Embedded SIM Remote Provisioning Architecture

Version 1.1

17 December 2013

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

Many machine-to-machine Devices will not be easily reachable for the purpose of Provisioning a Subscription. This will require a new solution to accommodate this special situation.

The requirement is to define a mechanism for 'over the air' remote Provisioning of machine-to-machine Devices with the necessary credentials to gain mobile network access, under the assumption that the same or similar authentication protocols as today will be used. The MNO will have to be able to respond to requests to change Subscription (contract) from one MNO A to a different MNO B, without having physical access to the Embedded UICC in the Device in question.

This document describes an architecture which, when implemented, will enable remote Provisioning and Subscription management, while at the same time maintaining at least the same level of security both for network operators and Customers as present solutions. This includes the safe keeping of MNO Network Access Credentials, such as keys for cryptographic functions, and identifiers such as IMSI and other Customer identities used.

1.2 Scoping the Problem

This document addresses:

- The Machine-to-Machine use cases as described in GSMA 'Embedded SIM Task Force Requirements and Use Cases' Version 1.0 [1]. This solution is not intended to apply to traditional consumer telecommunication devices as they are not concerned with the problem statement above.
- Architecture of the remote Provisioning system for Embedded UICCs i.e. its components and the related interfaces. The GSMA's Embedded UICC Ecosystem document [2], and the principles and assumptions stated in section 2 will support its definition.
- Security of the remote Provisioning system for Embedded UICCs.
- SM-SR and SM-DP integration options within network infrastructure.
- The necessary aspects of the Embedded UICC architecture and its external interface to ensure compatibility with the GSMA architecture prior to delivery of an ETSI standard.
- The standardisation of the Embedded UICC remote Provisioning architecture where appropriate.

1.3 Document Purpose

The aim of this document is to define a common global architecture framework to enable the remote Provisioning and management of the Embedded UICC (eUICC) in machine-to-machine Devices which are not easily reachable. The adoption of a common architecture framework will provide a basis for ensuring global interoperability between potentially different MNO deployment scenarios while utilising a standardised eUICC platform.

This document identifies the individual Roles and the potential Actors as well as the interfaces between each of the Roles in the architecture.

1.4 Intended Audience

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

1.5 Definition of Terms

Term	Description
Actor	An actor is a 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 terminal, and enables the secure changing of Subscriptions.
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 is certified by the EUM Certificate.
eUICC Manufacturer	Supplier of the eUICC modules and resident software (such as firmware and operating system)
EUM Certificate	A certificate issued to a GSMA accredited EUM to issue eUICC Certificates. This certificate is certified by the Root Certificate.
Fall-back Mechanism	eUICC based mechanism which enables the Profile with Fall-back Attribute set.
Fall-back Attribute	This is an attribute of a Profile which, when set, identifies the Profile to be enabled by the Fall-back Mechanism. Only one Profile on the eUICC can have the Fall-back attribute set at a time.
Form Factor	Manifestation of UICC. Specified in ETSI TS 102 221 [102221] and ETSI TS 102 671 [102671].
Generic Profile	Profile generated by the SM-DP following the MNO's specifications, but without the MNO's credentials and any specific data linked to the future targeted eUICC.

Term	Description
Integrated Circuit Card ID	Unique number to identify the Provisioning or Operational Profile in a eUICC Note: the ICCID throughout this document is used to identify the Profile (Provisioning and Operational Profile)
International Mobile Subscriber Identity	Unique identifier administered by regional authorities and allocated to Mobile network Operators to provision within their Network Access Applications to enable Devices to attach to a network and use services.
Mobile Network Operator	An entity providing access capability and communication services to its Customers through a mobile network infrastructure.
Network Access Application	An application residing on a UICC which provides authorisation to access a network. E.g. a USIM application.
Network Access Credentials	Data required to authenticate to an ITU E.212 [E212] 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 MNO's (e.g. STK) applications and 3rd party applications.
Operator Credentials	Set of credentials owned by Mobile Network 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, e.g. due to the termination of the Customer's contract with the MNO.
OTA Keys	The credentials included in the Profile, used in conjunction with OTA Platforms.
OTA Platform	An MNO platform used for remote management of UICCs and enabled MNO profiles on eUICCs.
Personalised Profile	Un-personalised Profile with the addition of the Personalisation Data for the eUICC targeted by the MNO.
Personalisation Data	Set of data derived from the input data provided by the MNO and generated by the SM-DP (e.g. NAC, Keys, etc.) and dedicated to the personalisation of a unique Personalised Profile.
Platform Management	A set of functions related to the transport, enabling, disabling and deletion of a Profile on 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.

Term	Description
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 transport, enable, disable and delete Profiles on the eUICC.
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.
Profile Description	Description of a Profile in a format specific to the MNO; Example formats include Excel table, xml format and plain text.
Profile Management	A set of functions related to the transport, downloading, installation and content update of a Profile in a dedicated ISD-P on the eUICC. Download and installation are protected by Profile Installer Credentials shared between the SM-DP and the ISD-P.
Profile Installer 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.
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.
Root Certificate	A certificate used to authenticate and authorise the entity that issues EUM Certificates.
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.

Term	Description
Subscriber	An entity (associated with one or more users) that is engaged in a Subscription with a Service Provider. The subscriber is allowed to subscribe and unsubscribe to services, to register a user or a list of users authorised to enjoy these 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 Service Provider.
Subscription Manager Data Preparation	Role that prepares Operational and Provisioning Profiles to be securely provisioned on the eUICC and manages the installation of the Profile on the eUICC
Subscription Manager Secure Routing	Role that securely performs functions which allow secure transport of both Platform and Profile management commands in order to load, enable, disable and delete Profiles on the eUICC.
Service Provider	Actor who provides services to its service Subscribers on a contractual basis and who is responsible for the services offered.
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
ECASD	eUICC Certificate Authority Security Domain
DAP	Data Authentication Pattern
DPID	ID of the relevant SM-DP
EUM	eUICC Manufacturer
EID	eUICC-ID
EIS	eUICC Information Set
EncP	Encrypted and integrity protected Personalised Profile
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
eUICC	Embedded Universal Integrated Circuit Card
GP	GlobalPlatform
GPCS	GlobalPlatform Card Specification
GSMA	GSM Association

Abbreviation	Description
ICCID	Integrated Circuit Card ID
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
ISO	International Standards Organisation
ITU	International Telecoms Union
LTE	Long Term Evolution
M2M	Machine to Machine
MNO	Mobile Network Operator
MNO-SD	Mobile Network Operator Security Domain
NAA	Network Access Application
OTA	Over The Air
POL1	Policy Rules within the Profile
POL2	Policy Rules associated to a Profile and stored in the relevant EIS at the SM-SR
SAS	Security Accreditation Scheme
SCP	Secure Channel Protocol
SD	Security Domain
SIM	Subscriber Identity Module
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
UMTS	Universal Mobile Telecommunications Service
USIM	Universal Subscriber Identity Module

1.7 References

Ref	Document Number	Title
[1]	NA	GSMA 'Embedded SIM Task Force Requirements and Use Cases' Version 1.0
[2]	12ESWG1_10r8	Embedded SIM Fast Track Working Group – Eco-system, Roles and Commercial Relationships
[102221]	ETSI TS 102 221	UICC-Terminal interface; Physical and logical characteristics
[102222]	ETSI TS 102 222	Administrative commands for telecommunications applications
[102223]	ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT)

Ref	Document Number	Title
[102225]	ETSI TS 102 225	Secured packet structure for UICC based applications
[102226]	ETSI TS 102 226	Remote APDU structure for UICC based applications
[102671]	ETSI TS 102 671	Smart cards; Machine to Machine UICC; Physical and logical characteristics
[103383]	ETSI TS 103 383	Embedded UICC; Requirements Specification
[GPCS]		GlobalPlatform Card Specification v.2.2.1
[GPUICC]		GlobalPlatform Card Specification v.2.2.1 UICC Configuration v1.0.1
[AmdA]		GlobalPlatform Card Specification v.2.2 Amendment A: Confidential Card Content Management, v1.0.1
[AmdB]		GlobalPlatform Card Specification v.2.2 Amendment B: v1.0.1
[AmdD]		GlobalPlatform Card Specification v.2.2 Amendment D: Secure Channel Protocol 03, v1.1
[AmdE]		GlobalPlatform Card Specification v.2.2 Amendment E: Security Upgrade for Card Content Management v1.0
[E212]	ITU E.212	The international identification plan for public networks and Subscriptions
[21133]	3GPP TS 21.133	3G Security, Security Threats and Requirements
[31102]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application
[31103]	3GPP TS 31.103	Characteristics of the IP Multimedia Services Identity Module (ISIM) application
[NIST]	NIST SP 800-57 Part 1	NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General (Revision 3)

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	Global Platform 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 requirements will be placed on the Device.
DEV3	No new certification requirements 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 [102221] for all standardised ETSI Form Factors.
DEV6	The Device manufacturer shall ensure that there is a method for the owner of the Device or 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 [21133] “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 will become mandatory for the eUICC because the entity which contains the Operator Credentials may be no longer under the design control of the MNO.
SEC5	The remote Provisioning architecture must avoid compromising the security of Customer 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 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 SIM Fast Track working group. Regulatory issues will be referred to the GSMA regulatory team.

2.3 The eUICC Ecosystem

ECO1	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 MNO’s Profile and in the SM-SR. 2. Policy Rules are enforced by the eUICC and the SM-SR on behalf of the MNO. 3. Control of Policy Rules lies with the MNOs.

2.3.1 Roles and Entities

2.3.1.1 eUICC Manufacturer

MAN1	1. The manufacturer of the eUICC 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 forwarded to the SM-SR to be associated with each eUICC. 4. The eUICC Manufacturer is responsible for the initial cryptographic configuration and security architecture of the eUICC. 5. The relevant parts of the eUICC Manufacturer’s products and processes are certified by a GSMA-approved certification process.

MAN2	The EUM shall issue the eUICC Certificate to allow: • the eUICC authentication and certification to other entities; • the authenticated keyset establishment between a SM-DP and an eUICC; • the authenticated keyset establishment between a SM-SR and an eUICC.
MAN3	The EUM Certificate and Root 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.

2.3.1.2 Machine to Machine Device Manufacturer

DMA1	1. The Device manufacturer builds machine to machine Devices which comprise a communication module and an eUICC. 2. A Provisioning Profile and/or Operational Profile may be enabled by default. Note: Any Enabled Profile requires the agreement of the respective MNO.

2.3.1.3 Mobile Network Operator (MNO)

MNO1	1. The MNO provides mobile network connectivity. 2. The MNO selects at least one SM-DP. 3. The MNO shall have a direct interface to the SM-SR. 4. In the event that a Customer has selected an MNO, that MNO initiates the download of a particular Profile to an identified target eUICC subject to current Policy Rules. 5. The MNO specifies the Profile characteristics and any features and applications, analogous to current UICCs. The MNO 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 requirements shall apply. 8. The MNO defines the Policy Rules that control the Profile management when this Profile is enabled. 9. After the download is ordered the MNO 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 MNO shall receive confirmation of the successfully completed download and installation of the Profile. 11. The enabled MNO 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 Customer the MNO 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 MNO should provide only limited service to a Device using a Provisioning Profile; the mechanism the MNO uses to enforce this limited service is out of scope of this architecture.

2.3.1.4 MNO Customer

CUS1	1. The MNO Customer is the actual contract partner of the MNO for the Subscription. He may not be identical to the end user. 2. The MNO Customer uses a machine to machine Device equipped with a eUICC from the Device manufacturer and a Profile (Subscription) from a selected MNO. 3. Prior to the download of a Profile the MNO Customer must provide his implicit or explicit acceptance. 4. The MNO Customer directly or indirectly identifies the machine to machine Device. 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 can be identical to the MNO Customer. 3. The eUICC is transparent to the end user. 4. The end user's relationship is with an MNO Customer or the MNO directly.

2.3.1.6 Subscription Manager – Data Preparation (SM-DP)

SMDP1	1. The SM-DP acts on behalf of the MNO. 2. The SM-DP receives a Profile Description from the MNO 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 MNO. 4. The SM-DP builds Personalised Profiles for the targeted eUICC. 5. The SM-DP shall secure the Profile package with the Profile Installer 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 MNO the SM-DP also initiates Profile enabling, and Profile deletion 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 to the SM-SR.
SMDP5	The SM-DP must always receive a request from an MNO to send a Profile via an SM-SR to an eUICC.
SMDP6	The SM-DP shall at least be GSMA SAS certified.
SMDP7	Given any eUICC, the SM-DP shall be able to generate a Personalised Profile for this eUICC.
SMDP8	The SM-DP and MNO are the only entities allowed to establish a secure and authenticated channel to the eUICC to manage a Profile.
SMDP9	The MNO shall be able to interface to an SM-DP of the MNO's choosing to serve any MNO 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 MNO.
SMDP11	The SM-DP shall support the Profile ordering procedure described in section 3.5.3 of this document.

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 MNO's Policy Rules.
SMSR3	The SM-SR obtains the Platform Management Credentials of the eUICC from the eUICC Manufacturer or from 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 and MNO. 3. The SM-SR shall at least be GSMA SAS-like 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.

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, SM-DP and MNO.
CIS3	The Certificate Issuer communicates with the MNO, SM-SR, SM-DP and EUM through interfaces that are out of scope of this specification.

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 can assumed to be a MNO.
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.

2.4 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. The eUICC shall contain a Profile with Fall-back Attribute set. Only one Profile can have the Fall-Back Attribute set. 4. The Profile with Fall-back Attribute set cannot be deleted. 5. The setting of the Fall-back Attribute is managed by the SM-SR. 6. All relevant UICC specifications shall apply.
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 identity of its associated SM-SR and have a means to authenticate it.
EUICC10	eUICCs delivered by the eUICC Manufacturer 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.

2.4.1 Profiles

PRO1	Profiles are the property of the issuing MNO.
PRO 2	Profiles shall be uniquely identified.
PRO 3	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 always remains an action that is executed only by the SM-SR acting on behalf of the Operator. 3. Actions shall be undertaken according to Policy Rules.
PRO 4	1. A Profile is under the control of the issuing MNO. 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.
PRO 5	Each Profile shall be isolated within its own dedicated secure container. The GlobalPlatform's Security Domain framework shall be considered.
PRO 6	Profiles can be used either for Provisioning (Provisioning Profile) or for operation (Operational 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.
PRO 7	There will always be one Provisioning Profile.
PRO 8	There may be several Operational Profiles.
PRO 9	Installed Profiles can have one of the following states: • enabled • disabled
PRO 10	In all operational uses the eUICC shall enforce that one, and only one, Profile is enabled at any point in time.

PRO 11	There will be a capability for eUICC–initiated enabling of the Profile with Fall-back Attribute set. The Profile with Fall-back Attribute set will consequently provide network connectivity to allow SM-SR to remotely manage the eUICC.
PRO 12	There will be no local Profile management by the machine to machine Device.
PRO 13	A Profile contains parameters for an authentication algorithm (e.g. OPc, ri, ci for the Milenage algorithm) but not the algorithm itself.
PRO 14	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.
PRO 15	A Profile contains a subset of Policy Rules to control external Profile management actions.
PRO 16	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 [102221])
PRO 17	Any function, feature or service which is possible on a current UICC shall be possible in an Operational Profile on an eUICC.
PRO 18	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.
PRO 19	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.
PRO 20	Profiles are stored only in the SM-DP and installed on the eUICC; they are not stored anywhere else and are encrypted in transit.

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 MNO.
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.

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.

