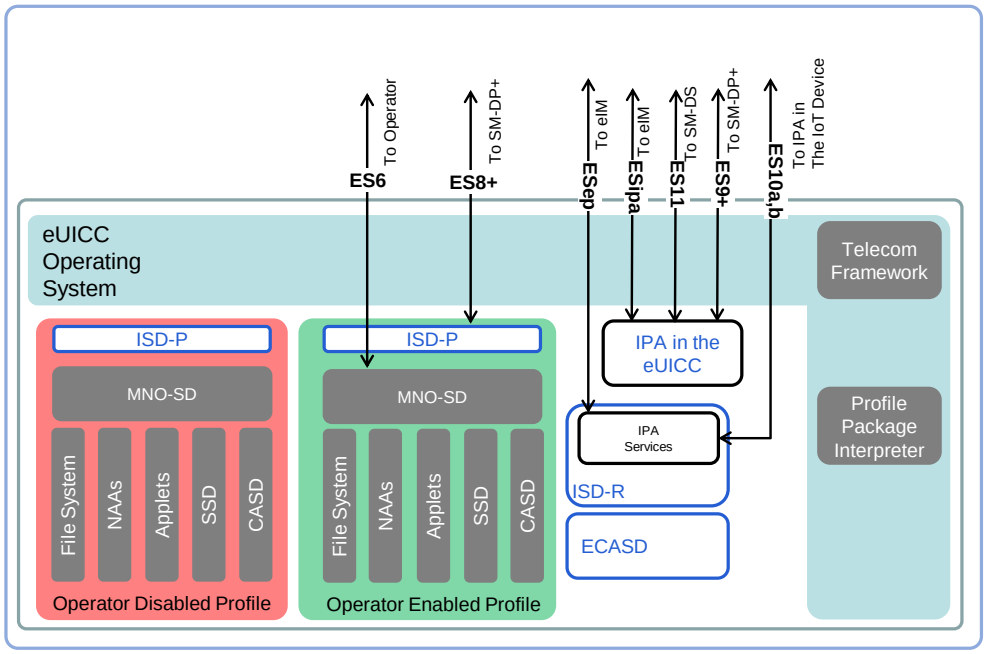

Figure 3 eUICC Architecture (IPA in eUICC)

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 is 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 and eCO 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 is 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 (ESep)

The ESep is a logical end-to-end interface between the eIM and the eUICC used for eUICC Package (PSMO and eCO).

Req no.	Description
ESEP1	The PSMO and eCO SHALL be integrity protected over ESep. NOTE: The solution shall not require associating at eUICC manufacturing the eUICC with a specific eIM.
ESEP2	The PSMO and eCO SHALL be protected against replay attacks.
ESEP3	The PSMO and eCO SHALL be protected in terms of integrity and authenticity.

Table 2 eIM – eUICC (ESep) 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 and eCO 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.
ESipa6	ESipa message SHALL be protected against replay attacks.
ESipa7	ESipa MAY support delivery of eCO between eIM and eUICC.

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.

Table 4 General Functional Requirements

5.1.2 eUICC Functional Requirements

All eUICC functional requirements specified in SGP.21 [1] SHALL apply to this specification, unless specified otherwise. This includes section 4.3 “eUICC Requirements” and 4.4 “ eUICC eligibility Check” of SGP.21 [1].

The following requirements from SGP.21 [1] are not applicable within the scope of this specification: EUICC36, EUICC46, EUICC47, EUICC53, EUICC57.

The below are additional 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 eCOs. 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 eCOs signed by the Associated eIM, except EUICCF6 and EUICCF16. The processing of this signed eIM Configuration Operations SHALL be handled as a signed PSMO.
EUICCF6	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.
EUICCF7	The eUICC SHALL support the Rollback Mechanism.
EUICCF8	If the eIM has requested use of the Rollback Mechanism (see EIMF8), and if the IPA informs the eUICC that Rollback is required (see IPAF1), the eUICC SHALL execute the Rollback Mechanism. NOTE: In this version only the requesting eIM is notified about the result.
EUICCF9	The eUICC SHALL provide a signed result of a requested PSMO, eCO or Profile installation to the IPA. NOTE: This signed result is included by the IPA within its responses to requests from the eIM.
EUICCF10	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].
EUICCF11	The eUICC SHALL be able to accept default SM-DP+ triggered Profile download and immediate enabling without signed PSMO from any potentially Associated eIM.
EUICCF12	The behavior in EUICCF11 SHALL be configurable in the eUICC.
EUICCF13	Changing the configuration in the eUICC (see EUICCF12 and EUICC15**)** 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 configure the behavior in eUICC manufacturing.

EUICCF14	The eUICC MAY be able to accept SM-DS triggered Profile download and immediate enabling without signed PSMO from any potentially Associated eIM. NOTE: technical implementation of this requirement is FFS.
EUICCF15	The behavior in EUICCF11 and EUICCF14 (if supported) SHALL be configurable in the eUICC. NOTE: technical implementation of this requirement for EUICCF14 is FFS.
EUICCF16	The eUICC MAY provide an interface to the IPA to read the eIM Configuration Data (e.g: eIM ID) stored in the eUICC.
EUICCF17	An eUICC SHALL indicate in the Eligibility Check Information if it is an eUICC as defined in this specification.
EUICCF18	The eUICC MAY support the Emergency Mechanism.
EUICCF19	If the Emergency Mechanism is supported, the eUICC SHALL provide an interface to the IPA to Enable and Disable the Emergency Profile.
EUICCF20	If the Emergency Mechanism is supported, the eUICC MAY contain the Emergency Profile.
EUICCF21	If the Emergency Mechanism is supported, the eUICC SHALL enable the previously enabled Profile when the Emergency Profile is disabled by the IPA.
EUICCF22	If Fallback Mechanism is supported, the eUICC SHALL provide an interface to the IPA to Enable and Disable the Fallback Profile.
EUICCF23	If Fallback Mechanism is supported, the eUICC SHALL contain at most one Profile with the Fallback Attribute set.
EUICCF24	When the IPA sends the request to disable the Fallback Profile, the eUICC SHALL enable the previously enabled Profile.
EUICCF25	The eUICC MAY provide an interface to set and unset the Fallback Attribute for a given Profile.
EUICCF26	If Fallback Mechanism is supported, the eUICC SHALL reject to set the Fallback Attribute for a Profile if Fallback for this Profile is not authorised by the Profile Owner.
EUICCF27	An Integrated eUICC SHALL be able to execute the test cases defined in SGP.33-1 [8].
EUICCF28	The eUICC SHALL support a set of standard functions and services including, but not limited to USIM Toolkit functions and GlobalPlatform features. The list of supported functions and services SHALL be explicitly referenced within the technical specification.
EUICCF29	The eUICC SHALL support at least the following USIM Toolkit commands: • PROVIDE LOCAL INFORMATION including the following fields: Location Information, IMEI, Network Measurement Results, Date & Time & Time zone, Access Technology • TERMINAL PROFILE • ENVELOPE (SMS-PP DOWNLOAD) • SEND SHORT MESSAGE REFRESH including the “UICC Reset” and “eUICC Profile Change” modes
EUICCF30	The eUICC SHALL support an IPAd (i.e.; ES10 interface).

Table 5 eUICC Functional Requirements

5.1.3 eIM Functional Requirements

Req no.	Description
EIMF1	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: • Profile Download from default SM-DP+ • Profile Download with Activation Code • Profile Download via SM-DS NOTE: Impact of this optionality on Profile Provisioning procedures is FFS.
EIMF2	The eIM SHALL be able to trigger a PSMO to be executed by the eUICC.
EIMF3	An eIM MAY be able to trigger an eCO to be executed by the eUICC.
EIMF4	The eIM MAY support the transfer of the Bound Profile Package and related communication between the SM-DP+ and IPA/eUICC.
EIMF5	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.
EIMF6	The eIM MAY support the transfer of the Event Records and related communication between the SM-DS and IPA/eUICC.
EIMF7	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.
EIMF8	The eIM SHALL be able to request of the eUICC the activation of the Rollback Mechanism.
EIMF9	The eIM SHALL support the transfer of Notifications and related communication between the SM-DP+ and IPA/eUICC.
EIMF10	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.
EIMF11	If Fallback Mechanism is supported by the eUICC, an Associated eIM SHOULD be able to request the eUICC to set and unset the Fallback Attribute.

Table 6 eIM Functional Requirements

5.1.4 IPA Functional Requirements

Req no.	Description
IPAF1	If the eIM has requested activation of the Rollback 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 Rollback is required if no communication with the eIM is possible.
IPAF2	If the eIM request contains a signed PSMO, or a signed eCO, 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.
IPAF3	The IPA SHALL retrieve pending Notifications from the eUICC and SHALL send the Notifications to the Notification Receivers.

IPAF4	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.
IPAF5	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+.
IPAF6	The IPA SHALL send Notifications on a best-effort basis when connectivity is available.
IPAF7	The IPA SHALL retain signed eUICC results until they can be sent in a response to the eIM.
IPAF8	IPA MAY support direct Profile download via ES9+.
IPAF9	IPA MAY support indirect Profile download via ESipa.
IPAF10	The IPA MAY support eCOs.
IPAF11	As per EIMF1, the IPA SHALL be able to accept a Profile Download trigger from the eIM.
IPAF12	The IPA SHALL support at least one of the following three mechanisms for Profile Download: • Profile Download from default SM-DP+ • Profile Download with Activation Code • Profile Download via SM-DS
IPAF13	IPA MAY support Profile download and immediate enabling through default SM-DP+ without eIM involvement.
IPAF14	There SHALL be at most one active IPA, either the IPAd or the IPAe, per eUICC at a given time (either IPAe or IPAd is active).
IPAF15	If more than one IPA is present, the IoT Device MAY have a means to set which IPA is active. Note: it is IoT Device implementation-specific to configure which IPA is active by default.
IPAF16	There SHALL be a mechanism for the IPA to provide its IPA Capabilities (e.g: verify Profile Metadata) to the eIM.
IPAF17	IPA MAY support Profile download and immediate enabling through SM-DS without eIM involvement. NOTE: technical implementation of this requirement is FFS.
IPAF18	The IPA MAY request to the eUICC to Enable or Disable the Emergency Profile.
IPAF19	If Fallback Mechanism is supported, the IPA SHOULD indicate to the eUICC the loss of connectivity in order to execute the Fallback Mechanism. NOTE: It's IoT Device implementation specific to detect the connectivity loss.
IPAF20	If the IPA indicated to the eUICC the enabling of Fallback Profile, the IPA SHALL (a) determine if communications with that eIM can be established using Fallback Profile; and (b) inform the eUICC to enable the previously enabled Profile if no communication with the eIM is possible. NOTE: It's IoT Device implementation specific to retry.

