Embedded SIM Remote Provisioning Architecture

Version 4.0

25 February 2019

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

Security Classification: Non-confidential

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

Copyright Notice

Disclaimer

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

Antitrust Notice

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

Table of Contents

1 Introduction

1.1 Overview

Many Machine to Machine (M2M) Devices will not be easily reachable for the purpose of Provisioning a Subscription.

This document provides an architecture approach as a proposed solution for the remote Provisioning and Subscription management of Devices, while at the same time maintaining at least the same level of security both for network operators and Subscribers as present solutions.

Additionally this document describes a solution to be able to locally switch to specific optionally supported Profiles, i.e. for testing/certification or for emergency cases.

1.2 Void

1.3 Scope

The aim of this document is to define a common architecture framework to enable the remote Provisioning and management of the Embedded UICC (eUICC) in Devices which are not easily reachable, and additionally a way to locally switch to specific Profiles for testing/certification or emergency cases. The adoption of this architecture framework will aim to provide a basis for ensuring global interoperability for Remote Provisioning between Operators in different deployment scenarios.

1.4 Intended Audience

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

1.5 Definition of Terms

Term	Description
Actor	Physical entity (person, company or organisation) that can assume a role in the functional architecture. It is possible for an actor to assume multiple Roles in the same functional architecture.
Customer	A paying party, legally responsible juridical person or entity.
Device	Equipment into which an Embedded UICC and a communication module are inserted during assembly. Examples include: Utility meter, car and camera.
Embedded UICC	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the Device, and enables the secure changing of Subscriptions.

Term	Description
Emergency Profile	An Operational Profile with a Profile Attribute allocated, indicating that this Profile is an Emergency Profile. 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)
Emergency Profile Attribute	This is an attribute allocated to a Profile which, when set, identifies the Emergency Profile.
Enabled Profile	The state of a Profile when its files and/or applications (e.g., NAA) are selectable over the UICC-Terminal interface.
eUICC Certificate	A certificate issued by the EUM for a specific, individual, eUICC. This certificate can be verified using the EUM Certificate.
eUICC Manufacturer	Supplier of the eUICCs and resident software (for example firmware and operating system)
eUICC OS Update	Mechanism to correct existing features on an eUICC by the original OS Manufacturer when the eUICC is in the field.
EUM Certificate	A certificate issued to a GSMA accredited EUM which can be used to verify eUICC Certificates. This certificate can be verified using the GSMA CI Certificate.
Fall-Back Attribute	This is an attribute allocated to a Profile which, when set, identifies the Profile to be enabled by the Fall-Back Mechanism or by the execution of the Disable Profile function on another Profile. Only one Profile on the eUICC can have the Fall-Back attribute set at a time.
Fall-Back Mechanism	eUICC based mechanism which enables the Profile with Fall-Back Attribute set when the Enabled Profile loses network connectivity.
Form Factor	Manifestation of UICC. Specified in ETSI TS 102 221 [3] and ETSI TS 102 671 [8].
Generic Profile	Profile generated by the SM-DP following the Operator's specifications, but without the Operator's credentials and any specific data linked to the future targeted eUICC.
GSMA CI Certificate	Self-signed certificate of the CI, used to authenticate certificates issued to other entities.
Integrated Circuit Card ID	Unique number to identify a Profile in an eUICC. The ICCID is coded as defined by ITU-T E.118 [24].
International Mobile Subscriber Identity	Unique identifier owned and issued by Operators as defined in 3GPP TS 23.003 [25].

Term	Description
Local Disable	A function of the interface between a Device and an eUICC that provides the capability for a Device to locally disable the Emergency Profile on the eUICC without involvement of an SM-SR and/or SM-DP.
Local Enable	A function of the interface between a Device and an eUICC that provides the capability for a Device to locally enable the Emergency Profile on the eUICC without involvement of an SM-SR and/or SM-DP.
M2M Service Provider (M2M SP)	A Service Provider relying on an Operator providing the Profiles on the eUICC.
Network Access Application	An application residing on a UICC which provides authorisation to access a network for example a USIM application.
Network Access Credentials	Data required to authenticate to an ITU E.212 [16] network. This MAY include data such as Ki/K and IMSI stored within a NAA.
Operational Profile	A Profile containing one or more Network Access Applications and associated Network Access Credentials and Operator's (e.g. STK) applications and 3rd party applications.
Operator	A Mobile Network Operator or Mobile Virtual Network Operator; a company providing wireless cellular network services.
Operator Credentials	Set of credentials owned by an Operator, including Network Access Credentials, OTA Keys for remote Profile management and authentication algorithm parameters.
Orphaned Profile	A Profile whose Policy Rules have become unmanageable, for example due to the termination of the Subscriber's contract with the Operator.
OTA Keys	The credentials included in the Profile, used in conjunction with OTA Platforms.
OTA Platform	An Operator platform used for remote management of UICCs of Enabled Operator Profiles on eUICCs.
Personalised Profile	Un-personalised Profile with the addition of the Personalisation Data for the eUICC targeted by the Operator.
Personalisation Data	Set of data derived from the input data provided by the Operator and generated by the SM-DP (e.g. NAC, Keys, etc.) and dedicated to the personalisation of a unique Personalised Profile.

Term	Description
Platform Management	A set of functions related to the, enabling, disabling and deletion of a Profile and the transport of Profile Management functions to an eUICC. Platform Management actions are protected by Platform Management Credentials shared between the SM-SR and the ISD-R. Platform Management does not affect the contents of a Profile.
Platform Management Credentials	Data required within an eUICC so that a secured communication can be set up between an external entity and the eUICC in order to, enable, disable and delete Profiles on the eUICC and to transport Profile Management functions.
Policy	Principles reflected in a set of rules that governs the behaviour of eUICC and/or entities involved in the remote management of the eUICC.
Policy Control Function	A function that defines, updates or removes Policy Rules to implement a Policy.
Policy Enforcement Function	A function that executes Policy Rules to implement a Policy.
Policy Rule	Defines the atomic action of a Policy and the conditions under which it is executed.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC and which allows, when enabled, the access to a specific mobile network infrastructure.
Profile Description	Description of a Profile in a format specific to the Operator; Example formats include Excel table, xml format and plain text.
Profile Lifecycle Management	Execution of certain Platform Management commands by the M2M SP on a Profile, based on prior PLMA from the Operator owning the Profile.
Profile Lifecycle Management Authorisation (PLMA)	Authorisation given by an Operator to an M2M SP to permit Profile Lifecycle Management. Such authorisations are managed by the SM-SR.
Profile Management	A set of functions related to the downloading, installation and content update of a Profile in a dedicated ISD-P on the eUICC. Download and installation are protected by Profile Management Credentials shared between the SM-DP and the ISD-P.
Profile Management Credentials	Data required within an eUICC so that a Profile downloaded from an external entity can be decrypted and installed on the eUICC
Provisioning	The downloading and installation of a Profile into an eUICC.

Term	Description
Provisioning Profile	A Profile containing one or more Network Access Applications, and associated Network Access Credentials which, when installed on an eUICC, enables access to communication network(s), only to provide transport capability for eUICC management and Profile management between the eUICC and an SM-SR.
Provisioning Subscription	A special purpose contract, with its associated Provisioning Profile, that enables a machine to machine Device to access a mobile network only for the purpose of management of Operational Profiles on the eUICC.
Roles	Roles are representing a logical grouping of functions.
Security Realm	An element or set of elements within the ecosystem sharing a common level of trust and securely managed by a single administrative authority. No specific level of trust is to be assumed.
Subscriber	An entity (associated with one or more users) that is engaged in a Subscription with a Telecommunication Service Provider. The subscriber is allowed to subscribe and unsubscribe to services, to register a user or a list of users authorised to enjoy those services, and also to set the limits relative to the use that associated users make of these services
Subscription	Describes the commercial relationship between the Subscriber and the Telecommunication Service Provider.
Subscription Manager Data Preparation	Role that prepares the Profiles to be securely provisioned on the eUICC and manages the secure download and installation of these Profile onto the eUICC
Subscription Manager Secure Routing	Role that securely performs functions of Platform Management commands and the transport of Profile Management commands.
Telecommunication Service Provider	Entity that provides Subscriptions to Subscribers either as part of an Operator or as a party with a wholesale agreement with an Operator. The Telecommunication Service Provider could also be the Operator.
Test Profile	A combination of data and applications to be provisioned on an eUICC to provide connectivity to test equipment for the purpose of testing the Device and the eUICC. A Test Profile does not allow access to an ITU-E.212 [16] network.
Un-personalised Profile	Representation of the Profile (e.g. script) without any personalised data in a machine readable format. This format can be processed by a targeted eUICC type.

1.6 Abbreviations

Abbreviation	Description
AID	Application Identifier
CASD	Controlling Authority Security Domain
CI	Certificate Issuer
DAP	Data Authentication Pattern
DPID	ID of the relevant SM-DP
ECASD	eUICC Certificate Authority Security Domain
ECKA	Elliptic Curve Key Agreement algorithm
EID	eUICC-ID
EIS	eUICC Information Set
EncP	Encrypted and integrity protected Personalised Profile
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
EUM	eUICC Manufacturer
eUICC	Embedded Universal Integrated Circuit Card
GP	GlobalPlatform
GPCS	GlobalPlatform Card Specification
GSMA	GSM Association
ICCID	Integrated Circuit Card ID
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
ISO	International Standards Organisation
ITU	International Telecoms Union
KDF	Key Derivation Function
LTE	Long Term Evolution
M2M	Machine to Machine
M2M SP	Machine to Machine Service Provider
MNO-SD	Mobile Network Operator Security Domain
NAA	Network Access Application
OTA	Over The Air
PLMA	Profile Lifecycle Management Authorisation
POL1	Policy Rules within the Profile
POL2	Policy Rules associated to a Profile and stored in the relevant EIS at the SM-SR
PRF	Pseudo Random Function

Abbreviation	Description
SAS	Security Accreditation Scheme
SCP	Secure Channel Protocol
SD	Security Domain
ShS	Shared Secret
SIM	Subscriber Identity Module
SM	Subscription Manager
SM-DP	Subscription Manager Data Preparation
SM-SR	Subscription Manager Secure Routing
SRID	ID of the relevant SM-SR
SSD	Supplementary Security Domain
STK	SIM Tool Kit
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications Service
USIM	Universal Subscriber Identity Module
XML	Extensible Markup Language
W3C	World Wide Web Consortium

1.7 References

Ref	Document Number	Title
[1]	Void	Void
[2]	Void	Void
[3]	ETSI TS 102 221	UICC-Terminal interface; Physical and logical characteristics
[4]	ETSI TS 102 222	Administrative commands for telecommunications applications
[5]	ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT)
[6]	ETSI TS 102 225	Secured packet structure for UICC based applications
[7]	ETSI TS 102 226	Remote APDU structure for UICC based applications
[8]	ETSI TS 102 671	Smart cards; Machine to Machine UICC; Physical and logical characteristics
[9]	ETSI TS 103 383	Embedded UICC; Requirements Specification
[10]		GlobalPlatform Card Specification v.2.2.1
[11]		GlobalPlatform Card Specification v.2.2.1 UICC Configuration v1.0.1
[12]		GlobalPlatform Card Specification v.2.2 Amendment A: Confidential Card Content Management, v1.0.1
[13]		GlobalPlatform Card Specification v.2.2 Amendment B: v1.0.1

Ref	Document Number	Title
[14]		GlobalPlatform Card Specification v.2.2 Amendment D: Secure Channel Protocol 03, v1.1
[15]		GlobalPlatform Card Specification v.2.2 Amendment E: Security Upgrade for Card Content Management v1.0
[16]	ITU E.212	The international identification plan for public networks and Subscriptions
[17]	3GPP TS 21.133	3G Security, Security Threats and Requirements
[18]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application
[19]	3GPP TS 31.103	Characteristics of the IP Multimedia Services Identity Module (ISIM) application
[20]	NIST SP 800-57 Part 1	NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General (Revision 3)
[21]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels, S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[22]	FS.08	FS.08 – Security Accreditaion Scheme for Subscription Manager - Standard v3
[23]	FS.04	FS.04 - Security Accreditation Scheme for UICC Production – Standard v8
[24]	ITU-T E.118	The international telecommunication charge card
[25]	3GPP TS 23.003	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification
[26]	SGP.14	GSMA eUICC PKI Certificate Policy Version 1.1
[27]	SGP.05	Embedded UICC Protection Profile Version 1.1
[28]	3GPP TS 34.108	Common test environments for User Equipment (UE); Conformance testing

1.8 Conventions

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document SHALL be interpreted as described in RFC 2119 [2119].

2 Basic Principles and Assumptions

This section contains the principles and assumptions related to the GSMA remote Provisioning system for Embedded UICC.

2.1 Basic Principles

BPR1	The solution SHALL reflect the most important UICC-related use cases and adequately support them in a context where the eUICC hardware is not easily accessible or removable from the machine to machine Device. It is possible, due to the different nature of the eUICC, that not all current use cases can be covered.
BPR2	The solution SHALL be designed to enable new business opportunities, e.g. in M2M segments, while keeping the proven benefits of the current UICC.
BPR3	The security of the eUICC and its overall management processes must at all times and under all circumstances be at least as good as with the current removable UICC and its Provisioning processes.
BPR4	Any function, feature or service which is possible on a current UICC SHALL be possible on the eUICC.
BPR5	The access to functions, features or services on the eUICC SHALL be identical to the current UICC, i.e. transparent for the terminal and the user.
BPR6	The remote management of functions, features or services on the eUICC SHALL have minimal impact on the operator's existing systems and infrastructure. This SHALL be achieved by using existing standards and specifications as far as possible.
BPR7	Keep it simple. Complexity is understood as a risk factor. A reasonably limited functional approach will support the time-to-market expectations and MAY evolve with future requirements and improvements.
BPR8	3rd-party applications which are outside of an Operational Profile are out of the scope of this document.
BPR9	Each entity SHALL be responsible for its operations.
BPR10	The applications and file system within a disabled Operational Profile are neither locally or remotely selectable.

2.2 General Assumptions

2.2.1 Use of Existing Standards

STD1	The definition of the eUICC and the related Provisioning systems SHALL be as efficient as possible, in terms of efforts and costs for all involved parties. This SHALL be achieved by using existing standards and specifications where possible.
STD2	GlobalPlatform specifications will be considered as a framework of choice for the implementation of the eUICC.

2.2.2 Machine to Machine Device Impact

DEV1	The implementation of the eUICC ecosystem will have minimal impact on the Device.
DEV2	No security certification requirement will be placed on the Device.
DEV3	No new certification requirement will be placed on the Device.
DEV4	Any Device approval impact SHALL be covered under existing Device type approval or certification schemes and be independent of the certification of the eUICC.
DEV5	The communication module within the Device SHALL conform to the terminal requirements within ETSI TS 102 221 [13] for all standardised ETSI Form Factors.

DEV6	The Device manufacturer SHALL ensure that there is a method for the owner of the Device or Telecommunication Service Provider to access the eUICC identification (EID).
DEV7	The Device manufacturer SHOULD print the eUICC identification (EID) on the Device so that it is human readable.

2.2.3 Security

SEC1	The overall security of the eUICC in combination with the related management processes must at all time and under all circumstances be at least equivalent to the current removable UICC and its Provisioning processes.
SEC2	The architecture of the eUICC and its remote Provisioning system complies with the requirements of 3GPP TS 21.133 [17] “3G Security, Security Threats and Requirements”.
SEC3	The architecture must support a level of security with respect to protection of Operator Credentials which is at least equal to present levels of security. This applies in particular to: • The confidentiality of cryptographic keys and authentication parameters. • The integrity of Subscriber identities (e.g. IMSI).
SEC4	Certification SHALL be mandatory for the eUICC.
SEC5	The remote Provisioning architecture must avoid compromising the security of Subscriber data.
SEC6	A trusted system is a system that is relied upon to a specified extent to enforce a specified security Policy. A trust model is defined as part of the security related project deliverables.
SEC7	For remote Platform and Profile management, all entities involved in the management have to be mutually authenticated.

2.2.4 Regulatory

REG1	Regulatory issues are considered outside the scope of the Embedded SIMworking group. Regulatory issues will be referred to the GSMA regulatory team.

2.3 The eUICC Ecosystem

ECO1	Remote subscription management functions are provided by two Roles – the SM-DP and the SM-SR.
ECO2	1. Profile management is governed by Policy Rules that are contained in the Operator’s Profile and in the SM-SR. 2. Policy Rules are enforced by the eUICC and the SM-SR on behalf of the Operator. 3. Control of Policy Rules lies with the Operators.

2.3.1 Roles and Entities

2.3.1.1 eUICC Manufacturer

MAN1	1. The eUICC Manufacturer (EUM) provides eUICCs containing a Provisioning Profile and/or one or more Operational Profiles. 2. The eUICCs are delivered to the machine to machine Device manufacturer. 3. Related Platform Management Credentials are sent to the SM-SR to be associated with each eUICC. 4. The EUM is responsible for the initial cryptographic configuration and security architecture of the eUICC. 5. The EUM production site SHALL be SAS-UP [23] certified. 6. The eUICC manufacturer MAY also provide eUICCs containing an Emergency Profile. 7. The eUICC Manufacturer MAY provide eUICCs also containing a Test Profile. EUM.
MAN2	The EUM SHALL issue the eUICC Certificate to allow: • the eUICC authentication and certification to other entities; • the authenticated keyset establishment between an SM-DP and an eUICC; • the authenticated keyset establishment between an SM-SR and an eUICC.
MAN3	The EUM Certificate and GSMA CI Certificate SHALL be delivered to other entities using reliable storage and communication channels.
MAN4	The EUM SHALL provide services, tools, scripts or documentation to the SM-DP enabling it to create an Un-personalised Profile for a eUICC produced by the EUM. It is not the role of the EUM to create the Un-Personalised Profile on behalf of the SM-DP.
MAN5	In case the eUICC OS Update mechanism is used, the EUM SHALL ensure the eUICC affected by such mechanism maintains the same level of security and functional compliance.

2.3.1.2 Device Manufacturer

DMA1	1. The Device manufacturer builds machine to machine Devices which comprise a communication module and an eUICC containing at least a Provisioning Profile or Operational Profile that is enabled. 2. A Provisioning Profile or Operational Profile SHALL be enabled. NOTE: Any Enabled Profile requires the agreement of the respective Operator.

2.3.1.3 Operator

MNO1	1. The Operator provides mobile network connectivity. 2. The Operator selects at least one SM-DP. 3. The Operator SHALL have a direct interface to the SM-SR. 4. In the event that a Subscriber has selected an Operator, that Operator initiates the download of a particular Profile to an identified target eUICC subject to current Policy Rules. 5. The Operator specifies the Profile characteristics and any features and applications, analogous to current UICCs. The Operator owns the Profile. 6. Profiles can be generated at the time the download is ordered. 7. To achieve a transparent fit with existing UICC processes and interfaces, Profiles can also be ordered in bulk, then securely stored at the SM-DP until ordered for download. SAS-SM [22] requirements SHALL apply. 8. The Operator defines the Policy Rules that control the Profile management when this Profile is enabled. 9. After the download is ordered the Operator SHALL be able to check and validate the certification and capabilities (manufacturer, memory size, algorithms etc.) of the target eUICC before the download of the Profile is started. 10. The Operator SHALL receive confirmation of the successfully completed download and installation of the Profile. 11. The enabled Operator SHALL be able to use an OTA Platform in order to manage the content of its enabled Profile in the eUICC.
MNO2	Upon request from a Subscriber the Operator SHALL be able to declare to the relevant entities a machine to machine Device as stolen so that appropriate measures can be taken.
MNO3	An Operator SHOULD provide only limited service to a Device using a Provisioning Profile; the mechanism the Operator uses to enforce this limited service is out of scope of this architecture.
MNO4	An Operator SHALL be able to send Platform Management commands and Profile Management commands to manage its own Profiles • either to an SM-DP to be transmitted to an SM-SR • either directly to an SM-SR These commands SHALL be executed only if the targeted Profile is owned by the Operator.
MNO5	The Operator SHALL be able to receive reports of a Profile status changes of its own Profiles, irrespective of the cause of the Profile status change.
MNO6	An Operator SHALL be able to define PLMAs for its own Profiles. No other entity than the Operator SHALL be able to define PLMA.
MNO7	The Operator SHALL be able to set and unset PLMAs whereby the M2M SP SHALL be able to receive a report about this change of authorisation.

MNO8	An Operator SHALL be able to grant PLMA to an M2M SP for: • Commands to enable, disable, delete a Profile. • Management (set or unset) of the Fall-Back Attribute of a Profile. • Management (set or unset) of the Emergency Profile Attribute of a Profile. • The reception of reports related to enabling, disabling, deleting, and management of the Fall-Back Attribute of a Profile. • The reception of reports related to management of the Emergency Profile Attribute of a Profile.
MNO9	MNO4 SHALL be independent of any given PLMA to an M2M SP.
MNO10	An Operator SHALL be able to request to an SM-SR, • the setting of the Fall-Back Attribute on its Profile, • the setting of the Emergency Profile Attribute on its Profile if another Profile has the Emergency Profile Attribute set, if and only if the appropriate PLMA have been set by the Operator owning the Profile with the Fall-Back Attribute or the Profile with the Emergency Profile Attribute to be unset.
MNO11	An Operator SHALL be able to send Profile Lifecycle Management commands to enable, disable and delete Profiles, targeting its own Profiles, issued by an M2M SP on an M2M SP/Operator interface. The Operator SHALL be able to send these commands • either to an SM-DP to be transmitted to an SM-SR • either directly to an SM-SR. These commands SHALL be executed only if the targeted Profile is owned by the Operator and PLMA has been set by the Operator owning the Profile , for the M2M SP.
MNO12	The Operator SHALL be able to route Profile change status reports to the M2M SP that is authorised on this Profile when M2M SP is using an Operator/M2M SP interface as specified in MNO11.
MNO13	The Operator SHALL be able to receive a report of setting the Emergency Profile Attribute of any Profile on the eUICC.

NOTE: The Operator MAY provide an interface to the M2M SP in order to allow the M2M SP to trigger Profile installation or perform Profile Lifecycle Management related to the Operator's Profiles. This interface is out of scope of this specification.

2.3.1.4 Operator Subscriber

CUS1	1. The Operator Subscriber is the actual contract partner of the Operator for the Subscription. It MAY not be identical to the end user. 2. The Operator Subscriber uses a Device equipped with a eUICC from the Device manufacturer and a Profile (Subscription) from a selected Operator. 3. Prior to the download of a Profile the Operator Subscriber must provide his/her implicit or explicit acceptance. 4. The Operator Subscriber SHALL have means to directly or indirectly obtain the machine to machine Device identifier. The identification of the machine to machine Device SHALL implicitly or explicitly identify the eUICC.

2.3.1.5 End User

END1	1. The end user uses the machine to machine Device and the services related to the Enabled Profile. 2. The end user MAY be identical to the Operator Subscriber. 3. The eUICC is transparent to the end user. 4. The end user's relationship is with an Operator Subscriber or the Operator directly.

2.3.1.6 Subscription Manager – Data Preparation (SM-DP)

SMDP1	1. The SM-DP acts on behalf of the Operator. 2. The SM-DP receives a Profile Description from the Operator and creates Un-personalised Profile accordingly. The SM-DP MAY have to utilise tools provided by the EUM to create the Un-personalised Profile. The information exchanged between the SM-DP and EUM is not standardised and MAY differ between different entities. 3. The SM-DP generates Personalisation Data for the targeted eUICC (e.g. Network Access Credentials and other data) based upon input data from the Operator. 4. The SM-DP builds Personalised Profiles for the targeted eUICC. 5. The SM-DP SHALL secure the Profile package with the Profile Management Credentials of the targeted eUICC. 6. The SM-DP installs the Personalised Profile on the eUICC through the SM-SR.
SMDP2	On request by the Operator the SM-DP also initiates Profile enabling, Profile disabling, Profile deletion and Fall-Back/Emergency Profile Attribute management requests to the eUICC via the SM-SR.
SMDP3	The SM-DP establishes a secure and authenticated channel to the eUICC to download and install Profiles on to the eUICC.
SMDP4	The interface between the SM-DP and the SM-SR SHALL have proper security level defined in order to support secure delivery of Profiles through the SM-SR.
SMDP5	The SM-DP must always receive a request from an Operator to send a Profile via an SM-SR to an eUICC.
SMDP6	The SM-DP SHALL be GSMA SAS-SM [22] certified.
SMDP7	Given any eUICC, the SM-DP SHALL be able to generate a Personalised Profile for this eUICC.
SMDP8	The SM-DP and Operator are the only entities allowed to establish a secure and authenticated channel to the eUICC to manage a Profile.
SMDP9	The Operator SHALL be able to interface to an SM-DP of the Operator's choosing to serve any Operator approved eUICC.
SMDP10	The SM-DP SHALL be able to generate a Personalised Profile that can be downloaded and installed on the eUICC targeted by the Operator.
SMDP11	The SM-DP SHALL support the Profile ordering procedure described in section 3.5.3 of this document.

SMDP12	The SM-DP SHALL be able to forward to the corresponding Operator any status change, including Attribute changes, of a Profile reported by the SM-SR to the SM-DP independently of the cause of the Profile change.
SMDP13	The SM-DP certificate SHALL be issued by a GSMA CI.
SMDP14	The SM-DP SHALL authenticate the Operator before executing Profile Management or forwarding Platform Management commands from this Operator to the SM-SR.
SMDP15	On request by the Operator the SM-DP SHALL be able to set, delete or retrieve PLMA in an SM-SR managing the Operator PLMA, as described in section 3.5.15.
SMDP16	The SM-DP SHALL be able to forward to the corresponding Operator the setting of the Emergency Profile Attribute for any Profile on the eUICC reported by the SM-SR.

2.3.1.7 Subscription Manager – Secure Routing (SM-SR)

SMSR1	The SM-SR is the only entity allowed to establish a secure and authenticated transport channel to the eUICC to manage the eUICC platform.
SMSR2	The SM-SR loads, enables, disables and deletes Profiles on the eUICC in accordance with the Operator's Policy Rules and PLMAs.
SMSR3	The SM-SR obtains the Platform Management Credentials of the eUICC from the EUM or establishes them through the previous SM-SR.
SMSR4	Only one SM-SR can be associated with an eUICC at any point in time, but it can be changed during the lifetime of the eUICC.
SMSR5	The interface between the SM-SR and the eUICC SHALL have proper security level defined in order to support the secure delivery to, and management of, Profiles in the eUICC.
SMSR6	1. The SM-SR SHALL NOT handle Operator Credentials in clear text. 2. The SM-SR has secure communications channels to the SM-DP, eUICC, Operator and M2M SP. 3. The SM-SR SHALL be GSMA SAS-SM [22]- certified.
SMSR7	The SM-SR SHALL be able to determine whether an eUICC is available for remote management.
SMSR8	The SM-SR SHALL be non-discriminatory with regards to other entities within the ecosystem.
SMSR9	The SM-SR certificate SHALL be issued by a GSMA CI.
SMSR10	The SM-SR SHALL support Profile Lifecycle Management. through an interface with an M2M SP.
SMSR11	The SM-SR SHALL support the PLMA function through an interface with an Operator as described in section 3.5.15.
SMSR12	The SM-SR SHALL authenticate the Operator and check that the Operator is the owner of the Profile before executing Platform Management commands.

SMSR13	The SM-SR SHALL authenticate the M2M SP and check that the M2M SP is authorised by the Operator through PLMA before executing Profile Lifecycle Management on the Profile owned by the Operator who has given the PLMA. If no PLMA is given, only the Operator is able to execute Platform Management on its Profiles.
SMSR14	The SM-SR SHALL be able to report any status change of a Profile, to 1. a corresponding Operator owning the affected Profile and interfacing with the SM-SR or 2. an M2M SP having PLMA set for the affected Profile and interfacing with the SM-SR or 3. a corresponding SM-DP being in charge of the affected Profile and interfacing with the SM-SR This SHALL be independent of the cause of the Profile change and SHALL also cover the case where the Operator acts on behalf of the M2M SP as described in MNO11.
SMSR15	In case of SM-SR change, no PLMA SHALL be transferred to the new SM-SR.
SMSR16	The SM-SR SHALL ensure no PLMAs are granted for: • The setting of POL2 • The setting of other PLMAs

2.3.1.8 Certificate Issuer

CIS1	The Certificate Issuer role issues certificates for Embedded UICC remote provisioning system entities and acts as a trusted third party for the purpose of authentication of the entities of the system.
CIS2	The Certificate Issuer provides certificates for the EUM, SM-SR and SM-DP.
CIS3	The Certificate Issuer communicates with the SM-SR, SM-DP and EUM through interfaces that are defined in SGP.14 [26].

2.3.1.9 Initiator

INT1	The Initiator is a virtual role that can be assumed by various entities. The Initiator is in charge of initiating specific procedures.
INT2	For the purpose of the procedures defined within this document the Initiator MAY be assumed to be an Operator or an M2M SP, having PLMAs set for the affected Operator Profiles.
INT3	At any time, only one entity MAY assume the Initiator role.
INT4	The interface between the Initiator and the SM-SR is based on the interfaces defined in this document.
INT5	The Initiator SHALL be authorised and authenticated by the SM-SR.