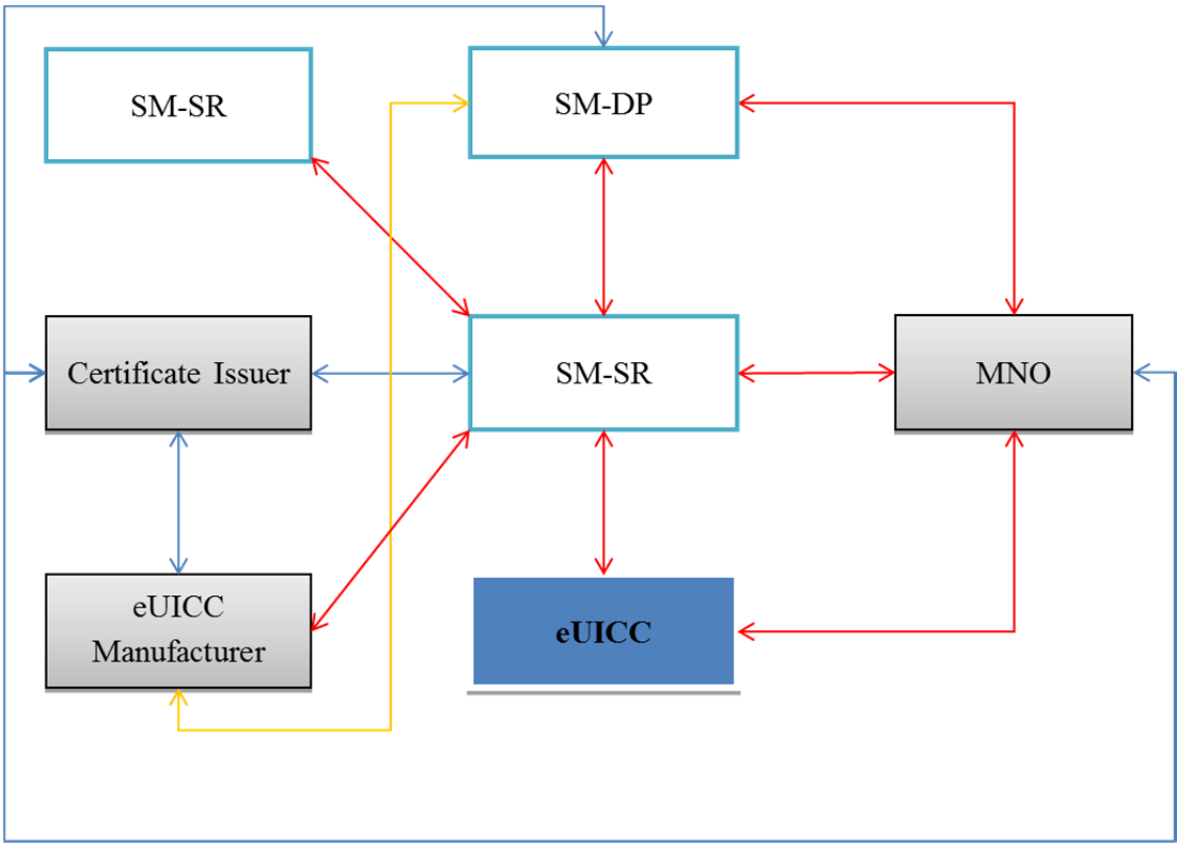

Figure 1: eUICC Remote Provisioning System

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 SCP02/03 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 [GPCS], it is also configured via privileges, and except for being there in the beginning, no major specific feature remains. This should allow MNOs 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 Global Platform Card Specification [GPCS]. Profiles are contained within security domains (SD) on the eUICC, thus making the security mechanisms of SDs available. Further information can be found in [GPCS].

The following figure outlines a schematic representation of the eUICC.

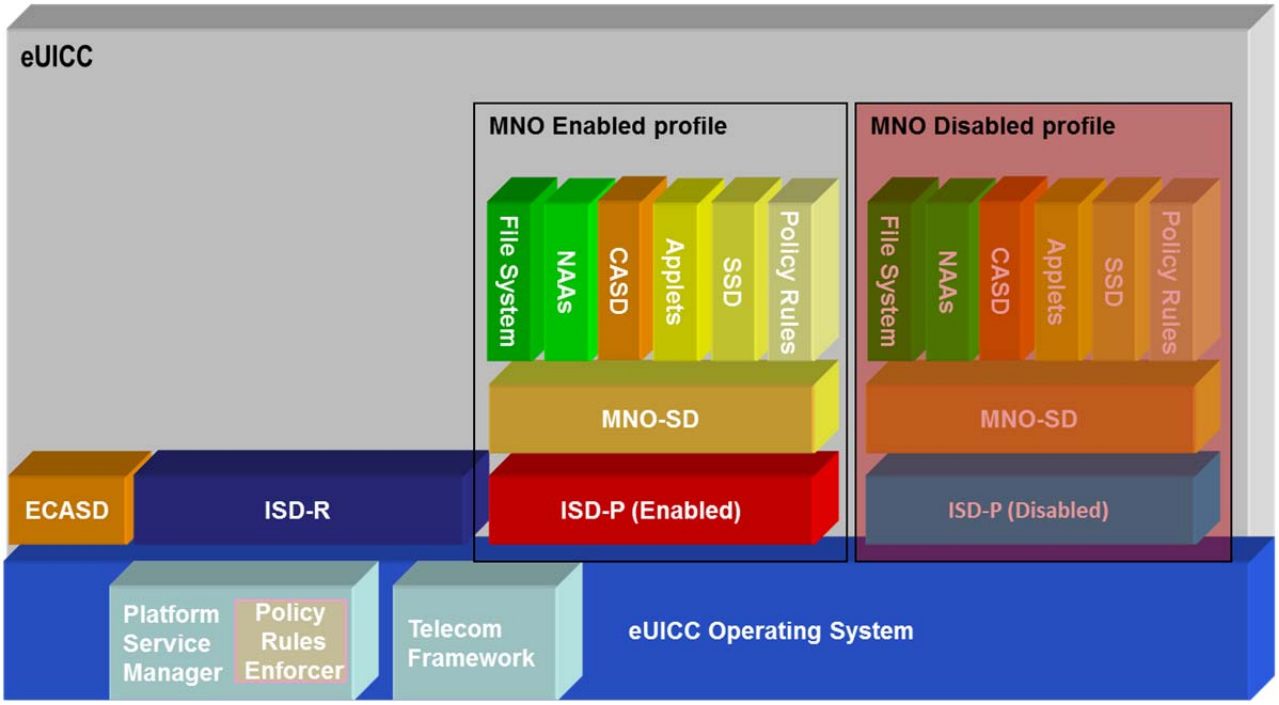

Figure 2:Schematic Representation of the eUICC

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

The ECASD (eUICC Certificate Authority Security Domain):

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

- Is based on the concept of CASD from Global Platform (see [GPCS], [AmdA] and [AmdE]);
- Is configured by the eUICC Manufacturer 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 manufacture;
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 [GPCS]) 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 memory quota (Note: memory quota management 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 MNO, or SM-DP if delegated by the MNO.

An ISD-P shall:

a) Be a separate and independent entity on the eUICC
b) Contain a Profile including 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 MNO.

An MNO-SD shall:

j) Be associated to itself;
k) Contain the MNO OTA Keys;
l) Provide a secure OTA channel (SCP80 or SCP81 as defined in [102225] and [102226]);
m) 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 MNO 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 [102221] and 3GPP TS 31 102 [31102]) 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 set up, the SM-DP, on behalf of the MNO, can create 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.

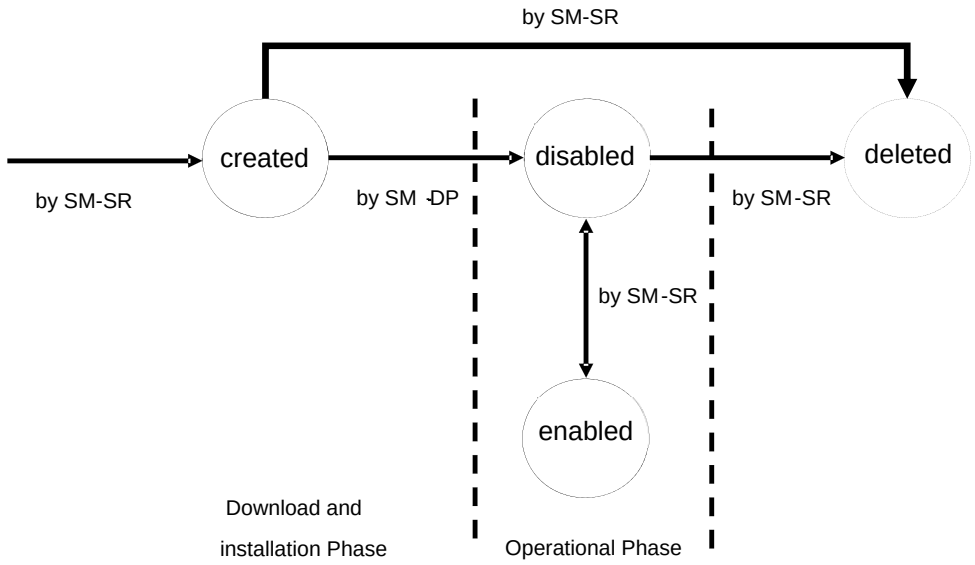

Figure 3: ISD-P State Diagram

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 MNO's Profile Description and the type of eUICC targeted.

The SM-DP generates the Un-personalised Profile using the services, scripts, tools or documentation provided by the EUM of the target eUICC(s). The information exchanged between the SM-DP and EUM is not standardised and may differ between different entities.

It is assumed the SM-DP tests the Un-personalised Profile with a sample of the target eUICC. The MNO 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.

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 MNO 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 MNO 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 MNO (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 MNO. 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, the services, scripts, tools or documentation supplied by the EUM must support at least the following eUICC attributes which may be delivered by the MNO. 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 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 deals with the download and installation of a Personalised Profile into the targeted eUICC.

3.3.1.2.3 Profile Content Update Function

This is realised by an MNO OTA Platform.

3.3.1.2.4 Policy Rules Update Function

This covers the update of 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.

3.3.1.3 Functions for Platform Management

3.3.1.3.1 ISD-P Creation Function

This deals with the creation of an ISD-P in the eUICC in preparation for Profile content to be loaded.

3.3.1.3.2 ISD-P Deletion Function

This deals with 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.

The deletion of an ISD-P can only happen when it is in disabled state (see state diagram in section 3.2.3).

3.3.1.3.3 Master Delete Function

This deals with 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.

3.3.1.3.4 Profile Enabling Function

This deals with the enabling of a Profile.

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

3.3.1.3.5 Profile Disabling Function

This deals with the disabling of a Profile.

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

3.3.1.3.6 Set Fall-back Attribute

This deals with the setting of the Fall-back Attribute of the Profile(s) 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 machine to machine 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 deals with the registration of an eUICC in a SM-SR.

3.3.1.4.2 SM-SR Change Function

This deals with the change of a 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 deals with the enabling of the Profile with Fall-back Attribute set.

This function automatically 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.

3.3.2 Assignment of Functions to Relevant Actors and Roles

Function	MNO	SM-DP	SM-SR	eUICC
Data Preparation:				
Un-personalised Profile Creation		X		
Profile Ordering	X			
Generation of Personalisation Data	X	X		
Profile Personalisation		X		
Profile Management:				
eUICC eligibility verification	X	X	X	
Profile Download and Installation		X		
Profile Content Update	X			
Policy Rules Update	X			
Platform Management:				
ISD-P Creation			X	
ISD-P Deletion			X	
Master Delete			X	
Profile Enabling			X	
Profile Disabling			X	
Set Fall-back Attribute			X	
Transport			X	
Policy Enforcement			X	X
eUICC Management:				
eUICC Registration			X	
SM-SR Change			X	
eUICC Functions:				
Fall-back Function				X

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 [31102], 3GPP TS 31.103 [31103] and ETSI TS 102 221 [102221]).

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

For an MNO OTA Platform, the Enabled Profile is equivalent to an UICC as per ETSI TS 102 225 [102225], TS 102 226 [102226] and TS 102 223 [102223]. The Policy Rules POL1 attached to the Profile are managed through the MNO 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 Customer and a 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 MNO 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
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.

3.5.1 eUICC Registration at SM-SR

eUICCs are manufactured, according to given standards, generally independent from machine to machine Device makers, mobile operators or Service Providers. The machine to machine Device manufacturers can select any certified eUICC that fits their purpose and order it in the necessary quantity directly from the EUM. As a mandatory step in the production process and prior to shipment, 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 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 MNO 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:

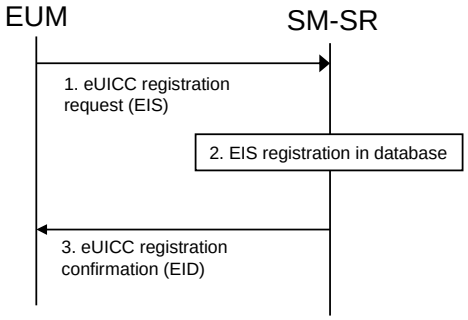

Figure 4: eUICC Registration at SM-SR

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. The confirmation message includes the EID.

End Condition: The eUICC is registered at the SM-SR and ready for Profile download. It can now be shipped to the machine to machine Device manufacturer.

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

Following registration and shipment, the eUICCs are embedded into machine to machine Devices during the Device manufacturing process.

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 MNOs and SM-DPs (Profile validation strategy, which tests may be performed by the MNO, which may be done by the SM-DP, what may be exchanged between the MNO 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 MNO to the SM-DP and the Un-personalized 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 MNO 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 MNO), 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 MNO.

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 MNOs.

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

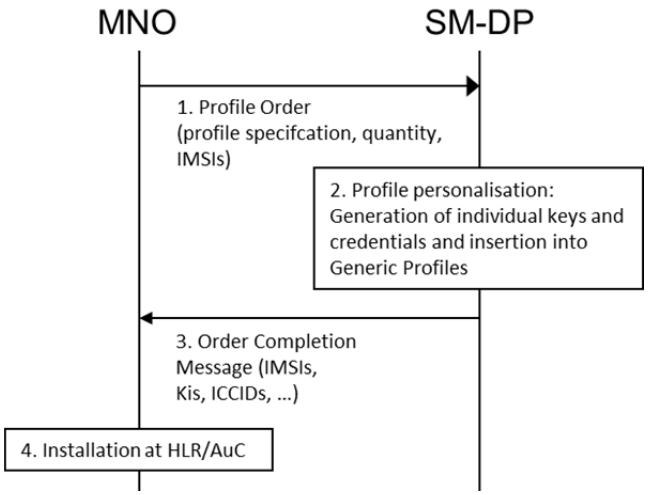

Figure 5: Profile Ordering

Start Conditions:

a. An Un-personalised Profile has been created by the SM-DP based on the Profile Description provided by the MNO.
b. The MNO 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 MNO 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 MNO. 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 MNO, including all data necessary to register the Profiles in the MNO's backend systems. Each Profile is uniquely identified at least by its ICCID.
4. The MNO installs the Profiles in the related systems, e.g. HLR, AuC, CRM. These procedures are no different from current UICC registration processes at the MNO.