Table 7 IPA Functional Requirements

5.1.5 SM-DP+ Functional Requirements

All SM-DP+ requirements specified in SGP.21 [1] section 4.10.2 apply for this specification, unless otherwise specified. The below are additional requirements:

Req no.	Description
SMDPF1	An SM-DP+ SHALL be able to identify an eUICC, as defined in this specification, through eUICC Eligibility Check Information.

Table 8 SM-DP+ Functional Requirements

5.1.6 Profile Functional Requirements

All Profile requirements specified in SGP.21 [1] section 4.7 SHALL apply to this specification, unless otherwise specified.

The following requirements from SGP.21 [1] are not applicable within the scope of this specification: PPRO2, PPRO3, PPRO4, PPRO5.

The below are additional requirements:

Req no.	Description
PRF1	It SHALL be possible for the Profile Owner to indicate, as part of Profile Metadata, whether a Profile is allowed as a Fallback Profile.
PRF2	The Profile MAY contain Connectivity Parameters.
PRF3	If a Profile contains Connectivity Parameters, these parameters MAY be managed via ES6.

Table 9 Profile Functional Requirements

5.2 Security Requirements

5.2.1 eUICC Security Requirements

All eUICC security requirements specified in SGP.21 [1] SHALL apply to this specification, unless specified otherwise. This includes section 4.14.1 “eUICC Certification” of SGP.21 [1].

The following requirement from SGP.21 [1] isn’t applicable within the scope of this specification : CERTEU2.

The below are additional 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 eCO 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 immediateenabling through default SM-DP+ is authorised.
EUICCS6	The eUICC MAY have means to verify that Profile download and immediateenabling through SM-DS is authorised. NOTE: technical implementation of this requirement is FFS.

Table 10 eUICC Security Requirements

5.2.2 eIM Security Requirements

Req no.	Description
EIMS1	Any PSMO sent to the eUICC SHALL be signed by the eIM.
EIMS2	An eIM that supports eIM configuration, SHALL sign eCO.
EIMS3	The eIM SHALL support an asymmetric cryptographic scheme for signing PSMO and eCO.
EIMS4	An eIM SHALL be implemented and operated with security measures to protect against threats listed in Annex A.2, A.3 and A.6.
EIMS5	With regard to EIMS4, evidence MAY be provided by a third party security evaluation (e.g., SAS accreditation, IEC/ISO 27001:2022 [6], or similar).

Table 11 eIM Security Requirements

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 authenticity and anti-replay. It SHOULD also be protected in terms of confidentiality when necessary. NOTE: The security and the mechanisms other than the signed eIM request is left to the implementation.

Table 12 General Security Requirements

5.2.4 EUM Functional Requirements

All EUM requirements specified in SGP.21 [1] section 3.1 SHALL apply to this specification, unless specified otherwise.

The following requirement from SGP.21 [1] isn't applicable within the scope of this specification : EUM5.

The below are additional requirements:

Req no.	Description
EUMF1	The EUM SHALL declare eUICC product compliance according to GSMA SGP.24 [7].

EUMF2	The EUM SHALL be responsible for the implementation of any IPA elements that reside in the eUICC and the compliance of these IPA elements according to IPA requirements in 5.1.4

Table 13 EUM Security Requirements

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 immediate 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
endrnote

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

@enduml
```

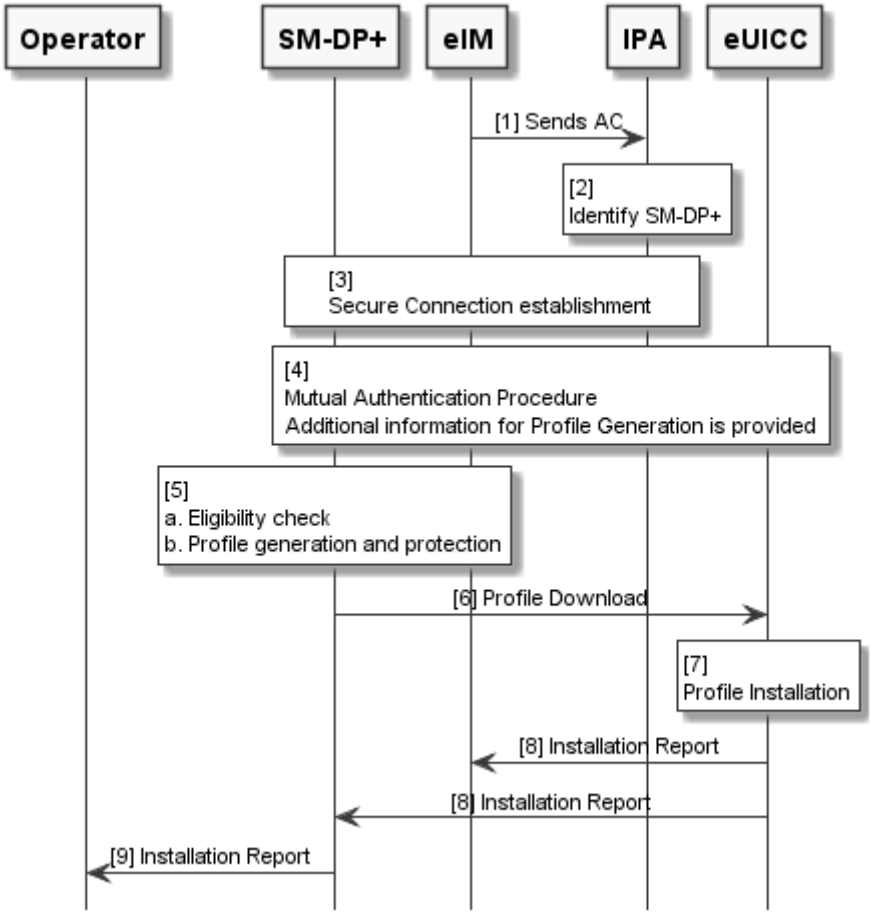

Figure 4 Profile Download Triggered by eIM with Activation Code

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 immediate 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
```