2.3.1.10M2M Service Provider

M2MSP1	An M2M SP MAY have a direct interface to the SM-SR to perform Profile Lifecycle Management for which PLMAs have been set by the Operator.
M2MSP2	An M2M SP SHALL be able to request to an SM-SR the enabling of a Profile for which PLMAs have been set by the Operator.
M2MSP3	An M2M SP SHALL be able to request to an SM-SR the disabling of a Profile for which PLMAs have been set by the Operator.
M2MSP4	An M2M SP SHALL be able to request to an SM-SR the deletion of a Profile for which PLMAs have been set by the Operator.
M2MSP4-B	An M2M SP SHALL be able to request to an SM-SR the setting of the Fall-Back Attribute on a Profile, if and only if the appropriate PLMA has been set by both the Operator whose Profile has the Fall-Back Attribute currently set, and the Operator whose Profile will have the Fall-Back Attribute set by the request.
M2MSP4-C	A M2M SP SHALL be able to request to an SM-SR the setting of the Emergency Profile Attribute on a Profile, if and only if the appropriate PLMA has been set by the Operator whose Profile will have the Emergency Profile Attribute set by the request. In case a Profile exists that already has the Emergency Profile Attribute set, an M2M SP SHALL be able to request to an SM-SR the setting of the Emergency Profile Attribute on a Profile, if and only if the appropriate PLMAs have been set by both, the Operator whose Profile has the Emergency Profile Attribute currently set, and the Operator whose Profile will have the Emergency Profile Attribute set by the request.
M2MSP5	The M2M SP SHALL be able to receive reports of a Profile enabling, disabling, or deletion and Fall-Back or Emergency Profile Attribute change, based on a Platform Management command executed by an SM-SR, irrespective of the cause of the changes to the Profile.
M2MSP6	The M2M SP SHALL be able to receive reports whenever its PLMAs have been changed.
M2MSP7	The reception of reports in M2MSP5 SHALL be configured via PLMAs.

2.4 The eUICC

EUICC1	The eUICC is a discrete hardware component in a standardised ETSI Form Factor.
EUICC2	In general, the eUICC is non-removable.
EUICC3	From a machine to machine Device perspective, the behaviour of the eUICC is generally identical to the UICC.

EUICC4	1. The eUICC can contain one or more Profiles. 2. Only one Profile SHALL be enabled at any point in time. 3. Void. 4. Void. 5. Void. 6. All relevant UICC specifications SHALL apply.
EUICC4-B	The eUICC SHALL contain a Profile with Fall-Back Attribute set. The eUICC SHALL NOT contain more than one Profile with the Fall-Back Attribute set. The Profile with Fall-Back Attribute set SHALL NOT be deleted. The setting of the Fall-Back Attribute SHALL be managed by the SM-SR.
EUICC4-C	The eUICC MAY contain a Profile with Emergency Profile Attribute set. The eUICC SHALL NOT contain more than one Profile with the Emergency Profile Attribute set. A Profile SHALL NOT have the Emergency Profile attribute and the Fall-Back attribute set at the same time. The setting of the Emergency Profile Attribute SHALL be managed by the SM-SR.
EUICC4-D	The eUICC MAY contain a Test Profile. The eUICC SHALL NOT contain more than one Test Profile. The eUICC SHALL ensure that the Test Profile does not have the Fall-Back Attribute set or the Emergency Profile Attribute set.
EUICC4-E	The eUICC SHALL ensure that the Profile Attribute requirements described in 2.5 are fulfilled.
EUICC5	The behaviour of a (U)SIM or ISIM within a Profile on an eUICC is expected to be identical to a present (U)SIM or ISIM. No changes to existing 3GPP (U)SIM and ISIM specifications are expected.
EUICC6	The eUICC SHALL implement the Milenage network authentication algorithm.
EUICC7	The eUICC SHOULD implement the TUAK algorithm in addition to Milenage when TUAK is included within 3GPP specifications.
EUICC8	The ownership of the physical eUICC MAY change throughout its lifetime.
EUICC9	The eUICC SHALL contain the address of its associated SM-SR and have a means to authenticate it.
EUICC10	eUICCs delivered by the EUM SHALL always be registered to an SM-SR.
EUICC11	If any command, such as Profile enabling, Profile disabling and Profile download and installation does not complete successfully, the eUICC SHALL maintain the state it was in before it received the request.

EUICC12	The eUICC MAY support Local Enable and Local Disable functions of an Emergency Profile without interaction with the SM-SR.
EUICC12-B	The eUICC MAY support Local Enable and Local Disable functions of a Test Profile without interaction with the SM-SR.
EUICC13	The eUICC SHALL NOT send a report to the SM-SR when an Emergency Profile has been enabled using the Local Enable function.
EUICC14	The eUICC SHALL enable the previously enabled Profile when the Emergency Profile has been disabled using the Local Disable function.
EUICC15	When an Emergency Profile has been disabled using the Local Disable function the eUICC MAY send a report to the SM-SR.
EUICC16	The eUICC supporting Local Enable and Local Disable SHALL allow these functions only for the Emergency Profile.
EUICC17	In case the execution of the Local Disable fails (e.g. previously enabled Profile deleted, previously enabled Profile not providing network connectivity), the eUICC SHALL trigger the Fall-Back Mechanism.
EUICC18	The eUICC MAY support Local Enable and Local Disable functions for a Test Profile without interaction with the SM-SR.
EUICC19	The eUICC SHALL NOT send a report to the SM-SR when the Test Profile has been enabled using the Local Enable function.
EUICC20	The eUICC SHALL enable the previously enabled Profile when the Test Profile has been disabled using the Local Disable function.
EUICC21	When a Test Profile has been disabled using the Local Disable function the eUICC MAY send a report to the SM-SR.
EUICC22	In case the execution of the Local Disable fails (e.g. previously enabled Profile deleted, previously enabled Profile not providing network connectivity), the eUICC SHALL trigger the Fall-Back Mechanism.
EUICC23	The eUICC SHALL perform the necessary action to ensure that the values of the Test Profile are in accordance with 3GPP TS 34.108 [28] and to ensure that the Test Profile does not allow access to an ITU-E.212 [16] network.
EUICC24	In case the execution of the Local Disable fails, the eUICC triggering the Fall-Back Mechanism SHALL ensure that the previously enabled Profile is the Profile that was enabled before the Local Enable.

2.4.1 Profiles

PRO1	Profiles are the property of the issuing Operator.
PRO2	Profiles SHALL be uniquely identified.

PRO3	1. Only one Profile SHALL be enabled at any point in time. 2. Other Profiles MAY exist on the Embedded UICC, but the Enabling/Disabling of Profiles, except an Emergency Profile and a Test Profile, always remains an action that is executed only by the SM-SR acting on behalf of the Operator, except under specific circumstances described by PRO11 or by an M2M SP based on PLMAs set by the Operator. 3. Enable/Disable/Delete actions SHALL be undertaken according to Policy Rules.
PRO4	1. A Profile is under the control of the issuing Operator. The Operator MAY delegate part of the Profile Lifecycle Management via PLMAs. 2. A Profile in combination with a eUICC carries all logical characteristics of a UICC. All relevant UICC specifications SHALL apply with the exceptions defined by the eUICC specifications.
PRO5	Each Profile SHALL be isolated within its own dedicated secure container. The GlobalPlatform's Security Domain framework SHALL be considered.
PRO6	Profiles MAY be used either for Provisioning (Provisioning Profile), for operation (Operational Profile) or for testing (Test Profile). They are clearly distinguished. 1. An Operational Profile MAY be used as a Provisioning Profile. 2. A Provisioning Profile SHALL NOT be used as an Operational Profile. 3. A Test Profile SHALL NOT be used as a Provisioning or Operational Profile.
PRO7	There SHALL be zero or one Provisioning Profile.
PRO8	There MAY be several Operational Profiles.
PRO9	Installed Profiles SHALL have one of the following states: • enabled • disabled
PRO10	In all operational uses the eUICC SHALL enforce that one, and only one, Profile is enabled at any point in time.
PRO11	There SHALL be a capability for eUICC–initiated enabling of the Profile with Fall-Back Attribute set, in the case of loss of network connectivity. In case this mechanism is used, the POL1 "disabled not allowed" and "Profile deletion is mandatory when it is disabled" SHALL be ignored.
PRO11-B	In case a Profile with Fall-Back Attribute set is enabled by the eUICC as per PRO11, the eUICC SHALL inform its associated SM-SR. The Profile with Fall-Back Attribute set will consequently provide network connectivity to allow the SM-SR to remotely manage the eUICC.
PRO12	The local Profile management SHALL only be possible: • Under specific circumstances described by PRO11 • For Emergency Profile • For Test Profile
PRO13	A Profile contains parameters for an authentication algorithm (e.g. OPc, ri, ci for the Milenage algorithm) but not the algorithm itself.

PRO14	The eUICC MAY support other network authentication algorithms; if such algorithms are supported, the eUICC SHALL implement a mechanism to configure its parameters. NOTE: The accessibility of these other network authentication algorithms to Profiles is out of the scope of this document.
PRO15	A Profile contains a subset of Policy Rules to control external Profile management actions.
PRO16	A Profile MAY contain identifiers for entities in the ecosystem, keys, PINs, certificates, algorithm parameters, as well as first and second level applications. (Ref: ETSI TS 102 221 [3]).
PRO17	Any function, feature or service which is possible on a current UICC SHALL be possible in an Operational Profile on an eUICC.
PRO18	The access to functions, features or services in a Profile on an eUICC SHALL be identical to the current UICC, i.e. transparent for the terminal and the user.
PRO19	The remote management of functions, features or services in a Profile on an eUICC SHALL have minimal impact on the operator's existing systems and infrastructure.
PRO20	Profiles are stored only in the SM-DP and installed on the eUICC; they are not stored anywhere else and are encrypted in transit.
PRO21	It SHALL be possible to update a Test Profile with restriction defined by the EUICC23.
PRO22	The deletion of the Test Profile SHALL NOT be possible.
PRO23	It SHALL NOT be possible to remotely enable or disable the Test Profile.

2.4.2 Policies & Policy Control

PPC1	Each Profile has an associated Policy. A Policy contains rules which govern the change of operational states of the Profile. These state transitions are: • disabling • enabling • deletion
PPC2	Update-access to a Profile's Policy is restricted to the issuing Operator.
PPC3	The Policy Rules of a disabled Profile can only apply to itself. The Policy Rules of a disabled Profile cannot affect any other Profile, except for the reasons listed by PPC4.
PPC4	If the previously Enabled Profile has the POL1 rule "disable not allowed" set, then the eUICC SHALL only switch back to this Profile: as long as POL1 rule "disable not allowed" is set, it SHALL only be possible to delete this Profile by the Master Delete function.

2.5 Profile Attributes

In this version of the specification the following Profile Attributes are defined:

- Fall-Back Attribute
- Emergency Profile Attribute

PRA1	A Profile Attribute MAY be set for a Profile.
PRA2	The support of the Emergency Profile Attribute is optional.
PRA3	If a specific Profile Attribute is supported, it SHALL be possible to set such Profile Attribute for a Profile.
PRA4	A Profile SHALL NOT have the Fall-Back Attribute and the Emergency Profile Attribute set at the same time.

3 Architecture

3.1 Architecture Diagram

This section defines the functional architecture required to support the remote Provisioning of eUICCs. The basic building blocks of the architecture consist of the functions to be performed, the Roles and the assigned Actors.

The figure below represents the eUICC remote Provisioning system. Details of the Roles, the associated functions and interfaces are described in section 3.3 and Annex A.

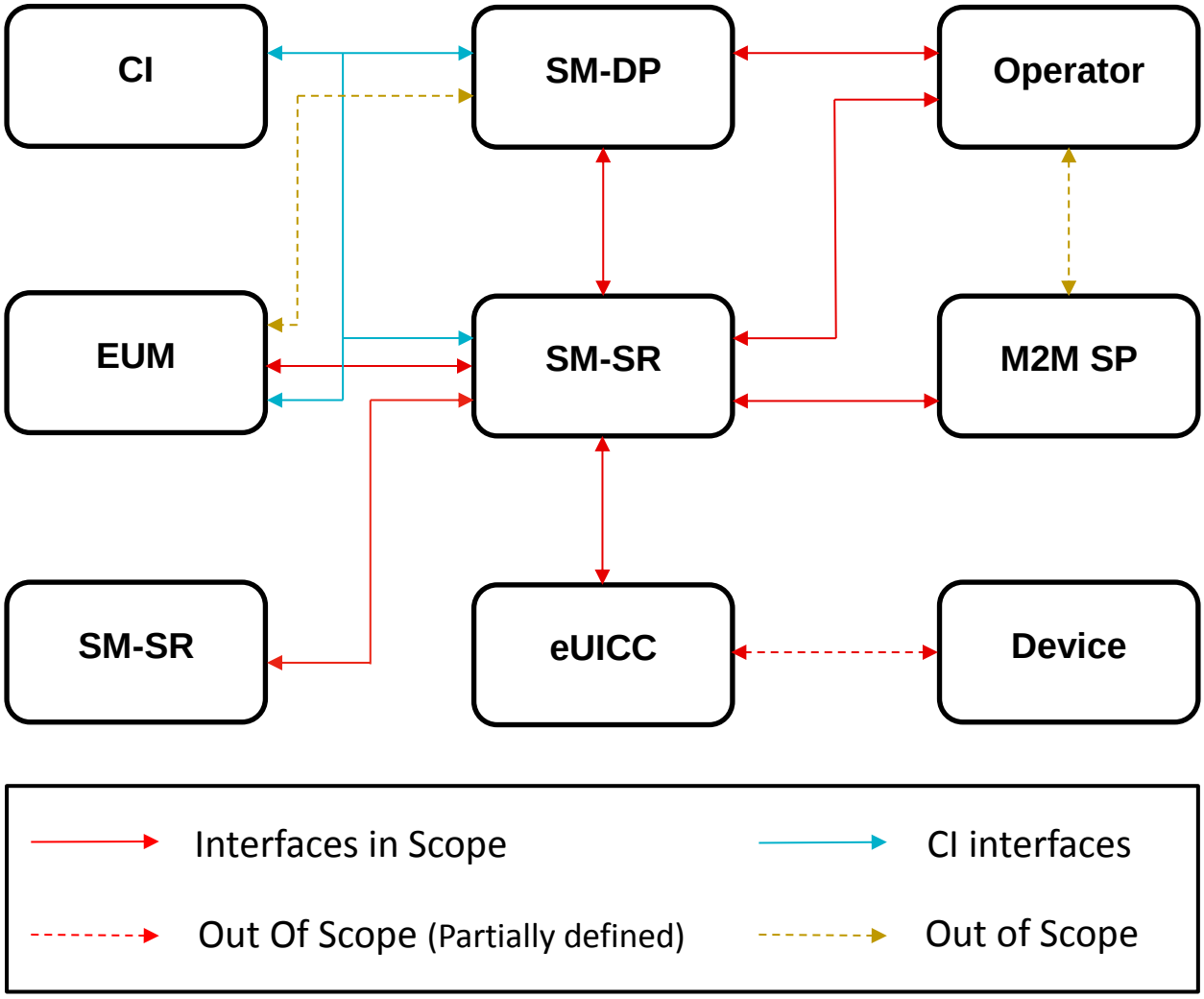

Figure 1: eUICC Remote Provisioning System

3.2 Card Architecture

3.2.1 Security Domains

GlobalPlatform provides the notion of Security Domains (SD). These are on-card representatives of off-card entities that provide:

- Secure storage for cryptographic keys;
- Access for off card entities using (GP) secure channel protocols;
- A mechanism for loading applications;
- Security services for applications.

The properties of SDs are configured via GP privileges (e.g. Delegated or Authorised Management, DAP Verification, Token Management, Global Delete), by the Provisioning of keys (e.g. for SCP03 or SCP80/81) and by associating an SD to another SD with other rights, by associating an SD to itself (and thus removing all management rights of a superior SD) or by assigning memory quotas for the SD and all its contents.

In earlier versions, the ISD (Issuer Security Domain) had several unique privileges. However, in the latest GlobalPlatform Card Specification [10], it is also configured via privileges, and except for being there in the beginning, no major specific feature remains. This SHOULD allow Operators to have the same benefits as they do today with the current ISD in a UICC.

The way forward is:

- To build the eUICC on a structure of SDs, and
- To define additional properties (e.g. via privileges) so that the different SDs can represent the Actors for the various Roles in remote Provisioning of Profiles.

3.2.2 Card Architecture

This section describes how Profiles SHOULD be designed, for example, using an extended version of the concepts and information models from GlobalPlatform Card Specification [10]. Profiles are contained within security domains (SD) on the eUICC, thus making the security mechanisms of SDs available. Further information can be found in [10].

The following figure outlines a schematic representation of the eUICC.

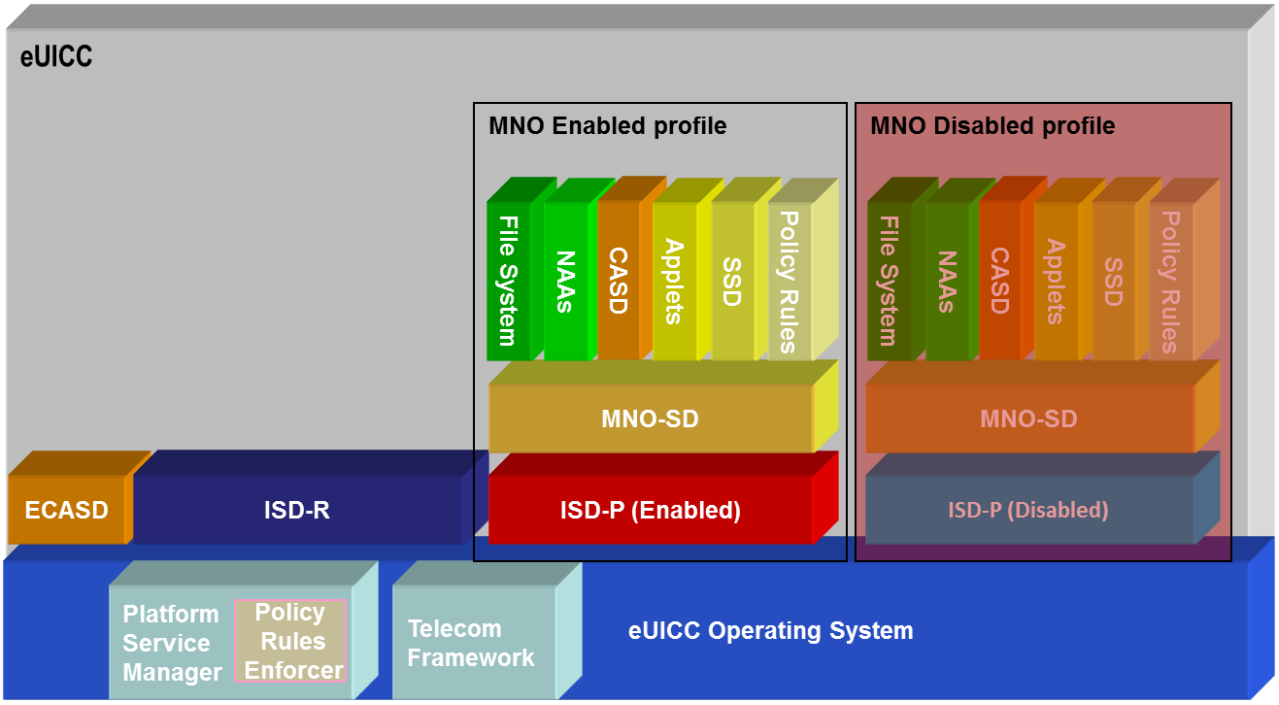

Figure 2:Schematic Representation of the eUICC

The operating system (OS) contains the basic platform features, e.g. support of the features defined in the GlobalPlatform Card Specification [10].

The ECASD (eUICC Certificate Authority Security Domain):

- Is created within an eUICC at time of manufacturing;
- Cannot be deleted or disabled after delivery;

- Is based on the concept of CASD from Global Platform (see [10], [12] and [15]);
- Is configured by the EUM at pre-issuance;
- Contains a non-modifiable eUICC private key, the associated Certificate, the CI's root public keys and the EUM keyset for key/certificate renewal;
- Is associated to the ISD-R, which provides the underlying secure OTA channel;
- Is required for, and is not limited to, the establishment of new keysets in the ISD-P(s) and ISD-R;
- Does not support the Mandated DAP verification feature.

ISD-R and ISD-P are security domains with special features.

The ISD-R (ISD-Root) is the on-card representative of the SM-SR that executes the Platform Management commands (see the functions for Platform Management in section 3.3.1.3).

An ISD-R SHALL:

a) Be created within an eUICC at time of manufacturing;
b) Be associated to an SM-SR;
c) Not be deleted or disabled;
d) Provides a secure OTA channel using Platform Management Credentials (SCP80 or SCP81 as defined in [10]) to the SM-SR;
e) Implement a key establishment protocol for the support of the change of SM-SR;
f) Offers wrapping and unwrapping service of the transport part during Profile download;
g) Be able to create new ISD-Ps with the required cumulative granted memory (CGM)
NOTE: memory management at SM-SR level is for further study;
h) Not be able to create any SD except an ISD-P;
i) Executes Platform Management functions in accordance to the Policy Rules;
j) Not be able to perform any operation inside an ISD-P.

The ISD-P (ISD-Profile) is the on-card representative of the Operator, or SM-DP if delegated by the Operator.

An ISD-P SHALL:

a) Be a separate and independent entity on the eUICC;
b) Contain a Profile including MNO-SD, Connectivity Parameters, file system, NAAs and Policy Rules;
c) Contain a state machine related to creating, enabling and disabling the Profile;
d) Contain keys for Profile management for the loading and installation phase;
e) Implement a key establishment protocol to generate a keyset for the personalisation of the ISD-P;
f) Be able to receive and decrypt, load and install the Profile created by the SM-DP;
g) Be able to set its own state to disabled once the Profile is installed;
h) Provide SCP03 capabilities to secure its communication with the SM-DP;
i) Be able to contain a CASD. This CASD is optional within the Profile and provides services only to security domains of the Profile and only when the Profile is in Enabled state.

The MNO-SD is the on-card representative of the Operator.

An MNO-SD SHALL:

a) Be associated to itself;
b) Contain the Operator OTA Keys;
c) Provide a secure OTA channel (SCP80 or SCP81 as defined in [6] and [7]);
d) Have the capability to host Supplementary Security Domains.

Once the Profile is installed in its ISD-P on the eUICC, the Profile and ISD-P SHALL be considered to be in union and thereafter it is the state of the ISD-P that is managed.

The SM-DP performs the Profile Management functions (see section 3.3.1.2) on the ISD-P during the load and install phase. The MNO-SD is managed by an Operator OTA Platform once the Profile is enabled. The MNO-SD is managed in an equivalent way to the ISD of a current UICC.

The Platform Service Manager is an OS service that offers Platform management functions and Policy Rules enforcement mechanism (Policy Rules Enforcer). Called by the ISD-R or ISD-P it executes the functions according to the Policy Rules (see section 3.6). In addition it can retrieve ISD-P generic information (i.e. Profile ID, Profile State) that can be shared with authorised entities on request.

The Telecom Framework is an OS service that provides standardised network authentication algorithms to the NAAs hosted in the ISD-Ps. Furthermore it provides the capabilities to configure the algorithm with the needed parameters.

Contained in the ISD-P are the well-known card structure with applications, SDs for other entities, the file system (MF tree, ADFs, etc.) (as per ETSI TS 102 221 [3] and 3GPP TS 31 102 [18]) and the Policy Rules.

3.2.3 State Diagram for an ISD-P

The states and state transitions for an ISD-P are as follows:

After an ISD-P is created and keys are set up, the SM-DP, on behalf of the Operator, can create a Profile containing SDs, applications, NAAs, and the file system. When the Profile is installed, the SM-DP sets the state of the ISD-P to disabled, effectively handing it over to the SM-SR for Platform Management.

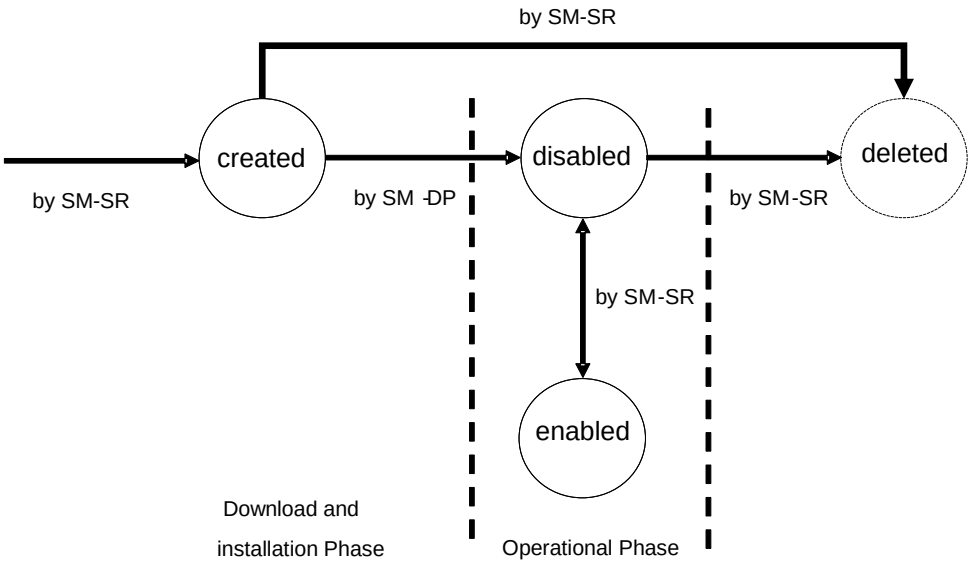

Figure 3: ISD-P State Diagram

In the created state shown in the diagram above, the Profile is downloaded and installed in the ISD-P. In the created, disabled or deleted state, the Profile is not visible to the machine to machine Device.

3.3 Relevant Roles and Functions

This section introduces and defines the relevant Roles and functions needed to support the remote Provisioning of Embedded UICCs.

The functions describe what actions are either performed internally by the role, or what actions are performed when communicating with another role or entity of the architecture. The role is agnostic to the business Actor to which this role is assigned.

3.3.1 Functions Definition

3.3.1.1 Functions for Data Preparation

3.3.1.1.1 Un-personalised Profile Creation

Un-personalised Profile Creation covers the building of the Un-personalised Profile based on the Operator's Profile Description and the type of eUICC targeted.

The SM-DP generates the Un-personalised Profile using the documentation provided by the Operator.

It is assumed the SM-DP tests the Un-personalised Profile with a sample of the target eUICC. The Operator validates the Un-personalised Profile by testing a sample of the target eUICC personalised with a test Personalised Profile created from the Un-personalised Profile developed by the SM-DP. The downloadable Profile SHALL be provided in a standardised format.

3.3.1.1.2 Profile Ordering

Profile ordering covers the processes for the preparation and generation of the Personalised Profiles by the SM-DP based on the input data provided by the Operator to the SM-DP. The input data includes (but is not limited to):

- The quantity of the Profiles to be generated;
- IMSI value(s) or range;
- ICCID value(s) or range;
- Un-personalised Profile type(s);
- Information about the target eUICC(s), such as the EID.

How and when the input data is provided by the Operator to the SM-DP is out of scope.

3.3.1.1.3 Generation of Personalisation Data

This function creates the credential and key values (e.g. NAC, PINs, OTA Keys) in a secure environment based on the input data provided by the Operator (e.g. IMSI, ICCID).

3.3.1.1.4 Profile Personalisation

SM-DP inserts the Personalisation Data into the Un-personalised Profile with respect to the order placed by the Operator. This function addresses the procedures which ensure a created Personalised Profile can only be installed on a specific eUICC.

3.3.1.1.5 EUM Services, Scripts, Tools or Documentation

To allow any SM-DP to undertake the above functions on any eUICC or the documentation supplied by the EUM must support at least the following eUICC attributes which MAY be delivered by the Operator. Some attributes are related to the function of Un-personalised Profile Creation and some to Profile Personalisation and in some cases the function to which they apply MAY be dependent on the particular eUICC.

The attributes are:

- Applications (and assignment of the applications) to be used or loaded, including USIM, ISIM, CAT and third party application SSDs;
- Algorithm selection, algorithm parameter assignment, and algorithm parameter loading within the eUICC platform;
- Application Key and PIN assignment and loading;
- Optional and variable data fields in the USIM application file structure;
- Additional data fields and file structures to support other applications – both SIM-based and device-based applications.

The information exchanged between the SM-DP and EUM is not standardised and MAY differ between different entities.

3.3.1.2 Functions for Profile Management

3.3.1.2.1 eUICC Eligibility Verification Function

The eUICC Eligibility Verification function covers the following aspects:

- Verification of the targeted eUICC for installing the Profile in preparation.
- Verification of the eUICC certification.

3.3.1.2.2 Profile Download and Installation Function

This function allows the download and installation of a Personalised Profile into the targeted eUICC.

3.3.1.2.3 Profile Content Update Function

This is handled by an Operator OTA Platform.

3.3.1.2.4 Policy Rules Update Function

This function updates the Policy Rules.

The Policy Rules to be updated MAY be the ones in the SM-SR, or the ones within a Profile already installed in the ISD-P on the eUICC.

3.3.1.2.5 Profile Lifecycle Management Authorisation Function

This covers the setting, unsetting and status enquiry of the PLMA in the SM-SR, initiated by the Operator.

3.3.1.3 Functions for Platform Management

3.3.1.3.1 ISD-P Creation Function

This function creates an ISD-P within the eUICC in preparation for Profile content to be loaded.

3.3.1.3.2 ISD-P Deletion Function

This function allows the deletion of an ISD-P. ISD-P deletion is the permanent removal of an ISD-P along with its content previously loaded and installed on the eUICC.

An ISD-P can be deleted only when it is in disabled state (see state diagram in section 3.2.3).

3.3.1.3.3 Master Delete Function

The Master Delete Function allows the deletion of an Orphaned Profile without the Fall-Back Attribute set regardless of the Profile's policy rules.

This function will delete the Profile and its ISD-P. The deletion of a Profile can only happen when the Profile is in disabled state and its Fall-Back Attribute is not set.

3.3.1.3.4 Profile Enabling Function

This function is used to Enable a Profile in Disable state.

This will make the applications and files within the Profile visible to and selectable by the M2M Device subject to relevant access control.