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

3.5.4 Profile Download and Installation

In order for the machine to machine 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:

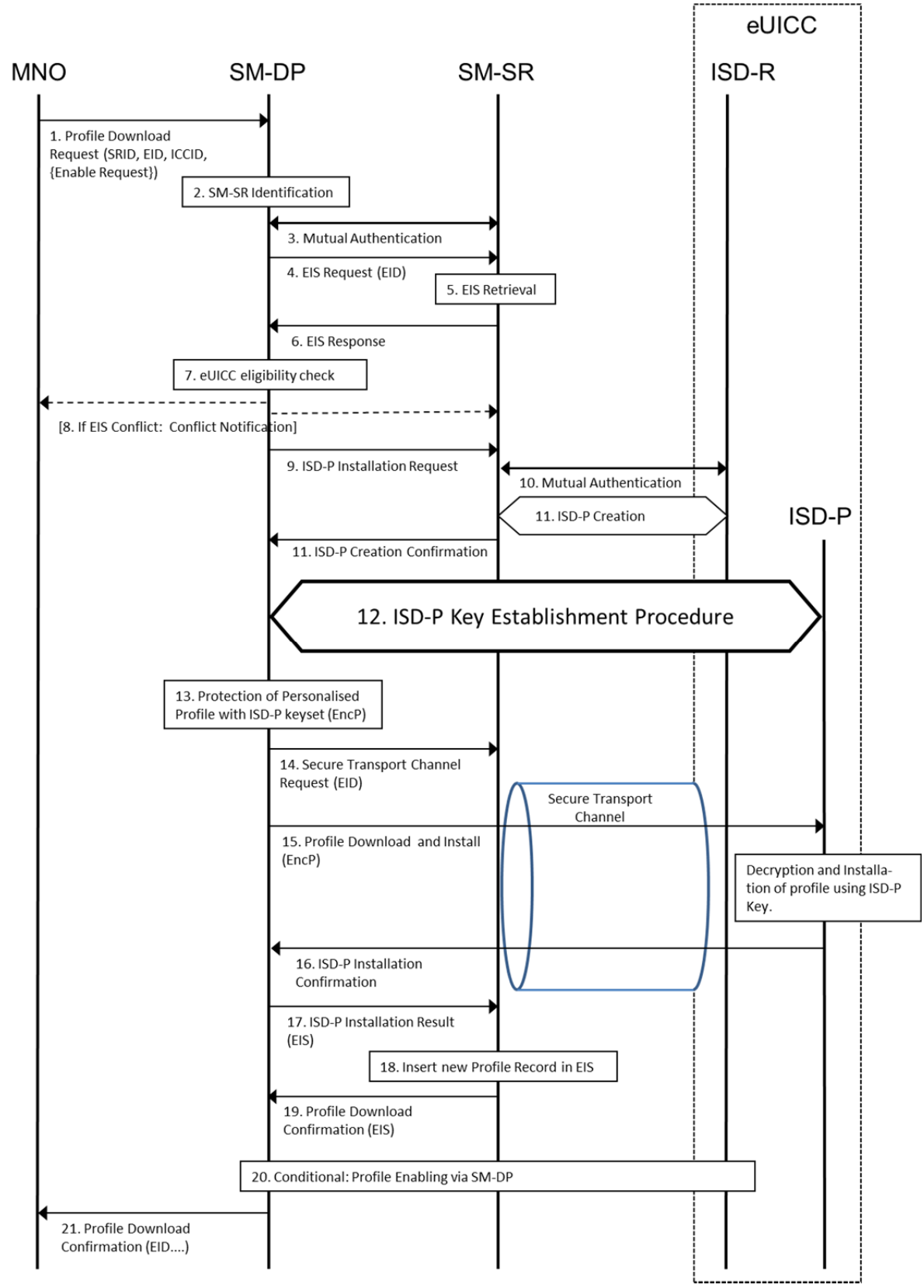

Figure 6: Profile Download

Start Conditions:

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

Procedure:

1. The MNO 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 MNO may also ask the SM-DP to enable the Profile once it is downloaded and installed.
2. Based on the information provided by the MNO, 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 a 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 MNO and the SM-SR.
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 authenticates the eUICC and a shared key set is established between the ISD-P and the SM-DP. 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, yielding 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 and state of the ISD-P to the SM-DP.

    The MNO 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 MNO.

    Note: If the MNO decides that the key set is retained by the SM-DP the MNO 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 and state of the ISD-P 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. This message includes the relevant parts of the EIS.
20. If the MNO 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 MNO. This message can include the EID and the information to identify the Profile.

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

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 MNO with the authorisation of the Customer.

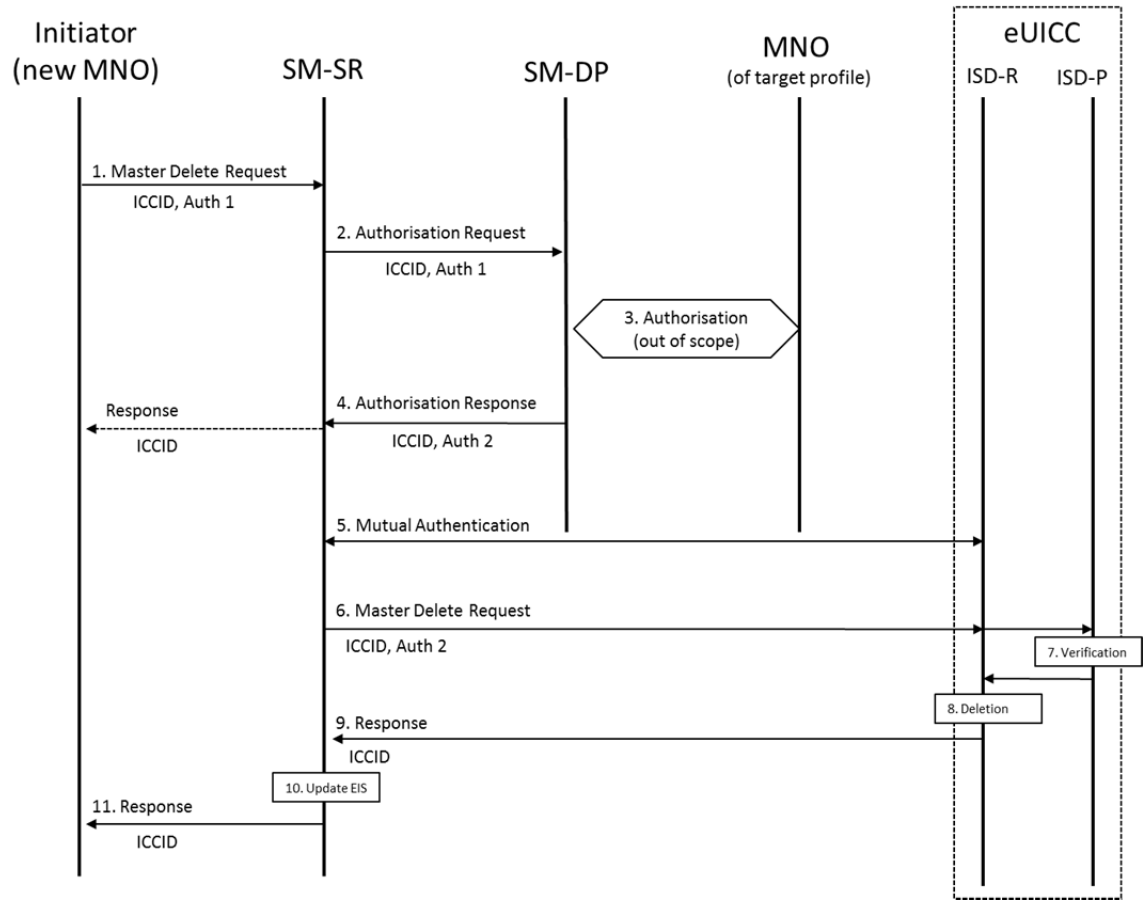

Figure 7: Master Delete

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 (or other unique identifier) 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 MNO owner of the target Profile. Note: The definition of this interface is out of the scope of this document.
4. If the MNO authorises the deletion or if there is no response from the MNO, 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 (or other unique identifier) 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 MNO to the SM-SR associated with the target eUICC.

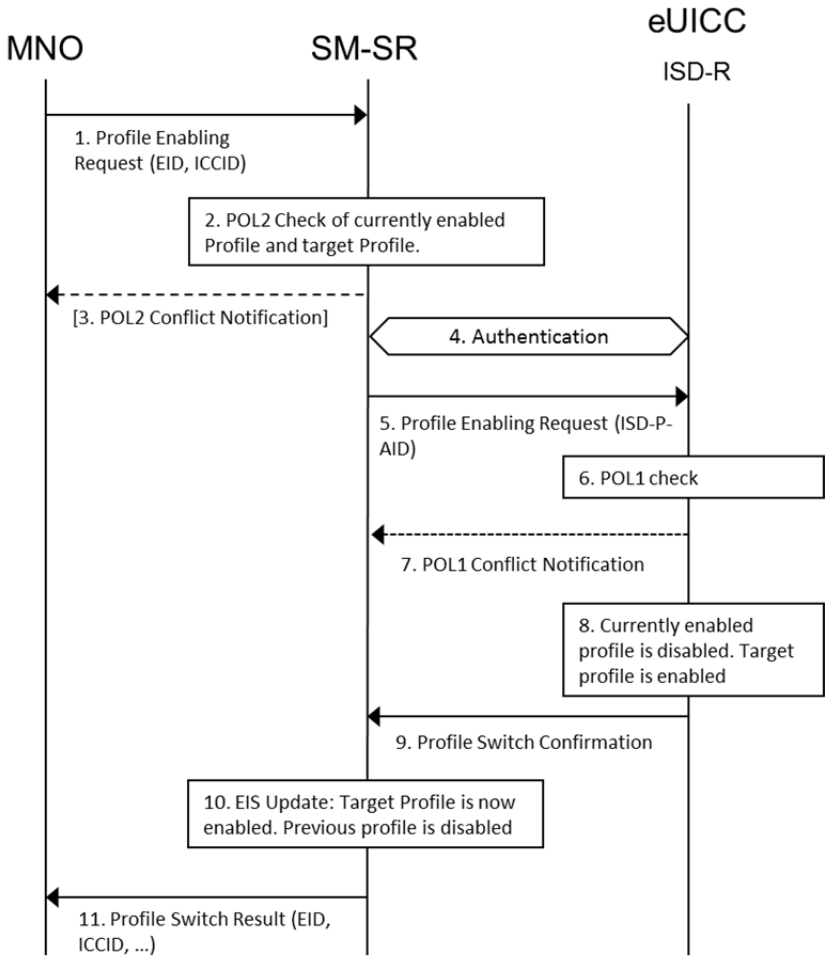

Figure 8: Profile Enabling

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 MNO'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 MNO.

Procedure:

1. The MNO sends a Profile Enabling request to the SM-SR. The request includes the target EID and at least the ICCID (or other unique identifier) 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.
3. If there is a conflict with POL2, the SM-SR aborts the procedure and informs the concerned MNO(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. 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 MNO(s). These messages will include the EID and the ICCID (or other unique identifier) of their respective 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 MNO to the SM-DP which forwards it to the SM-SR associated with the target eUICC. This way, the MNO does not have to be linked to the SM-SR and relies on the SM-DP to make the connection.

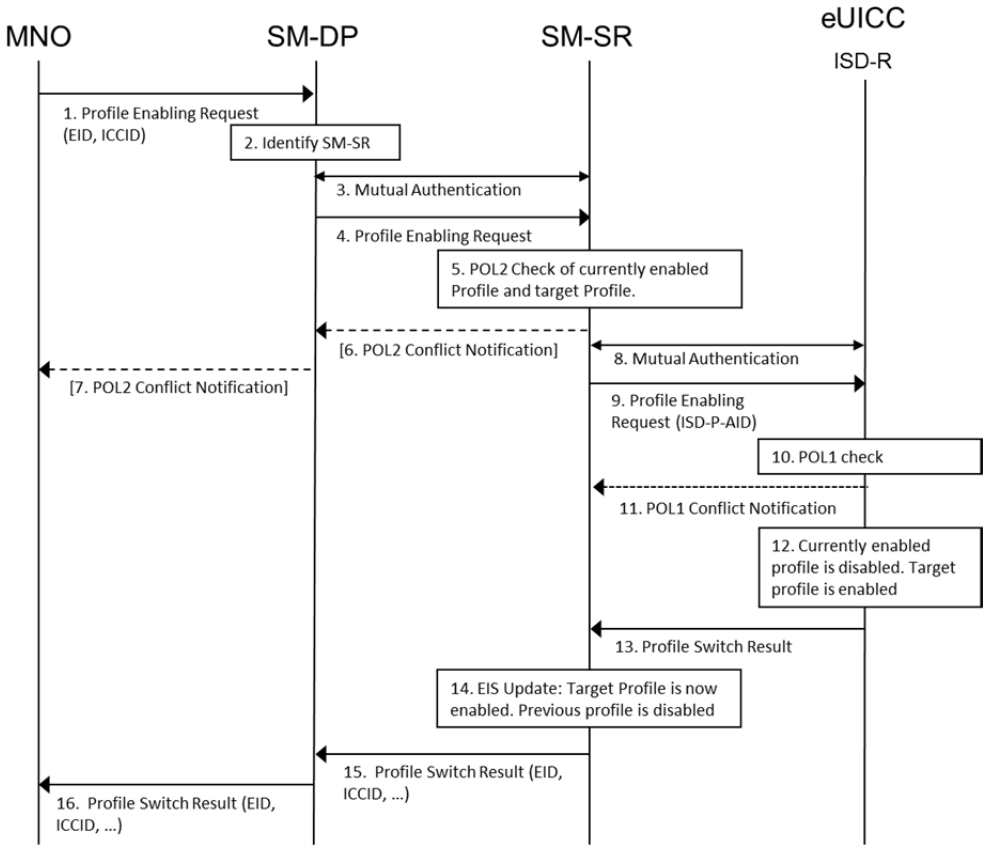

Figure 9: Profile Enabling via SM-DP

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 MNO's network.
c. The EID of the target eUICC, the SRID and the ICCID of the target Profile are known by the MNO.

Procedure:

1. The MNO sends a Profile Enabling request to the SM-DP. The request includes the target EID and at least the ICCID (or other unique identifier) 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 both the currently Enabled Profile and the target Profile permit 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 and the SM-DP or MNO of the disabled Profile.
7. If there is a conflict with POL2, the error message is forwarded by the SM-DP to the requesting MNO.
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 MNO of the disabled Profile. These messages will include the EID and the ICCID (or other unique identifier) of their respective Profiles.
16. The Profile switch result is forwarded to the requesting MNO.

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 MNO to the SM-SR associated with the target eUICC.

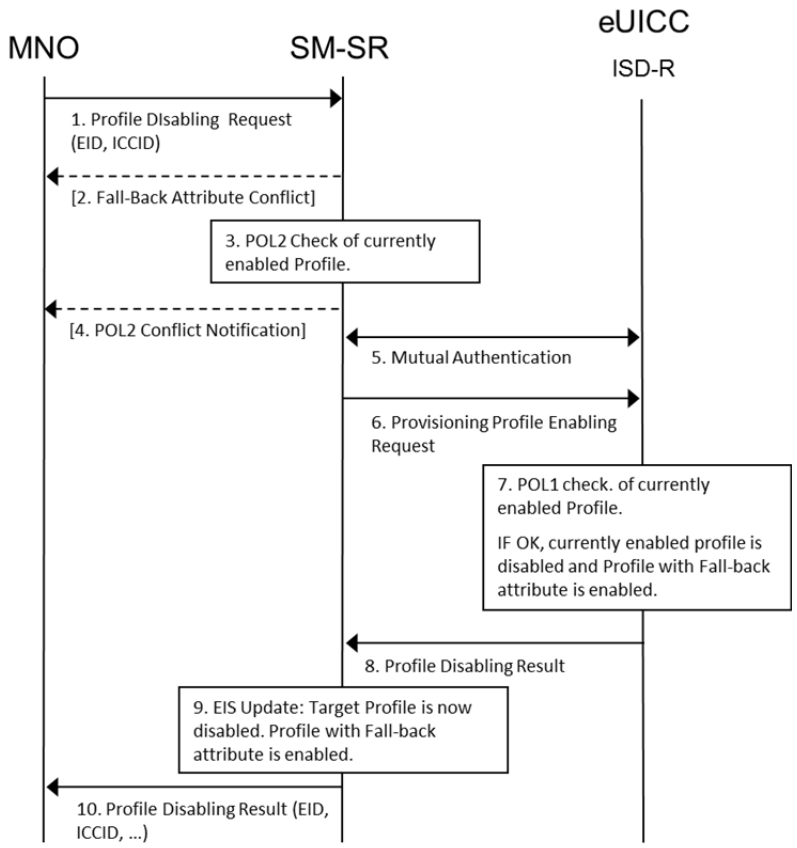

Figure 10: Profile Disabling

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

Procedure:

1. The MNO 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 MNO(s).
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. 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 MNO(s). This message includes the EID and the ICCID of the Profile(s).