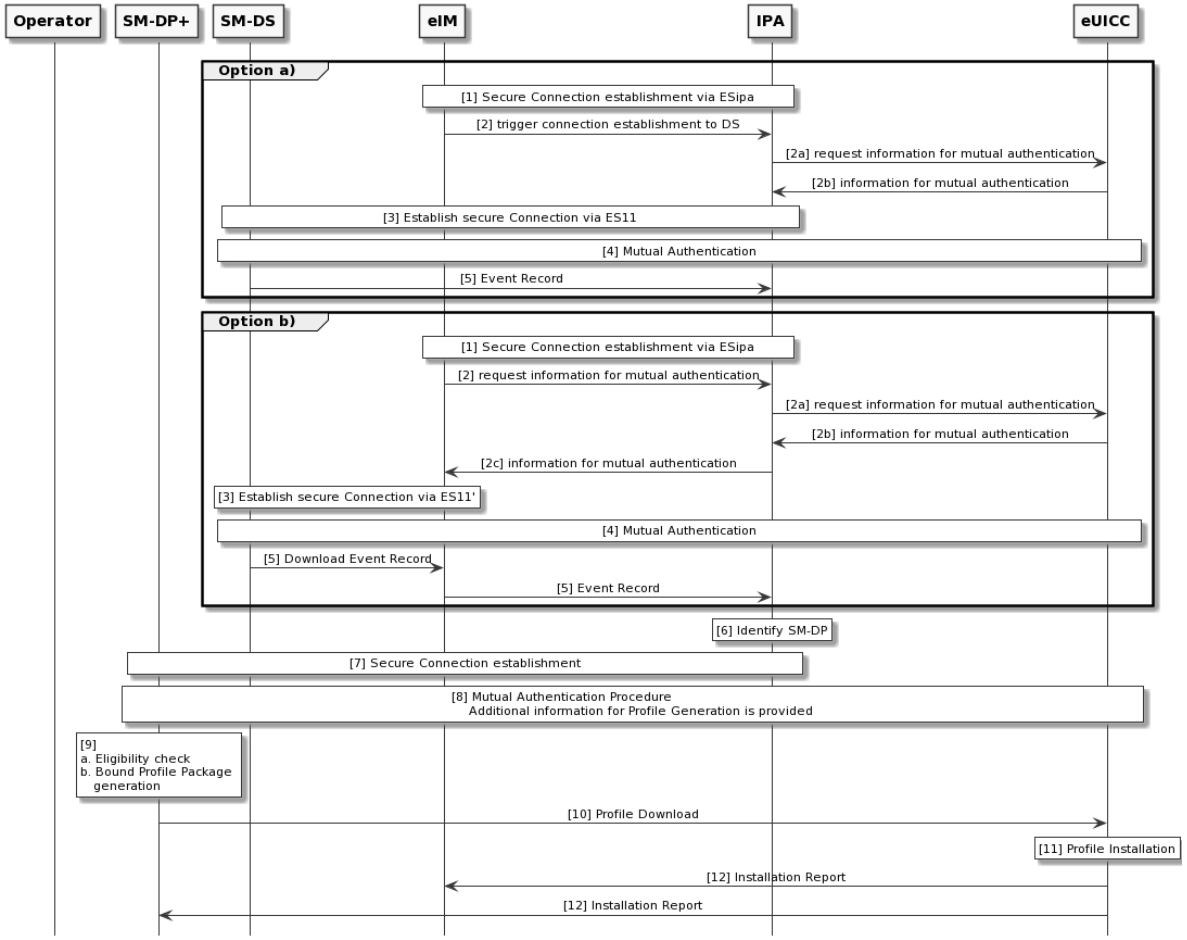

Figure 5 eIM Initiated Direct Profile Download with SM-DS

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 immediate 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 "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
```

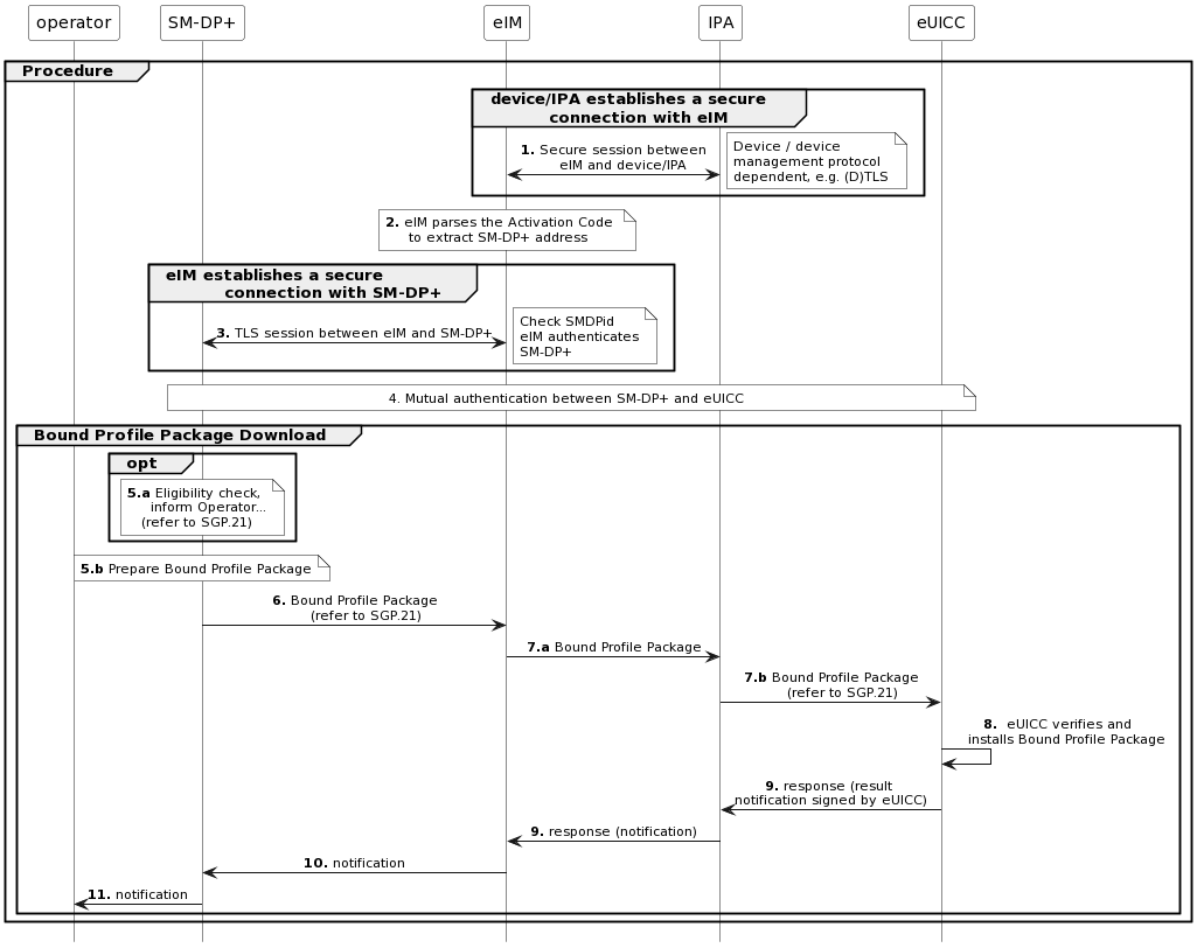

Figure 6 eIM Assisted Profile Download Triggered by eIM with Activation Code

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 (if any) and the SM-DP+ are notified.
8. The Operator is notified by the SM-DP+ about the Profile Installation
9. The IPA can request the eUICC to enable the Profile and continue with step 10. Otherwise, the procedure stops.
10. If the eUICC is configured to support immediate enabling using default SM-DP+, the eUICC enables the installed Profile. Otherwise, the procedure stops.
11. The SM-DP+ and the eIM (if any) are notified about the Profile enabling result.
12. The Operator is notified by the SM-DP+ about the Profile enabling result.

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

NOTE: steps 8 and 12 could be executed in parallel by the SM-DP+.

End Conditions:

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

```
@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

IPA -> E: [9] Enable using default SM-DP+

rnote over E #FFFFFF
[10] Profile Enabling
endrnote

E --> EIM: [11] Enabling Notification
E -> DP: [11] Enabling Notification

DP -> OPE: [12] Enabling Notification

@enduml
```

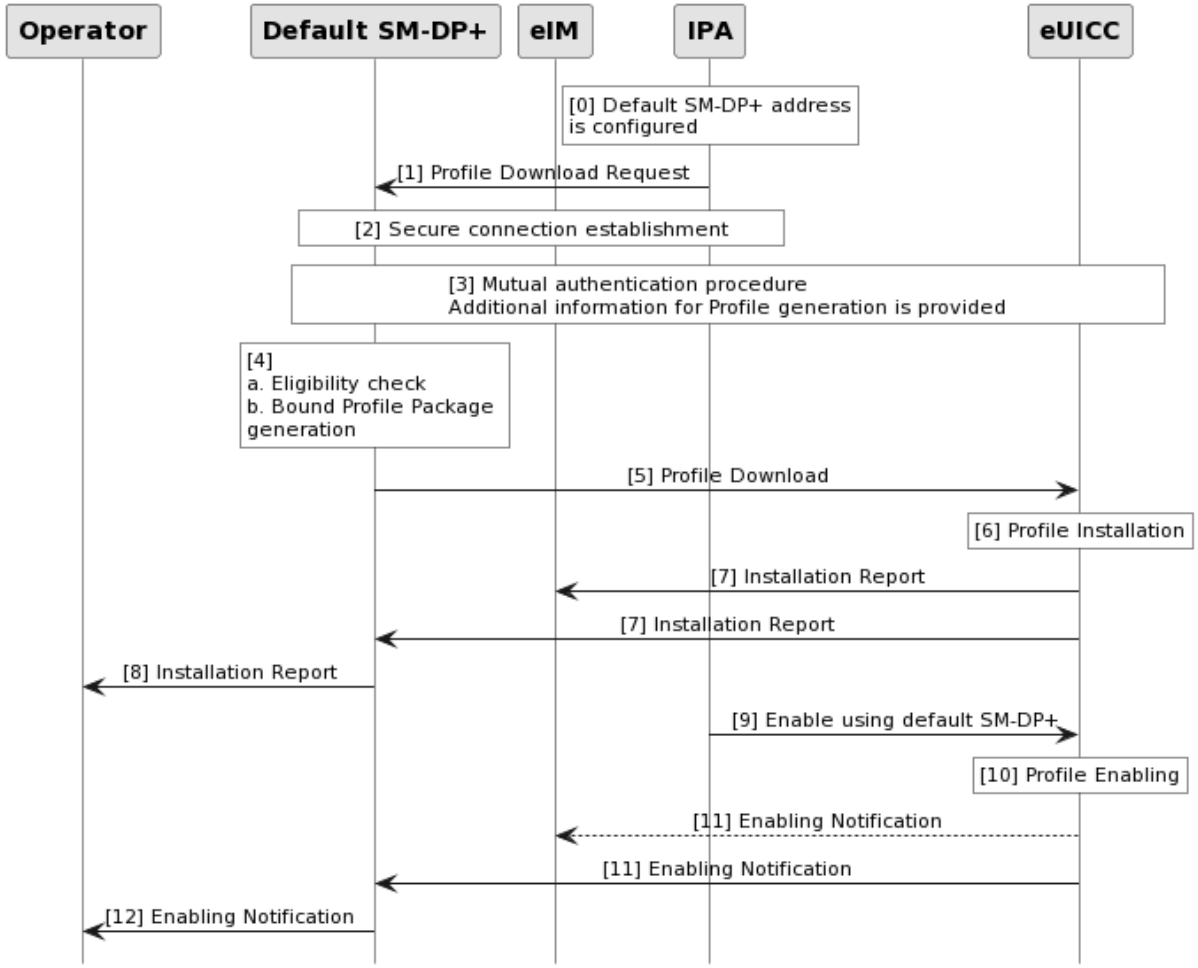

Figure 7 Profile Download with Default SM-DP+

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 immediate 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
```