3.3.1.3.5 Profile Disabling Function

This function is used to Disable a Profile in Enable state.

This will make all applications and files within the Profile invisible to and not selectable by the Device.

3.3.1.3.6 Set Fall-Back Attribute

This function sets the Fall-Back Attribute of a Profile on the eUICC

3.3.1.3.7 Transport Function

Transport function refers to the establishing of the communication channel between the SM-SR and the ISD-R on the eUICC.

Security of transport channel between the SM-SR and eUICC is also addressed by this function.

NOTE: The eUICC within a Device MAY be contacted over different type of network systems (such as GSM, GPRS, UMTS, or EPS) by the SM-SR. Furthermore,

the SM-SR will need to interface with the concerned network system accordingly. For instance the SM-SR would need to use SMPP to be able to communicate with SMS, or it MAY need to connect to an IMS gateway in order to establish an IP-based communication with the eUICC. These communications are being provided by the active Subscription.

3.3.1.3.8 Policy Enforcement Function

This deals with the enforcement of the policy rules on the eUICC and at the SM-SR.

3.3.1.4 Functions for eUICC Management

3.3.1.4.1 eUICC Registration Function

This function is called to register an eUICC in an SM-SR.

3.3.1.4.2 SM-SR Change Function

This function is called to initiate the change the change of an SM-SR for an eUICC. SM-SR change is the transfer of the EIS for an eUICC from one SM-SR to another SM-SR and the establishment of new key set, in the ISD-R, between the new SM-SR and the eUICC.

3.3.1.5 eUICC Functions

3.3.1.5.1 Fall-Back Function

This function activates the Fall-Back Mechanism that disables the currently Enabled Profile and enables the Profile with Fall-Back Attribute set. For example, in the case of permanent loss of network connectivity for the Enabled Profile.

3.3.1.6 Device Functions

3.3.1.6.1 Local Enable of the Emergency Profile

This function enables the Device to enable the Emergency Profile.

3.3.1.6.2 Local Disable of the Emergency Profile

This function enables the Device to disable the Emergency Profile.

3.3.1.6.3 Local Enable of the Test Profile

This function enables the Device to enable the Test Profile.

3.3.1.6.4 Local Disable of the Emergency Profile

This function enables the Device to disable the Test Profile.

3.3.2 Void

3.4 Profile Description

3.4.1 General Content of a Profile Installed on an eUICC

The following data is part of a Profile:

- The Applications and files as defined in the relevant specifications (in particular 3GPP TS 31.102 [18], 3GPP TS 31.103 [19] and ETSI TS 102 221 [3]).

In addition to the above, the following data which is not included in the above standards:

- The algorithm parameters associated with its corresponding Network Access Application (for instance with Milenage: the OPc, ri, ci values);
- Policy Rules attached to the Profile (POL1).

3.4.2 Access to the Content of a Profile

For the Device the Enabled Profile is equivalent to an UICC.

For an Operator OTA Platform, the Enabled Profile is equivalent to an UICC as per ETSI TS 102 225 [6], TS 102 226 [7] and TS 102 223 [5]. The Policy Rules POL1 attached to the Profile are managed through the Operator OTA Platform, as per the rest of the content of the Profile.

An applet in the Enabled Profile will work the same manner as an applet in an UICC as per relevant ETSI and 3GPP standards.

3.5 Procedures

The procedures described in this section involve both interactions between the Roles of the business environment (e.g. between a Subscriber and a Telecommunication Service Provider) and between entities of the remote Provisioning architecture (e.g. between eUICC and SM-SR).

For each procedure the main steps as well as the related “Start conditions” and “End conditions” are described. “Start conditions” describe a set of prerequisites which must hold before the procedure can be performed. “End conditions” describe a set of results which will hold after the procedure has been performed.

The following main procedures for the Provisioning and lifecycle management of eUICCs and related Profiles are identified:

No	Name	Purpose
1	eUICC Registration at SM-SR	To register a newly manufactured eUICC at a given SM-SR as a prerequisite for subsequent remote management
2	Profile Ordering	For the Operator to order at the SM-DP a quantity of Profiles ready for download
3	Profile Download and Installation	To download a Profile to a given eUICC
4	Master Delete	To delete an Orphaned Profile in a given eUICC
5	Profile Enabling	To enable a Profile in a given eUICC via SM-SR
6	Profile Enabling via SM-DP	To enable a Profile in a given eUICC via SM-DP

7	Profile Disabling	To disable the Enabled Profile and enable the Profile with Fall-Back Attribute set.
8	ISD-P Deletion	To delete a Profile and its ISD-P from a given eUICC via SM-SR.
9	ISD-P Deletion via SM-DP	To delete a Profile and its ISD-P from a given eUICC via SM-DP.
10	SM-SR Change	To change the SM-SR of a given eUICC
11	ISD-P Key Establishment	Key establishment procedure between the SM-DP and the ISD-P. NOTE: This procedure is part of the Profile Download and Installation procedure.
12	Fall-Back Mechanism	To enable the Profile with Fall-Back Attribute set in a given eUICC
13	eUICC Certificate Check	To verify whether the targeted eUICC is certified.
14	ProfileLifecycle Management Authorisation Function	To set, to delete or to enquire the status of PLMA in the SM-SR
15	Profile Enabling via M2M SP	To enable a Profile in a given eUICC via M2M SP.
16	Profile Disabling via M2M SP	To disable the enabled Profile and to enable the Profile with Fall-Back Attribute set via M2M SP.
17	ISD-P Deletion via M2M SP	To delete a Profile and its ISD-P from a given eUICC via M2M SP.

3.5.1 eUICC Registration at SM-SR

eUICCs are manufactured, according to given standards, generally independent from Device makers, mobile operators or Telecommunication Service Providers. The Device manufacturers can select any certified eUICC that fits their purpose and order it in the necessary quantity directly from the EUM. In order to allow subscription management procedures, the EUM registers the eUICC at a selected SM-SR. This means that related information which is relevant throughout its further lifetime, in particular the Platform Management Credentials, Provisioning MSISDN, are stored in the SM-SR database. Without this step, remote access to the eUICC for the purpose of subscription management will be impossible.

NOTE: It is assumed that at this stage the eUICC does contain a Provisioning Profile and is linked to an active Provisioning Subscription. How the Provisioning operator is selected and the nature of the related commercial and technical agreements between the EUM and the Provisioning Operator are out of scope of this document.

The following represents a functional representation of the eUICC Information Set:

```
EIS = {   EID,
                Type, Version, Production Date,
                Platform Management Credentials, Certificate,
                Available Memory, Total Memory,
                SRID,
                { Profile 0: Profile Type, ISD-P AID, ICCID, MSISDN, State, DPID, Allocated Memory, POL2
                  Profile 1: Profile Type, ISD-P AID, ICCID, MSISDN, State, DPID, Allocated Memory,  POL2
                    …
                  Profile n: …
```

```
            }
        }
```

The eUICC registration comprises the following steps:

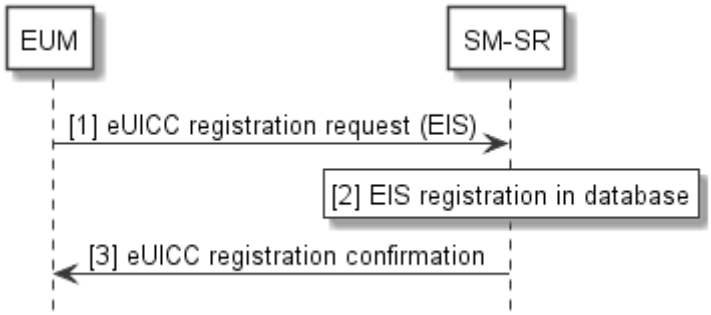

Figure 4: eUICC Registration at SM-SR

Start Condition: eUICCs are produced and a Provisioning Profile is loaded and active in the Provisioning operator's network. They are tested and ready for shipment. Each eUICC has a corresponding EIS.

Procedure:

1. The EUM sends a eUICC registration request to the selected SM-SR, containing the EIS.
2. The SM-SR stores the EIS in its database, with EID as the key parameter.
3. The SM-SR confirms the successful registration towards the EUM.

End Condition: The eUICC is registered at the SM-SR and ready for Platform and Profile Management operations.

Each eUICC MAY only be registered at one SM-SR. The communication link between the EUM and the SM-SR SHALL be secure.

3.5.2 Un-personalised Profile Verification (Proprietary)

Within the eUICC, the current functional scope of the UICC is represented by a Profile.

Similar to the verification of classic UICCs, Profiles SHALL be verified by the entity that creates the Profile, the SM-DP. For the verification of a Profile by the SM-DP, a similar procedure as for a classic UICC SHALL be used. One of the differences is that physical test eUICCs are only personalised by the SM-DP.

NOTE: The Profile verification processes and interfaces are not standardised and MAY differ between Operators and SM-DPs (Profile validation strategy, which tests MAY be performed by the Operator, which MAY be done by the SM-DP, what MAY be exchanged between the Operator and SM-DP, how this interface is secured, etc.).

For example, the Profile verification procedure MAY comprise the following steps:

Start Condition:

a. The Profile Description has been provided by the Operator to the SM-DP and the Un-personalised Profile has been generated by the SM-DP in a separate process.
b. The SM-DP has sample eUICCs of a specific type.

Procedure:

1. The Operator provides a test subscription to the selected SM-DP, as well as data such as applets, POL1 and Profile type. Other data, e.g. keys or ICCID, MAY be generated by the SM-DP.
2. The SM-DP creates a test Personalised Profile (Un-personalised Profile personalised with test data, including the data received from the Operator), then downloads and installs it onto an eUICC sample.
3. The SM-DP performs the necessary validation procedure to verify the combination of the eUICC sample and the test Personalised Profile.

End Condition: The Un-personalised Profile is valid and is now ready for the Profile ordering procedure for an eUICC type.

3.5.3 Profile Ordering (Proprietary)

Within the eUICC, the current functional scope of the UICC is represented by a Profile. Just as with current UICCs, Profiles are ordered under the responsibility of the Operator.

The same procedures SHALL apply with the only difference being that the UICCs are not produced in physical form but are kept at the SM-DP as Profiles.

NOTE: Profile ordering processes and interfaces are not standardised and MAY differ between Operators.

For example, the Profile ordering MAY comprise the following steps:

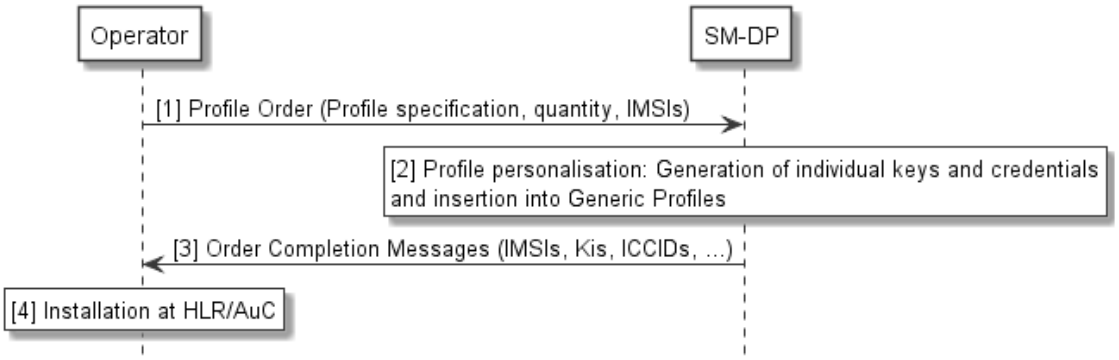

Figure 5: Profile Ordering

Start Conditions:

a. An Un-personalised Profile has been created by the SM-DP based on the Profile Description provided by the Operator.
b. The Operator has a demand for a quantity of eUICC Profiles.
c. The Un-personalised Profile has been validated on the target eUICC type using the Un-personalised Profile verification procedure in section 3.5.2

Procedure:

1. The Operator provides an order to a selected SM-DP. The order contains production data such as the quantity and a Start-IMSI, an IMSI range or a list of IMSIs and a reference to the Un-personalised Profile type. The POL1 and POL2 definitions for the Policy Rules to

be applied later by respectively the eUICC and SM-SR can also be delivered in this context.

2. The SM-DP then starts production, i.e. personalisation of Profiles using the data received from the Operator. Other data, e.g. keys or ICCID, MAY be generated by the SM-DP during the personalisation process. The Profiles are stored within the SM-DP.
3. Order completion is confirmed to the Operator, including all data necessary to register the Profiles in the Operator's backend systems. Each Profile is uniquely identified at least by its ICCID.
4. The Operator installs the Profiles in the related systems, e.g. HLR, AuC, CRM. These procedures are no different from current UICC registration processes at the Operator.

End Condition: The ordered quantity of Profiles is now ready for the Profile download procedure. Related Operator Credentials are available to the Operator.

3.5.4 Profile Download and Installation

In order for the Device to be used for communication services, the eUICC must be loaded with at least one Operational Profile. In general, this will be done over-the-air, using the Subscription represented by the currently Enabled Profile. If no other Operational Profile is enabled the Provisioning Profile is used.

The Profile download and installation procedure follows the following steps:

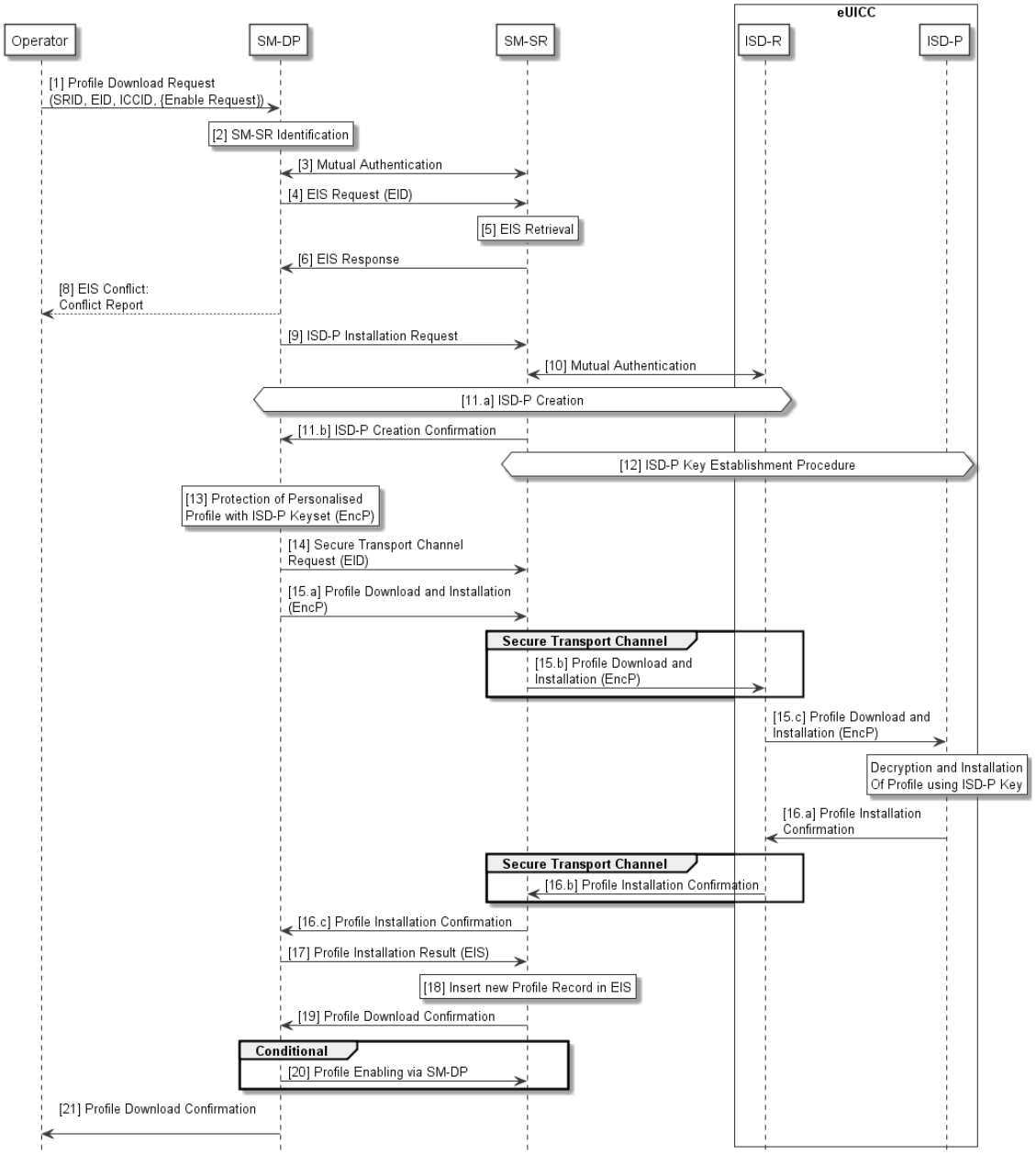

Figure 6: Profile Download

Start Conditions:

a. A Subscriber has subscribed to a selected Operator.
b. The EID of the target eUICC and the SRID are known by the Operator.
c. A Profile ordering procedure has been completed with a selected SM-DP.
d. The target eUICC is integrated into a Device and is associated to an SM-SR.
e. The Operator MAY activate the related Subscription in the network by the ICCID.

Procedure:

1. The Operator sends a Profile Download request to the SM-DP. The request must include the relevant information to allow the identification of the SM-SR, the target EID and ICCID.

   The Operator MAY also ask the SM-DP to enable the Profile once it is downloaded and installed.

2. Based on the information provided by the Operator, the SM-DP identifies the SM-SR, where the eUICC is currently registered.
3. The SM-SR and the SM-DP authenticate each other if not already authenticated.
4. The SM-DP requests from the SM-SR the EIS for that particular eUICC, identified by its EID.
5. Based on the EID, the SM-SR retrieves the EIS.
6. The SM-SR sends the relevant information from the EIS to the requesting SM-DP.

   NOTE: The rationale for saying “relevant information from the EIS” is that the SM-SR will not provide information to the SM-DP that is not appropriate for the particular SM-DP.
7. The SM-DP checks the eligibility of the eUICC (e.g. type, certificate and memory) based upon the received information from the EIS.
8. If a problem is detected with the eligibility of the eUICC, the SM-DP aborts the procedure and returns an error message to the requesting Operator.
9. If no problem is detected with the eligibility of the eUICC, the SM-DP issues an installation request for the ISD-P to the SM-SR.
10. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
11. The SM-SR contacts the ISD-R on the eUICC for ISD-P installation and an empty ISD-P is created in the eUICC. This is confirmed back to the SM-DP.
12. The SM-DP and the eUICC authenticate each other and a shared key set is established between the ISD-P and the SM-DP through the SM-SR. The Key Establishment Procedure is described in Security Section 4.5.
13. Now the SM-DP selects the Personalised Profile (e.g. based on the ICCID or Profile type) and protects it using the new ISD-P key set, producing the encrypted and integrity protected Profile EncP.
14. The SM-DP asks the SM-SR to establish a secure transport channel between the ISD-R on the eUICC and the SM-SR. This secure transport channel is for protection of Profile management commands not the Profile itself.
15. The SM-DP initiates the Profile Download and Installation by sending the EncP to the eUICC using a secure channel between the SM-DP and the newly created ISD-P on the eUICC, and within the established secure transport channel between the SM-SR and the ISD-R on the eUICC.
16. The eUICC sends the result of the installation of the Profile to the SM-DP.

    The Operator owner of the Profile decides whether, at the end of Profile installation, the SCP03 key set in the ISD-P SHALL be removed by the SM-DP, retained by the SM-DP or be handed over to the Operator.

    NOTE: If the Operator decides that the key set is retained by the SM-DP the Operator can instruct the SM-DP to handover or delete the key set at a later point in time.
17. SM-DP sends the result of the installation of the Profile to the SM-SR. This message includes the relevant EIS elements for this Profile.
18. The SM-SR updates its database. If the download and installation was successful, the SM-SR inserts a new Profile record into the EIS, with the status “disabled”.

19. The SM-SR confirms the status of the Profile download and installation back to the SM-DP.
20. If the Operator asked the SM-DP to enable the Profile once it is downloaded and installed, the SM-DP executes the Profile Enabling via SM-DP procedure (see 3.5.7).
21. The SM-DP confirms the status of the download and installation back to the Operator. This message includes the information to identify the Profile.

End Condition: An ISD-P has been created in the eUICC for the Operator, containing a Profile in disabled or enabled state. The SM-SR has updated the EIS for this eUICC accordingly.

3.5.5 Master Delete

This procedure deletes an Orphaned Profile without the Fall-Back Attribute set regardless of the Profile's Policy rules.

The successful execution of this procedure requires the authorisation of both the Initiator and the SM-DP.

NOTE: The actor who assumes the role of the initiator needs to be determined. In the example below we can assume the initiator will be the new Operator with the authorisation of the Subscriber.

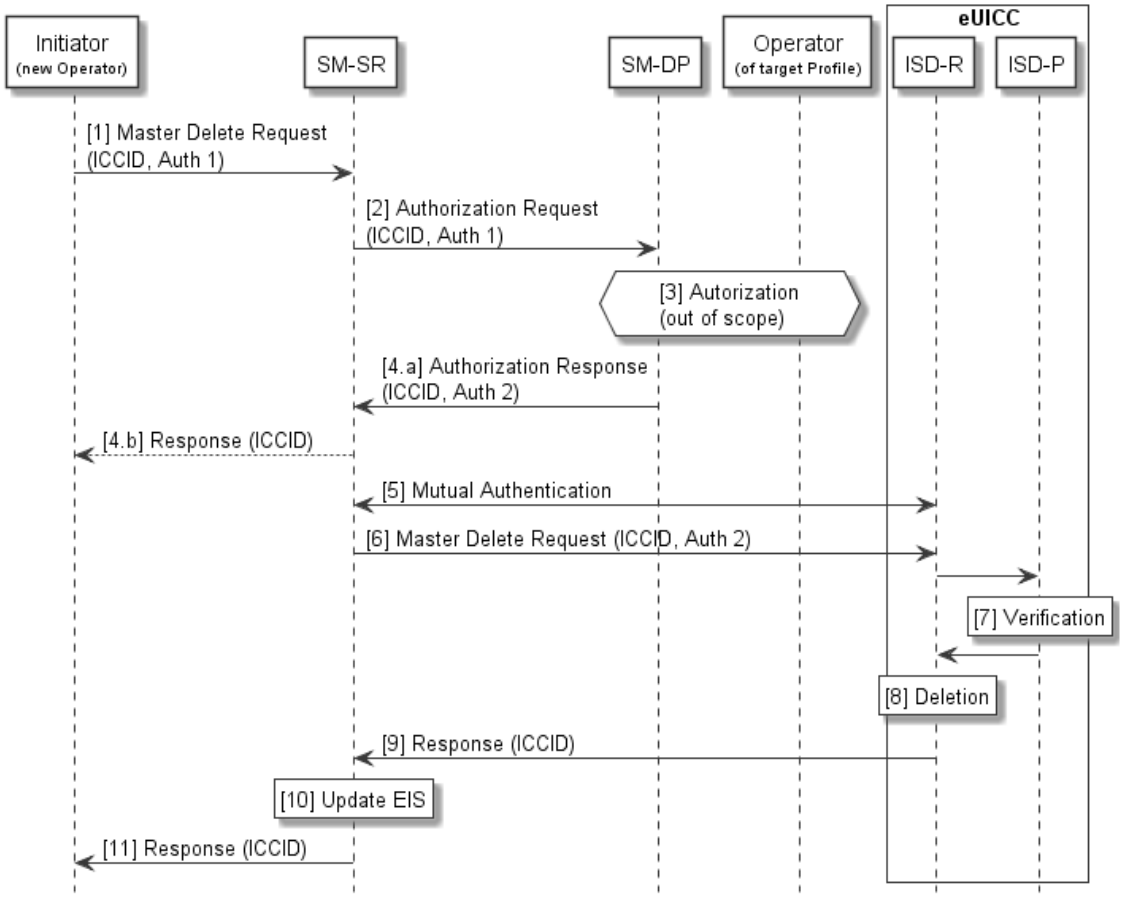

Figure 7: Master Delete

Start Conditions:

a. There is an Orphaned Profile on a eUICC which is, for example, blocking the loading of another Profile.
b. The Orphaned Profile cannot be deleted using the normal ISD-P deletion procedure.
c. The Initiator decides to delete the Orphaned Profile on the eUICC.
d. The Orphaned Profile is disabled.

Procedure:

1. The Initiator sends a master delete request to the SM-SR. The request includes the target EID and the ICCID of the target Profile. The request includes the Initiator's authorisation (Auth 1) for the master delete.
2. The SM-SR sends the authorisation request together with the initiator authorisation (Auth 1) to the SM-DP associated with the target Profile. The SM-DP verifies the authorisation (Auth 1).
3. The SM-DP also requests authorisation from the Operator owner of the target Profile.

   NOTE: The definition of this interface is out of the scope of this document.
4. If the Operator authorises the deletion or if there is no response from the Operator, the SM-DP sends a response to the SM-SR containing the SM-DP's authorisation (Auth 2) for the master delete. If the SM-DP does not give its authorisation for the master delete the SM-SR informs the Initiator.
5. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
6. The SM-SR sends the master delete request to the ISD-R on the eUICC. The request includes the ICCID of the target Profile and the authorisation of the SM-DP (Auth 2).
7. The ISD-P of the target Profile verifies the authorisation, thus verifying the master delete command.
8. The ISD-R deletes the target Profile and the related ISD-P without Policy Rule enforcement.
9. The ISD-R reports the status of the master delete to the SM-SR.
10. The SM-SR updates the EIS accordingly.
11. The SM-SR reports the status of the master delete to the Initiator.

End Condition: The target Profile is deleted from the eUICC. The EIS in the SM-SR is up to date.

3.5.6 Profile Enabling

A switch between two Profiles can be achieved by the following dedicated procedure. In this case the request is issued directly by the Operator to the SM-SR associated with the target eUICC.

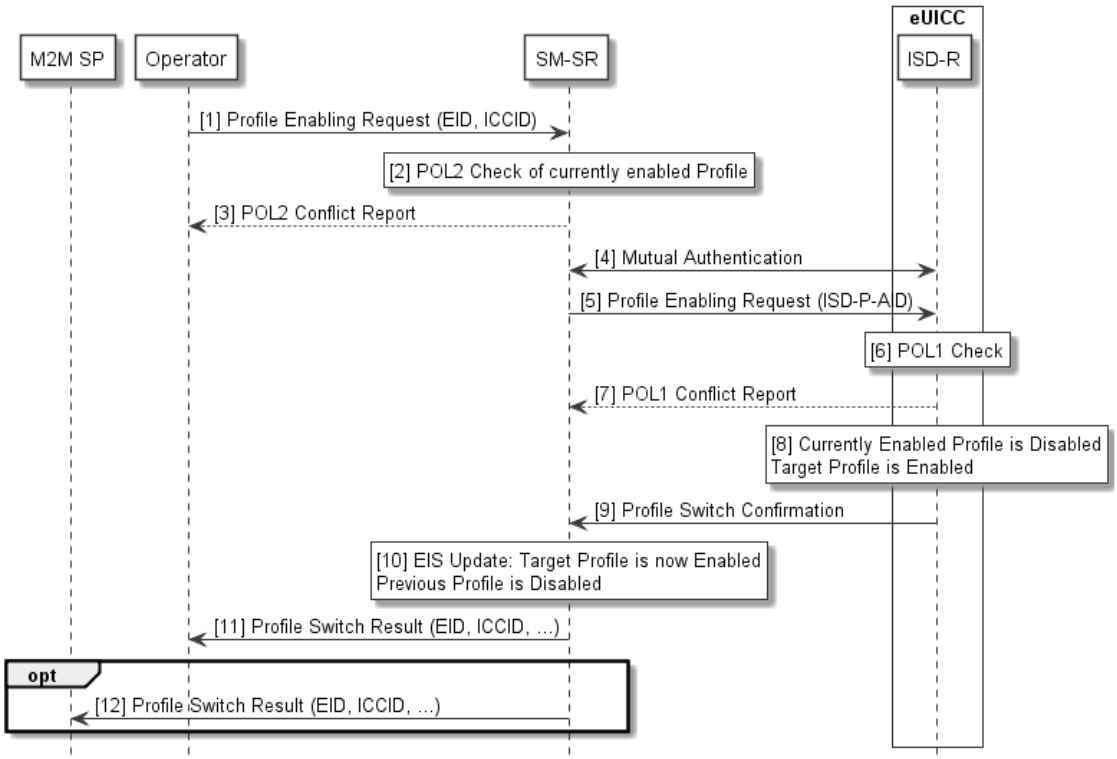

Figure 8: Profile Enabling

Start Conditions:

a. The target Profile is disabled on the eUICC. Another Profile is enabled.
b. The Subscription associated with the target Profile is active in the Operator's network.
c. The EID of the target eUICC, the SRID associated with the target Profile and the ICCID of the target Profile are known by the Operator.

Procedure:

1. The Operator sends a Profile Enabling request to the SM-SR. The request includes the target EID and at least the ICCID of the target Profile.
2. The SM-SR checks if the POL2 of the currently Enabled Profile permits the Profile switch to take place.
3. If there is a conflict with POL2, the SM-SR aborts the procedure and informs the concerned Operator accordingly.
4. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
5. If there is no conflict with POL2, the SM-SR issues a Profile Enabling request to the ISD-R on the eUICC including at least the ISD-P AID of the target Profile.
6. The eUICC performs a POL1 check.
7. If there is a conflict with POL1, the ISD-R aborts the procedure and informs the SM-SR.
8. If there is no conflict with POL1, the ISD-R performs the Profile switch resulting in the target Profile being enabled and the previously Enabled Profile being disabled.
9. The ISD-R reports the Profile switch result to the SM-SR.