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 MNO.

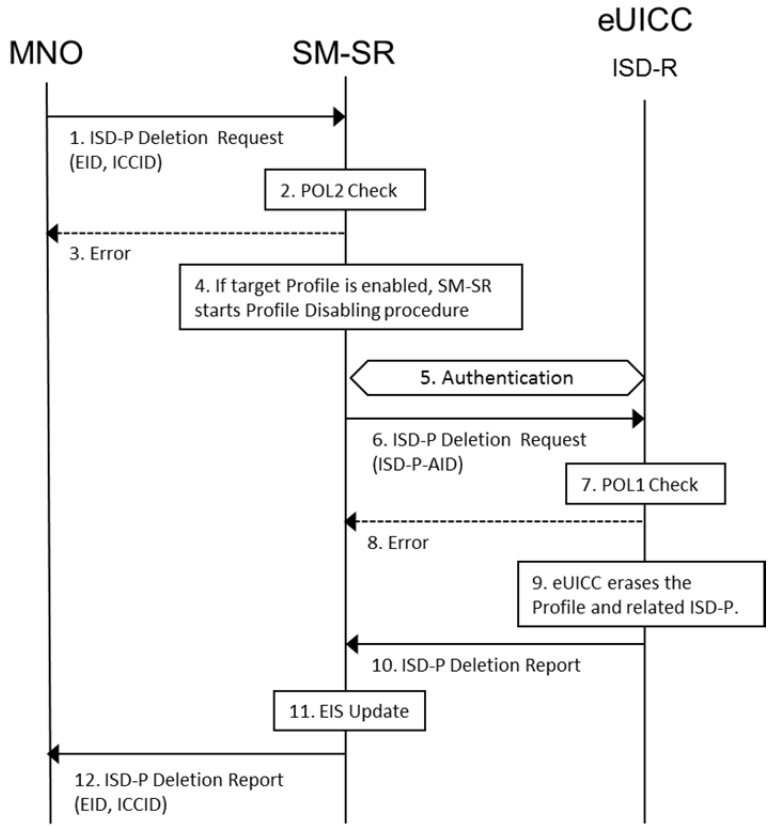

Figure 11: ISD-P Deletion

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

Procedure:

1. The MNO sends an ISD-P Deletion request to the SM-SR. The request includes the target EID and the ICCID (or other unique identifier) of the target Profile.
2. The SM-SR checks the POL2 of the target Profile.
3. If there is a conflict with POL2, the SM-SR aborts the procedure and informs the MNO(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.
8. If there is a conflict with POL1, 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 MNO.

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 MNO.

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

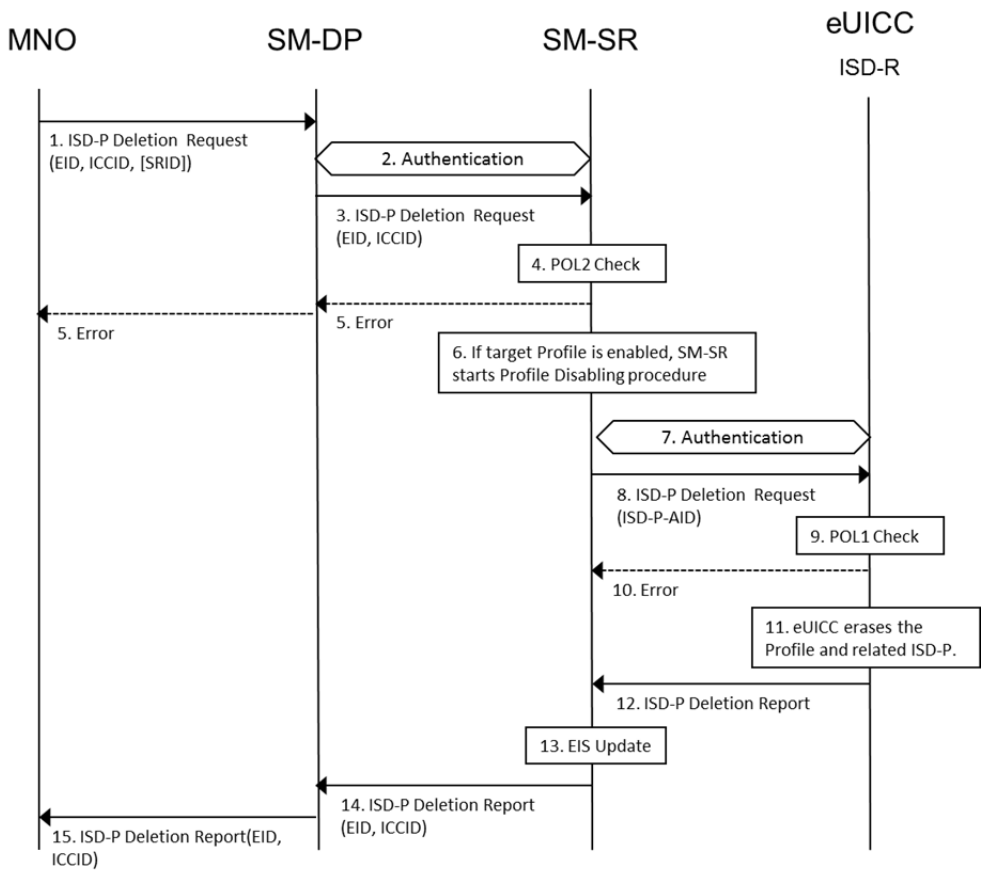

Figure 12: Operational Profile Deletion via SM-DP

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

Procedure:

1. The MNO sends an ISD-P Deletion request to the SM-DP. The request includes the target EID and the ICCID (or other unique identifier) of the target Profile. The MNO 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 MNO 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 of the target Profile.
5. If there is a conflict with POL2, the SM-SR aborts the procedure and informs the MNO(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.
10. If there is a conflict with POL1, 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 MNO.

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 MNOs 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, deletion of the Profile).

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

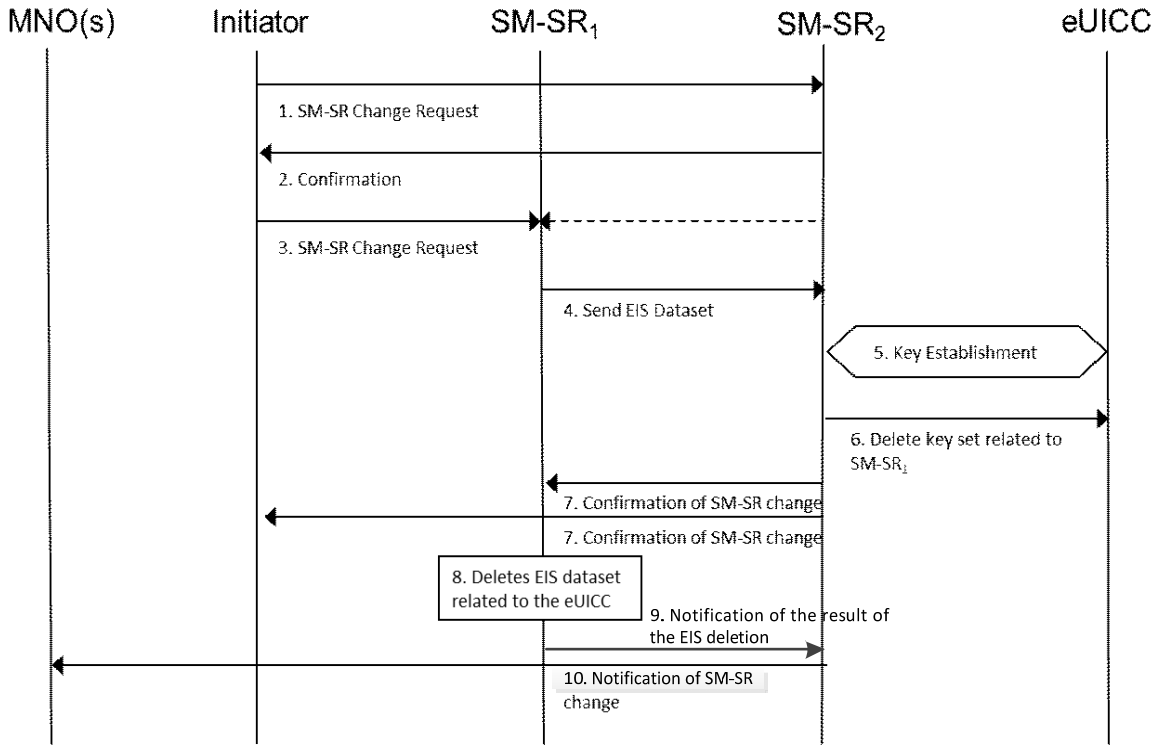

Figure 13: SM-SR Change

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 both SM-SR_1 and the initiator.
8. SM-SR_1 deletes the EIS dataset related to the eUICC.
9. SM-SR_1 sends a notification to SM-SR_2 on the deletion result of the EIS dataset related to the eUICC.
10. SM-SR_2 sends a notification to the MNO owner(s) of the Profile(s) on the eUICC, either directly or via the SM-DP, of the change of SM-SR.

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 MNO owner of the Profile(s) is aware of the change.

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 machine to machine Device, there is a need to change to the Profile with Fall-back attribute set. In this case the eUICC disables the currently Enabled Profile (Profile A) and enables the Profile with Fall-back Attribute set (Profile B).

For security reasons if Profile A has the POL1 rule “disabled not allowed” set then the eUICC can only switch back to Profile A until such time that the POL1 of Profile A is changed or Profile A is 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 machine to machine 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 machine to machine 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 owner(s) of the Profile(s).

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 MNO can verify if an eUICC is certified, in particular if the eUICC is designed according to the present specification.

Procedure:

1. The MNO, or SM-DP on behalf of the MNO, 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 MNO extracts the EUM information from the eUICC certificate (for example: certificates, SAS accreditation etc.). (Note: At present the SAS accreditation scheme for eUICCs is for future study).
3. With the information retrieved at step 2, the MNO 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 MNO verifies the validity and signature of the EUM certificate.
5. The MNO verifies the EUM signature of the eUICC certificate.

End Condition: The eUICC certificate and EUM certificate have been checked by the MNO.

3.6 Policy Control

3.6.1 Overview Diagram of Rule Management System

The figure below represents the Policy Rule management system:

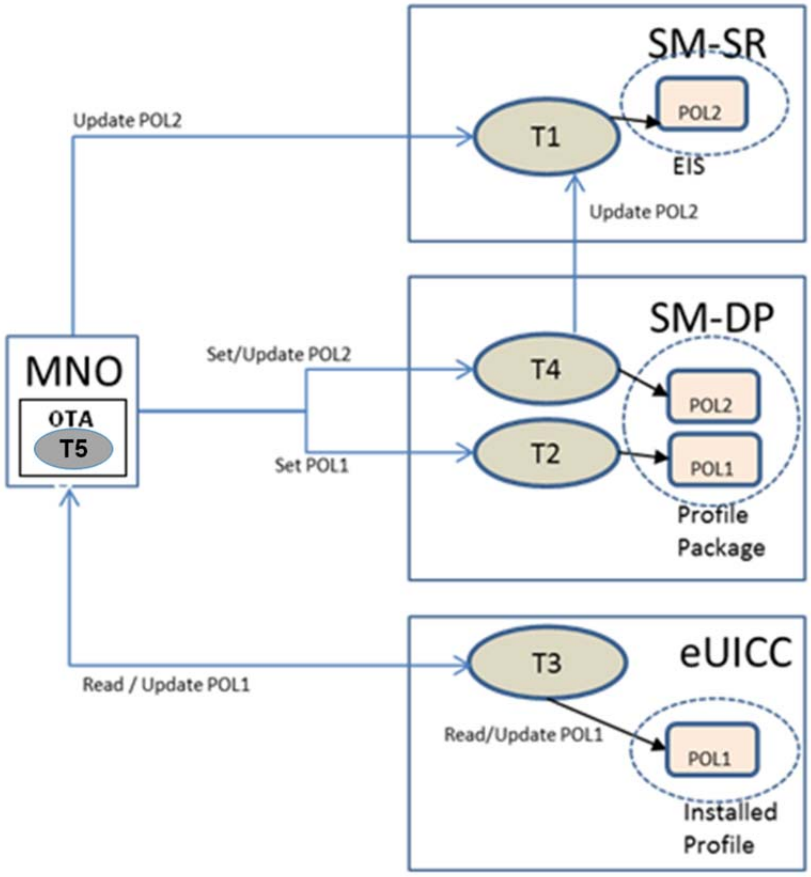

Figure 14: Policy Rule Management System

3.6.2 Policy Rules Management

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

This Policy control is under the control (or jurisdiction) of a single MNO 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 MNO 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 MNO Policy enforced in different locations/entities. The combination of POL1 and POL2 represent the contract between an MNO and a Customer 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 MNO request
2) Update POL2 as per MNO 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 MNO request and embed it in the Profile.

Task 4 accepts the following commands

1) “Update POL2” from the MNO, and passes it to the SM-SR for updating the EIS.
2) Set POL2 from the MNO 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 MNO request (commands are sent by the MNO’s respective OTA system).

3.6.2.4 OTA Policy Rule Update Mechanism

For Task 5 the MNO OTA Platform is used. In this case it is accepting POL1 update commands from the MNO 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 MNO 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 MNO 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 MNO can update the Policy Rules within his Profile using his 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 MNO.

	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 MNO (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.