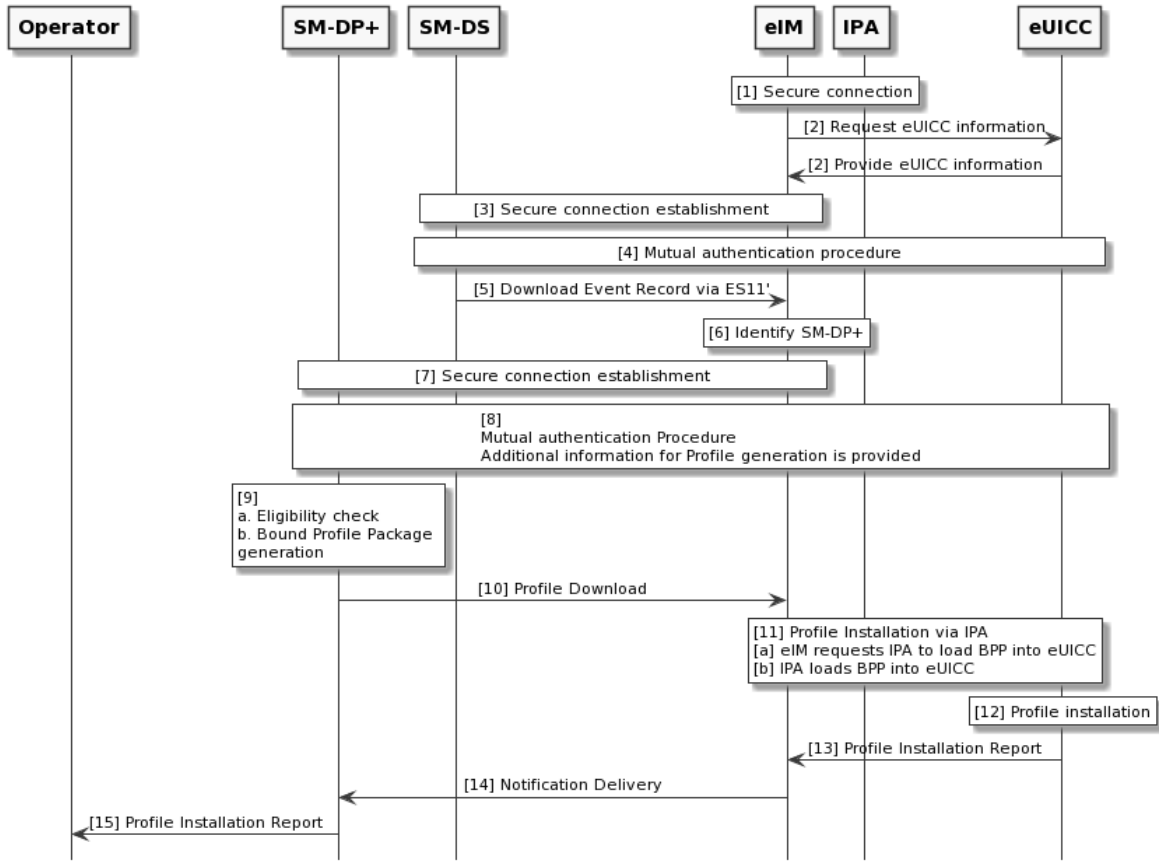

Figure 8 eIM Assisted Profile Download Triggered by eIM with SM-DS

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 Rollback Mechanism has been requested by the eIM, the IPA informs the eUICC to execute the Rollback 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 Rollback 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: Rollback Mechanism
rnote over E #FFFFFF
Disable target Profile,
Enable previously enabled Profile
endrnote
E -> IPA: Signed Profile Rollback information
IPA -> EIM: Signed Profile Rollback information
end


@enduml
```

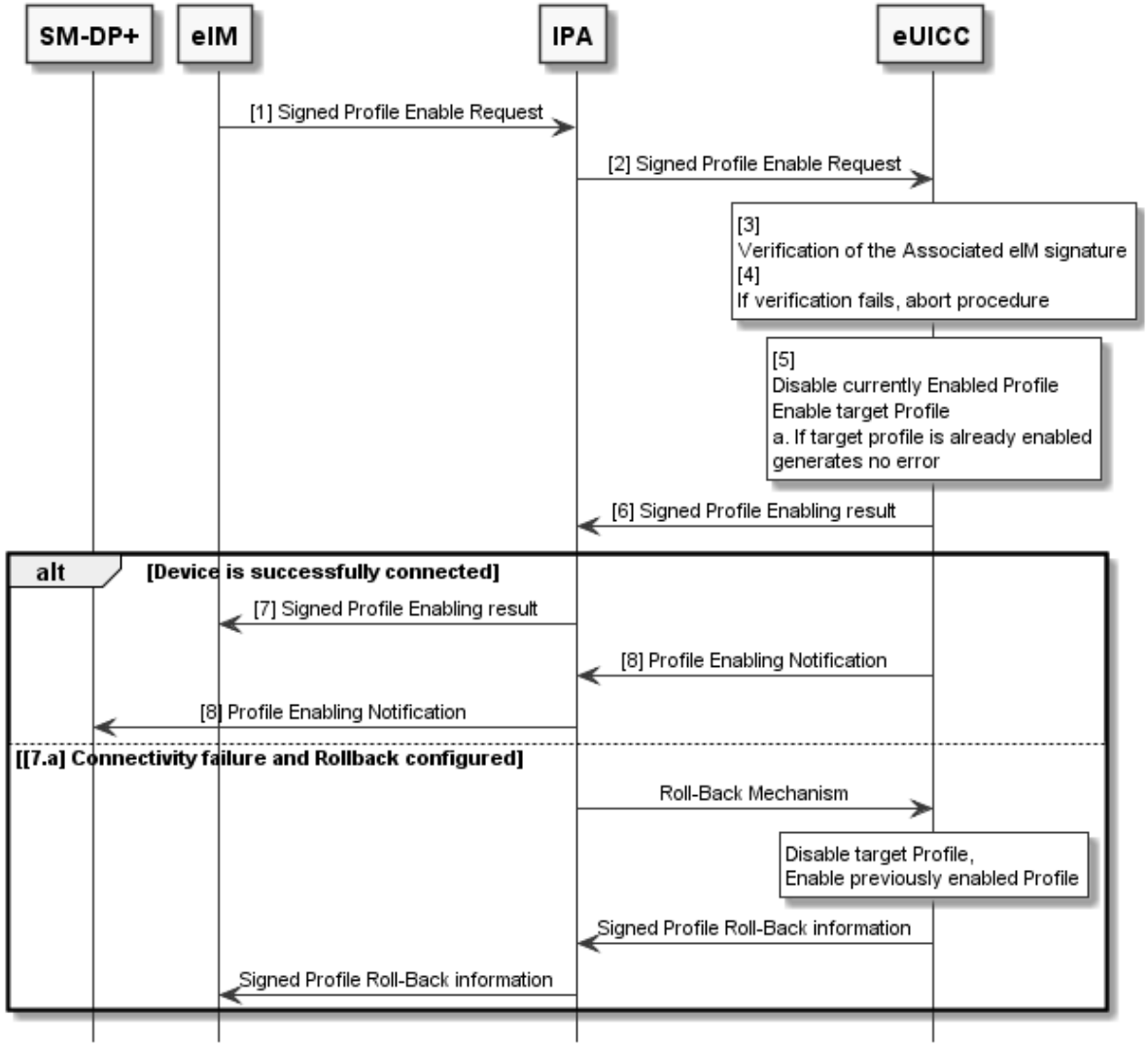

Figure 9 Profile Enabling via eIM

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 immediate 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
```