10. If the switch is successful the SM-SR records in the EIS that the target Profile is enabled and the previous Profile is disabled.
11. The SM-SR reports the Profile switch result back to the Operator(s). These messages will include the EID and the ICCID of their respective Profiles.
12. The SM-SR SHALL report the Profile switch result back to the M2M SP if requested by the Operator during PLMA registrations (see 3.5.155) . These messages will include the EID and the ICCID of the targeted Profiles.

End Condition: The target Profile is enabled on the eUICC. The previously Enabled Profile is disabled. The EIS is up to date.

3.5.7 Profile Enabling via SM-DP

A switch between two Profiles can be achieved by the following dedicated procedure.

In this case, the request is issued by the Operator to the SM-DP which forwards it to the SM-SR associated with the target eUICC. This way, the Operator does not have to be linked to the SM-SR and relies on the SM-DP to make the connection.

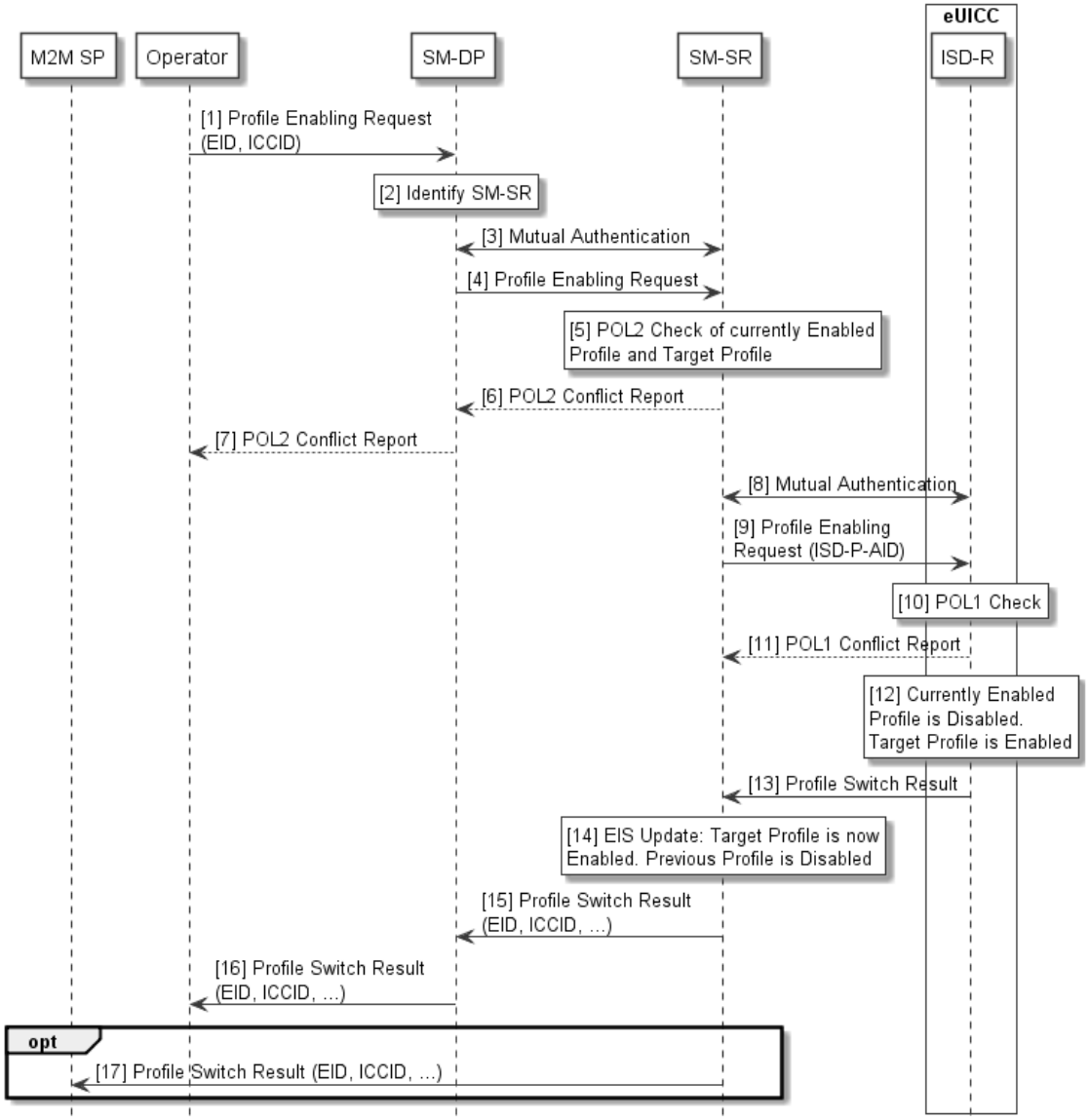

Figure 9: Profile Enabling via SM-DP

Start Conditions:

a. The target Profile is disabled on the eUICC. Another Profile is enabled.
b. The Subscription associated with the target Profile is active in the Operator's network.
c. The EID of the target eUICC, the SRID and the ICCID of the target Profile are known by the Operator.

Procedure:

1. The Operator sends a Profile Enabling request to the SM-DP. The request includes the target EID and at least the ICCID of the target Profile.
2. The SM-DP identifies the related SM-SR.
3. The SM-SR and the SM-DP authenticate each other if not already authenticated.
4. The SM-DP forwards the Profile Enabling request to the SM-SR.
5. The SM-SR checks if the POL2 of the currently Enabled Profile permits the Profile switch to take place.

6. If there is a conflict with POL2, the SM-SR aborts the procedure and informs the requesting SM-DP.
7. If there is a conflict with POL2, the error message is forwarded by the SM-DP to the requesting Operator.
8. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
9. If there is no conflict with POL2, the SM-SR issues a Profile Enabling request to the ISD-R on the eUICC including at least the ISD-P AID of the target Profile.
10. The eUICC performs a POL1 check.
11. If there is a conflict with POL1, the ISD-R aborts the procedure and informs the SM-SR.
12. If there is no conflict with POL1, the ISD-R performs the Profile switch resulting in the target Profile being enabled and the previously enable Profile being disabled.
13. The ISD-R reports the Profile switch result to the SM-SR.
14. If the switch is successful the SM-SR records in the EIS that the target Profile is enabled and the previous Profile is disabled.
15. The SM-SR reports the Profile switch result back to the requesting SM-DP and the SM-DP or Operator of the disabled Profile. These messages will include the EID and the ICCID of their respective Profiles.
16. The Profile switch result is forwarded to the requesting Operator.
17. The SM-SR SHALL report the Profile switch result back to the M2M SP if requested by the Operator during PLMA registration (see 3.5.15). These messages will include the EID and the ICCID of the targeted Profiles.

End Condition: The target Profile is enabled on the eUICC. The previously Enabled Profile is disabled. The EIS is up to date.

3.5.8 Profile Disabling

Profile disabling can be achieved by the following procedure. The request is issued directly by the Operator to the SM-SR associated with the target eUICC.

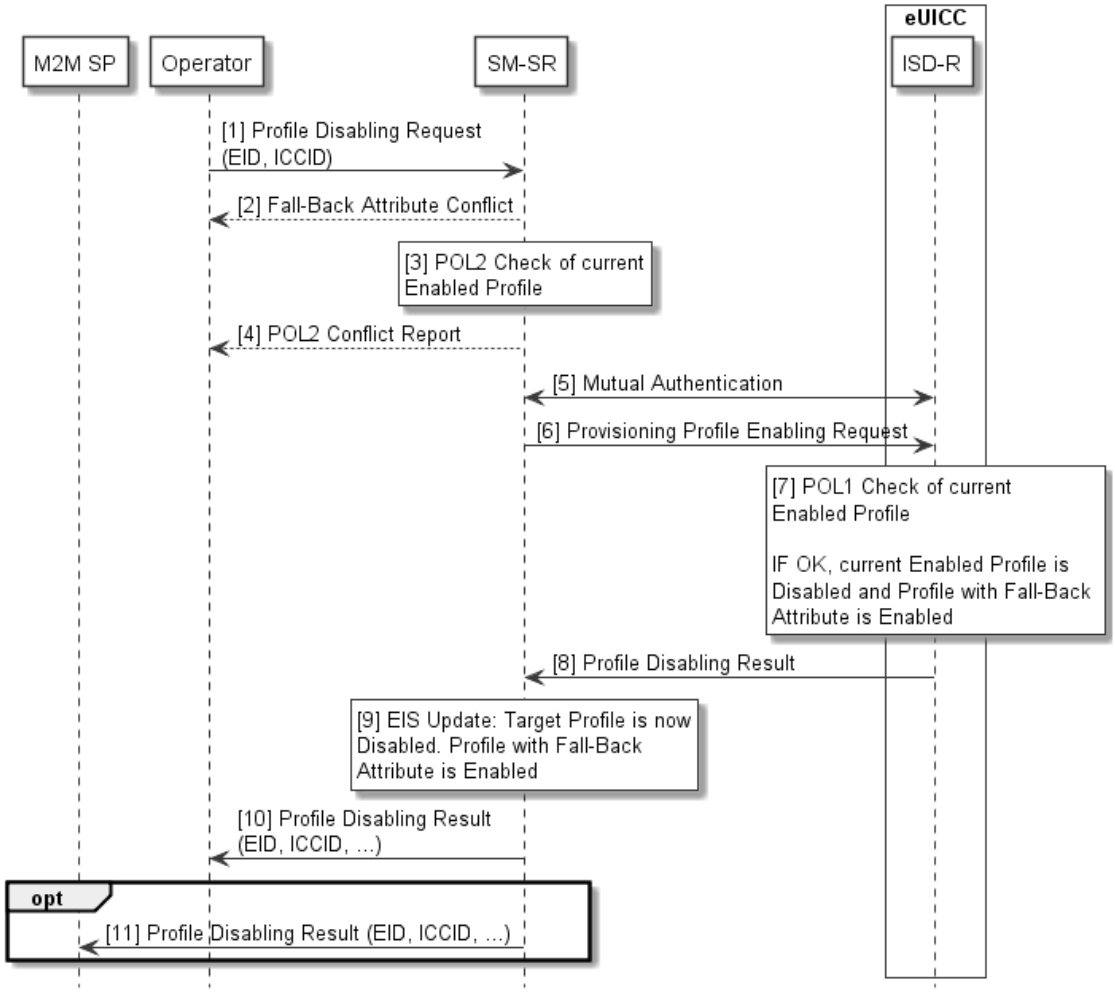

Figure 10: Profile Disabling

Start Condition: The target Profile is enabled on the eUICC.

Procedure:

1. The Operator sends a Profile Disabling request to the SM-SR. The request includes the target EID and at least the ICCID of the target Profile.
2. If the target Profile for disabling is the Profile with Fall-Back Attribute set then the Profile disabling SHALL NOT be executed.
3. The SM-SR checks if the POL2 of the Enabled Profile permits the Profile to be disabled
4. If there is a POL2 conflict, the SM-SR aborts the procedure and send error message to Operator.
5. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
6. If there is no POL2 conflict, the SM-SR issues a Profile enabling request to the ISD-R on the eUICC for the Profile with Fall-Back Attribute set.
7. The eUICC performs an internal POL1 check for the currently Enabled Profile, and verifies that the currently Enabled Profile does not have the Fall-Back Attribute set. If permitted, the Enabled Profile is disabled and the ISD-R enables the Profile with Fall-Back Attribute set.
8. The ISD-R sends reports the Profile disabling result to the SM-SR.

9. If the disabling is successful the SM-SR records in the EIS that the target Profile is disabled.
10. The SM-SR reports the Profile disabling result to the Operator(s). This message includes the EID and the ICCID of the Profile(s).
11. The SM-SR SHALL report the Profile disabling result back to the M2M SP if requested by the Operator during PLMA registration (see 3.5.155). These messages will include the EID and the ICCID of the targeted Profiles.

End Condition: The target Profile is now disabled on the eUICC, and the Profile with Fall-Back Attribute set is enabled.

3.5.9 ISD-P Deletion

A Profile can be deleted by its Operator.

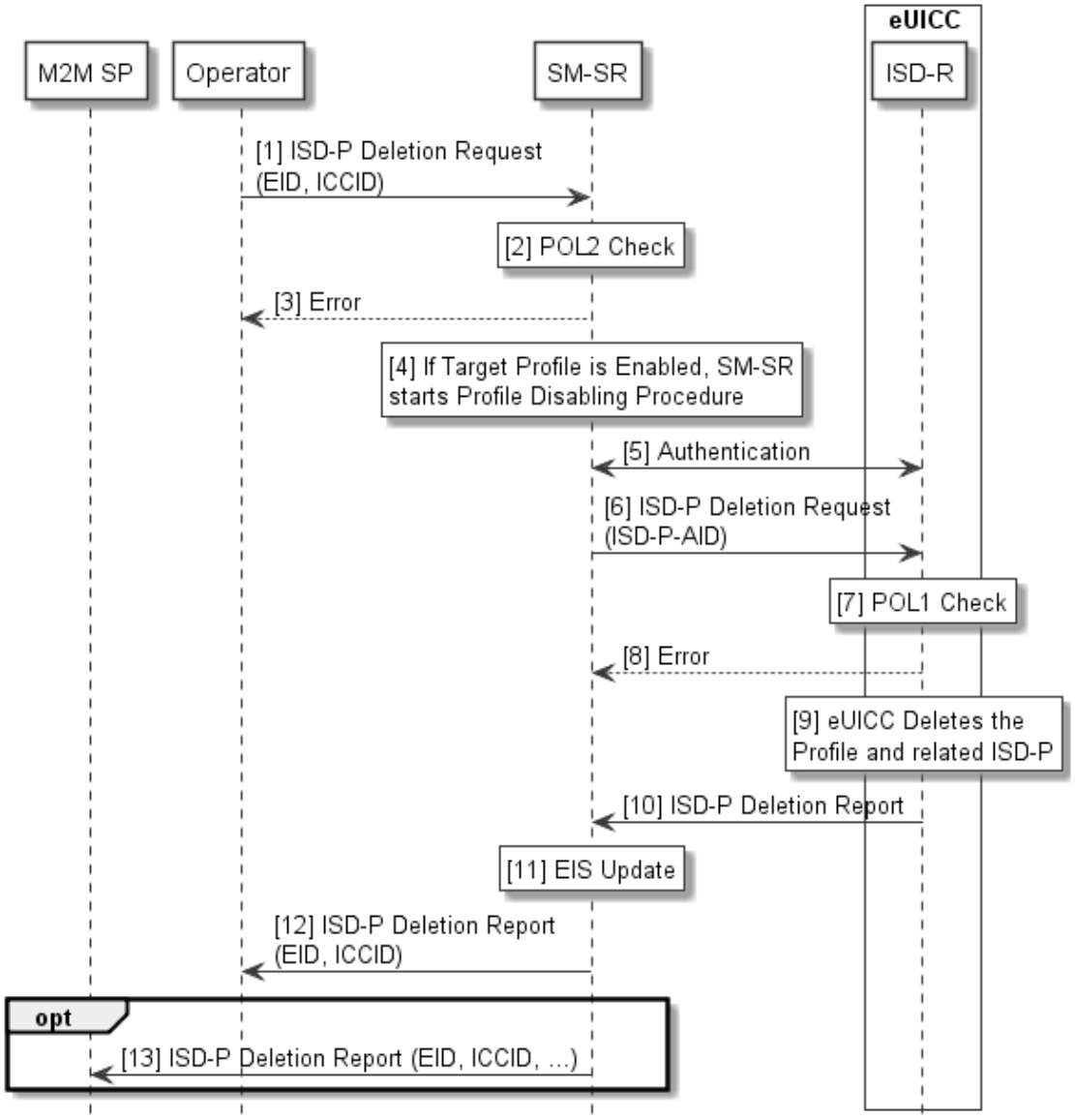

Figure 11: ISD-P Deletion

Start Condition: The Operator decides to permanently delete a Profile on a eUICC.

Procedure:

1. The Operator sends an ISD-P Deletion request to the SM-SR. The request includes the target EID and the ICCID of the target Profile.
2. The SM-SR checks the POL2 of the target Profile, and verifies that the target Profile does not have the Fall-Back Attribute set.
3. If there is a conflict with POL2 or with the Fall-Back Attribute, the SM-SR aborts the procedure and informs the Operator(s) accordingly
4. If the target Profile is enabled, the SM-SR starts the Profile Disabling procedure.
5. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
6. The SM-SR sends the ISD-P Deletion request to the ISD-R on the eUICC. The request includes the ISD-P AID of the target Profile.
7. The eUICC performs a POL1 check and a Fall-Back Attribute check.
8. If there is a conflict with POL1 or with the Fall-Back Attribute, the ISD-R aborts the procedure and informs the SM-SR.
9. If there is no conflict, the ISD-R then erases the target Profile and the related ISD-P.
10. The ISD-R reports the status of the ISD-P deletion to the SM-SR.
11. The SM-SR updates the EIS appropriately.
12. The SM-SR reports the status of the ISD-P deletion to the requesting Operator.
13. The SM-SR SHALL report ISD-P deletion result back to the M2M SP if requested by the Operator during PLMA registration (see 3.5.15). These messages will include the EID and the ICCID of the targeted Profiles.

End Condition: The target Profile is deleted from the eUICC. The EIS in the SM-SR is up to date.

3.5.10 ISD-P Deletion via SM-DP

A Profile can be deleted by its Operator.

ISD-P deletion would be requested via the SM-DP. In this case, the Operator does not have to be linked to all SM-SRs and relies on the SM-DP to make the connection.

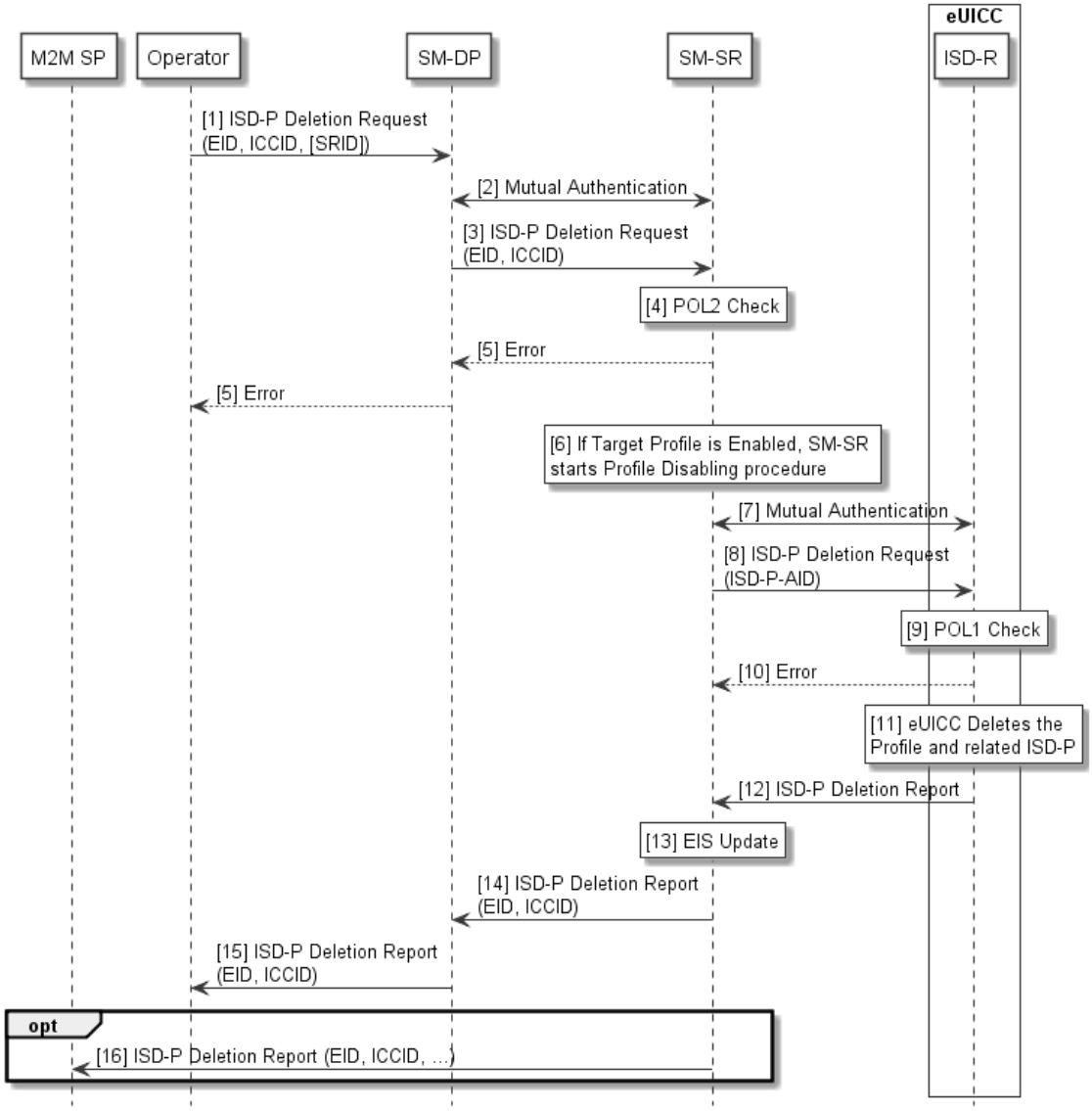

Figure 12: Operational Profile Deletion via SM-DP

Start Condition: The Operator decides to permanently delete a Profile on a eUICC.

Procedure:

1. The Operator sends an ISD-P Deletion request to the SM-DP. The request includes the target EID and the ICCID of the target Profile. The Operator MAY also provide the SRID.
2. The SM-SR and the SM-DP authenticate each other if not already authenticated.
3. If the SRID was not provided by the Operator the SM-DP identifies the related SM-SR. The request is passed on to the dedicated SM-SR.
4. The SM-SR checks the POL2 and the Fall-Back Attribute of the target Profile.
5. If there is a conflict with POL2 or with the Fall-Back Attribute, the SM-SR aborts the procedure and informs the Operator(s) accordingly
6. If the target Profile is enabled, the SM-SR starts the Profile Disabling procedure.
7. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.

8. The SM-SR sends an ISD-P Deletion request to the ISD-R on the eUICC. The request includes the ISD-P AID of the target Profile.
9. The eUICC performs a POL1 check and a Fall-Back Attribute check.
10. If there is a conflict with POL1 or with the Fall-Back Attribute, the ISD-R aborts the procedure and informs the SM-SR.
11. If there is no conflict, the ISD-R then erases the target Profile and the related ISD-P.
12. The ISD-R reports the status of the ISD-P deletion to the SM-SR.
13. The SM-SR updates the EIS appropriately.
14. The SM-SR reports the status of the ISD-P deletion to the requesting SM-DP.
15. The SM-DP reports the status of the ISD-P deletion to the requesting Operator.
16. The SM-SR SHALL report ISD-P deletion result back to the M2M SP if requested by the Operator during PLMA registration (see 3.5.15). This message will include the EID and the ICCID of the targeted Profile.

End Condition: The target Profile is deleted from the eUICC. The EIS in the SM-SR is up to date.

3.5.11 SM-SR Change

This procedure assumes that, prior to the procedure being executed, the Operators with installed Profiles on the concerned eUICC might request to be informed of the change by the current SM-SR ($SM\text{-}SR_1$) and be allowed to take action as it relates to the desired disposition of their Profile (e.g. do nothing, update Policy rules, delete the Profile).

In the case where the SM-SR has to be changed, the credentials of the individual eUICCs must remain confidential.

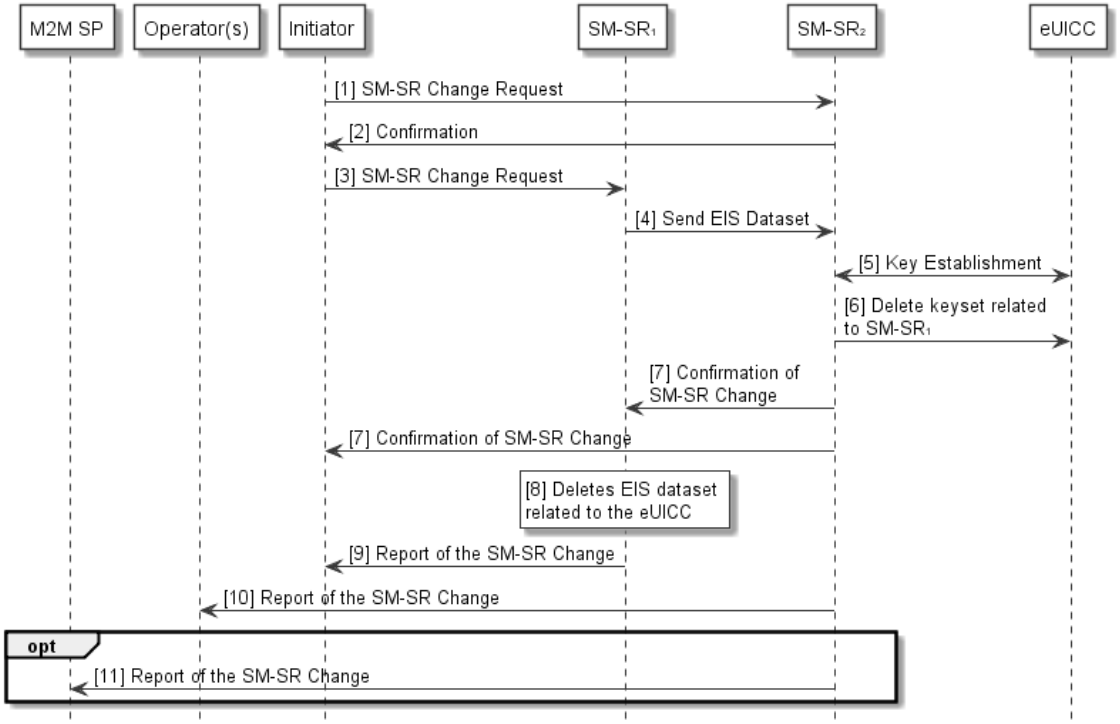

Figure 13: SM-SR Change

Start Conditions:

a. The EID of the eUICC is known
b. The SRIDs of SM-SR1 and SM-SR2 are known.
c. The ISD-R is personalised with the keys of SM-SR1.
d. The change of SM-SR is allowed.

Procedure:

1. The initiator sends a request to SM-SR_2 for a change of SM-SR.
2. SM-SR_2 confirms that it can take over this role.
3. The initiator, or SM-SR_2 acting for the initiator, requests the change from SM-SR_1.
4. SM-SR_1 sends the EIS dataset of the specified EID to SM-SR_2.
5. A new shared key set is established between SM-SR_2 and the ISD-R via the secure channel provided by SM-SR_1. The Key Establishment Procedure is described in the Annex D.2.
6. Now SM-SR_2 can address the ISD-R directly, and SM-SR_2 requests the eUICC to delete the key set related to SM-SR_1.
7. SM-SR_2 sends a confirmation of the change to the SM-SR_1.
8. SM-SR_1 deletes the EIS dataset related to the eUICC.
9. SM-SR_1 sends a response to the Initiator, indicating the success of the overall SM-SR change operation.
10. SM-SR_2 sends a report to the Operator owner(s) of the Profile(s) on the eUICC, either directly or via the SM-DP, of the change of SM-SR.
11. If applicable, SM-SR_2 sends a report to the M2M SP managing the eUICC.

End Conditions:

a. The ISD-R is personalised with the keys of the target SM-SR (SM-SR2).
b. The eUICC is registered within the target SM-SR (SM-SR2).
c. The EIS and EID reside within the target SM-SR (SM-SR2).
d. SM-SR1 is no longer related to the eUICC.
e. The Operator(s) owner of the Profile(s) is/are aware of the change.
f. The M2M SP managing the eUICC is aware of the change.

NOTE1: This procedure MAY not support the transfer of the PLMA. If such transfer is supported, this is out of scope of this specification. In all cases, the Operator MAY set the same or different PLMA on SM-SR2, as described in procedure 3.5.15.1.

NOTE2: In this procedure, the Initiator SHOULD be the Operator1 as it is the one requesting the transfer from SM-SR1 to SM-SR2.

3.5.12 ISD-P Key Establishment Procedure

This procedure is defined within section 4.5 of this document.

3.5.13 Fall-Back Mechanism

In the event of loss of network connectivity, as detected by the Device, there is a need to change to the Profile with Fall-Back attribute set. In this *c*ase the eUICC disables the currently Enabled Profile (Profile A) and enables the Profile with Fall-Back Attribute set (Profile B). If Profile A has POL1 rule “disable not allowed” set then the eUICC will overrule this setting. If Profile A has POL1 rule “Profile deletion is mandatory when it is disabled” set, the eUICC SHALL NOT automatically delete this Profile.

For security reasons if Profile A has the POL1 rule “disabled not allowed” or “Profile deletion is mandatory when it is disabled” set then the eUICC can only switch back to Profile A except if Profile A has been deleted by use of the Master Delete function. Profile A cannot be deleted with a normal delete command in this situation.

Start Conditions:

a. The Device reports network loss to the eUICC.
b. The eUICC is configured to perform the Fall-Back mechanism if certain network connectivity issues are reported by the Device.
c. The Profile with Fall-Back attribute set is not the presently Enabled Profile.

Procedure:

1. The eUICC disables the currently Enabled Profile (overruling POL1 if necessary) and enables the Profile with Fall-Back Attribute set.
2. The eUICC reports the change of Enabled Profile to the SM-SR. The SM-SR updates the EIS.
3. The SM-SR reports the change to the respective owners of the targeted Profiles. and to the M2M SP, if requested by the Operator during PLMA registration (see 3.5.15).

End Condition: The eUICC has enabled the Profile with Fall-Back Attribute set and the EIS of the SM-SR is up-to-date.

3.5.14 eUICC Certificate Verification

This procedure defines how an SM-DP on behalf of the Operator can verify if an eUICC is certified, in particular if the eUICC is designed according to the present specification.