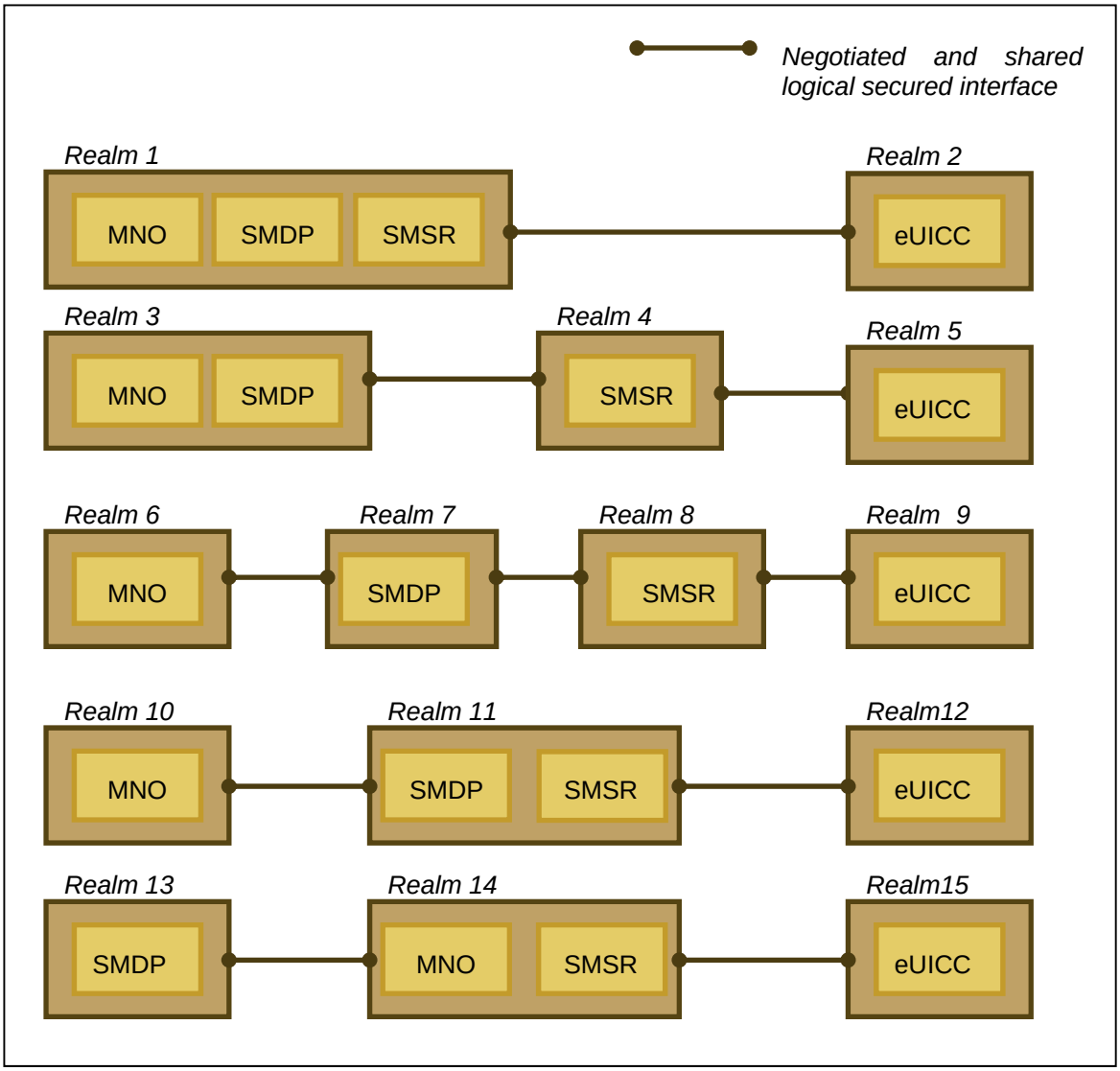

Figure 15: Examples of security realms organisation in the security model

4.4 Security Requirements

This section lists security requirements.

In the security model we consider the Customer, MNO, SM-DP, SM-SR, eUICC and eUICC Manufacturer.

We consider the MNO, SM-DP, SM-SR, eUICC and eUICC Manufacturer 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;
- Machine to Machine Device.

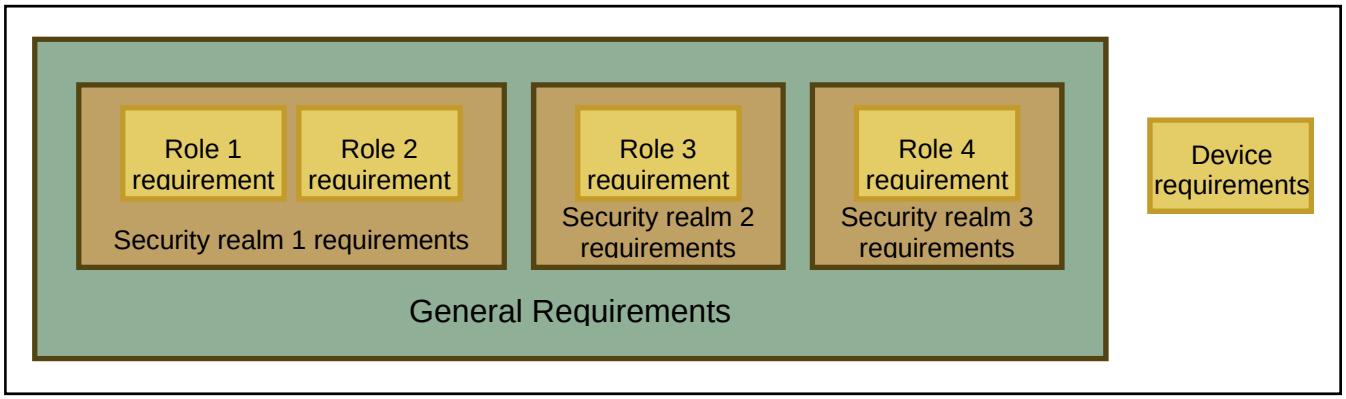

Figure 16: Example of security requirements organisation

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 [NIST].
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 [if used].
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 MNO security policies (e.g. force an operator to share its secrets with a third party).
SG10	The MNO 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-repudiable. 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 Protection Profile defined in GSMA Fast Track Project. Note: Need to refer to the GSMA Protection Profile document once available.

SE2	The eUICC Protection Profile should at least include the following elements: Platform Service Manager, ISD-R, Profile storage and isolation of Profiles. Note: Related Actors, Roles and environmental conditions will be defined in the eUICC Protection Profile
SE3	The eUICC protection Profile shall be compatible with existing accepted Protection Profile.
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 [21133], 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 machine to machine 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 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.

4.4.4 SM-SR and SM-DP Requirements

#	**Requirement**
SM1 (SM-DP)	SM-DP shall be certified according to a GSMA agreed certification scheme.
SM2 (SM-SR)	SM-SR shall be certified according to a GSMA agreed certification scheme.

SM3 (SM-SR)	SM-SR shall implement an access control mechanism on the request for execution of the SMSR functions only to authorised security realms.
SM4 (SM-DP)	SM-DP shall implement an access control mechanism on the request for execution of the SMDP 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 Installer 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 MNO 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. Note: Need to study the possibility for the MNO by itself to update the Network Access Credentials.
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 machine to machine Device.
SD2	The machine to machine 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:

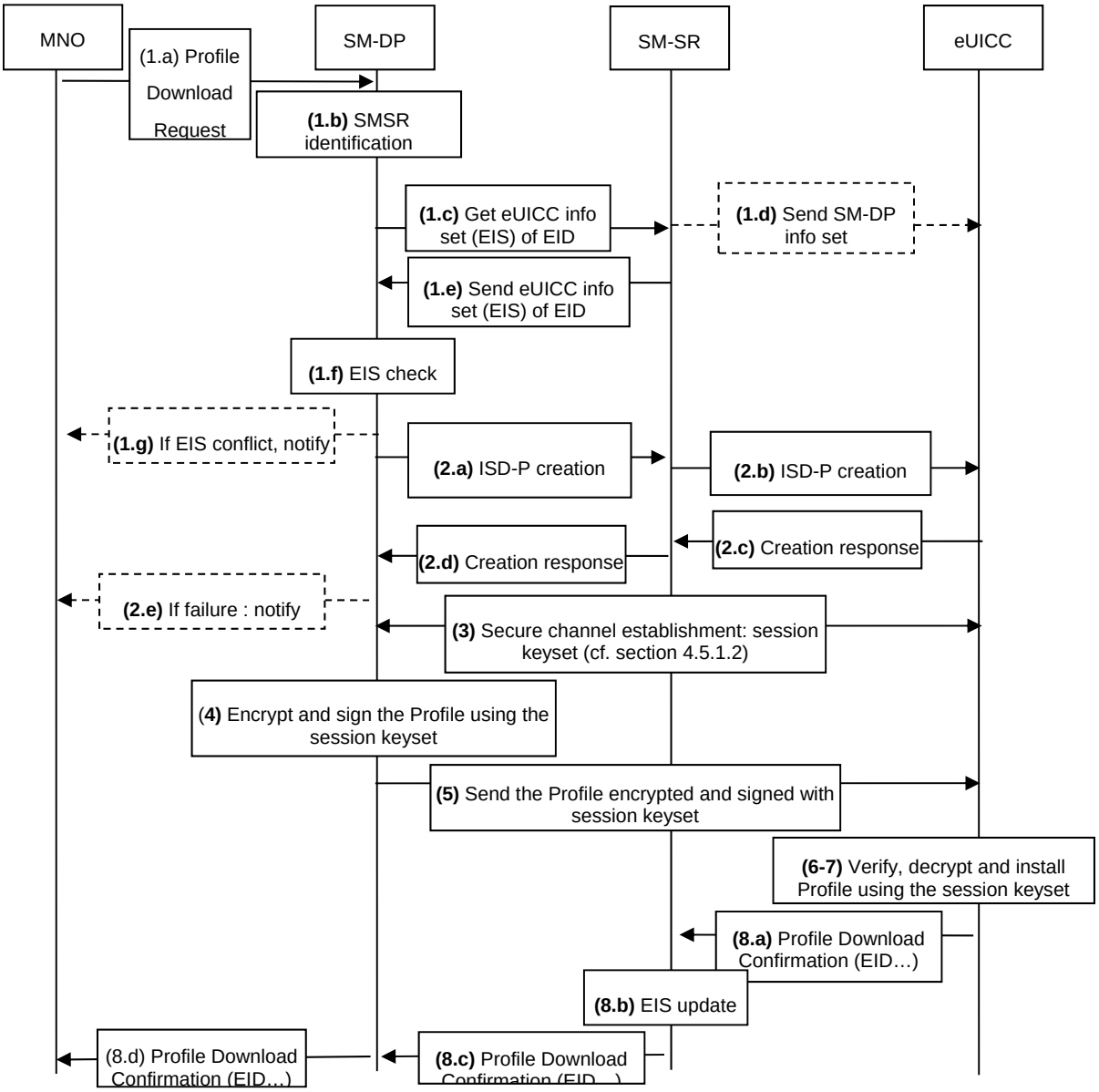

Figure 17: Secure Download and Installation of a Profile

The process between the MNO and the eUICC shall be as follows:

Start Conditions:

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

Procedure:

1. (a) The MNO 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 MNO. 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.

We distinguish two options for the ShS generation:

1. Key agreement: the ShS is generated locally by both entities SM-DP and eUICC using a Key Agreement Algorithm.
2. Key distribution: the ShS is generated by one entity and sent to the other. We distinguish two models:
    a. Push model: generated by the SM-DP and sent to the eUICC
    b. Pull model: generated by the eUICC and sent to the SM-DP

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 17.

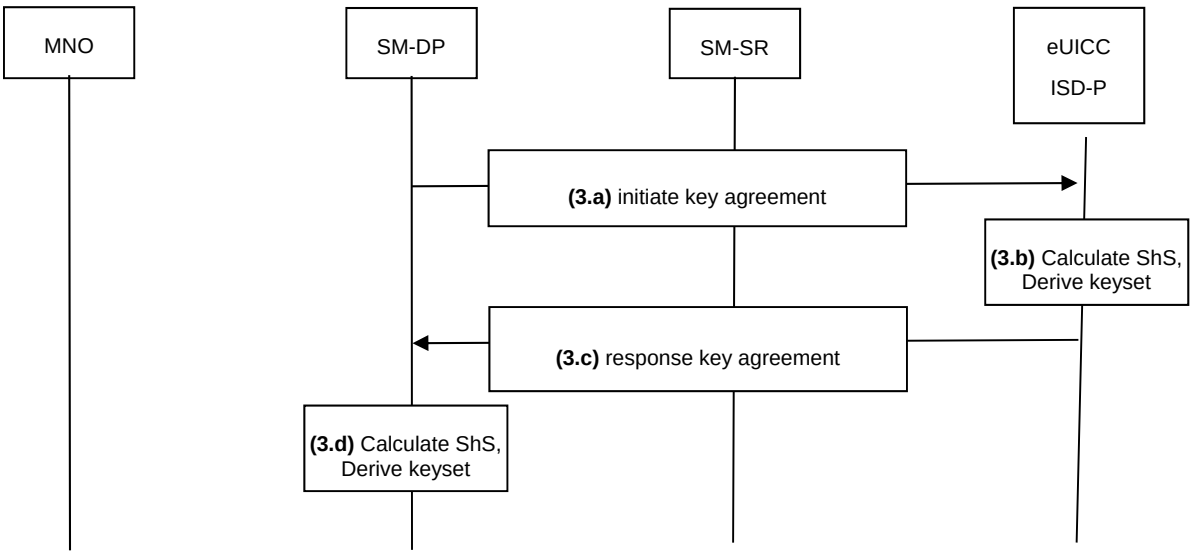

Figure 18: Key Set Establishment: Key Agreement Protocol (overview)

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);
2. Mutual authenticated transport level security, e.g. SSL.

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 eUICC Manufacturer – 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 MNO – 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 MNO 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 [31102], 3GPP TS 31.103 [31103] and ETSI TS 102 221 [102221].)
  - 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 MNO so that the MNO 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, MNO Policy Rules and regulatory data retention obligations.

A.4 MNO – 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 MNO;
- Policy Rule (POL2) update from the MNO;
- The EID of the targeted eUICCs.

The MNO takes as input:

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

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 MNO – eUICC interface

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

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 machine to machine 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 machine to machine Device	If Profiles are erasable directly from the machine to machine Device without authorisation by using a software or hardware switch, it might enable malicious 3rd parties to resell a stolen machine to machine 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	MNO	MNO, eUICC	3 to 4
Authentication Algorithm Key	MNO	MNO, eUICC, SM-DP	2 (one eUICC affected) to 4 (a set of eUICCs affected)
Authentication Algorithm Parameters (e.g. Opc, Ri-Ci etc.)	MNO	MNO, eUICC, SM-DP	2 (one eUICC affected) to 4 (a set of eUICCs affected)
IMSI	MNO	MNO, eUICC, SM-DP	1 (one IMSI affected) to 2 (a set of IMSIs affected)
MSISDN	MNO	MNO, SM-DP, SM-SR	1 (one MSISDN affected) to 2 (a set of MSISDNs affected)
Root Certificate	Root CA owner	Root CA owner	4
EUM Certificate	Root CA owner	EUM	3
eUICC Certificate	EUM	EUM, eUICC	2 to 3
EID	eUICC Manufacturer	SM-SR, eUICC, SM-DP, MNO, , eUICC Manufacturer	1 (one EID affected) to 2 (a set of EIDs affected)
Profile	MNO	MNO, eUICC, SM-DP	3 to 4
MNO OTA Keys	MNO	MNO, eUICC, SMDP	3 to 4

Sensitive Asset	Asset Originator Owner	Asset Handled In Clear By:	Criticality
PCF rules	MNO	eUICC, MNO, 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

D.1 Additional Key Establishment Mechanisms

In addition to the key agreement protocol outlined above, two key distribution models are considered:

1 – The Push Model, in which the ShS is generated by SM-DP.

2 – The Pull Model, in which the ShS is generated by the eUICC.

D.1.1 Push Model (ShS generated by SM-DP)

The following steps shall be executed:

1. The SM-DP asks the SM-SR for the public key of eUICC (PK_{eUICC}). This message is part of step 1.a in Figure 17 in section 4.
2. The SM-SR sends to SM-DP the public key of eUICC (PK_{eUICC}). This message is part of step 1.b in Figure 17 in section 4.
3. The SM-DP verifies that PK_{eUICC} (Public Key of eUICC) is signed by the EUM Certificate.

4. SM-DP generates the Shared Secret (ShS) and sends it to the eUICC (ISD-P) encrypted with the public key of eUICC (PK_{eUICC}). It may send its signed public key to the eUICC if it is not done by the SM-SR (if step 1.c is not executed).
5. The eUICC decrypts and verifies the integrity of the ShS.
6. The eUICC sends a confirmation receipt signed with its private key (SK_{eUICC}) back to the SM-DP.
7. The SM-DP and eUICC generate the keyset.

The following figure details step 1 of figure 17 in section 4.