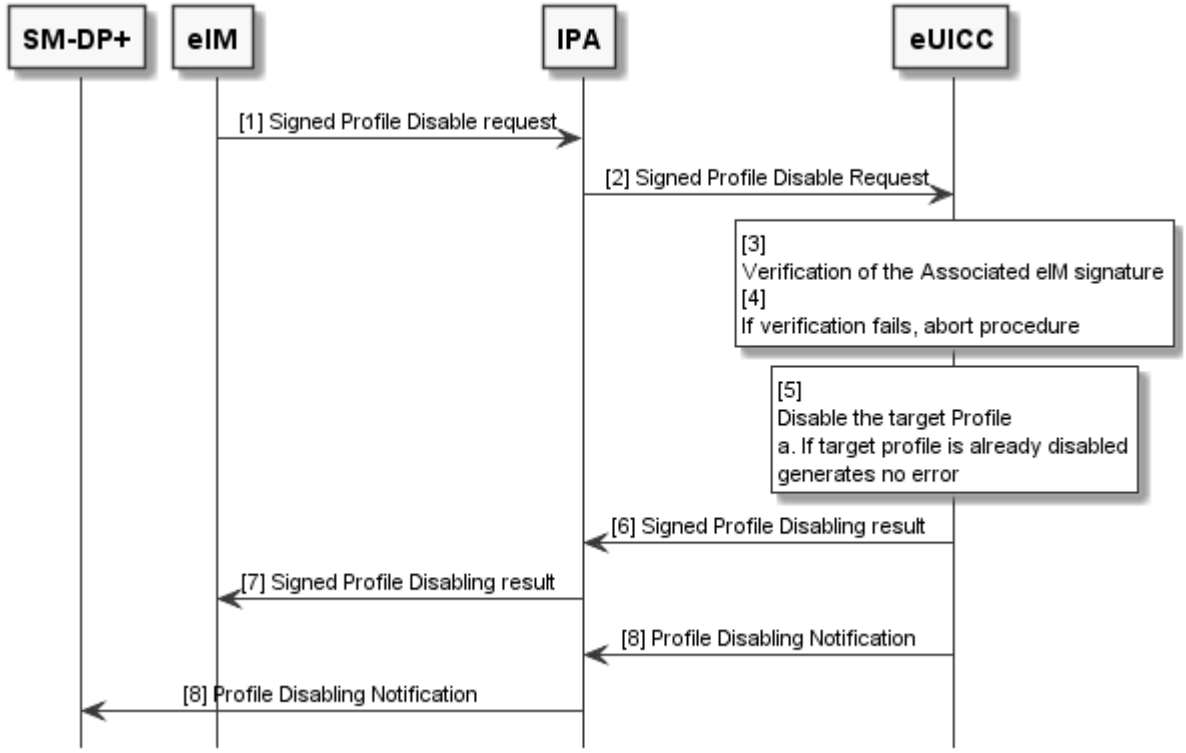

Figure 10 Profile Disabling via eIM

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
```

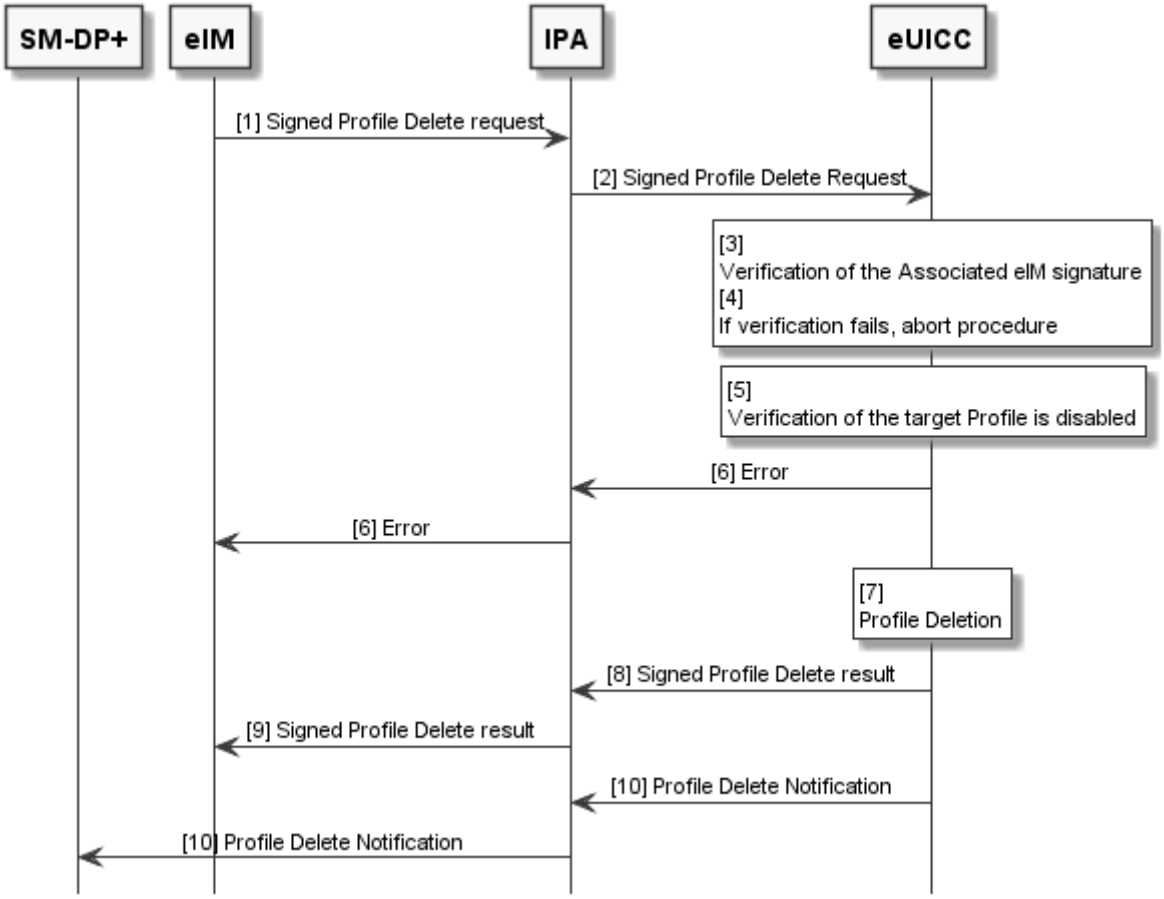

Figure 11 Profile Delete via eIM

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 eCO, 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 eCO, else
    b. the eUICC aborts the procedure.
3. The IPA retrieves the result of the eCO 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] eCO
rnote over E #FFFFFF
[2]
eIM is already associated to the eUICC ?
[a]: no eIM associated -> execute eCO
[b]: eIM associated -> abort procedure
endrnote

E -> IPA: [3] eCO result
@enduml
```