Procedure:

1. The OperatorSM-DP, SHALL be able to retrieve the eUICC certificate from:
   a. The EIS stored within the SM-SR in which the eUICC is registered

   OR

   b. The EUM

      NOTE: this interface is out of scope of this document).
2. The SM-DP extracts the EUM information from the eUICC certificate (for example: certificates, SAS-UP [23 UP [23] accreditation etc.).
3. With the information retrieved at step 2, the SM-DP requests the EUM certificate from the SM-SR, the EUM or the GSMA.

   NOTE: The interface to the EUM and GSMA are out of the scope of this document).
4. The SM-DP verifies the validity and signature of the EUM certificate.
5. The SM-DP verifies the EUM signature of the eUICC certificate.

End Condition: The eUICC certificate and EUM certificate have been checked by the SM-DP.

3.5.15 Profile Lifecycle Management Authorisation Registration at SM-SR

In some circumstances, on one hand, an M2M SP MAY have to manage the lifecycle of Operator Profiles by its own, and to be notified of any change in Operator Profiles lifecycle on the eUICCs they are responsible for.

On the other hand, it is important for an Operator to be able to control which M2M SP is allowed to perform Profile Lifecycle Management on Operator's Profile(s).

The Profile Lifecycle Management Authorisation (PLMA) mechanisms described in this chapter will allow Operators to provide Profile Lifecycle Management functionality to an M2M SP while keeping the control of allowed commands and reports.

Furthermore, an Operator might be willing to receive or not reports when an authorised M2M SP is changing the lifecycle of its own Profile(s).

All PLMA requests defined below will require a prior mutual authentication between the Operator and the SM-SR.

In case an Operator does not have a dedicated interface with an SM-SR, it SHALL be possible to manage PLMA via its SM-DP interface. The SM-DP SHALL forward PLMA management commands to the SM-SR without any further processing and SHALL NOT host any PLMA.

NOTE: It SHOULD be considered that the role of an M2M SP can also be played by a partner Operator or affiliate from the Operator.

3.5.15.1 Set Profile Lifecycle Management Authorisation

This procedure sets the PLMAs on the SM-SR and includes which Platform Management commands are allowed to be executed by an M2M SP and which reports SHALL be sent to M2M SP and Operator.

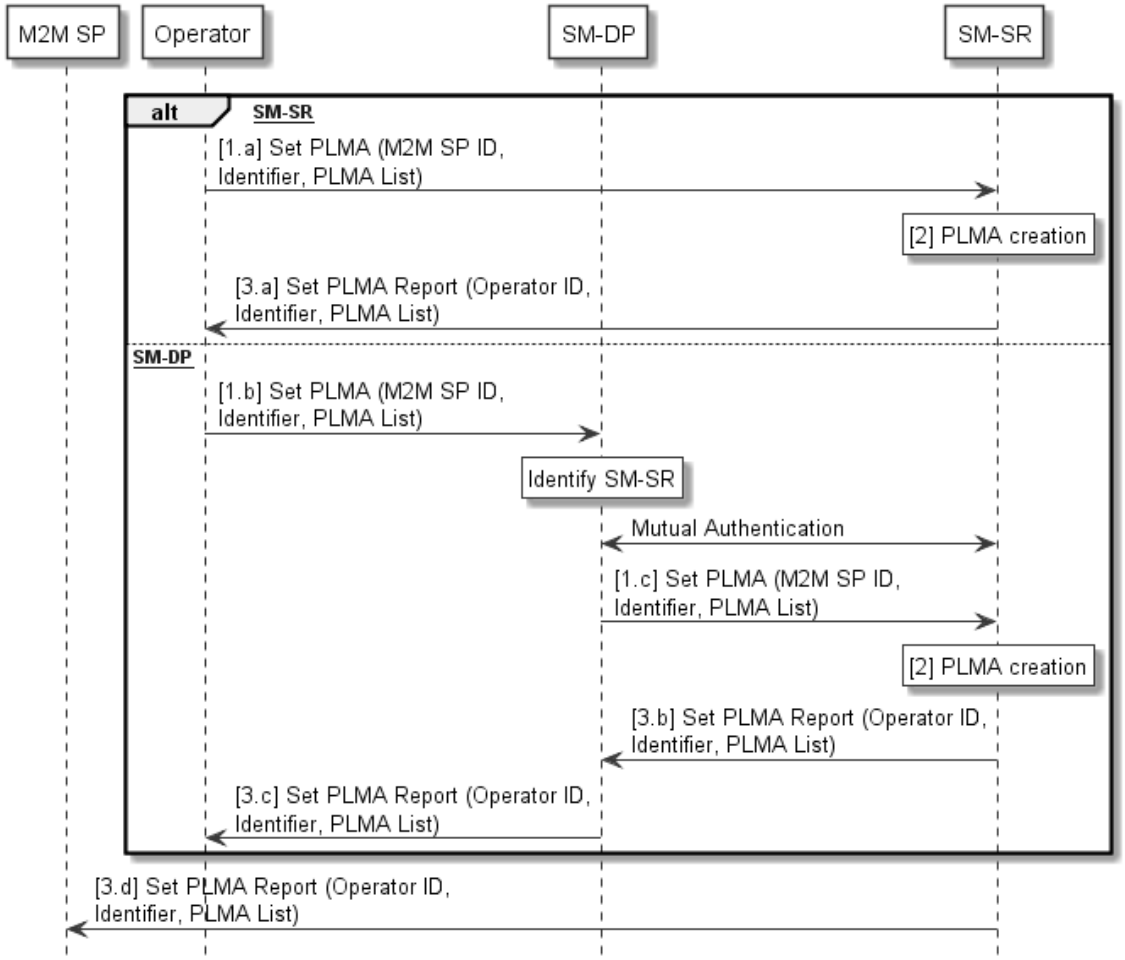

Figure 14: Set Profile Lifecycle Management Authorisation

Start Condition:

The Operator opened a dedicated interface with the SM-SR, either directly or through its SM-DP, for PLMA management.

Procedure:

1. The Operator whose Profile is resident on a set of eUICCs sends a PLMA request to the SM-SR managing those eUICCs, either directly (1.a) or through its SM-DP (1.b, 1.c), to set PLMA.
2. The SM-SR creates the corresponding PLMA for a specific set of eUICCs and/or Profiles based on dedicated identifier provided to the SM-SR.
3. The SM-SR confirms the successful creation of the PLMA by notifying the requesting Operator, either directly (3.a) or through its SM-DP (3.b, 3.c), as well as the correspondent M2M SP (3.d).

NOTE: The definition of needed identifier to set the PLMA on eUICC and /or Profiles is out of scope of this specification.

End Condition: The SM-SR has set the Profile Lifecycle Management functionality for the addressed M2M SP. The M2M SP is able to manage the lifecycle of the targeted Profile on a set of eUICCs and to receive reports related to those Profiles. In case of change done on the referenced Profile by the referenced M2M SP, the Operator is receiving relevant reports.

The Operator is able to send the set PLMA requests only for its own Profiles. Any changes to the PLMA (e.g. removal of reports to be sent to M2M SP) must be done by this procedure. Depending on the Operator choice, the PLMA will allow:

a. The referenced M2M SP to:
    - Request to enable the referenced Profile.
    - Request to disable the referenced Profile.
    - Request to delete the referenced Profile.
    - Request to set the Fall-Back Attribute on the referenced Profile.
    - Un-Set the Fall-Back Attribute on the referenced Profile as a result of setting it on another Profile.
    - Request to set the Emergency Profile Attribute on the referenced Profile.
    - Un-Set the Emergency Profile Attribute on the referenced Profile as a result of setting it on another Profile.
b. The referenced M2M SP to receive reports on:
    - Referenced Profile enabling.
    - Referenced Profile disabling.
    - Referenced Profile deletion.
    - Referenced Profile Fall-Back Attribute setting/un-setting.
    - Referenced Profile Emergency Profile Attribute setting/un-setting.
c. Optionally (if supported by the SM-SR), the Operator to not receive reports on:
    - Referenced Profile enabling.
    - Referenced Profile disabling.
    - Referenced Profile deletion.
    - Referenced Profile Fall-Back Attribute setting/un-setting.
    - Referenced Profile Emergency Profile Attribute setting/un-setting.

NOTE: When no PLMA is provided to the M2M SP but the M2M SP has the need to get status changes on Profiles being resident on eUICCs it is responsible for, it is up to the Operator, owning the Profiles on the eUICC, to forward reports about Profile status changes to the correspondent M2M SP. This is outside of this specification.

3.5.15.2 Retrieve Profile Lifecycle Management Authorisation– by Operator

With this procedure the Operator retrieves the PLMA set on the SM-SR.

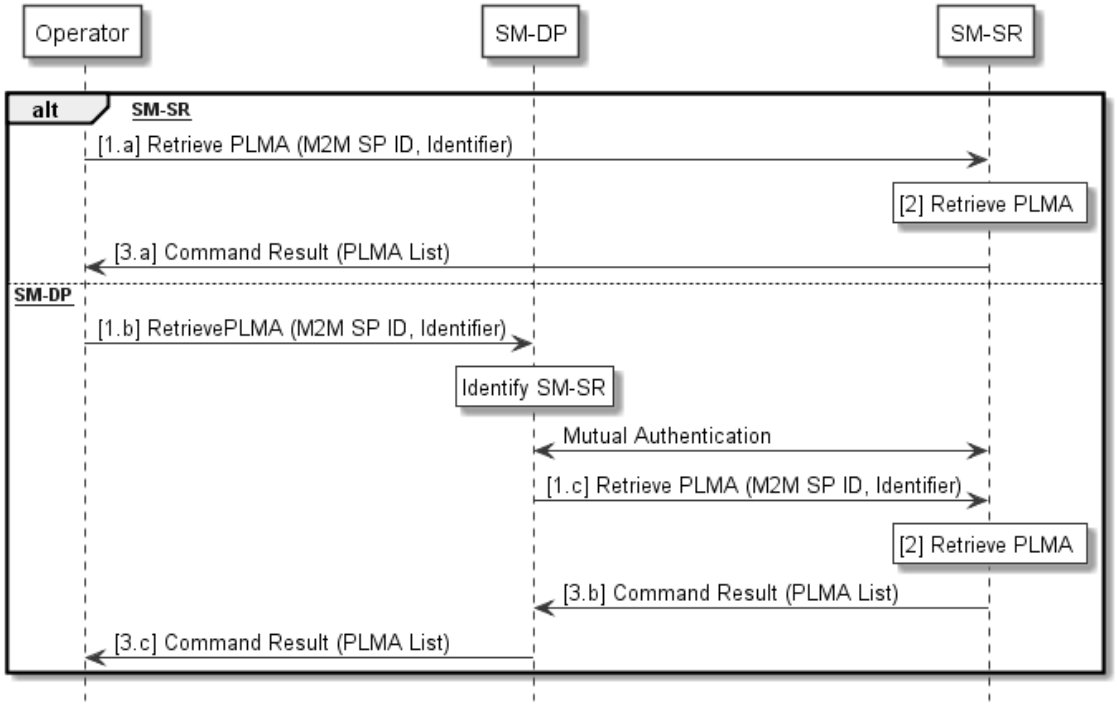

Figure 15: Retrieve Profile Lifecycle Management Authorisation by Operator

Start Condition:

a. The Operator opened a dedicated interface with the SM-SR, either directly or through its SM-DP, for PLMA management.

b. PLMA MAY exist in the SM-SR.

Procedure:

1. The Operator whose Profile resides on a set of eUICCs sends a PLMA request to the SM-SR managing those eUICCs, either directly (1.a) or through its SM-DP (1.b, 1.c), to retrieve PLMA, applying to its Profile(s) for an M2M SP.
    - It SHALL be possible for the Operator to set in the request only the M2M SP ID and / or any identifier pointing to a set of eUICCs and/or Profiles.
2. The SM-SR retrieves the PLMA applying to the identifier sent in the request.
3. The SM-SR return the corresponding PLMA to the requesting Operator (3.a, 3.b, 3.c).

NOTE: The definition of needed identifier to retrieve PLMA applying to a set of eUICCs and/or Profiles is out of scope of this specification.

End Condition: The Operator has received the PLMA according to input parameters the Operator has provided in the request.

An Operator is able to send the retrieve PLMA request for its own Profiles only.

3.5.15.3 Retrieve Profile Lifecycle Management Authorisation– by M2M SP

With this procedure, the M2M SP retrieves the PLMA the Operator has set on the SM-SR.

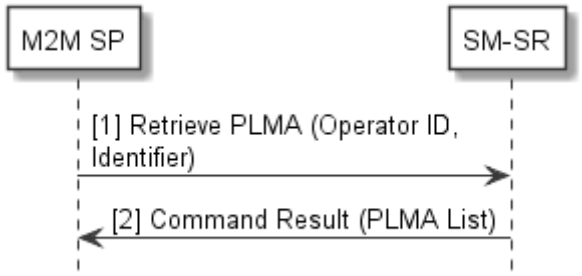

Figure 16: Retrieve Profile Lifecycle Management Authorisation by M2M SPStart Condition:

a. The M2M SP opened a dedicated interface with the SM-SR to be able to retrieve its own PLMA.

b. PLMA MAY exist in the SM-SR.

Procedure:

1. An M2M SP who wants to retrieve PLMA applying to a set of Operator owned Profiles, sends a PLMA request to the SM-SR, managing those eUICCs having the targeted Operator Profiles installed
   - It SHALL be possible for the M2M SP to set in the request the Operator ID only and / or any identifier pointing to a set of eUICCs and/or Profiles.
2. The SM-SR return the corresponding PLMA to the requesting M2M SP.

NOTE: The definition of needed identifier to retrieve PLMA applying to a set of eUICCs and/or Profiles is out of scope of this specification.

End Condition: The M2M SP has received the PLMA according to the input parameter the M2M SP has provided in the request.

An M2M SP is able to retrieve PLMA only for Profiles it has authorisations for.

An M2M SP is able to send the retrieve PLMA request only for its own eUICCs.

3.5.15.4 Delete Profile Lifecycle Management Authorisation

The delete PLMA requests comprises the following steps:

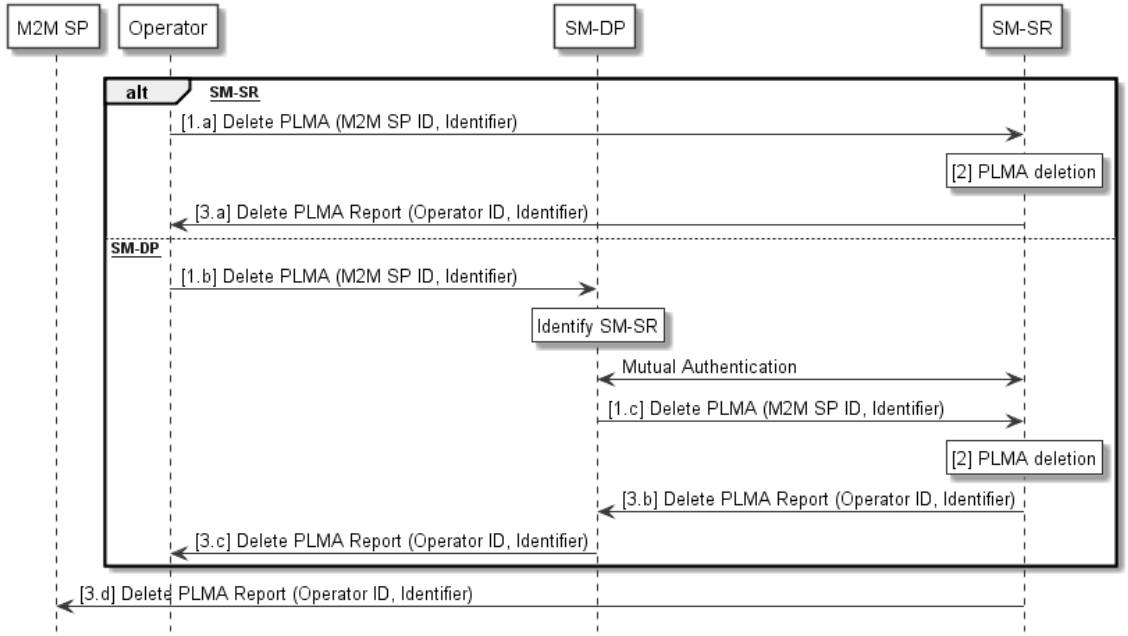

Figure 17: Delete Profile Lifecycle Management Authorisation

Start Condition:

a. The Operator opened a dedicated interface with the SM-SR, either directly or through its SM-DP, for PLMA management.
b. PLMA exists in the SM-SR.

Procedure:

1. An Operator whose Profile is resident on a set of eUICCs sends a PLMA request to the SM-SR managing those eUICCs, either directly (1.a) or through its SM-DP (1.b, 1.c), to delete PLMA.
    - It SHALL be possible for the Operator to set in the request only the M2M SP ID and / or any identifier pointing to a set of eUICCs and/or Profiles.
2. The SM-SR deletes the PLMA applying to the identifier sent in the request.
3. The SM-SR confirms the successful deletion of the PLMA by notifying the requesting Operator, either directly (3.a) or through its SM-DP (3.b, 3.c), as well as the corresponding M2M SP (3.d).

End Condition: The SM-SR has deleted the Profile Lifecycle Management functionality for the addressed M2M SP. The referenced M2M SP is no more able to manage the lifecycle of the Operator Profile(s) for the set of eUICCs as well as to receive reports related to those Profiles.

An Operator is able to send the delete PLMA requests only for its own Profiles.

NOTE: In case that the M2M SP has still the need to get status changes on Profiles being resident on eUICCs it is responsible for, it is up to the Operator, owning the Profiles on the eUICC, to forward reports about Profile status changes to the correspondent M2M SP. This is outside of this specification.

3.5.16 Profile Enabling via M2M SP

A switch between two Profiles can be achieved by the following dedicated procedure. In this case the request is issued directly by the M2M SP to the SM-SR associated with the target eUICC. To be successful, the authorisation for the M2M SP SHALL be configured in the SM-

SR (see Profile Lifecycle Management Authorisation **Registration at SM-SR** chapter 3.5.15 for details).

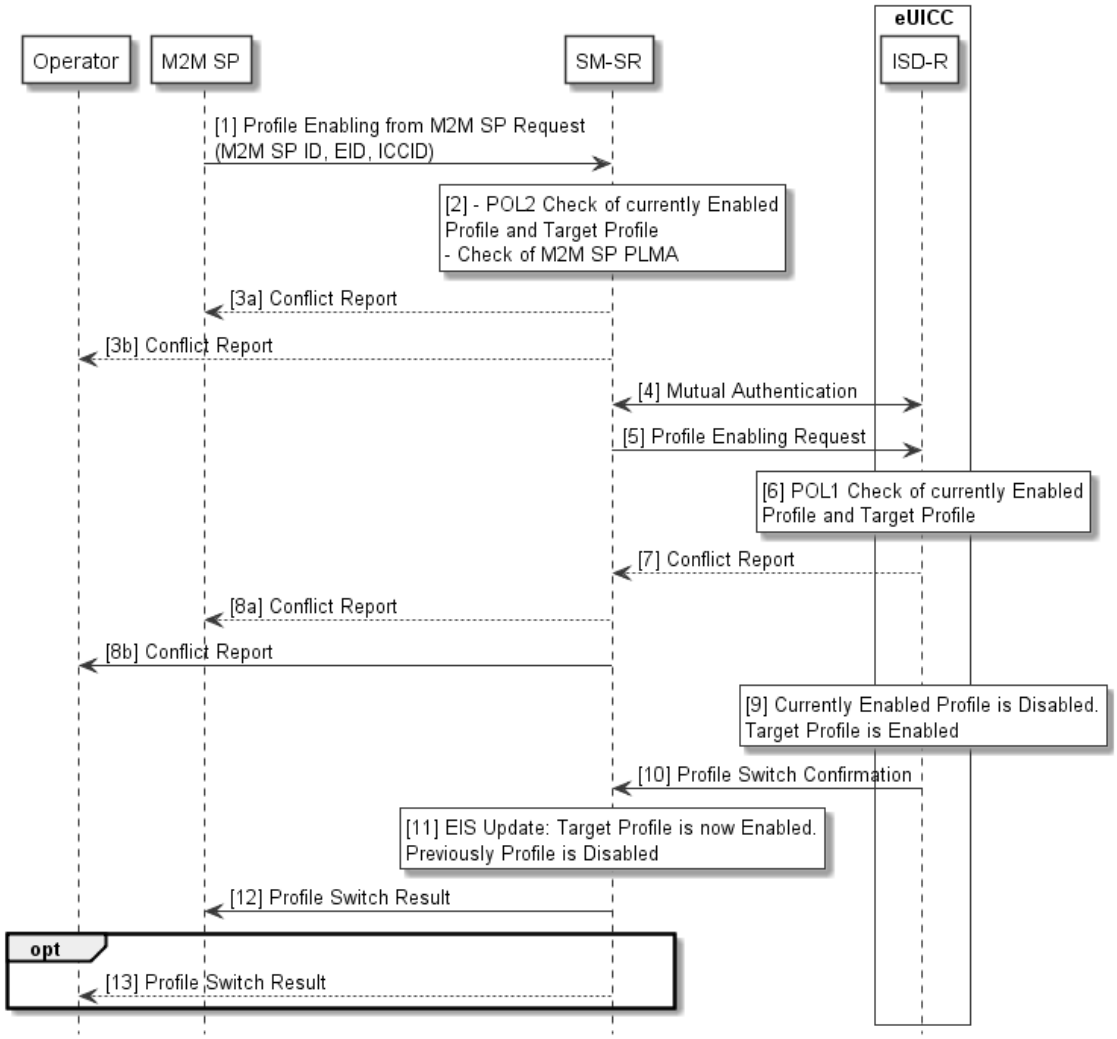

Figure 18: Profile Enabling via M2M SP

Start Conditions:

a. The target Profile is disabled on the eUICC. Another Profile is enabled.
b. The Subscription associated with the target Profile is active in the Operator's network.
c. The EID of the target eUICC, the SRID associated with the target Profile and the ICCID of the target Profile are known by the M2M SP.

Procedure:

1. The M2M SP sends a Profile Enabling from M2M SP request to the SM-SR. The request includes the target EID and the ICCID of the target Profile.
2. The SM-SR checks if the POL2 of both the currently Enabled Profile and the target Profile permit the Profile switch to take place. The SM-SR checks if the M2M SP has the authorisations to enable the targeted Profile.
3. If there is a conflict with POL2 or with the M2M SP authorisations, the SM-SR aborts the procedure and MAY inform the M2M SP. In addition the SM-SR MAY inform the corresponding Operator(s) accordingly.

4. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
5. If there is no conflict with POL2, the SM-SR issues a Profile Enabling request to the ISD-R on the eUICC including at least the ISD-P AID of the target Profile.
6. The eUICC performs a POL1 check.
7. If there is a conflict with POL1, the ISD-R aborts the procedure and informs the SM-SR.
8. In addition the SM-SR MAY inform the concerned M2M SP and Operator(s) accordingly.
9. If there is no conflict with POL1, the ISD-R performs the Profile switch resulting in the target Profile being enabled and the previously Enabled Profile being disabled.
10. The ISD-R reports the Profile switch result to the SM-SR.
11. If the switch is successful the SM-SR records in the EIS that the target Profile is enabled and the previous Profile is disabled.
12. The SM-SR reports the Profile switch result back to the M2M SP.
13. The SM-SR SHALL report the Profile switch result back to the Operator(s) if requested by the Operator(s). These messages will include the M2M SP OID, the EID and the ICCID of their targeted Profiles.

End Condition: The target Profile is enabled on the eUICC. The previously Enabled Profile is disabled. The EIS is up to date.

3.5.17 Profile Disabling via M2M SP

Profile disabling can be achieved by the following procedure. In this case the request is issued directly by the M2M SP to the SM-SR associated with the target eUICC. To be successful, the authorisation for the M2M SP SHALL be configured in the SM-SR (see Profile Lifecycle Management Authorisation **Registration at SM-SR** chapter 3.5.15 for details).

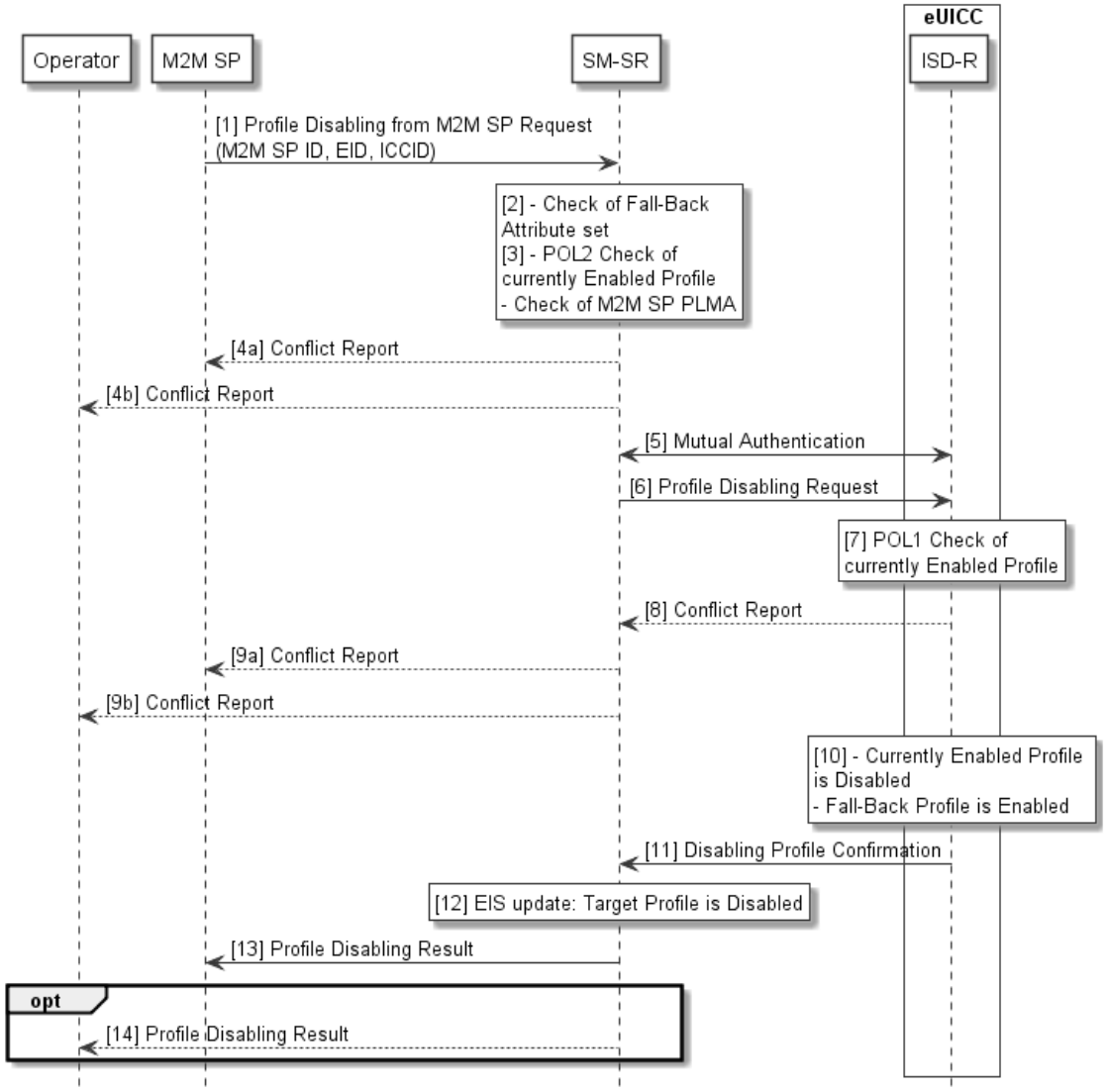

Figure 19: Profile Disabling via M2M SP

Start Conditions:

The target Profile is enabled on the eUICC.

Procedure:

1. The M2M SP sends a Profile Disabling from M2M SP request to the SM-SR. The request includes the target EID and the ICCID of the target Profile.
2. If the target Profile for disabling is the Profile with Fall-Back Attribute set then the Profile disabling SHALL NOT be executed.
3. The SM-SR checks if the POL2 of the Enabled Profile permits the Profile to be disabled. The SM-SR checks if the M2M SP has the authorisations to disable the targeted Profile

4. If there is a conflict with POL2 or with the M2M SP authorisations, the SM-SR aborts the procedure and MAY inform the M2M SP. In addition the SM-SR MAY inform the corresponding Operator accordingly.
5. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
6. If there is no POL2 conflict, the SM-SR issues a Profile enabling request to the ISD-R on the eUICC for the Profile with Fall-Back Attribute set.
7. The eUICC performs an internal POL1 check for the currently Enabled Profile.
8. If there is a conflict with POL1, the ISD-R aborts the procedure and informs the SM-SR.
9. In addition the SM-SR MAY inform the corresponding M2M SP and Operator accordingly.
10. If permitted, the Enabled Profile is disabled and the ISD-R enables the Profile with Fall-Back Attribute set.
11. The ISD-R sends reports of the Profile disabling result to the SM-SR.
12. If the disabling is successful the SM-SR records in the EIS that the target Profile is disabled.
13. The SM-SR reports the Profile disabling result back to the M2M SP.
14. The SM-SR SHALL report the Profile disabling result back to the Operator(s) if requested by the Operator(s). These messages will include the M2M SP OID, the EID and the ICCID of their targeted Profiles.

End Condition: The target Profile is now disabled on the eUICC, and the Profile with Fall-Back Attribute set is enabled.

3.5.18 ISD-P Deletion via M2M SP

A Profile can be deleted by the following procedure. In this case the request is issued directly by the M2M SP to the SM-SR associated with the target eUICC. To be successful, the authorisation for the M2M SP SHALL be configured in the SM-SR (see Profile Lifecycle Management Authorisation **Registration at SM-SR** chapter 3.5.15 for details).