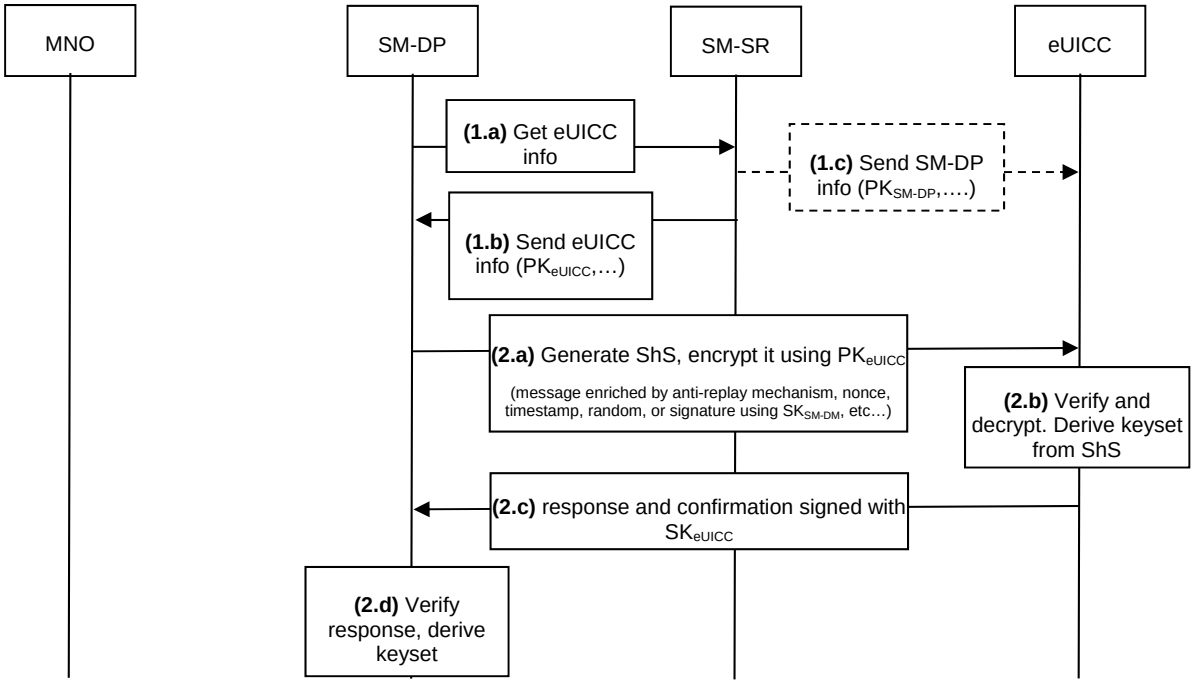

Figure 19: Session key set establishment: key distribution, push model

In step (2.a) SM-DP can also generate the keyset and sends it to eUICC. In this case, the eUICC has to retrieve the keyset directly from the received message.

In a GP based model, the SM-DP addresses the ISD-P. The ISD-P has to ask the ECASD to decrypt the received message using SK_{eUICC} =SK.CASD.CT [AmdA]. The SM-DP uses PK.CASD.CT to encrypt the message. PK.CASD.CT is part of CERT.CASD.CT which is signed by the EUM. The eUICC signs the receipt using SK.CASD.AUT and the SM-DP verifies the receipt using PK.CASD.AUT

D.1.2 Pull model (ShS generated by the eUICC)

It is similar to the push model, except that the eUICC generates ShS.

The following steps shall be executed:

1. The SM-DP asks the SM-SR for the public key of eUICC (PK_{eUICC}). This message is part of step 1.a in Figure 17.
2. The SM-SR sends to SM-DP the public key of eUICC (PK_{eUICC}). This message is part of step 1.b in Figure 17.
3. The SM-DP verifies that PK_{eUICC} (Public Key of eUICC) is signed by the EUM Certificate.

4. The SM-SR sends to the eUICC the public key of SM-DP (PK_{SM-DP}). This message is part of step 1.c in Figure 17**.**
5. The eUICC generates the Shared Secret (ShS), and sends it to the SM-DP signed with the private key (SK_{eUICC}) and encrypted with the public key of SM-DP (PK_{SM-DP}). It may send its signed public key to the SM-DP if it is not done by the SM-SR.
6. The SM-DP sends a confirmation receipt signed with its private key (SK_{SM-DP}) back to the eUICC.
7. The SM-DP and eUICC generate the keyset

In a GP based model, the eUICC uses SK.CASD.AUT to sign the message and SM-DP uses PK.CASD.AUT to verify the signature [AmdA]. PK.CASD.AUT is part of CERT.CASD.AUT which is signed by the EUM.

D.2 Details on the ElGamal Key Agreement

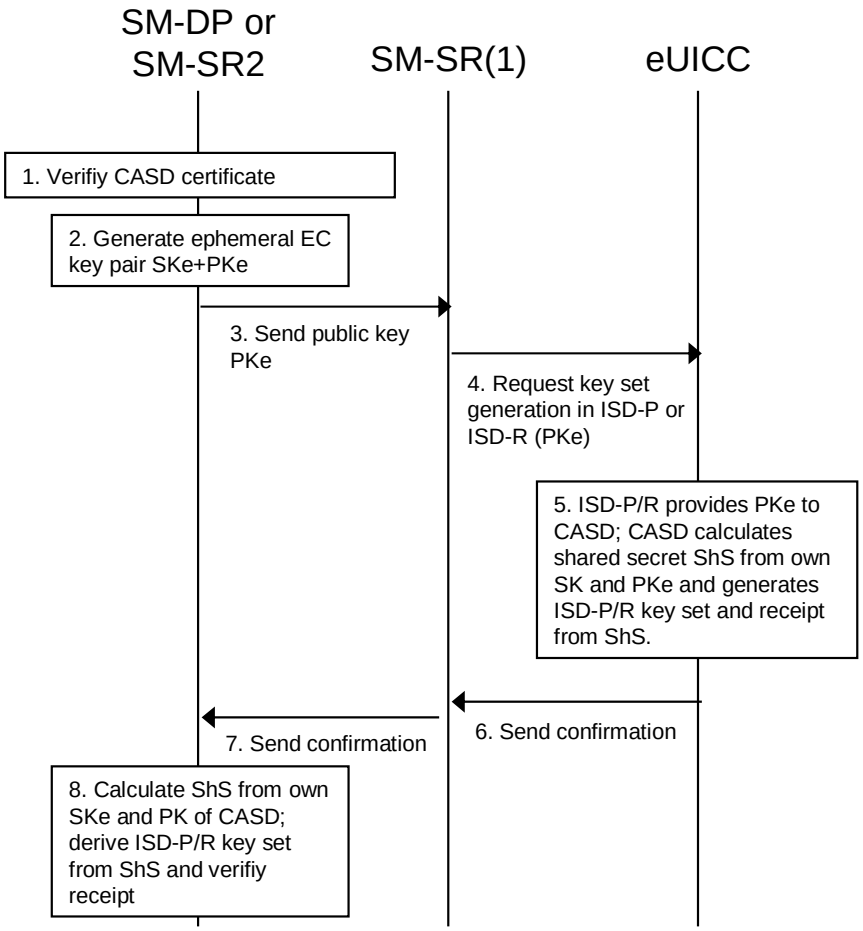

Figure 20: ElGamal Key Agreement

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 17.

2. The SM-DP generates an ephemeral EC (elliptic curve) key pair, named SKe and PKe.
3. The SM-DP sends a key set generation request to the SM-SR, including the ephemeral public key PKe. The SM-SR passes the request for key set generation to the ISD-P on the eUICC, providing the PKe.

5a. The eUICC now performs the following actions: The ISD-P provides the ECASD with the PKe.

5b. The ECASD generates a Shared Secret ShS from its own secret key and received ephemeral PKe and returns it to the ISD-P.

5c. The ISD-P uses ShS to generate its own key pair as well as a receipt from the operation.

6. The ISD-P passes a confirmation (with receipt) of the generation back to the SM-SR..
7. The SM-SR passes the confirmation back to the SM-DP.

8a. The SM-DP generates ShS from the ephemeral secret key SKe and the eUICCs public key.

8b. The SM-DP uses this calculated ShS to derive the same key set as generated by the ISD-P.

8c. 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.

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: optional 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 (MNO), 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 MNO, 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 could be used:

1. WS-Security standard.
2. Mutual authenticated transport level security (SSL).

Both mechanisms require the use of digital signed certificates. For WS-Security mutual authentication at least X.509 certificate needs to be supported.

Both parties are required to have X.509 certificates (and public-private key pairs) which is used to authenticate each other using their certificates.

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 Flowcharts for basic remote Provisioning events (Informative)

This annex suggests macroscopic flows for remote Subscription management. These flows are designed to enable an MNO using remote Subscription management services to manage eUICCs according to Customer demands.

This also illustrates how the various procedures link together and how processes external to the Subscription management architecture (such as Subscription activation) need to interact with these procedures.

An important issue is to avoid situations of dead-lock or unmanageable Profiles as unintended consequences of a particular management practise. These situations may be avoided by ensuring the proper process flow when managing Subscriptions and their associated Profiles.

The following codes of conduct should be observed by any MNO:

1. When a Customer terminates a contract with an MNO, this MNO should clean up its part of the eUICC(s) and associated Subscription Manager(s) of this Customer (SIM-card analogy: cards for which Subscriptions no longer exist are destroyed)
2. When an MNO terminates a contract with a Customer, this MNO should clean up its part of the eUICC(s) and associated Subscription Manager(s) of this Customer (SIM-card analogy: SIM-cards become useless (and are destroyed)
3. The contents of a Profile including policy settings should at all times reflect the contract between MNO and the Customer (i.e. if there is no valid exclusivity clause in the contract, the Profile should reflect this.)

The flows illustrated below are to be used for situations of management for:

- a single Subscription for a single machine-to-machine Device a single Subscription for multiple machine-to-machine Devices multiple Subscriptions for a single machine-to-machine Device
- multiple Subscriptions for multiple machine-to-machine Devices

It is advised that these flows are used as guidelines in the general case.

The flowcharts are built around the procedures of the architecture. To keep complexity low two macros have been created, “Provisioning” and “De-Provisioning”. Those are the first two charts illustrated after the legend below. Following this are use-cases which are described in the GSMA’s Ecosystem document [2]. In addition the use of the “Master Delete” and “Fall-back” mechanisms is illustrated. Note that “Fall-back” is a mechanism which is triggered within the eUICC and not by an entity in the Subscription Management architecture directly.

E.1 Legend

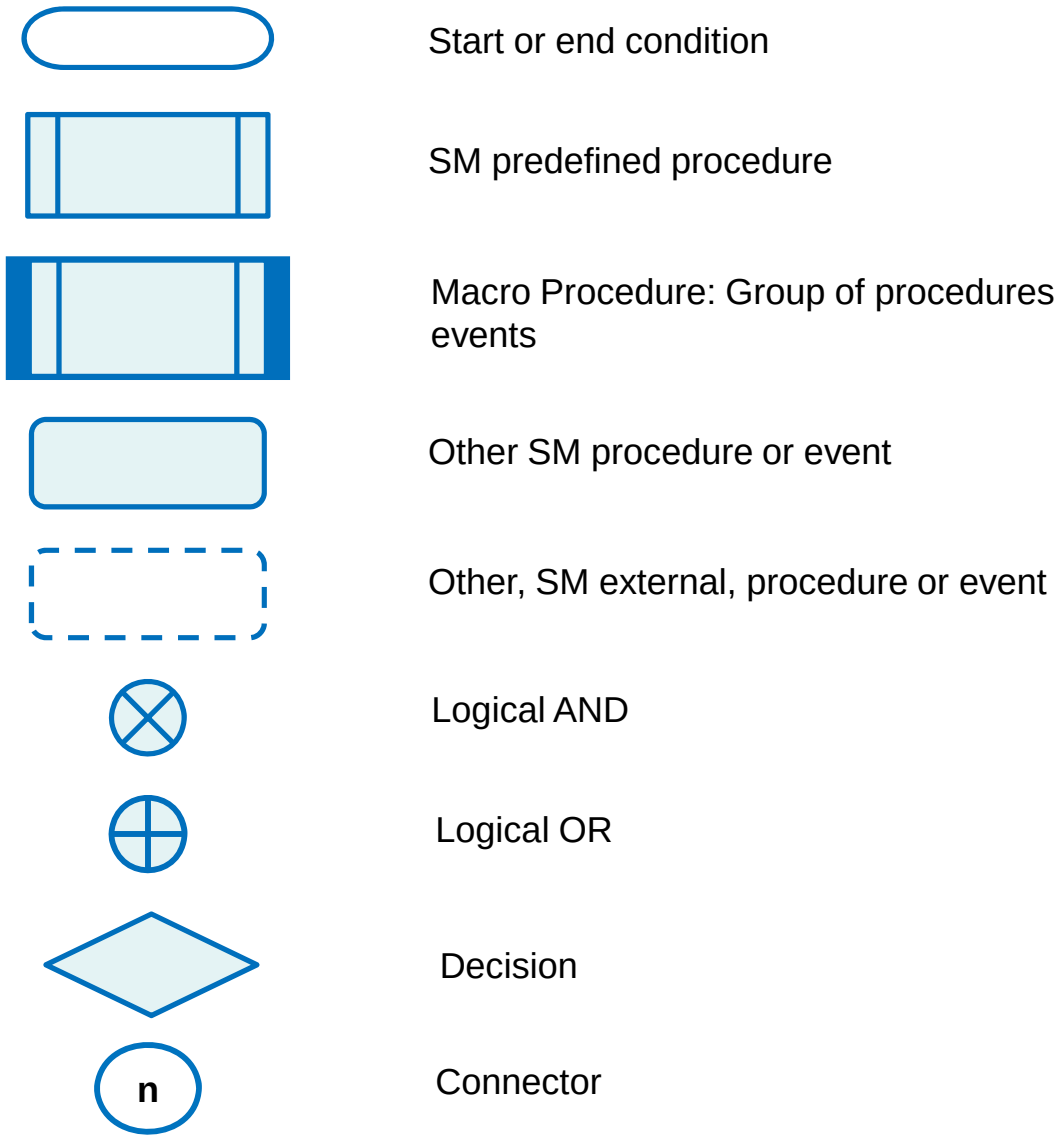

Figure 21: Legend – following conventional flowchart notation

E.2 Macro procedure: «Provisioning of a Machine to Machine Device»

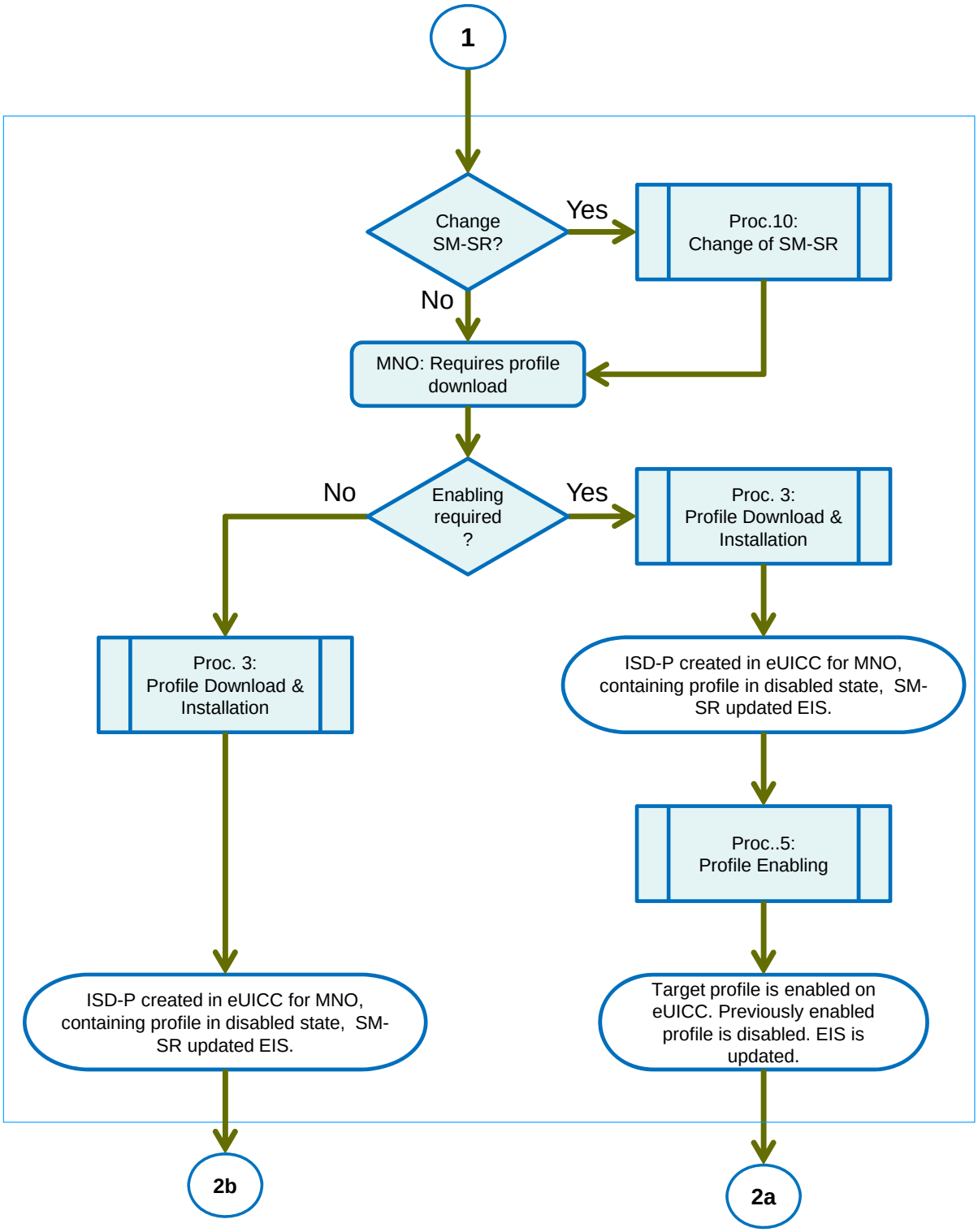

Figure 22- Macro: "Provisioning of Device" – showing the flow following a Customer demand to provision a machine to machine Device.