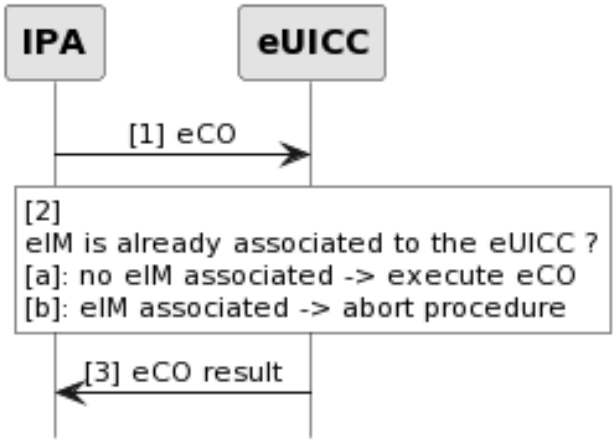

Figure 12 Add eIM Configuration Data via IPA

6.5.2 eIM Configuration via eIM

The following procedure describes adding eIM Configuration Data to the eUICC 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 eCO and sends it to the IPA.
2. The IPA sends the signed eCO to the eUICC.
3. The eUICC verifies that the eCO 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 eCO 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 eCO
IPA -> E: [2] Signed eCO
rnote over E #FFFFFF
[3]
Operation is signed by an Associated eIM ?
[a]: Signature verification succesful -> execute eCO
[b]: Signature verification fails -> abort procedure
Endrnote
E -> IPA: [4] Signed eCO result
IPA -> EIM: [5] Signed eCO result
@enduml
```

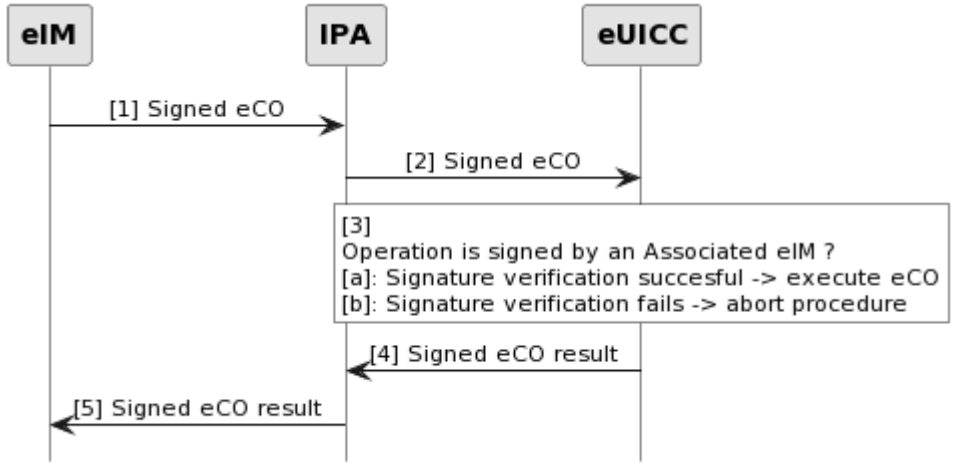

Figure 13 eIM Configuration via eIM

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
rnote over E #FFFFFF
[2]
eUICC removes all eIM Configuration Data stored in it
endrnote

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

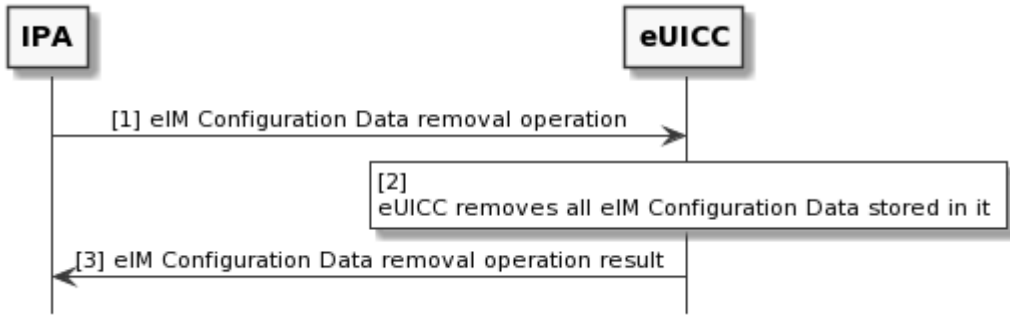

Figure 14 Complete Removal of eIM Configuration Data from the eUICC

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 14 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 eCO on a number of eUICCs.

Table 15 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 eCO on a number of eUICCs.
MeIM3	Malicious eIM is able to tamper with ES9+' communications.

Table 16 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 17 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 18 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 19 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 20 Profile Switching Risks

A.8 Profile Swap

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

Table 21 Profile Swapping Risks

A.9 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 22 Cryptographic Related Risks

A.10 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 23 Quality of Service Risks

A.11 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, EUM…).

Table 24 Non-human or Unpredictable Risks

A.12 New Profile during Subscriber Journey

Risk no.	Risk description
EXN1	Malicious pairing of new IoT Device using unattended IoT 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.
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 25 New Profile during Subscriber Journey Risks

A.13 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 26 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.

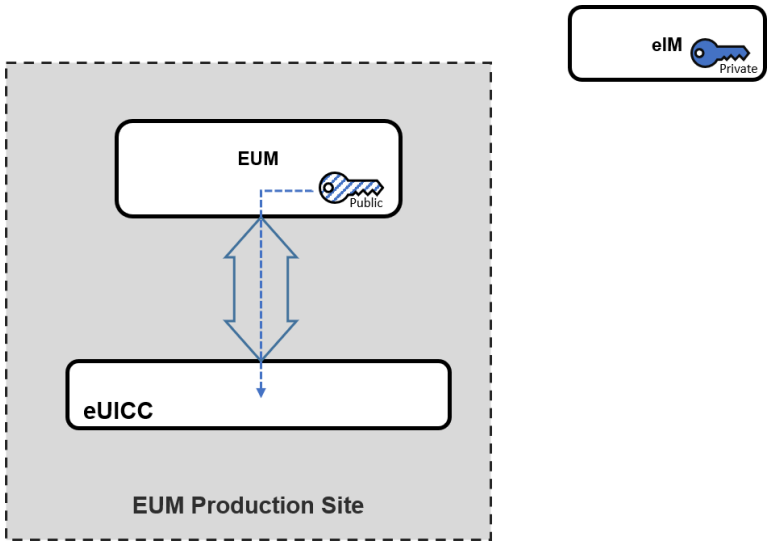

Figure 15 eIM Configuration performed by the EUM