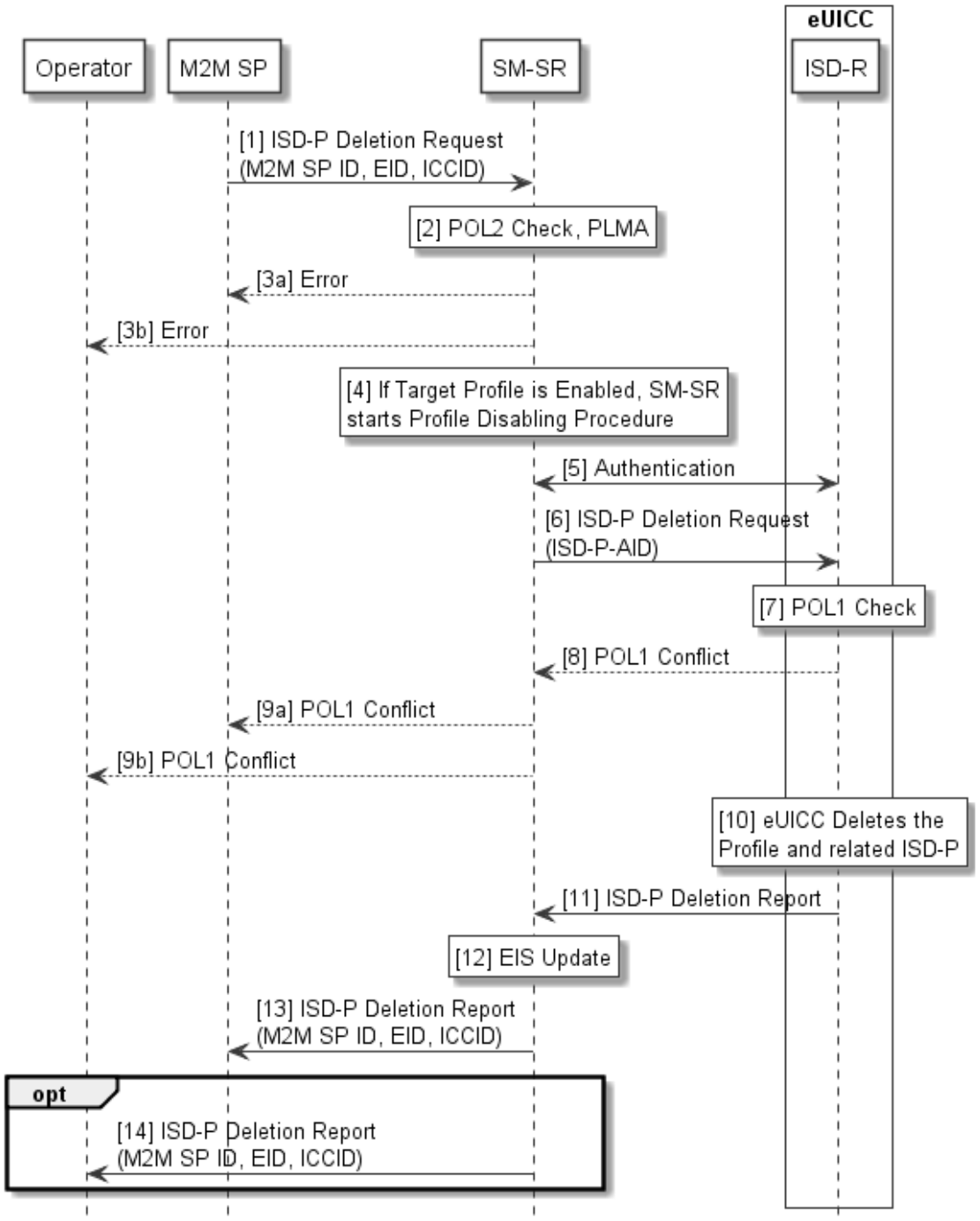

Figure 20: ISD-P Deletion via M2M SP

Start Conditions:

The M2M SP decides to permanently delete a Profile on a eUICC.

Procedure:

1. The M2M SP sends an ISD-P Deletion from M2M SP request to the SM-SR. The request includes the target EID and the ICCID of the targeted Profile.
2. The SM-SR checks the POL2 of the target Profile. The SM-SR checks if the M2M SP has the authorisations to delete the targeted Profile

3. If there is a conflict with POL2 or with the M2M SP authorisations, the SM-SR aborts the procedure and MAY inform the M2M SP. In addition the SM-SR MAY inform the corresponding Operator accordingly.
4. If the target Profile is enabled, the SM-SR starts the Profile Disabling procedure.
5. The SM-SR and the eUICC, using the key set in the ISD-R, authenticate each other if not already authenticated.
6. The SM-SR sends the ISD-P Deletion request to the ISD-R on the eUICC. The request includes the ISD-P AID of the targeted Profile.
7. The eUICC performs a POL1 check.
8. If there is a conflict with POL1, the ISD-R aborts the procedure and informs the SM-SR.
9. In addition the SM-SR MAY inform the corresponding M2M SP and Operator accordingly.
10. If there is no conflict, the ISD-R then erases the targeted Profile and the related ISD-P.
11. The ISD-R sends reports of the ISD-P deletion result to the SM-SR.
12. If the ISD-P deletion is successful the SM-SR updates the EIS appropriately
13. The SM-SR reports the ISD-P deletion result back to the M2M SP.
14. The SM-SR SHALL report the ISD-P deletion result back to the Operator(s) if requested by the Operator(s). These messages will include the M2M SP OID, the EID and the ICCID of the deleted Profile.

End Condition: The target Profile is deleted from the eUICC. The EIS in the SM-SR is up to date.

3.5.19 Fall-Back Attribute Management

This procedure contains the steps needed to change the Fall-Back Attribute from one Profile to another.

The Operator1 owning the Profile that currently has the Fall-Back Attribute set and the Operator2 that wants to set the Fall-Back Attribute on its own Profile need to have an agreement. This agreement is materialised by the Operator1 settings a PLMA where it MAY grant Operator2 the authorisation to unset the Fall-Back Attribute on its Operator1 Profile as a consequence of setting the Fall-Back Attribute on the Operator 2 Profile by Operator 2.

NOTE: There is no operation that explicitly un-sets the Fall-Back Attribute on a Profile. The Fall-Back Attribute is only un-set as the consequence of setting the Fall-Back Attribute on another Profile.

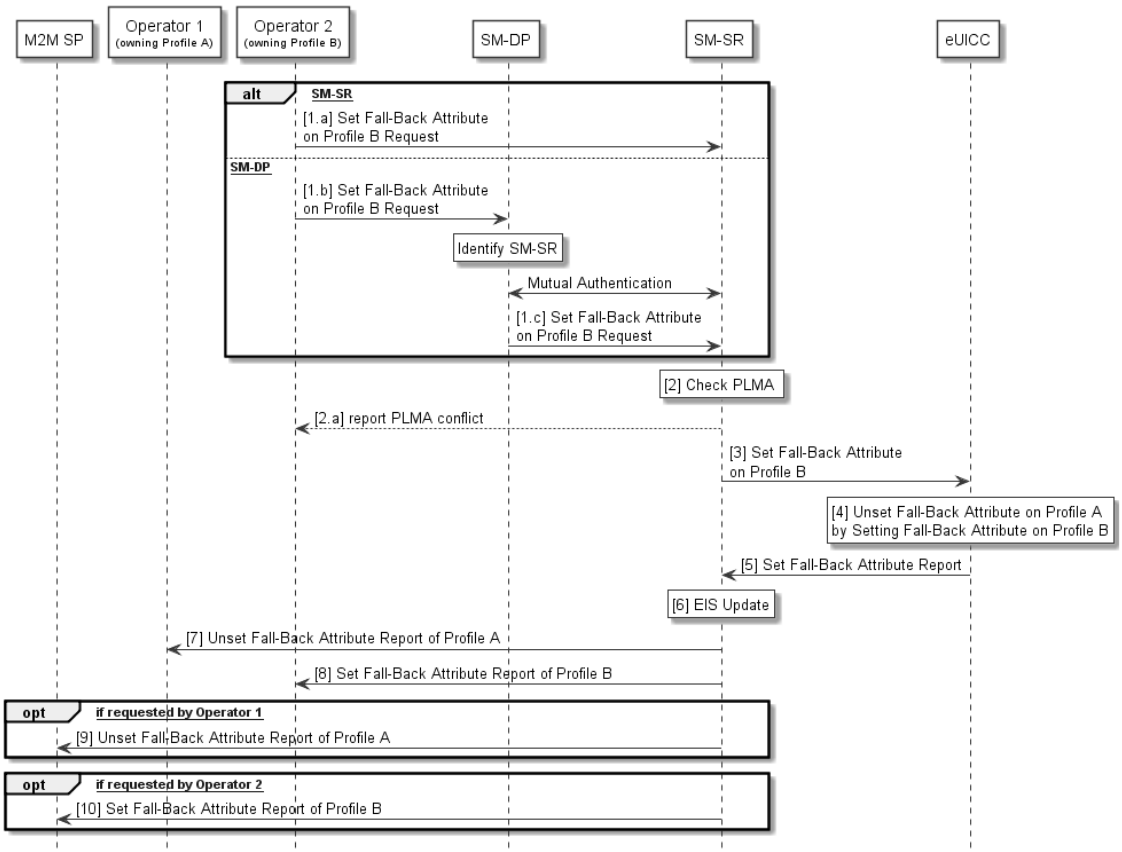

Figure 21: Fall-Back Attribute Management

Start Conditions:

a. Profile A with Fall-Back Attribute set.
b. Profile B, targeted to have the Fall-Back Attribute set, present on the eUICC.
c. Profile A owner Operator1 has configured a PLMA authorizing Operator2 to unset the Fall-Back Attribute on Profile A.

Procedure:

1. The Operator2 owning Profile B requests setting of the Fall-Back Attribute on Profile B to the SM-SR, either directly (1.a) or through its SM-DP (1.b, 1.c).
2. The SM-SR checks if Operator1 has configured a PLMA authorizing Operator2 to unset the Fall-Back Attribute on Profile A.
    a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the Operator 2.
3. The SM-SR, by calling Set Fall-Back Attribute function, requests the eUICC to set the Fall-Back Attribute to the Profile B.
4. The eUICC performs the operation. This will remove the Fall-Back Attribute from Profile A.
5. The eUICC reports the status of the Set Fall-Back operation to the SM-SR
6. The SM-SR update the EIS accordingly.
7. The SM-SR reports to the Operator1 owning the Profile A that the Fall-Back Attribute has been unset on its Profile.
8. The SM-SR reports to Operator2 that Profile B now has the Fall-Back Attribute set.
9. The SM-SR SHALL report to the M2M SP that the Profile A has the Fall-Back Attribute unset, if requested by the Operator1 during PLMA registration (see 3.5.155).
10. The SM-SR SHALL report to the M2M SP that the Profile B has the Fall-Back Attribute set, if requested by the Operator2 during PLMA registration (see 3.5.155).

End Conditions:

The Profile B has the Fall-Back Attribute set. The Profile A has the Fall-Back Attribute unset.

3.5.20 Fall-Back Attribute Management via the M2M SP

Operators MAY also authorise an M2M SP to change the Fall-Back Attribute from one Profile to another. This procedure contains the steps needed to execute such an operation.

The Operator1 owning the Profile that currently has the Fall-Back Attribute set and the Operator2 that agree to have the Fall-Back Attribute set on its own Profile need to have an agreement with the M2M SP. This agreement is materialised by the Operator2 and Operator1 settings PLMAs where they MAY grant the M2M SP the authorisation to set or unset the Fall-Back Attribute on their respective Profile.

NOTE: There is no operation that explicitly un-sets the Fall-Back Attribute on a Profile. The Fall-Back Attribute is only unset as the consequence of setting the Fall-Back Attribute on another Profile.

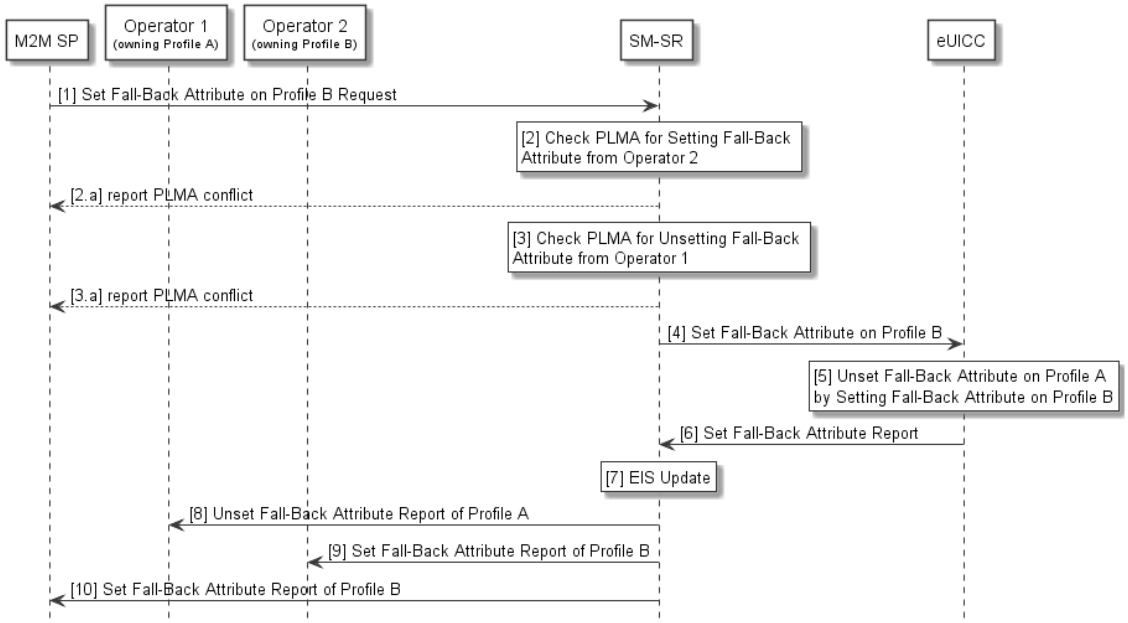

Figure 22: Fall-Back Attribute Management via M2M SP

Start Conditions:

a. Profile A with Fall-Back Attribute set.
b. Profile B, targeted to have the Fall-Back Attribute set, present on the eUICC.
c. Profile A owner Operator1 has configured a PLMA authorizing the M2M SP to unset the Fall-Back Attribute.
d. Profile B owner Operator2 has configured a PLMA authorising the M2M SP to set the Fall-Back Attribute.

Procedure:

1. The M2M SP requests setting of the Fall-Back Attribute on Profile B to the SM-SR.
2. The SM-SR checks if a PLMA from Operator2 authorises the M2M SP to set the Fall-Back Attribute on Profile B.
    a) If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the M2M SP.

3. The SM-SR checks if a PLMA from Operator1 authorises the M2M SP to unset the Fall-Back Attribute on Profile A.
    a) If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the M2M SP.

4. The SM-SR, by calling Set Fall-Back Attribute function, requests the eUICC to set the Fall-Back Attribute to the Profile B.
5. The eUICC Sets the Fall-Back Attribute on the Profile B. This will remove the Fall-Back Attribute from Profile A.
6. The eUICC sends a report of the operation to the SM-SR
7. The SM-SR update the EIS accordingly.
8. The SM-SR reports to the Operator1 that Profile A now has the Fall-Back Attribute unset.
9. The SM-SR reports to Operator2 that Profile B now has the Fall-Back Attribute set.
10. The SM-SR reports to the M2M SP that the Fall-Back Attribute is now set in Profile B.

End Conditions:

The Profile B has the Fall-Back Attribute set. The Profile A has the Fall-Back Attribute unset.

3.5.21 Emergency Profile Attribute Management

Under certain circumstances, it MAY be necessary to set the Emergency Profile Attribute for a Profile when no other Profile has the Emergency Profile Attribute set (case 1), or, a change regarding the Profile that has the Emergency Profile Attribute set is needed (case 2). This procedure contains the steps needed to execute such operations. For case 2. the Operator1 owning the Profile that currently has the Emergency Profile Attribute set and the Operator2 that wants to set the Emergency Profile Attribute on its own Profile need to have an agreement. This agreement is materialised by the Operator1 settings a PLMA where it MAY grant Operator2 the authorisation to unset the Emergency Profile Attribute on this Operator1 Profile.

NOTE: There is no operation that explicitly unsets the Emergency Profile Attribute on a Profile. The Emergency Profile Attribute is only unset as a consequence of setting the Emergency Profile Attribute on another Profile.

For case 1 the procedure below applies:

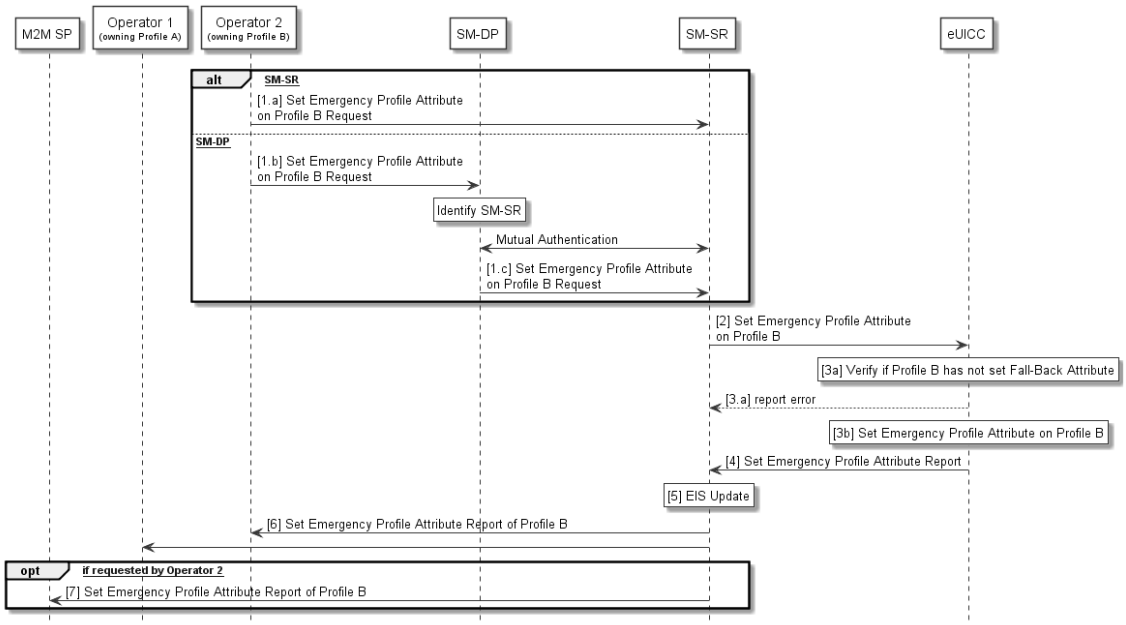

Figure 23: Emergency Profile Attribute Management (case 1)

Start Conditions (case 1):

a. No Profile with Emergency Profile Attribute set exists.
b. Profile B, targeted to have the Emergency Profile Attribute set, present on the eUICC and disabled
c. Profile B does not have the Fall-Back Attribute set.

Procedure (case 1):

1. The Operator2 owning Profile B requests setting of the Emergency Profile Attribute on Profile B to the SM-SR, either directly (1.a) or through its SM-DP (1.b, 1.c).
2. The SM-SR, by calling Set Emergency Profile Attribute function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.
3. The eUICC verifies that Profile B does not have the Fall-Back Attribute set (3a) and performs the operation (3b).
    a. If the conditions (3a) is not true, the eUICC aborts the procedure and reports an error to the SM-SR.
4. The eUICC reports the status of the Set Emergency Profile Attribute operation to the SM-SR
5. The SM-SR updates the EIS accordingly.
6. The SM-SR reports to all Operators, having a Profile on this eUICC, that a Profile now has the Emergency Profile Attribute set. This report MAY include the Profile ID.
7. The SM-SR SHALL report to the M2M SP that the Profile B has the Emergency Profile Attribute set, if requested by the Operator2 during PLMA registrations (see 3.5.155).

End Conditions (case 1):

The Profile B has the Emergency Profile Attribute set.

For case 2 the procedure below applies

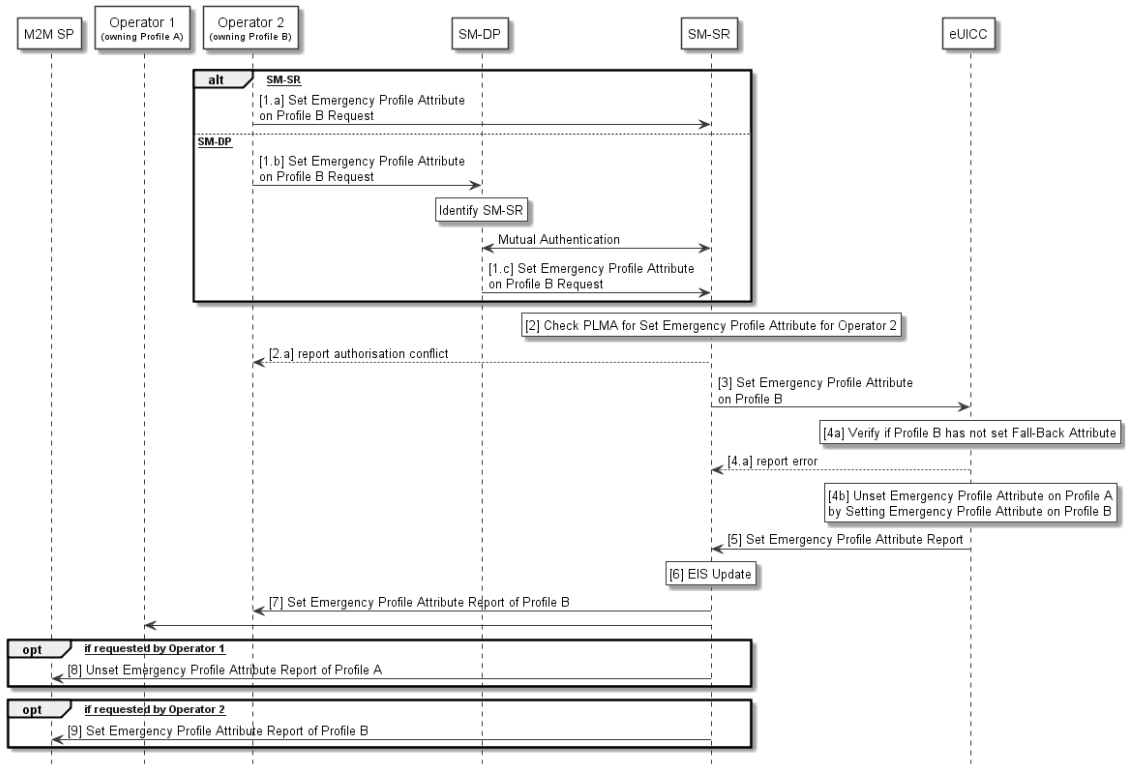

Figure 24: Emergency Profile Attribute Management (case 2)

Start Conditions (case 2):

a. Profile A with Emergency Profile Attribute set.
b. Profile B, targeted to have the Emergency Profile Attribute set, present on the eUICC.
c. Profile A owner Operator1 has configured a PLMA authorizing Operator2 to unset the Emergency Profile Attribute on Profile A.

Procedure (case 2):

1. The Operator2 owning Profile B requests setting of the Emergency Profile Attribute on Profile B to the SM-SR, either directly (1.a) or through its SM-DP (1.b, 1.c).
2. The SM-SR checks if Operator2 has PLMA configured to unset the Emergency Profile Attribute from the Operator1 owning the Profile that currently has the Emergency Profile Attribute set.
    a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the Operator 2.
3. The SM-SR, by calling Set Emergency Profile Attribute function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.
4. The eUICC verifies that Profile B does not have the Fall-Back Attribute set (4a) and performs the operation (4b). This will remove the Emergency Profile Attribute from Profile A.
    a. If the conditions (4a) is not true, the eUICC aborts the procedure and reports an error to the SM-SR.
5. The eUICC reports the status of the Set Emergency Profile Attribute operation to the SM-SR
6. The SM-SR updates the EIS accordingly.
7. The SM-SR reports to all Operators, having a Profile on this eUICC, that another Profile now has the Emergency Profile Attribute set. This report MAY include the Profile ID.
8. The SM-SR SHALL report to the M2M SP that the Profile A has the Emergency Profile Attribute unset, if requested by the Operator1 during PLMA registrations (see 3.5.155).

9. The SM-SR SHALL report to the M2M SP that the Profile B has the Emergency Profile Attribute set, if requested by the Operator2 during PLMA registrations (see 3.5.155).

End Conditions (case 2):

The Profile A has the Emergency Profile Attribute unset. The Profile B has the Emergency Profile Attribute set.

3.5.22 Emergency Profile Attribute Management via the M2M SP

Operators MAY also authorise an M2M SP to change which Profile has the Emergency Profile Attribute set.

Under certain circumstances, it MAY be necessary to set the Emergency Profile Attribute for a Profile when no other Profile has the Emergency Profile Attribute set (case 1), or, a change regarding the Profile that has the Emergency Profile Attribute set is needed (case 2). This procedure contains the steps needed to execute such operations.

For case 1 the Operator2 that agrees to have the Emergency Profile Attribute set on its own Profile need to have an agreement with the M2M SP. This agreement is materialised by the Operator2 setting PLMAs where Operator2 MAY grant the M2M SP the authorisation to set the Emergency Profile Attribute on its respective Profile.

For case 2. the Operator1 owning the Profile that currently has the Emergency Profile Attribute set and the Operator2 that agree to have the Emergency Profile Attribute set on its own Profile need to have an agreement with the M2M SP. This agreement is materialised by the Operator2 and Operator1 setting PLMAs where Operator2 MAY grant the M2M SP the authorisation to set the Emergency Profile Attribute on its respective Profile and where Operator1 MAY grant the M2M SP the authorisation to un-set the Emergency Profile Attribute on its respective Profile.

NOTE: There is no operation that explicitly unsets the Emergency Profile Attribute on a Profile. The Emergency Profile Attribute is only unset as a consequence of setting the Emergency Profile Attribute on another Profile.

For case 1 the procedure below applies:

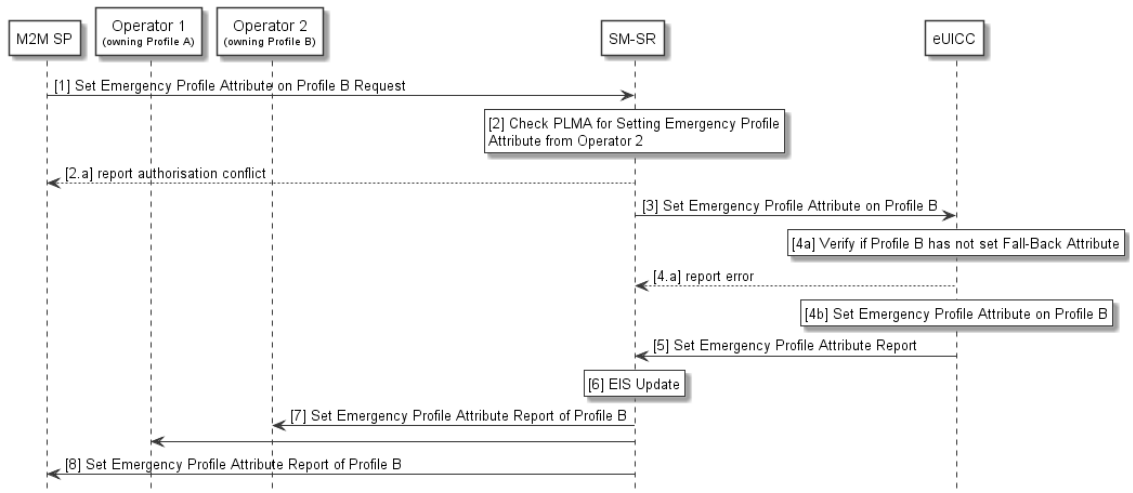

Figure 25: Emergency Profile Attribute Management via M2M SP (case 1)

Start Conditions:

a. Profile B, targeted to have the Emergency Profile Attribute set, present on the eUICC.
b. Profile B owner Operator2 has configured a PLMA authorizing the M2M SP to set the Emergency Profile Attribute.

Procedure:

1. The M2M SP requests setting of the Emergency Profile Attribute on Profile B to the SM-SR.
2. The SM-SR checks if a PLMA from Operator2 that authorises the M2M SP to set the Emergency Profile Attribute on Profile B is configured
   a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the M2M SP.
3. The SM-SR, by calling Set Emergency Profile Attribute function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.
4. The eUICC verifies that Profile B does not have the Fall-Back Attribute set (4a) and then sets the Emergency Profile Attribute to the Profile B (4b).
   a. If the conditions (4a) is not true, the eUICC aborts the procedure and reports an error to the SM-SR.
5. The eUICC sends a report of the operation to the SM-SR
6. The SM-SR updates the EIS accordingly.
7. The SM-SR reports to all Operators, having a Profile on this eUICC, that a Profile now has the Emergency Profile Attribute set. This report MAY include the Profile ID.
8. The SM-SR reports to the M2M SP that the Emergency Profile Attribute is now set for Profile B.

End Conditions:
The Profile B has the Emergency Profile Attribute set.