E3. Macro Procedure: “De-Provisioning of Machine to Machine Device”

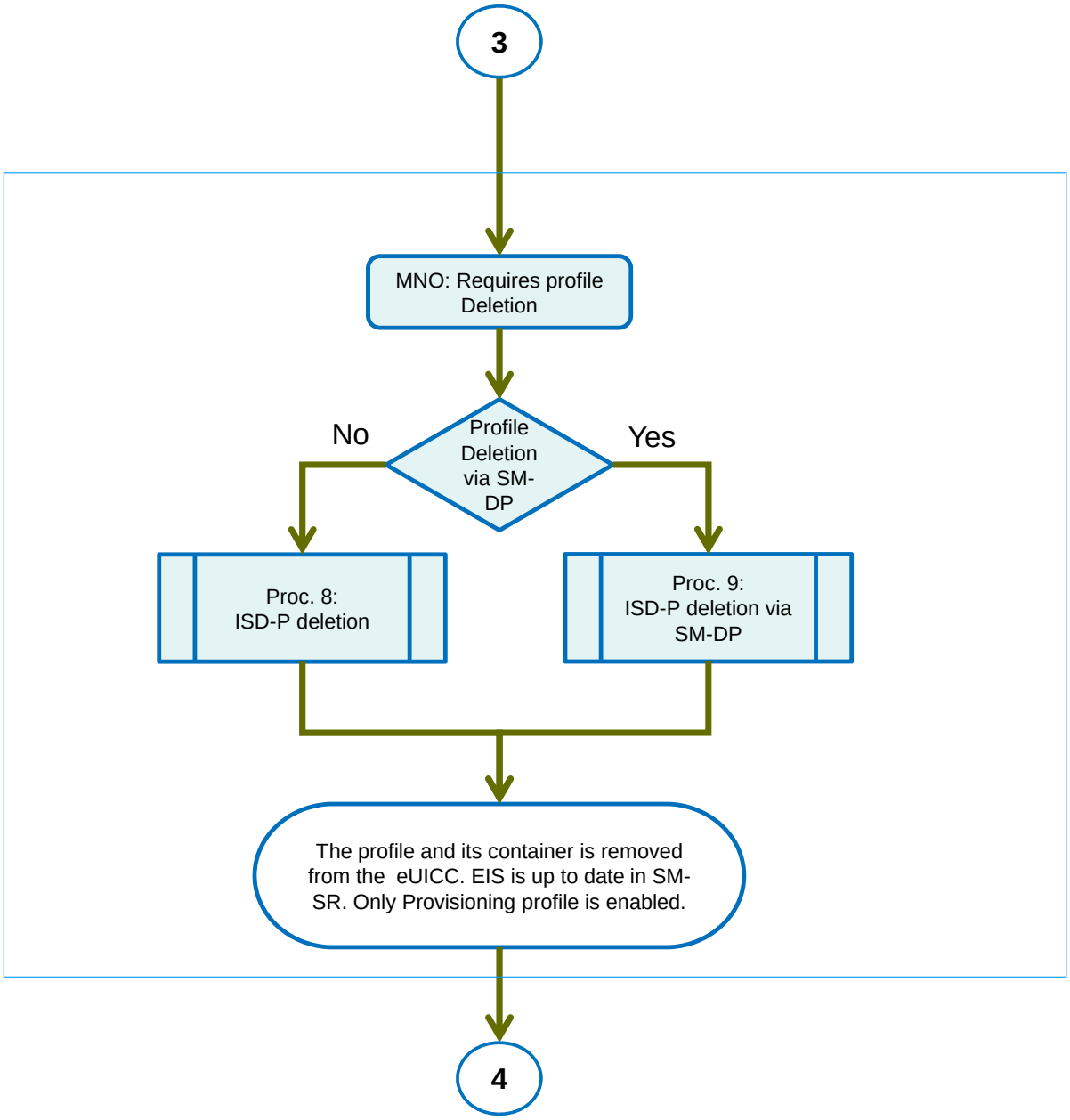

Figure 23- Macro: “De-Provisioning of machine to machine Device” – showing the flow resulting from a Customer demand to delete a Profile or as part of the termination of a Subscription.

E.4 A. From eUICC registration to operative machine to machine Device – Customer enters Subscription with MNO (Ecosystem Lifecycle worked example 3.1.1)

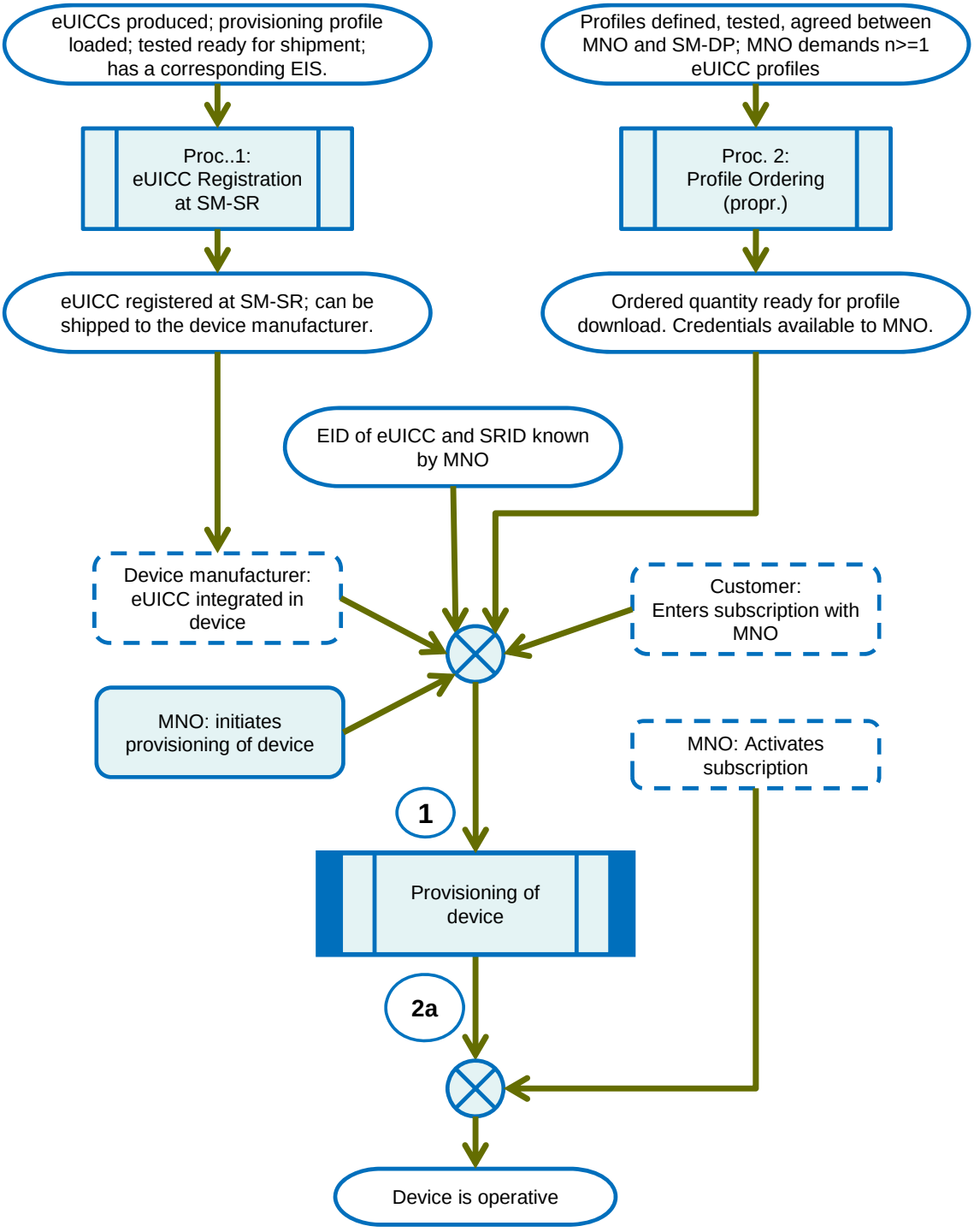

Figure 24: The flow describing the way from registration of the eUICC/Device with the SM-SR to the Provisioning of the machine to machine Device on demand from the first Customer

E.5 B. End of contract with MNO A. Re-Provisioning with MNO B (Ecosystem: 3.1.2 worked example – Re-Provisioning, case 2)

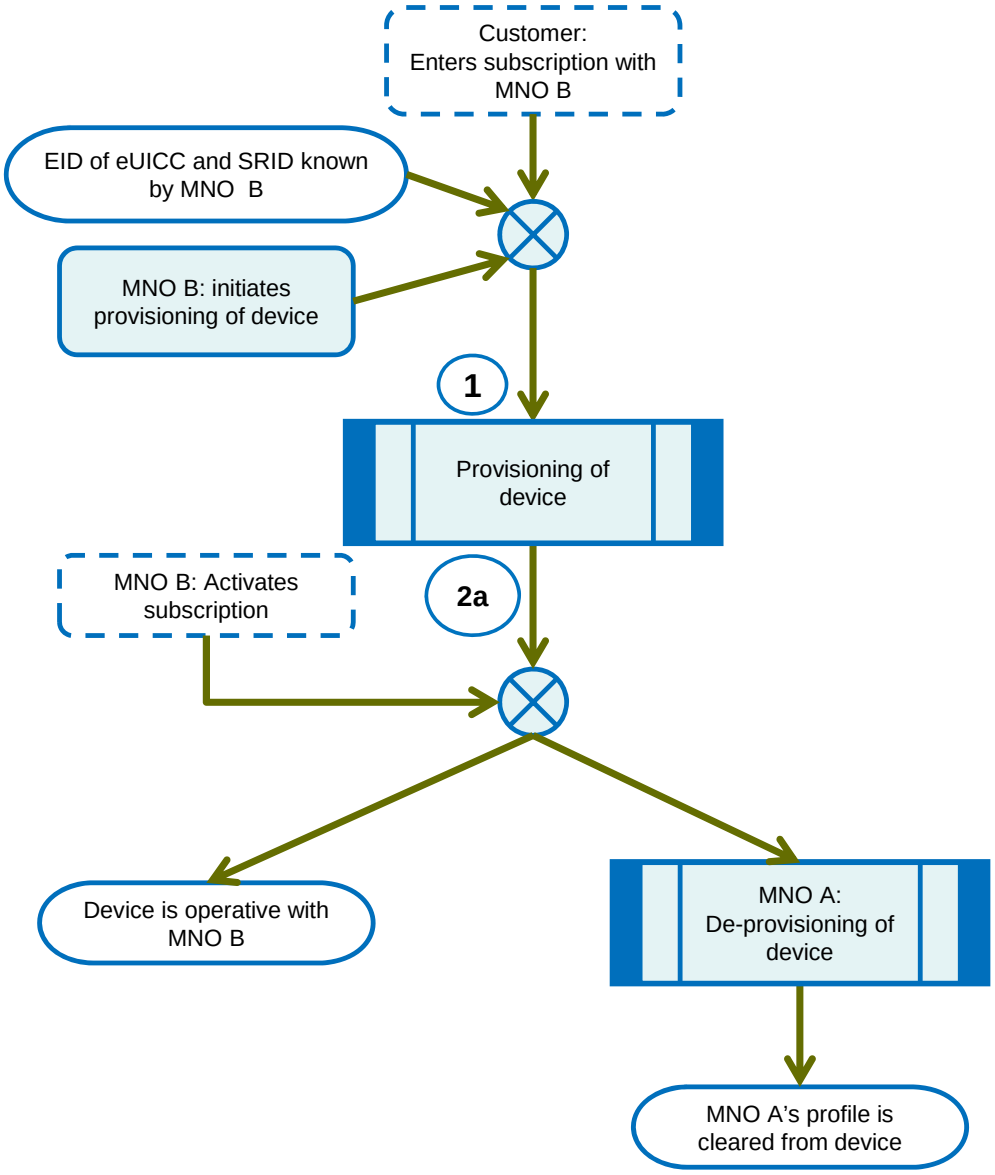

Figure 25: End of contract between Customer and MNO A. Customer Re-Provisioning with MNO B. MNO A performs a De-Provisioning, thus clearing his Profiles from the Customer's machine to machine Device.