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 eCO 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.).

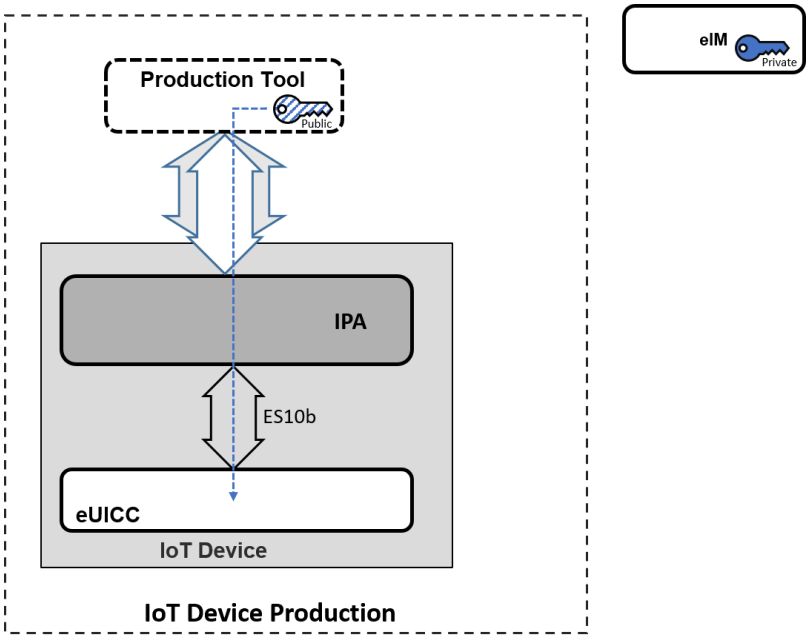

Figure 16 eIM Configuration performed in IoT Device production

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 eCO. The IPA transfers the eCOs 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 17, the eIM can, but does not have to be part of the backend system.

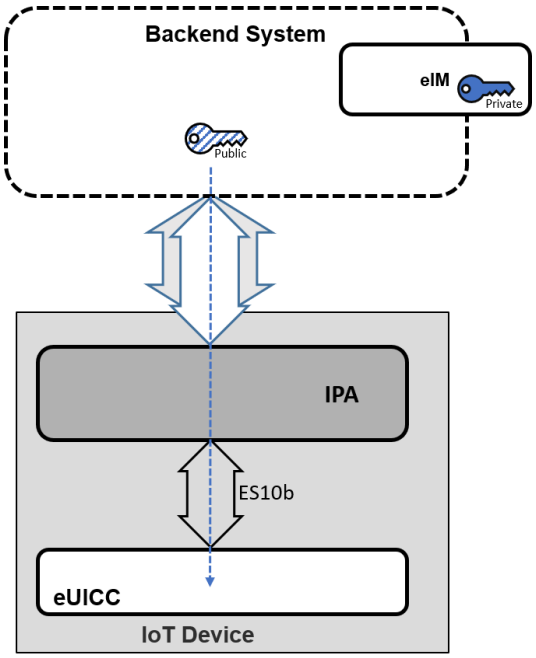

Figure 17 eIM Configuration performed in the field by a backend system

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 eCO including the public key information of eIM_B and signs the eCO with its private eIM_A key. The eIM_A sends the signed eCO to the IPA and the IPA forwards the eCO to the eUICC, which proves the signature before executing the eCO. After succeful execution eIM_B is associated to the eUICC.

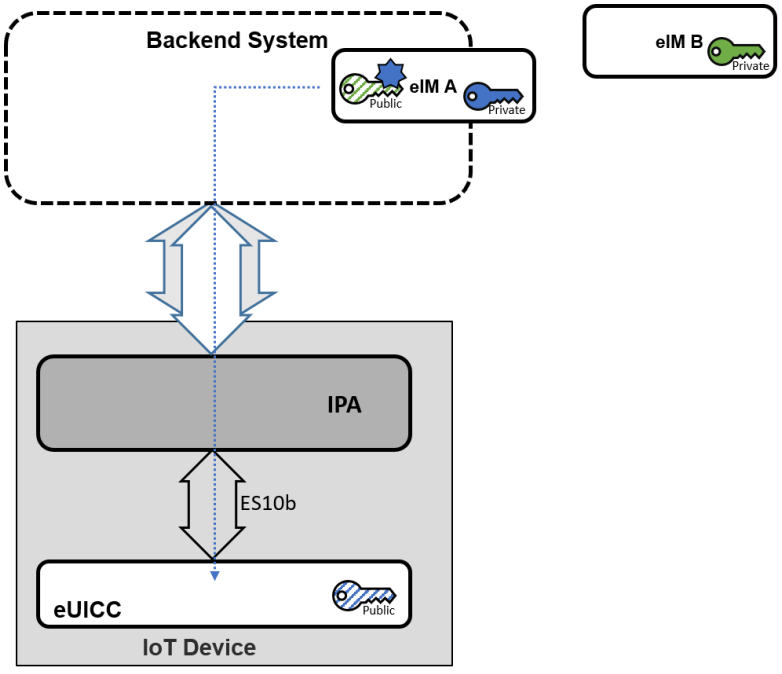

Figure 18 eIM Configuration performed by an eIM

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 Data.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 19, the eIM can, but does not have to be part of the backend system.

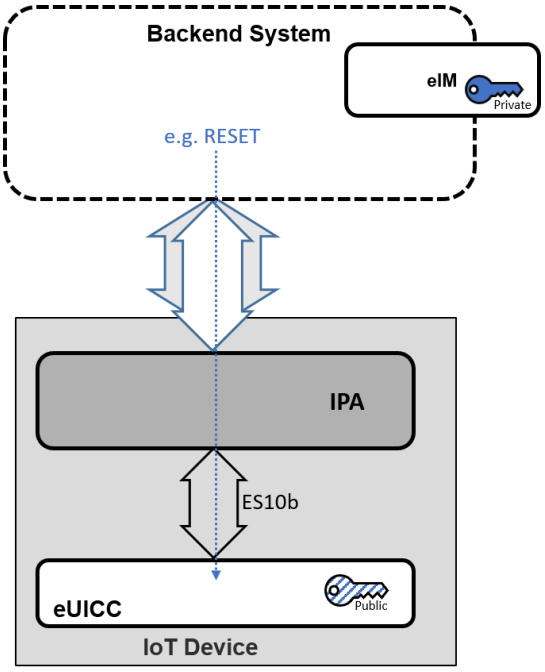

Figure 19 Removal of eIM Configuration

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 20), the Profile download is triggered using the Activation Code.

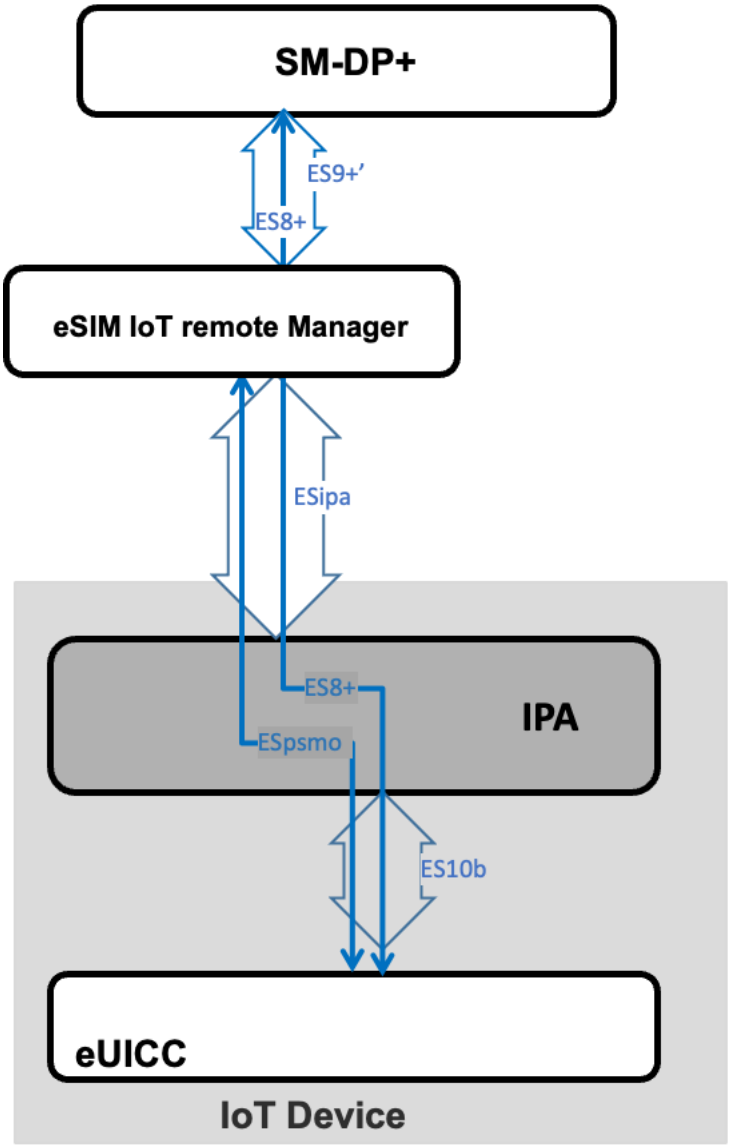

Figure 20 Indirect Profile download assisted by eIM using AC

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

In the example shown in Figure 21, the Profile download is triggered using SM-DS. The Profile download Event Record is retrieved by the eIM using ES11'.

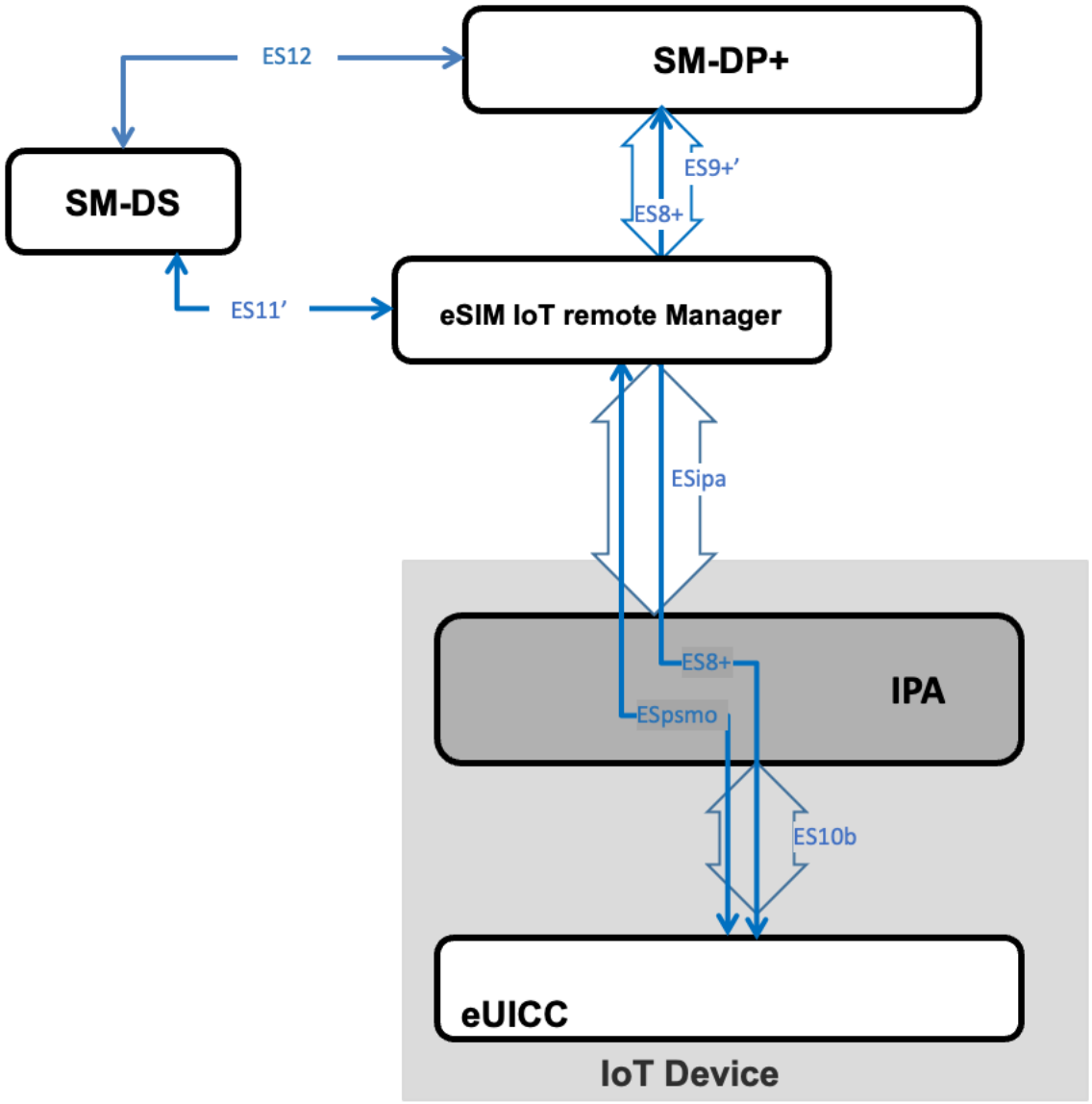

Figure 21 Indirect Profile download assisted by eIM using SM-DS

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 22), the eIM instructs the IPA using an Activation Code.

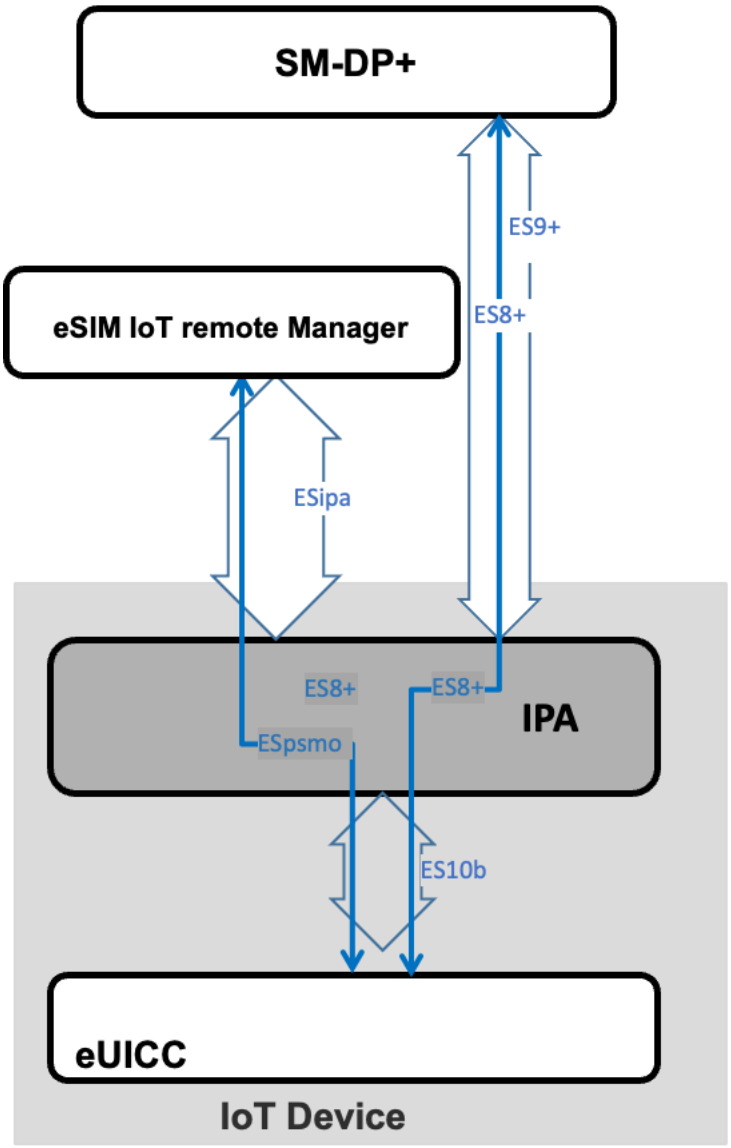

Figure 22 Direct Profile Download assisted by eIM using AC

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

In this example (see Figure 23), the Profile download Event Record is retrieved by the eIM using ES11'. This Event is sent to the IPA using ESipa.

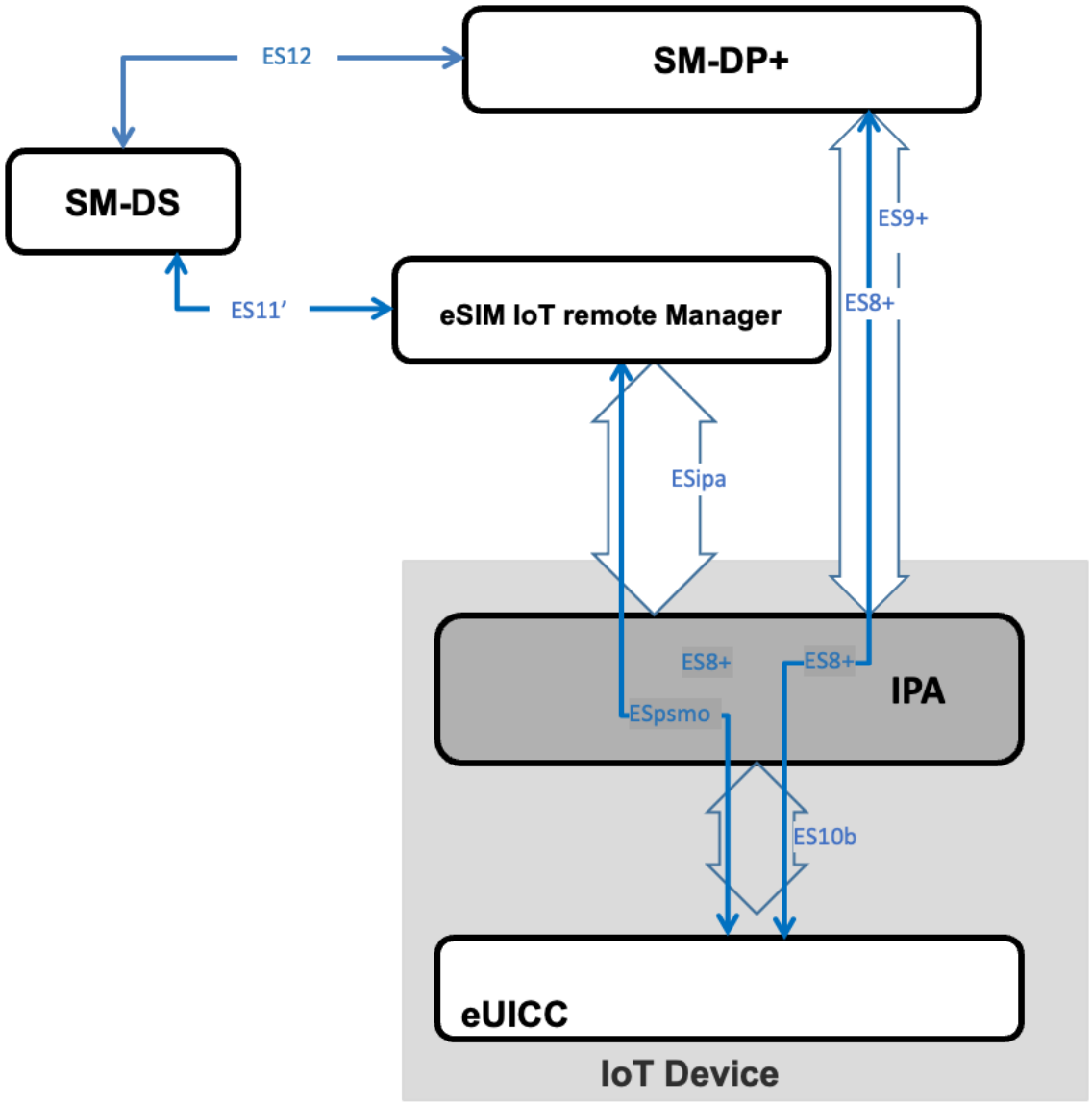

Figure 23 Direct Profile Download assisted by eIM using SM-DS

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

In this example (Figure 24), the IPA retrieves the Profile download Event Record from the SM-DS using ES11.

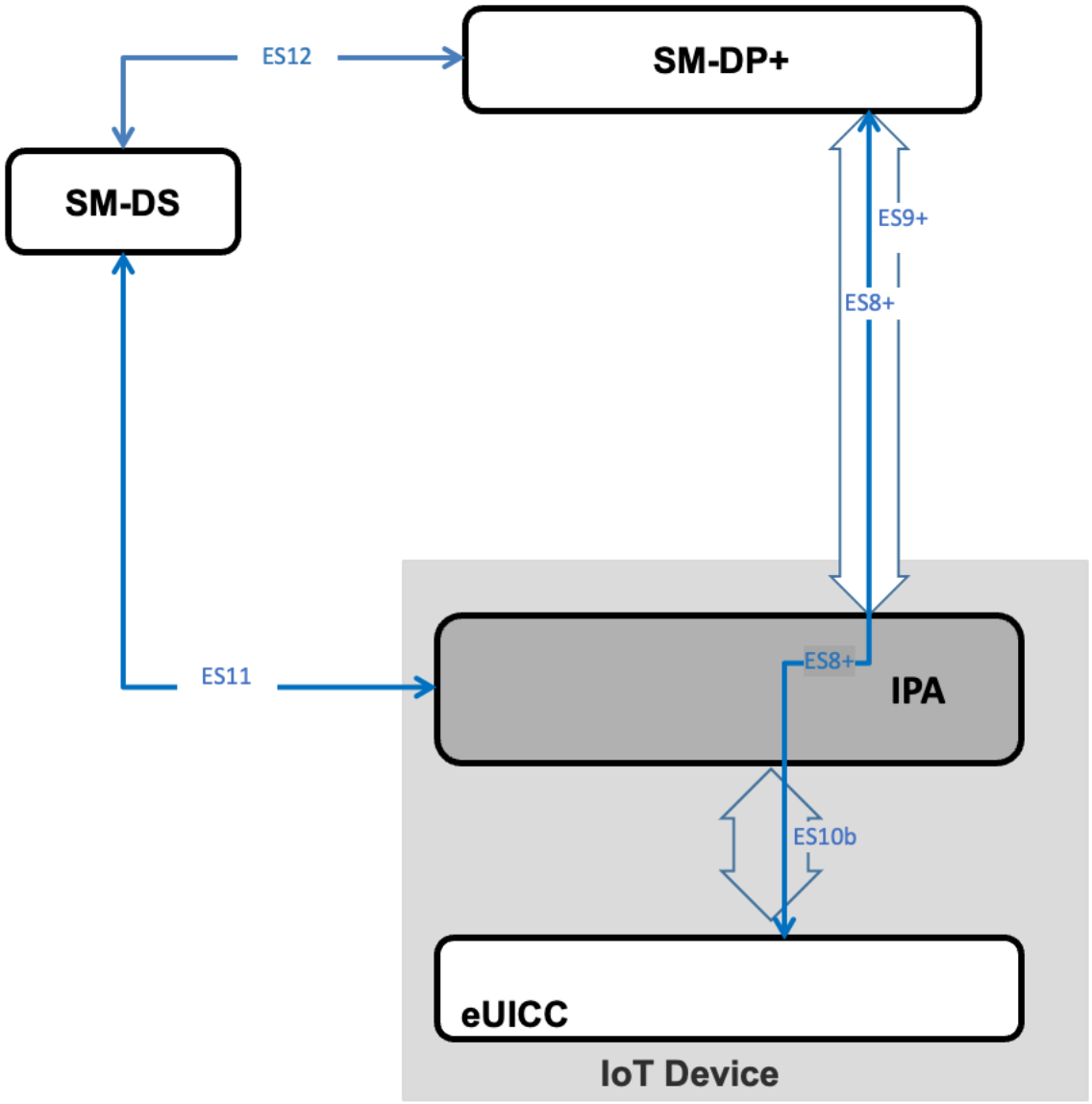

Figure 24 Direct Profile download unassisted by eIM using SM-DS

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+.

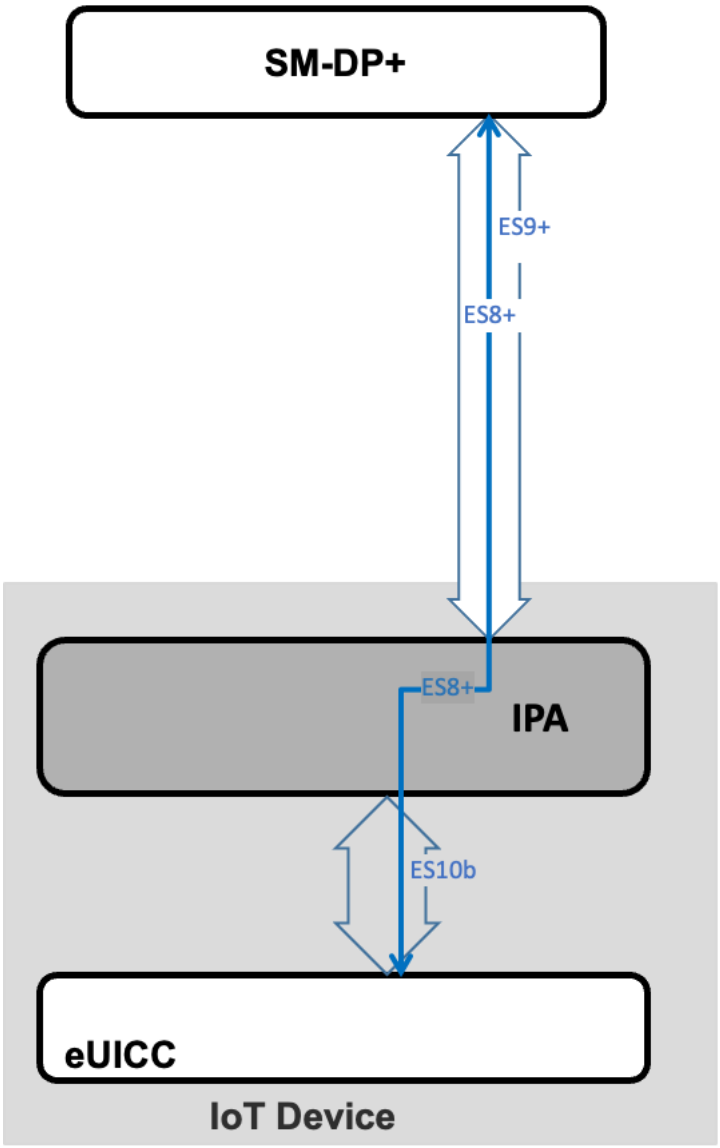