For case 2 the procedure below applies:

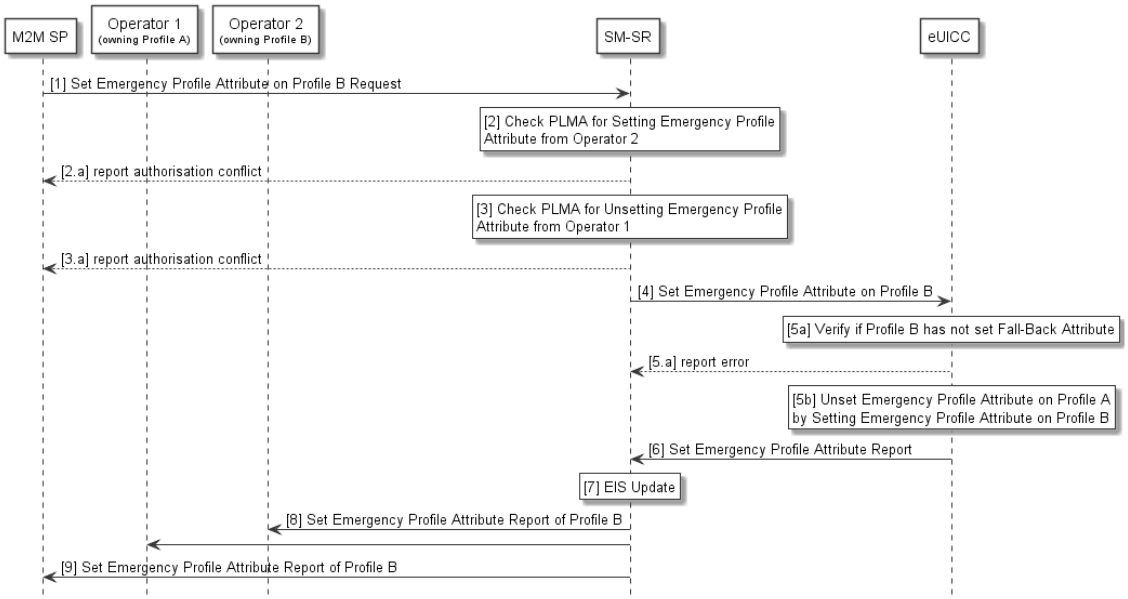

Figure 26: Emergency Profile Attribute Management via M2M SP (case 2)

Start Conditions:

a. Profile A with Emergency Profile Attribute set.
b. Profile B, targeted to have the Emergency Profile Attribute set, present on the eUICC.

c. Profile A owner Operator1 has configured a PLMA authorizing the M2M-SP to unset the Emergency Profile Attribute.
d. Profile B owner Operator2 has configured a PLMA authorizing the M2M-SP to set the Emergency Profile Attribute.

Procedure:

1. The M2M SP requests setting of the Emergency Profile Attribute on Profile B to the SM-SR.
2. The SM-SR checks if a PLMA from Operator2 that authorises the M2M SP to set the Emergency Profile Attribute on Profile B is configured.
    a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the M2M SP.
3. The SM-SR checks if a PLMA from Operator1 that authorises the M2M SP to unset the Emergency Profile Attribute on Profile A is configured.
    a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the M2M SP.
4. The SM-SR, by calling Set Emergency Profile Attribute function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.
5. The eUICC verifies that Profile B does not have the Fall-Back Attribute set (5a) and then sets the Emergency Profile Attribute to the Profile B (5b). This will remove the Emergency Profile Attribute from Profile A.
    a. If the conditions (5a) is not true, the eUICC aborts the procedure and reports an error to the SM-SR.
6. The eUICC sends a report of the operation to the SM-SR
7. The SM-SR updates the EIS accordingly.
8. The SM-SR reports to all Operators, having a Profile on this eUICC, that another Profile now has the Emergency Profile Attribute set. This report MAY include the Profile ID.
9. The SM-SR reports to the M2M SP that the Emergency Profile Attribute is now set for Profile B.

End Conditions:
The Profile A has the Emergency Profile Attribute unset. The Profile B has the Emergency Profile Attribute set.

3.5.23 Local Enable of the Test Profile

A switch from Operational Profile to the Test Profile can be achieved by the following dedicated procedure. The request is issued directly from the Device to the eUICC.

Start Conditions:
An Operational Profile is enabled.

Procedure:

1. The Device sends a Local Enable request to the eUICC.
2. The eUICC performs a verification that the Profile to be enabled is a Test Profile.
3. If the Profile to be enabled is not a Test Profile, the eUICC SHALL abort the procedure and informs the Device.
4. The eUICC performs the Profile switch, without enforcing POL1, resulting in the Test Profile being enabled and the previously Enabled Profile being disabled.

5. The eUICC stores the ISD-P AID of the previously enabled Operational Profile.
6. The eUICC reports the Profile switch to the Device.

End Condition: The Test Profile is enabled on the eUICC. The previously enabled Operational Profile is disabled.

3.5.24 Local Disable of the Test Profile

Local Disable can be achieved by the following procedure. The request is issued directly by the Device to the eUICC.

Start Condition:
The Test Profile is enabled on the eUICC.

Procedure:

1. The Device sends a Local Disable request to the eUICC.
2. If the Profile to be disabled is not a Test Profile then the Local Disable SHALL NOT be executed.
3. The eUICC enables the previously enabled Operational Profile.
4. If the network attach fails, the eUICC SHALL activate the Fall-Back Mechanism.
5. The eUICC reports the Profile switch to the Device.
6. The eUICC MAY report the successful Local Disable result to the SM-SR.

End Condition: The Test Profile is disabled on the eUICC, and the previously Enabled Profile or the Profile with Fall-Back Attribute set is enabled.

3.6 Policy Control

3.6.1 Overview Diagram of Rule Management System

The figure below represents the Policy Rule management system:

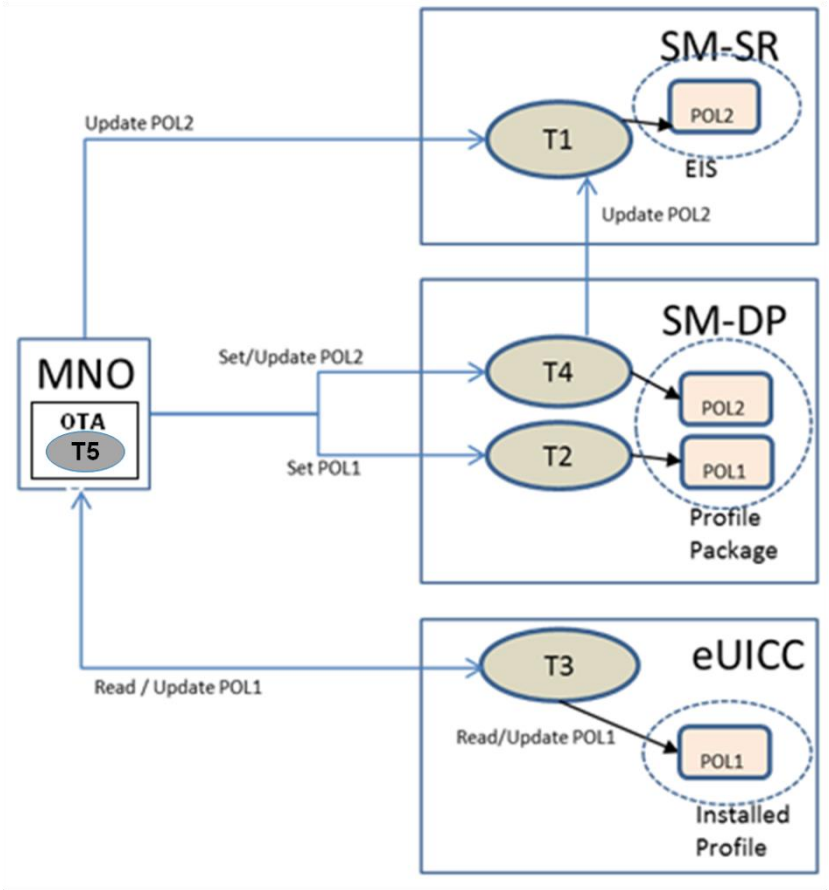

Figure 27: Policy Rule Management System

3.6.2 Policy Rules Management

Policy control, as it relates to a Profile, is required by the Operator and is achieved through the use of rules set by the Operator.

This Policy control is under the control (or jurisdiction) of a single Operator Policy. This Policy MAY be comprised of sub-policies whose enforcement lies with different entities.
There are two types of rules:

- POL1 – these rules resides within a Profile and would be enforced by the eUICC.
- POL2 – these rules would be stored at and enforced by the SM-SR. The Operator sends POL2 directly to the SM-SR or through the SM-DP for attaching as metadata to a Profile.

POL1 and POL2 are representations of a common Operator Policy enforced in different locations/entities. The combination of POL1 and POL2 represent the contract between an Operator and a Subscriber as applied to the Profile.

In this section all commands are considered as being updates; in the first instance when a rule is first established is considered a special case of update.

3.6.2.1 SM-SR Policy Rule Management Engine

The SM-SR has a Policy Rule management engine identified as “Task 1” in the diagram.
Task 1 accepts the following commands:

1) Update POL2 as per Operator request

2) Update POL2 as per Operator request via SM-DP

Task 1 sets the POL2 as per the metadata supplied with a Profile from SM-DP. Task 1 enforces POL2 rules right after installation of the related Profile. Furthermore Task 1 updates the relevant EIS accordingly. The SM-SR is responsible for enforcing the POL2 rules when managing an eUICC.

3.6.2.2 SM-DP Policy Rule Management Engine

The SM-DP has a Policy Rule management engine identified as “Task 2” and “Task 4” in the diagram.
Task 2 accepts the following commands:

1) Set POL1 as per Operator request and embed it in the Profile.

Task 4 accepts the following commands

1) “Update POL2” from the Operator, and passes it to the SM-SR for updating the EIS.
2) Set POL2 from the Operator and attach it to a Profile as metadata for transmission to the SM-SR.

3.6.2.3 eUICC Policy Rule Management Engine

The eUICC has a Policy Rule management engine identified as “Task 3” in the diagram.

Task 3 can read the POL1 rules that reside within the installed Profiles. Furthermore it enforces the POL1 rules right after the installation of the related Profile (see role of Platform Service Manager in Section 3.2.2).
Task 3 accepts the following command:

1) Read/Update POL1 as per Operator request (commands are sent by the Operator’s respective OTA system).

3.6.2.4 OTA Policy Rule Update Mechanism

For Task 5 the Operator OTA Platform is used. In this case it is accepting POL1 update commands from the Operator Rule Maker and issues POL1 updates to the eUICC.

3.6.3 Policy Control Mechanism

The Policy Control Mechanism within the eUICC is a combination of:

- The Policy Rules stored within the ISD-P under Operator authority;
- The Policy Rules Enforcer, which is the process delivering the Policy Enforcement Function and resides within the Platform Service Manager.

See the diagram in Section 3.2.2

3.6.3.1 Policy Rules

Policy Rules are checked at different state changes of Profiles. They MAY impact both the state of the Profile that is associated with the rule and the state of other Profiles.

Depending on the nature of the rule, Policy enforcement can happen at the eUICC and/or at the SM-SR level. Only the Operator which is the owner of the Profile is able to modify the Policy Rules. At the eUICC level, the rules are part of the Profile package and are enforced by the eUICC operating system through the interaction with the Platform Service Manager.

The Operator can update the Policy Rules within its Profile using its own OTA Platform(s). Updating can only be done when the Profile is in enabled state.

The policy enforcement mechanisms defined in this document to enforce the contractual provisions governing the remote Provisioning of an Embedded SIM are subject to applicable competition and regulatory law. The following principles apply to the enforcement of contractual provisions:

- Participating Operators must not abuse policy enforcement mechanisms to block or impede in any way the legitimate installation, enabling, disabling and deletion of a Profile on an Embedded SIM.
- Participating Operators can enforce policy rules provided such actions comply with applicable competition and regulatory law.

The following Policy Rules are defined:

NOTE: This assumes the SM-SR to be GSMA certified and trusted by the Operator.

	Policy Rules	Enforcement when the Profile is	Enforced at
1	Disabling of this Profile not allowed	Enabled	eUICC via POL1 SM-SR via POL2
2	Deletion of this Profile not allowed	Enabled or Disabled	eUICC via POL1 SM-SR via POL2
3	Profile deletion is mandatory when it is disabled.	N/A	eUICC via POL1 SM-SR via POL2

POL1 and POL2 settings MAY or MAY not be the same. POL1 and POL2 are enforced by different entities (eUICC for POL1; SM-SR for POL2) and will be enforced independently.

The explicit setting of POL1 and POL2 rules is the choice of the Operator (e.g. to set POL1 rules to be empty).

3.6.3.2 eUICC Policy Rules Enforcer Function

The Policy Rules Enforcer is able to read and enforce all the POL1 present on the eUICC. The only case where the eUICC can overrule POL1 is the Fall-Back Mechanism.

3.6.3.3 SM-SR Policy Rules Enforcer Function

The SM-SR Policy Rules Enforcer is able to read and enforce the Policy Rules contained in the EIS of the targeted eUICC.

4 Security Model: Threats Analysis & Risk Assessment Model

4.1 Security Challenges

As mentioned in the basic assumptions section, one of the major expectations of this architecture is to provide a solution offering a security level at least equivalent to the security reached by the current UICC and its management systems.

Considering the new delivery of Profiles in the eUICC compared to the existing model, the following main security challenges SHALL be considered and fixed in the security analysis:

a) Different Actors MAY be involved in Profile creation, load, install and enabling and be involved in managing the eUICC during its lifecycle.

b) A Profile can be replaced in the eUICC.

c) Several Profiles MAY be hosted at a given time in the eUICC.

d) Authentication algorithms MAY be shared between operators.

e) Profile and Platform Management are controlled through rules and/or commands which need to be considered in the assets to be protected.

f) Remote installation/Provisioning of a Profile.

g) Remote management of the Profile.

NOTE: The support of proprietary authentication algorithms and the upgradability of authentication algorithms are for further study.

Therefore, the challenge is to deliver a solution offering a sufficient security level, but with enough flexibility to permit interconnection of various subsystems provided by different sources, delivering a part of, or an entire, solution.

4.2 Security Analysis Methodology

Because the design of the solution for eUICC and its remote Provisioning system must be driven by security concerns, it is of primary importance to identify the key risks on the whole architecture in order to derive security recommendations and principles that will shape the final design.

The proposed methodology is based on a 4 step process:

1. Identification of assets (see Annex C);
2. Identification of functions;
3. Identification of threats & risks (see Annex B);
4. Description of security requirements.

4.3 Aim of the Security Realm Approach

A Security Realm is defined as the clustering of Roles and Actors connected through a single protected private network and operated by a sole entity.

This entity, in charge of day to day operations of a Security Realm is defined as an “administrative entity” and might be comprised of one or several actors bound by a unique commercial or legal agreement.

The segmentation in realms allows for the application of adequate protection levels related to a specific context applying to an administrative entity and its realm. This might be due to local specificities such as regulations, lawful enforcement, corporate policies or geographic context.

The requirements pertaining to Security Realms also ensure for a common level of security when addressing communications between Security Realms.

The security requirements applied to the Profile, Platform Management commands and Profile transport security are not addressed by Security Realms.

The eUICC, being a shared asset between different administrative entities, is considered to be an independent Security Realm.

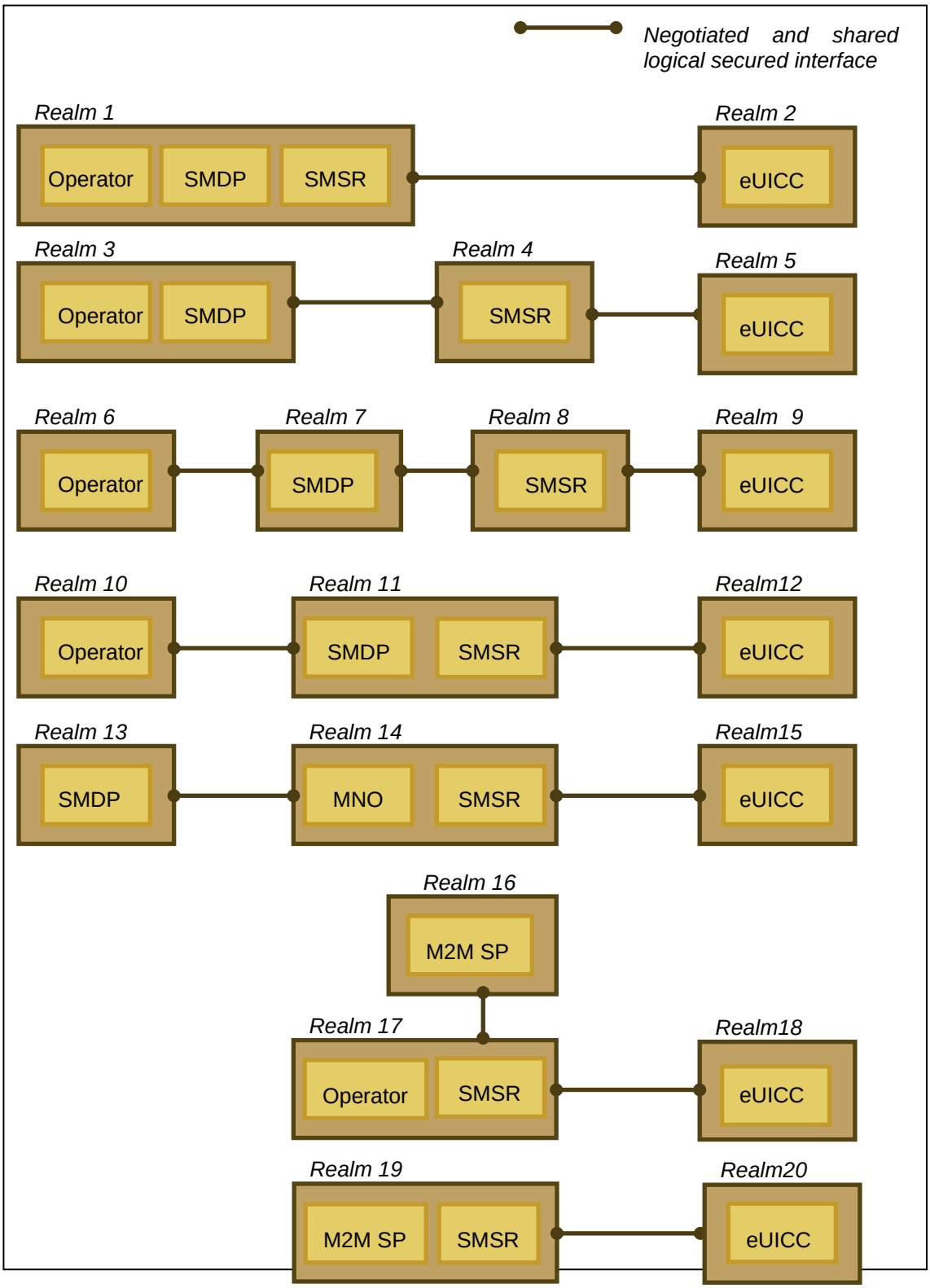

Figure 28: Examples of security realms organisation in the security model

4.4 Security Requirements

This section lists security requirements.

In the security model we consider the Subscriber, Operator, M2M SP, SM-DP, SM-SR, eUICC and EUM.

We consider the Operator, M2M SP, SM-DP, SM-SR, eUICC and EUM as elements that can belong to a Security Realm.

The requirements section is organised in three layered parts:

- General requirements, to be applied to the whole architecture, including any security realm and its Actor(s) and role(s);
- Security requirements attached to a security realm, i.e. including to all of the role(s) attached to the security realm;
- Security requirements attached to a particular role; a section is dedicated to each of the following Roles:
  - eUICC;
  - SM-SR;
  - SM-DP;
  - Device.

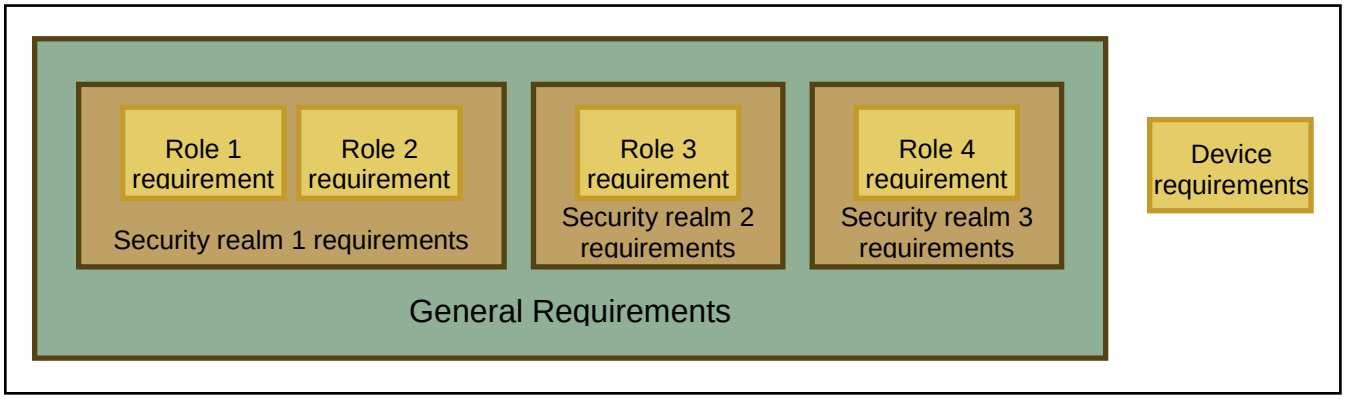

Figure 29: Example of security requirements organisation

4.4.1 General Security Requirements

#	Requirement
SG1	Cryptographic solutions used within the eUICC ecosystem SHALL offer strength at least conform to NIST cryptographic recommendations in NIST SP800-57 [20].
SG2	Past or future communications associated with Profile download and installation, between the SM-DP and the eUICC, whenever trappable by third party SHALL NOT be recoverable based upon the compromise of a single long-term key used for message encryption. A similar requirement for Platform Management is for further study.
SG3	The certificate chains SHALL be highly secure, highly reliable and verifiable.
SG4	All cryptographic keys SHALL be kept in secure environment (e.g. HSM, eUICC).
SG5	The keys used by the EUM for eUICC Certificate generation SHALL be stored in a secure environment (i.e. in a Hardware Security Module).

SG6	The solution SHALL NOT prevent a further release allowing the capability to upgrade the network authentication algorithms used within the ecosystem.
SG7	The architecture SHALL provide a flexible solution including on the base of its security principles, meaning the security applied to a subsystem of the global ecosystem SHALL NOT challenge the security of the overall ecosystem once interconnected.
SG8	The architecture SHALL provide an interoperable solution including on the base of its security principles, meaning the security applied to a subsystem of the global ecosystem SHALL NOT challenge the security of the overall ecosystem once interconnected.
SG9	Multiple Roles and functions MAY be played by a single Actor as long as: 1. It respects local lawful obligations; 2. It does not lower the overall security level of the system; 3. It does not conflict with own Operator security policies (e.g. force an operator to share its secrets with a third party).
SG10	The Operator and the M2M SP SHALL be able to reject to use a non-trusted system for the Embedded UICC management.

4.4.2 Security Realms Requirements

#	**Requirement**
SR1	Security realms SHALL be identifiable and mutually authenticated for the purpose of any communication.
SR2	Communication between the SM-SR and the eUICC SHALL be protected against replay attacks.
SR3	An entity within a security realm MAY need authorisation before communication exchange.
SR4	Any end to end data communication between two security realms of the eUICC ecosystem SHALL be origin authenticated, integrity and confidentiality protected, protected against replay attacks and non-reputable. Non-repudiation MAY not apply to communication with the eUICC.
SR5	Network communication links used inside a security realm SHALL be dedicated – i.e. neither public network, neither mutualised. E.g. solutions such as MPLS or GRE are not considered as dedicated links; a solution such as an authenticated and secured VPN is considered as dedicated.
SR6	When two security realms are exchanging data, they SHALL at first engage a security negotiation (e.g. EAP, IPSEC, TLS handshake…) resulting in the application of an agreed security level between them.
SR7	Security realms SHALL enforce filtering rules so that only authorised entities are granted access to allowed services.
SR8	When negotiating a communication, at least the lowest acceptable common cryptographic suite SHALL apply.

4.4.3 eUICC Requirements

#	**Requirement**
SE1	eUICC SHALL be certified according to the GSMA Embedded UICC Protection Profile [27] .
SE2	Void
SE3	Void
SE4	The eUICC platform SHALL be in line with Common Criteria EAL4+ - EAL4 augmented by AVA_VAN.5 and ALC_DVS.2.
SE5	Upon Profile deletion, the eUICC SHALL ensure of the complete wipe of the Profile.
SE6	eUICC SHALL only accept Platform and Profile Management commands sent from an authorised SM-SR or SM-DP.
SE7	The integrity of the Profile SHALL be ensured before its installation in the eUICC.
SE8	eUICC SHALL reject any Platform and Profile Management commands that are in conflict with the Policy Rules of any Profile on the eUICC the only exception being for the master delete command.
SE9	eUICC SHALL be resistant to tamper attacks (physical and logical).
SE10	Profile keys and algorithm parameters SHALL NOT be extractable from the eUICC.
SE11	A Profile SHALL NOT be exported from the eUICC.
SE12	According to 3GPP TS21.133 [17], eUICC SHALL be able to play a role in deterring terminal theft; e.g. this could be achieved by the definition of a particular configuration for the eUICC preventing normal use of the Device but allowing emergency services.
SE13	The eUICC SHALL provide a secure way for the SM-DP and SM-SR to check its identity and status in such a way that the entity has a proof of identity and origin. This capability is offered through the verification of the eUICC certificate during the Eligibility Verification function.
SE14	All cryptographic functions SHALL be implemented in a robust tamper-proof way and resistant to side-channel attacks.
SE15	The Operator Credentials SHALL NOT be extractable from a Profile on the eUICC.
SE16	The eUICC SHOULD support a secure mechanism to allow the eUICC OS Update. In case it supports such mechanism, it SHALL be declared in the EIS.
SE17	If the mechanism in SE16 is supported, the eUICC SHALL implement a mechanism to report the updated OS version identifier to the SM-SR.

4.4.4 SM-SR and SM-DP Requirements

#	Requirement
SM1 (SM-DP)	SM-DP SHALL be certified according to a GSMA SAS-SM scheme [22].
SM2 (SM-SR)	SM-SR SHALL be certified according to a GSMA SAS-SM scheme [22].
SM3 (SM-SR)	SM-SR SHALL implement an access control mechanism on the request for execution of the SM-SR functions only to authorised security realms.
SM4 (SM-DP)	SM-DP SHALL implement an access control mechanism on the request for execution of the SM-DP functions only to authorised security realms.
SM5 (SM-SR)	Security realm of SM-SR and SM-DP, and eUICC interfaces SHALL have proper counter measures against denial of services attacks.
SM6 (SM-SR)	The donor SM-SR SHALL NOT be able to access the eUICC once the SM-SR switch procedure has been completed.
SM7 (SM-DP)	The SM-DP SHALL be able to establish Profile Management Credentials on the eUICC for the secure end-to-end communication used for the Profile loading in a reliable and confidential way.
SM8 (SM-SR)	The SM-SR SHALL be able to establish Platform Management Credentials on the eUICC for the secure end-to-end communication used for the Platform Management in a reliable and confidential way.
SM9	The Operator SHALL be able to update the OTA Keys in its Profile on the eUICC in a secure and confidential way reusing existing OTA Platform mechanisms.
SM10	There SHALL be a secure end to end communication channel between the Security Realms which host the SM-DP function and the eUICC during the Profile installation.

4.4.5 Machine to Machine Device Requirements

#	Requirement
SD1	The security of the system SHALL NOT be dependent upon the security mechanisms within the Device.
SD2	The Device SHALL NOT be able to access nor modify sensitive Profile data, i.e. credentials, management commands, Policy Rules, authentication algorithm parameters.

4.4.6 Policy Control Function

#	Requirement

SP1	Policy Rules are to be protected against modification by unauthorised entities when they are stored within, and transported between, the SM-SR, SM-DP and eUICC.
SP2	Policy Rule transport SHALL be treated as per SR2.

4.5 Security Architecture

4.5.1 Secure Download and Installation of a Profile

This section describes the security details related to the procedure stated in section 3.5.4.