E.6 C. Termination of a Subscription (Ecosystem: 3.1.2 worked example - end of contract)

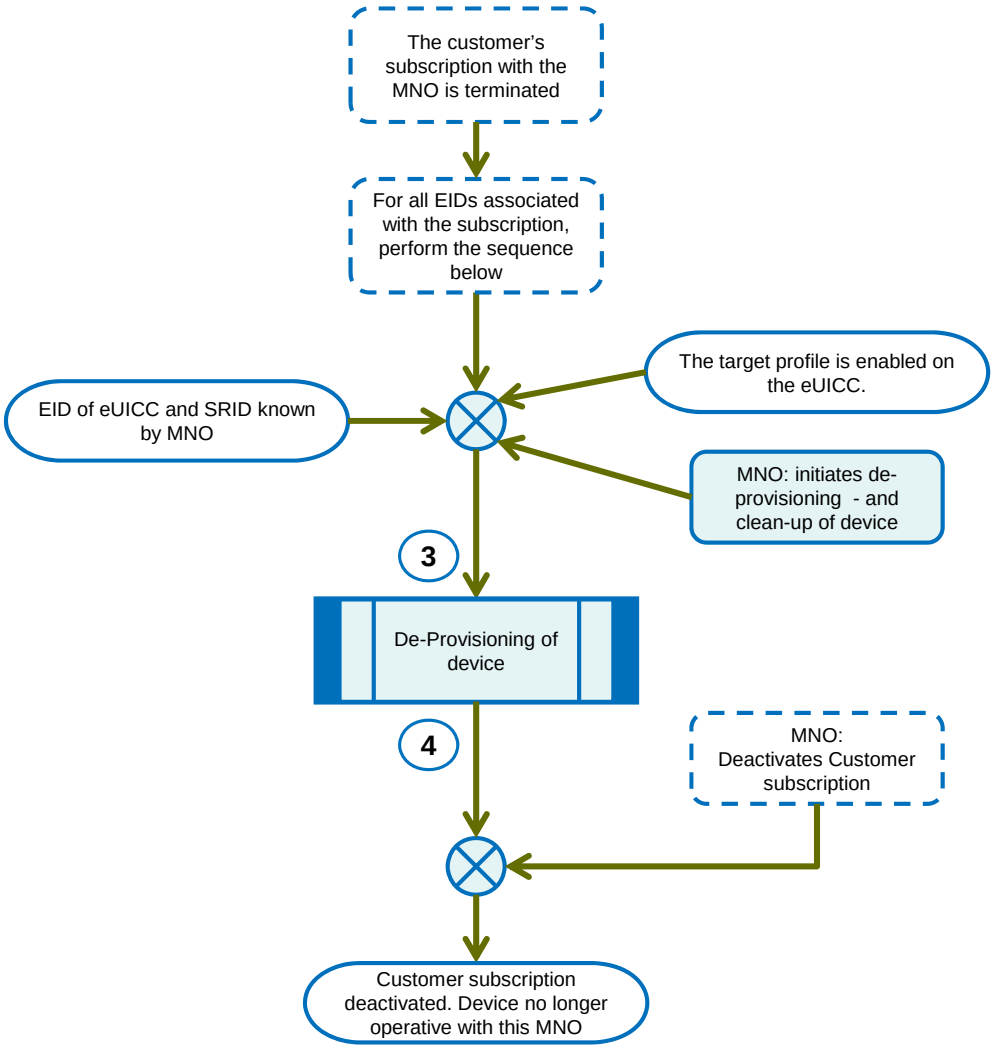

Figure 26: Customer terminates his Subscription with MNO and MNO de-provisions the machine to machine Device, removing Profiles.

E.7 D: Customer Changes Machine to Machine Device but not MNO. (Ecosystem 3.1.3 worked example)

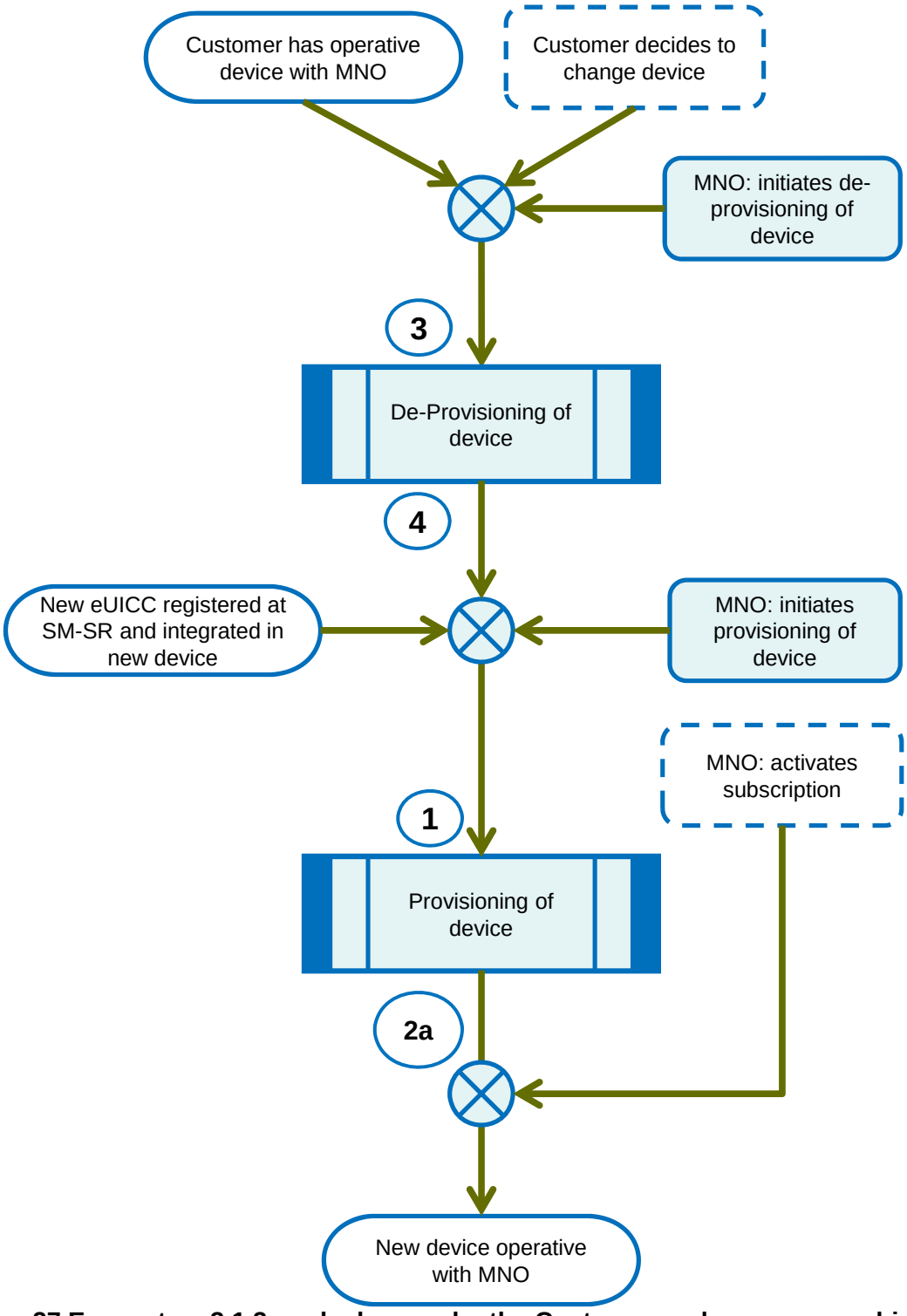

Figure 27 Ecosystem 3.1.3 worked example: the Customer replaces one machine to machine Device for another without changing MNO.

E.8 E. Switch of Enabled Profile from MNO A to MNO B. (Both Subscriptions are active)

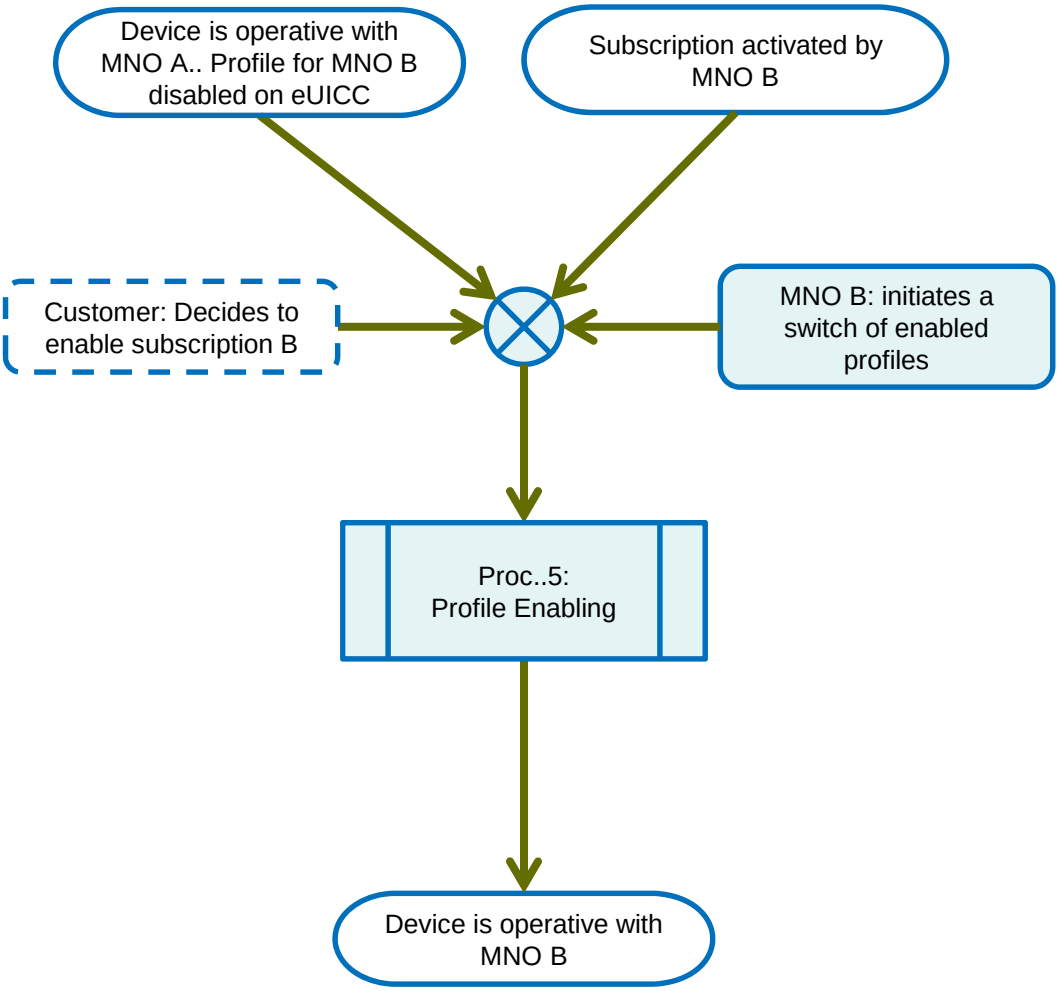

Figure 28 Switching of Enabled Profile from MNO A to MNO B. Both Subscriptions with MNO A and B are active.

E.9 F. Use of Master Delete Mechanism

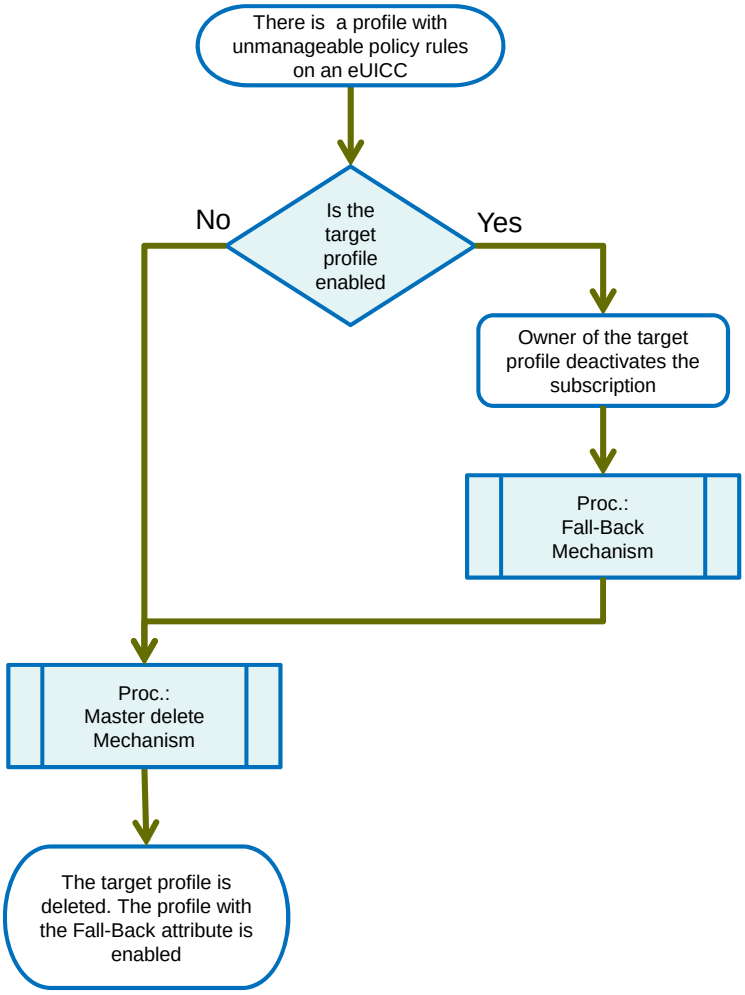

Figure 29: Using the Master Delete mechanism to remove a Profile with unmanageable policy rule(s).

E.10 G. Use of Fall-back Mechanism

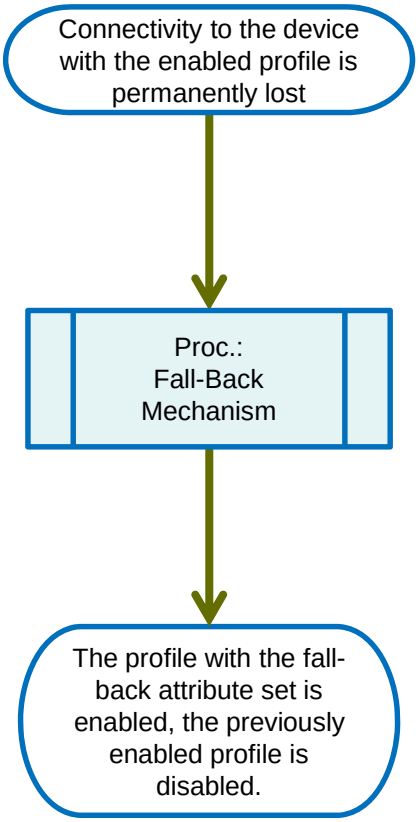

Figure 30: Use of the (on-card) Fall-back Mechanism.

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.

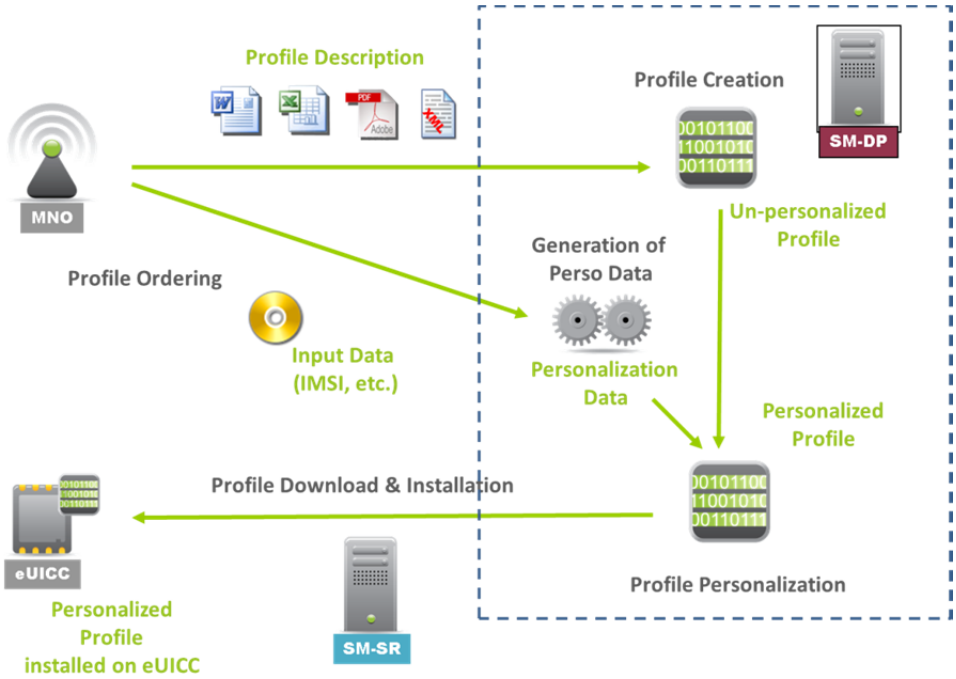

Figure 31: Profile Creation, Ordering and Personalisation

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

Other Information

Type	Description
Document Owner	Embedded SIM
Editor / Company	Ian Smith, GSMA

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

Your comments or suggestions & questions are always welcome.