Figure 25 Direct Profile download unassisted by eIM using Default SM-DP+

Annex D Document Management

D.1 Document History

Version	Date	Additions
V1.0	15/04/2022	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

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

		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 deelgates
		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 - Comprensive 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 Donwload procedure with AC CR0126R01 – Additional Editorial Corrections
V1.1	26 May 2023	CR0127R00 – Definition of event registration CR0128R00 – Capitalisation of term 'associated'
		CR0129R03 - IPAe_IPAd Requirements CR0131R00 Editorials
		CR0132R01 - Add IPA Capabilities in support of Indirect Profile Downlaod
		CR0133R00 - Editorials – Add some missed alphabets and symbols
		CR0134R01 - Editorials -Delete some extra symbols and words CR0135R00 - Comment about General Security Requirements CR0136R00 – Added ESipa messages protection requirement CR0137R01 - Clarification of eIM Security Requirement
		CR0141R00 - Add Event Retrieval definition
		CR0138R02 - IPA to retireve eIM Configuration Data CR0140R03 - Clarification of automatic enable option using default DP+
		CR0139R07 - Security protection of the Eim CR0142R00 - Editorial modification changing Roll-Back to Rollback CR0143R00 - Changes to section Basic Principles CR0144R02 - Clarification eCO over ESpsmo CR0145R01 - IoT eSIM eligibility check
		CR0146R03 eIM as RSP server attacker risk CR0148R01 Voiding requirements on automatic enabling with SM-DS - Alt to CR0147 CR0149R00 Mandatory support of eUICC to return eIM Configuration Data
		CR0150R00 - Update of References
V1.2	26 April 2024	CR0151R02 - Add requirement to enable switching to an emergency call profile
		CR0153R05 - Introduce connectivity parameters for constrained devices
		CR0154R01 - Introduce connectivity parameters for constrained devices
		CR0152R03 - Clarify IPA Requirement IPAF14 CR155R00 - Rename automatic profile enabling to immediate profile enabling
		CR156R01 - Add field test eUICC

		CR0157R00 - Update of References (Editorial) CR0158R02 - Clarification of which SGP.21 requirements apply to SGP.31 CR0160R00 - Removal of Editors Note
		CR0161R03 – IPAd Support clarification CR0162R00 – Adding requirements adapted to IoT from SGP.21 EUICC45 and EUICC46 CR0163R00 – Clarify optionality of emergency profile support CR0164R00 - eIM Notification Delivery support
		CR0166R01 - Editorial clean-up

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

Your comments or suggestions & questions are always welcome.