Download and installation of a Profile SHALL be done in a secure way, as follows:

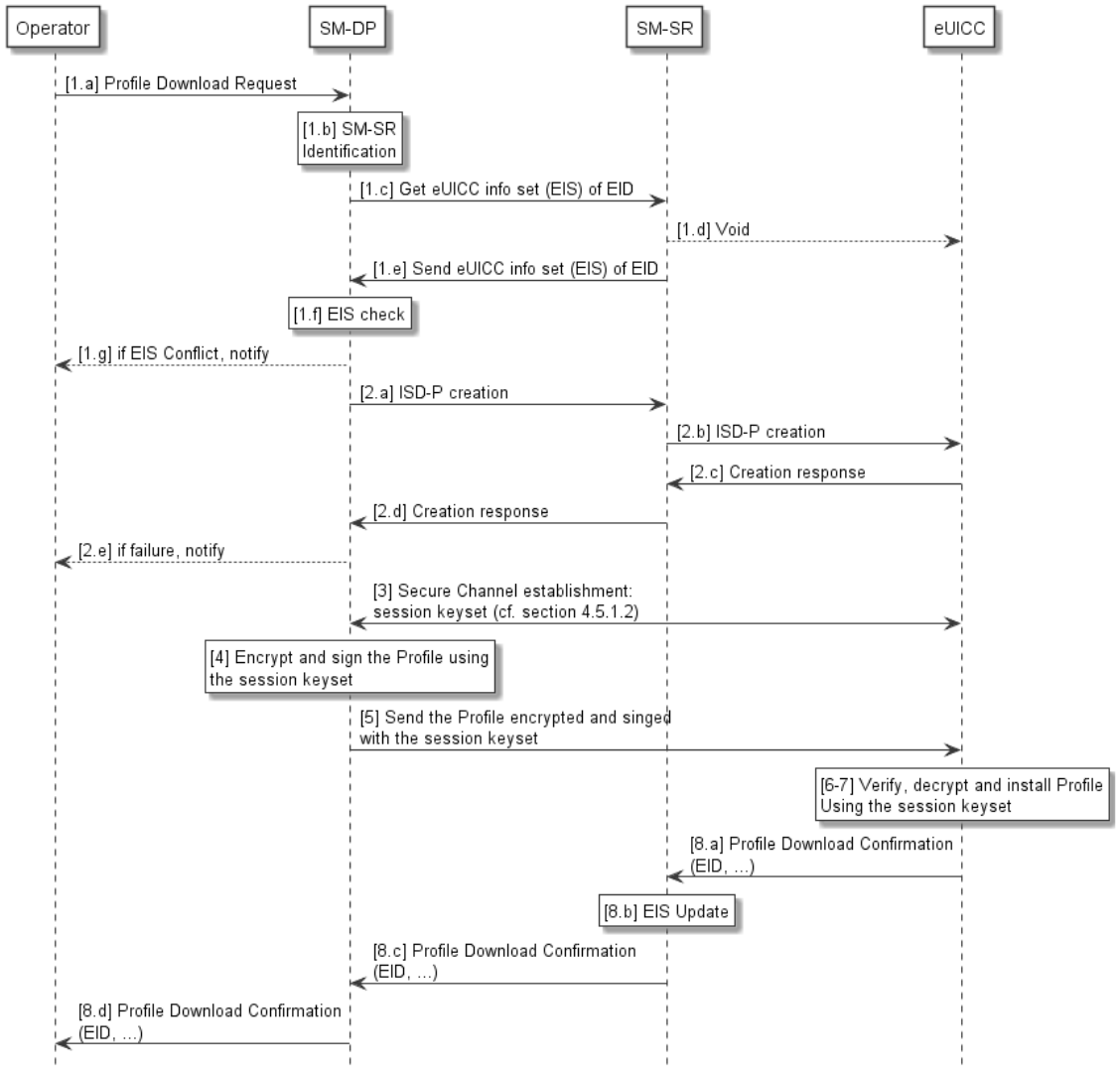

Figure 30: Secure Download and Installation of a Profile

The process between the Operator and the eUICC SHALL be as follows:

Start Conditions:

A. Operator and SM-DP share the Network Access Credentials associated to the Profile.

Procedure:

1. (a) The Operator requests a Profile download and installation to the SM-DP

1. (a) If not already done in earlier transactions, the SM-DP and the SM-SR authenticate each other and will use secure communication for all further data exchanges.

1. (b-f) The SM-DP requests the SM-SR for the relevant part of the eUICC information set (EIS).

2. (a-e) The SM-DP requests that the SM-SR creates an ISD-P on the eUICC.

3. The SM-DP establishes a keyset between itself and this new ISD-P within the eUICC (See section 4.5.1.1 regarding Establishment of the Keyset)

4. The SM-DP encrypts and signs the Profile using the keyset established in step 3 according to the secure channel protocol.

5. The SM-DP sends the encrypted and signed Profile to the ISD-P for download and installation in the eUICC using the secure channel protocol based on the keyset established in step 3

6. The eUICC decrypts and verifies the integrity of the Profile using the keyset established in step 3.

7. The Profile is installed on the eUICC.

8. (a to d) The eUICC notifies the status of the download and installation process to the SM-SR, to the SM-DP and the Operator. The SM-SR updates the EIS information of the corresponding eUICC in its database.

End Conditions:

A. The Profile is installed on the eUICC.

4.5.1.1 Establishment of the Keyset

This chapter details the establishment of the keyset in step 3 in the Secure Download and Installation process.

The keyset is calculated by both the SM-DP and the eUICC on the base of a shared secret called ShS.

The ShS is generated locally by both entities SM-DP and eUICC using a Key Agreement Algorithm.

4.5.1.2 Key Agreement

A key agreement protocol is executed between the SM-DP and the eUICC to generate the Shared Secret ShS.

The ShS is generated by both SM-DP and the eUICC using a key agreement protocol (e.g. Elliptic Curve Key Agreement based on Diffie-Hellman or ElGamal – ECKA-DH, ECKA-EG).

The result of the key agreement protocol must provide authentication which will help protect against man-in-the-middle attacks Authentication of the eUICC to the SM-DP is mandatory.

The mutual authentication of the SM-DP and the eUICC is mandatory.

The following figure details the step 3 of Figure 30.

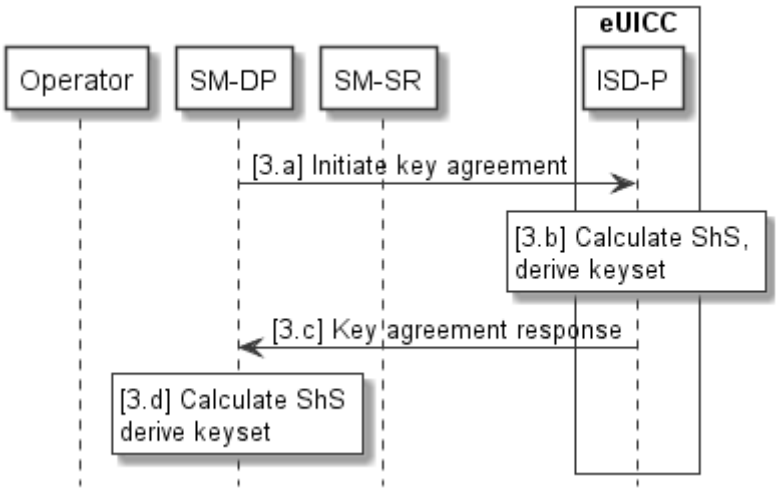

Figure 31: Key Set Establishment: Key Agreement Protocol (overview)

4.5.2 Mutual Authentication

This section details the mutual authentication mechanism between two entities in the architecture. The entities concerned within this section to authenticate each other are SM-DP to SM-SR and SM-SR to SM-SR. Authentication between other entities in the system MAY use other solutions for authentication and is not in the scope for this section.

To secure the messages being sent between the entities from an authentication point of view, at least one of the following two mechanisms SHALL be used:

1. Security within a message allowing it to be authenticated, e.g. Web Service Security (WS-Security);

Mutual authenticated transport level security, e.g. TLS.

5 Compliance requirements

5.1 SM-SR and SM-DP Compliance Requirements

#	Requirement
SMC1	Site Security of SM-DP and SM-SR SHALL be certified according to GSMA SAS-SM scheme [22].
SMC2	Functional compliance of SM-DP and SM-SR SHALL be verified through vendor or third party test suite according to the GSMA test plan.

5.2 eUICC Compliance requirements

#	Requirement
EUC1	eUICC SHALL be certified according to the GSMA Embedded UICC Protection Profile [27].
EUC2	Functional compliance of eUICC SHALL be verified through an independent GSMA industry-approved certification scheme.

5.3 EUM Compliance requirements

#	Requirement
EMC1	The EUM production site SHALL be GSMA SAS-UP [23] certified.

Annex A Interfaces

The purpose of this section is to provide additional information about the various interfaces required between the different elements of the architecture, and the functions to be supported over these interfaces.

A.1 EUM – SM-SR interface

The procedure “eUICC Registration at SM-SR” in section 3.5.1 mainly addresses this interface.

The main purpose is to enable the registration of the eUICC platform at the SM-SR.

A.2 Operator – SM-DP Interface

This interface covers the Profile ordering aspects and the procedure as defined in section 3.5.3. This interface is also used during the Profile Download and Installation procedure as defined in section 3.5.4, the Profile enabling via SM-DP as defined in section 3.5.7 and the ISD-P deletion via SM-DP as defined in section 3.5.10.

The following information is exchanged between the Operator and the SM-DP:

- The description of the Subscriptions e.g.:
  - The IMSI range or list of IMSIs, the ICCID range or list of ICCIDs
  - The Applications and files as defined in the relevant specifications (in particular 3GPP TS 31.102 [18], 3GPP TS 31.103 [19] and ETSI TS 102 221 [3].)
  - The algorithm parameters associated with its corresponding Network Access Application (for instance with Milenage: the OPc, ri, ci values)
- Other data or applications which are part of the Profiles.
- All relevant information needed to configure the future ISD-P, the Remote File Management and Remote Application Management applications.
- The Policy Rules.
- All relevant known information on the target eUICC and its SM-SR e.g.:
  - The geographical location of the SM-SR.
  - The type of communication supported by the SM-SR.
  - the security level to be supported by the SM-SR (in particular, the security association methods that can be used between the SM-DP and the SM-SR (see security section for proper recommendations))
  - The methods to be supported by the SM-SR to communicate with the eUICC (e.g. support of SMS and/or RAM over HTTP(s) over LTE/EPS)
  - The conditions under which the Profiles prepared and encrypted by the SM-DP are to be delivered directly (via SM-SR) to the specified eUICC.

The SM-DP provides:

- The relevant information for the Profiles to the Operator so that the Operator can provision the information relevant to the Subscription in its mobile network.

A.3 SM-DP – SM-SR Interface

This interface is used during the Profile download and installation, the Profile enabling via SM-DP, Profile disabling via-SM-DP, Profile deletion via SM-DP procedures.

The entity taking the role of SM-DP and/or the SM-SR MAY retain certain information related to the Profile according to the commercial agreement, Operator Policy Rules and regulatory data retention obligations.

A.4 Operator – SM-SR interface

This interface is used during the Profile enabling, Profile disabling, and Profile deletion procedures.

The SM-SR takes as input:

- Platform management requests from the Operator;
- Policy Rule (POL2) update from the Operator;
- The EID of the targeted eUICCs.

The Operator takes as input:

- The relevant parts of the EIS of the targeted eUICCs;
- Receipts/responses to Operator Platform management requests;
- Receipts/responses to Operator Policy Rule updates;
- Platform management-related events.

This interface is also used when managing the PLMA, allowing M2M SP to manage a Profile owned by an Operator on its behalf, and under PLMAs.

The related procedure is described in section 3.5.15.

A.5 SM-SR – eUICC interface

This interface is used during the Profile download and installation, the Profile enabling, the Profile enabling via SM-DP, Profile disabling, Profile disabling via-SM-DP, Profile deletion, Profile deletion via SM-DP procedures.

A.6 SM-SR – SM-SR Interface

This interface is used during the SM-SR Change procedure as defined in 3.5.11.

A.7 Operator – eUICC interface

This corresponds to the interface between the Operator and the eUICC.

A.8 M2M SP – SM-SR interface

This interface is used during the Profile enabling, Profile disabling, and Profile deletion via M2M SP procedures as defined in 3.5.16, 3.5.17 and 3.5.18.

A.9 Device – eUICC interface

This interface provides the possibility for a Device supporting Local Enable / Local Disable functionality to enable or disable the Test Profile or the Emergency Profile. Local Enable and Local Disable functions are only possible for the Test Profile or the Emergency Profile.

A Device supporting Emergency Calls, requiring a dedicated Emergency Profile, can use this interface to enable the Emergency Profile in situations requiring to set up an Emergency Call to specific Emergency Call number(s). The Device can use this interface to disable the Emergency Profile when the emergency situation has ended.

NOTE: An emergency situation MAY not end immediately after an Emergency Call, as it MAY be necessary to receive a call back from the Public Safety Answering Point (PSAP).

Annex B Risk Matrix (Informative)

This section lists risks, related impacted sensitive assets and impacted properties (C=Confidentiality, I=Integrity, A=Availability).

#	Risks	Definition	Assets	Impacts		
				C	I	A
Generic Risks						
V01	Failure in certificates or private keys chain	Penetration on a server managing master keys or private keys, loss of confidentiality due to human error or malevolence might lead to loss of trust in the entire process chain.	→all certificates	✓	✓	✓
V02	Authentication algorithm breach	Weakening of authentication algorithms due to malevolence, human error or other means.	→eUICC →authentication algorithm	✓	✓	
V03	Cryptographic breakthrough	A breakthrough in cryptographic research might lead to the weakening or total loss of authentication and ciphering schemes.	→All assets using cryptographic primitives	✓	✓	
V04	EID tampering	Installation of Profile on a wrong eUICC	→Profile		✓	
Provisioning & Delivery Risks						
V05	Denial of service on public network facing components	Denial of service using vulnerabilities in public interfaces or basic resource exhaustion techniques might lead to the impossibility of Provisioning and management of eUICC, and cause loss of services.	→Profiles →connectivity chain to eUICC			✓
V06	Critical component communication interception	Lax policies in network access or interconnection might lead to the interception and loss of confidentiality in critical assets such as Profiles.	→eUICC	✓		
V07	Penetration of the Subscription Management network	Lax policies in network access or interconnection might lead to the interception, alteration or deletion of critical assets such as Profiles.	→network components	✓		
V08	Rogue component insertion within trusted network (e.g. SM-SR or SM-DP)	A malicious or compromised partner might introduce a rogue component within a security domain leading to loss of integrity or confidentiality of critical information such as the Profile or a management command.	→All	✓	✓	✓
V09	Confidentiality loss of transport keys used to deliver the Profile up to the eUICC	Interception of transport key might lead to unsolicited connection to the eUICC or network component in order to perform denial of service, theft of service or impersonation.	→data protection key and its certificate	✓		
V10	Confidentiality or integrity loss of Profile during Provisioning or delivery	Communication of Profiles over non protected networks might lead to the interception or tampering of transiting Profiles	→Profiles →eUICC	✓	✓	

V11	Poor isolation of Profiles on the eUICC	Insufficient isolation of Profiles on the eUICC might lead to the reuse or leaking of critical part of the Profile such as the ISD-P or keys such as the K.	→eUICC →Profiles	✓	✓	
V12	Rogue Profile and Platform Management commands	Human error, malevolence or action from a malicious 3rd party might lead to unsolicited Profile or Platform Management commands resulting in loss of service, impersonation or fraud.	→management function key →eUICC		✓	✓
V13	PCF breach	Human error, malevolence or compromising of the PCF might enable scenarios where a Profile is able to bypass operators Profile policies	→PCF files →Profiles →eUICC	✓	✓	✓
eUICC Risks						
V14	eUICC tampering	Failure in providing a secure eUICC might lead to physical or logical attacks that might allow leaking or modifying of installed Profiles.	→eUICC	✓	✓	✓
V15	Installation of Profile within a non-certified eUICC	It might be possible for an attacker to install a valid Profile on a non-trusted eUICC (being soft or hardware) thus allowing for the extraction or replication of the Profile. This might lead to fraud or impersonation attacks	→eUICC	✓	✓	✓
V16	eUICC cloning	Failure to prevent Profile extraction or loss of confidentiality in the Profile creation database might lead to the leak of data enabling the cloning of eUICC and embedding them in soft or rogue eUICC in order to perpetuate fraud or impersonation.	→eUICC →data protection key and its certificate →OTA Keys → Profile keys	✓	✓	
Dependability						
V17	Failure to recover from a damaged Profile	Delivery of a malformed Profile might result in a loss of communication abilities and ultimately to Device loss.	→eUICC			✓
V18	Enabling of degraded Profiles	Inability for a eUICC to verify the integrity of a delivered Profile, might lead to the installation of a malformed or forged Profile leading to loss of service, OTA ping-pong storm, fraud or impersonation scenarios.	→eUICC		✓	✓
V19	Inability to wipe Profile	Inability to remove old Profiles from an eUICC might lead to the dead occupancy of a Profile slot, rendering Profile switching or Provisioning impossible.	→eUICC		✓	

V20	Failure to make emergency call	In case of forged, malformed or absence of a valid Profile, it might be impossible for a user to make emergency calls.	→ eUICC → Baseband		✓	✓
Device						
V21	Unauthorised ability to wipe Profile for reselling of stolen Device	If Profiles are erasable directly from the Device without authorisation by using a software or hardware switch, it might enable malicious 3rd parties to resell a stolen Device.	→ eUICC		✓	✓

Annex C List of Sensitive Assets (Informative)

This section lists the sensitive assets to be protected. The management of such assets is the most critical when they are available in clear and impacts the components accessing these assets (see 2nd column). However they MAY be transferred between entities as long as their security properties (integrity, confidentiality, authentication…) are not compromised. The fourth column of the following table corresponds to the criticality of the asset for the Embedded UICC ecosystem. The criticality illustrates a security impact on the architecture and the potential cost impact on the Actor(s) in case of security failure.

The following criticalities are considered:

- Criticality 4: the Embedded UICC ecosystem MAY be at risk with severe business risks for several or all Actors.
- Criticality 3: one part of the Embedded UICC ecosystem is affected; the affected Actor(s) MAY suffer strong effects which MAY endanger their whole business.
- Criticality 2: the service is temporarily interrupted; the affected Actor(s) have a major business impact.
- Criticality 1: the service is temporarily interrupted; the affected Actor(s) have a minor business impact.

Sensitive Asset	Asset Originator Owner	Asset Handled In Clear By:	Criticality
Authentication Algorithm	Operator	Operator, eUICC	3 to 4
Authentication Algorithm Key	Operator	Operator, eUICC, SM-DP	2 (one eUICC affected) to 4 (a set of eUICCs affected)
Authentication Algorithm Parameters (e.g. Opc, Ri-Ci etc.)	Operator	Operator, eUICC, SM-DP	2 (one eUICC affected) to 4 (a set of eUICCs affected)
IMSI	Operator	Operator, eUICC, SM-DP	1 (one IMSI affected) to 2 (a set of IMSIs affected)
MSISDN	Operator	Operator, SM-DP, SM-SR	1 (one MSISDN affected) to 2 (a set of MSISDNs affected)
GSMA CI Certificate	Root CA owner	Root CA owner	4
EUM Certificate	Root CA owner	EUM	3
eUICC Certificate	EUM	EUM, eUICC	2 to 3
EID	EUM	SM-SR, eUICC, SM-DP, Operator, , EUM	1 (one EID affected) to 2 (a set of EIDs affected)
Profile	Operator	Operator, eUICC, SM-DP	3 to 4

Sensitive Asset	Asset Originator Owner	Asset Handled In Clear By:	Criticality
Operator OTA Keys	Operator	Operator, eUICC, SMDP	3 to 4
PCF rules	Operator	eUICC, Operator, SM-SR, SM-DP	3 to 4

Profile Management Sensitive Data	Asset Originator Owner	Asset Handled In Clear By:	Criticality
Platform management keyset	SM-SR	SM-SR, eUICC	2 to 4
Profile Management keyset	SM-DP	SM-DP, eUICC	4

Annex D Additional Information Related to Section 4.5 (Informative)

Nomenclature used in this annex:

Acronym	Definition
EC	Elliptic Curves
Ke	The key from the keyset used for encryption
Km	The key from the keyset used for message authentication and integrity protection.
Ku	The key from the keyset used for protection of key values.
PK_{euicc}	This Public key is part of the eUICC Certificate. In GlobalPlatform, it corresponds to the public key of the ECASD. For ElGamal Elliptic Curves key agreement this key is PK.CASD.ECKA [GP Am. E] For signature verification by external entities this key is PK.CASD.AUT [GP Am. A] For confidentially (encryption by external entity) this key is PK.CASD.CT [GP Am. A]
SK_{euicc}	Private key of the eUICC. In GlobalPlatform, it corresponds to the private key of the ECASD. For ElGamal Elliptic Curves key agreement this key is SK.CASD.ECKA [GP Am. E] For signature by eUICC this key is SK.CASD.AUT[GP Am. A] For decryption by eUICC this key is SK.CASD.CT [GP Am. A]
PK_{SM-DP}	Public Key of the SM-DP
SK_{SM-DP}	Private Key of the SM-DP
PK_{eph}	Ephemeral Public Key generated by the SM-DP
SK_{eph}	Ephemeral Private Key generated by the SM-DP

D.1 Void

Void

D.2 Details on the ElGamal Key Agreement

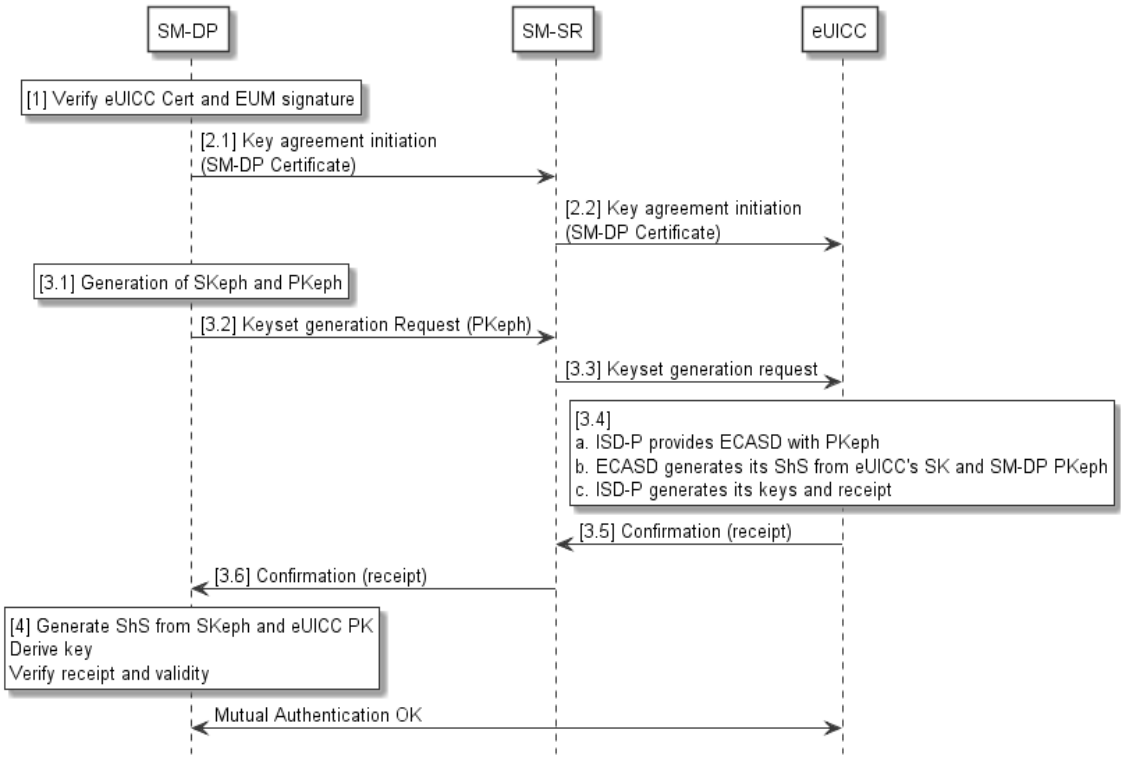

Figure 32 : ElGamal Key Agreement

Start Condition: The SM-SR has connectivity with the eUICC.

1. The SM-DP verifies the eUICC Certificate, which carries a signature from the EUM. This is part of step 1.e of Figure 30.

2.1 and 2.2 The SM-DP sends its certificate to the eUICC through the SM-SR

3.1 The SM-DP generates an ephemeral EC (elliptic curve) key pair, named SKeph and PKeph and sends PKeph to the SM-SR.

3.2 and 3.3 The SM-DP sends a key set generation request to the SM-SR, including the ephemeral public key PKeph. The SM-SR passes the request for key set generation to the ISD-P on the eUICC, providing the PKeph.

3-4. The eUICC now performs the following actions: The ISD-P provides the ECASD with the PKeph.

The ECASD generates a Shared Secret ShS from its own secret key and received ephemeral PKeph and returns it to the ISD-P.

The ISD-P uses ShS to generate its own key pair as well as a receipt from the operation.

3-5. The ISD-P passes a confirmation (with receipt) of the generation back to the SM-SR..

3-6. The SM-SR passes the confirmation back to the SM-DP.

4. The SM-DP generates ShS from the ephemeral secret key SKeph and the eUICCs public key.

The SM-DP uses this calculated ShS to derive the same key set as generated by the ISD-P.

The SM-DP verifies the receipt it received from the eUICC to verify the validity of the entire operation. Together with the eUICC Certificate verified in step 1, this also confirms the authenticity of the eUICC, and confirms the correct keyset derivation on both the eUICC and the SM-DP server.

End Condition: A secret key set, whose contents are only known within the ISD-P and by the SM-DP has been generated and the eUICC is authenticated to the SM-DP.

In a GP based model, for key agreement the PK_{euicc} corresponds to PK.CASD.ECKA which is part of CERT.CASD.ECKA signed by the EUM.

D.3 Calculation of the keyset (Ke, Km, Ku)

The keyset is constituted of 3 keys, derived from the ShS, calculated both by eUICC and SM-DP entities as follow:

- Ke: encryption key used to encrypt the Profile;
- Km: integrity key used for MAC;
- Ku: key from the keyset used for protection of key values.

To be calculated, these keys SHALL use a Key Derivation Function (KDF).

The KDF could be a PRF (Pseudo Random Function) which is a combination of one way hash functions. Several PRFs can be used in the Key Derivation Function.

The KDF could take as parameters information related to the eUICC, the Profile owner (Operator), the Profile itself, the SM-DP or the card issuer.

These different keys are calculated as follow:

Ke=KDF(ShS, additional_information, diversified_parameter*1);*

Km=KDF(ShS, additional_information, diversified_parameter2);

Ku=KDF(ShS, additional_information, diversified_parameter3);

With,

additional_information is a common diversification input to generate the three keys; it could include information relating to Operator, SM-DP, eUICC, Profile and a nonce.

*Diversified_parameter*s are diversification parameters to generate different keys.

The Profile can be sent from the SM-DP to the eUICC on the base of a secure channel protocol using this keyset.

D.4 Role of the EUM in the Certificate Chain

The EUM is required in the different key establishment scenarios to sign the eUICC Certificate which contains the public key of the asymmetric key pair of the eUICC (stored in the ECASD in the GlobalPlatform scenario). By verifying this signature and by checking the response produced by the eUICC in the key establishment procedure, the SM-DP can authenticate the eUICC independently of the SM-SR.

D.5 Mutual Authentication Binding to a SOA Environment

This section provides information when deploying eUICC remote management system in SOA environment using Web Services technology, following the OASIS and W3C WS-* standard. This standard provides interoperability and loose coupling between parties named as “message requester” and “message receiver”.

The architecture does not prevent from using another type of technology if the security requirements detailed in this document are met. It implies that both message requester and message receiver uses the same technology.

D.5.1 Authentication

To secure the messages being sent between the entities, at least one of the following two mechanisms SHALL be used:

1. WS-Security standard for client authentication and transport level security (TLS) for server authentication.
2. Mutual authenticated transport level security (TLS).

In both cases the authentication at TLS level requires the use of digital signed certificates.

A platform that needs to prove its identity at TLS level is required to have X.509 certificates (and public-private key pairs).

The specifics of who is trusted to issue X.509 certificates depend on the organisation's PKI setup. For authentication, the subject of the X.509 certificate identifies the Actor. We also assume that the issuer of the X.509 certificates is a general Certificate Authority not directly involved in any authorisation of the web service transactions, but is relied on for the validity of the X.509 certificate in a manner out of scope of the scenarios covered.

Annex E Void

Annex F Profile Creation, Ordering and Personalisation (Informative)

The following diagram shows an example of how the functions defined in section 3.3.1.1 MAY be performed.

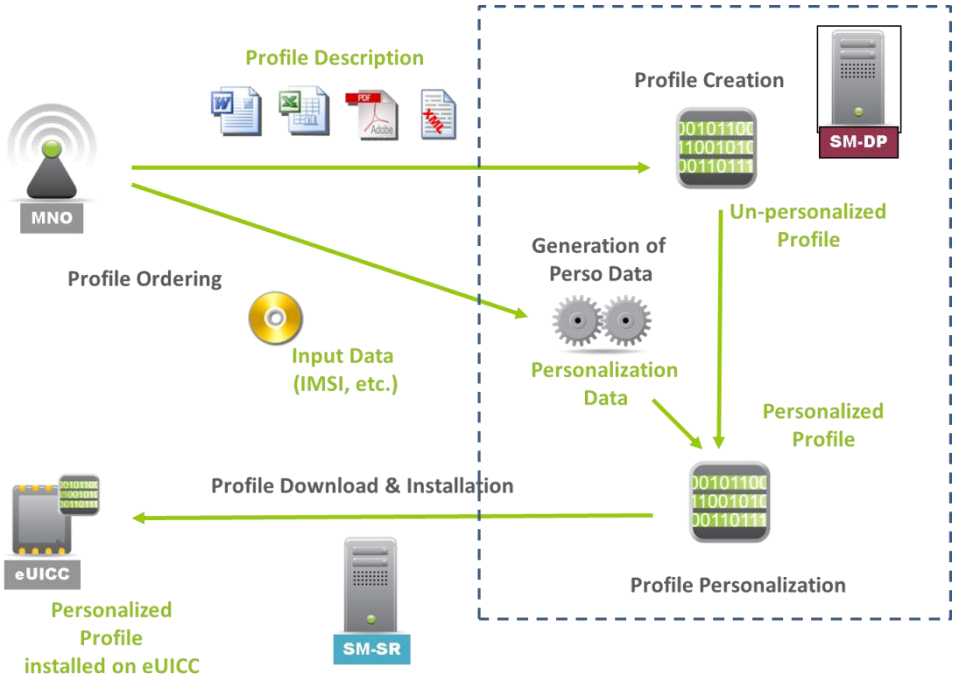

Figure 33: Profile Creation, Ordering and Personalisation

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	01/7/2013	1st Release of Document, submitted to DAG#108 and PSMC#116 for approval	GSMA Embedded SIM Leadership Team and PSMC	Ian Smith, GSMA
V1.1	06/12/2013	2nd Release of Document, submitted to DAG#108 and PSMC#116 for approval	GSMA Embedded SIM Leadership Team and PSMC	Ian Smith, GSMA
V4.0	25/02/2019	Version 4 is released (skipping v2.0 and v3.0) to align with SGP.02 version V4.0. .	GSMA Embedded SIM Leadership Team and TG	Yolanda Sanz, GSMA

Other Information

Type	Description
Document Owner	Embedded SIM
Editor / Company	Alejandro Pulido, VALID

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.