Remote Provisioning Architecture for Embedded UICC Technical Specification

Version 4.3

25 January 2023

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

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

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

This document provides a technical description of the GSMA's 'Remote Provisioning Architecture for Embedded UICC' [1].

1.2 Scope

This specification provides a technical description of:

- The eUICC Architecture
- The interfaces used within the Remote Provisioning Architecture and
- The security functions used within the Remote Provisioning Architecture

1.3 Document Purpose

The aim of this document is to define a technical solution for the remote provisioning and management of the Embedded UICC (eUICC) in machine-to-machine Devices which are not easily reachable. The adoption of this technical solution will provide the basis for ensuring global interoperability between potentially different Operator deployment scenarios, different makes of network equipment (for example SM-DP, SM-SR) and different makes of eUICC platforms.

1.4 Intended Audience

Technical experts working within Operators, 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	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.
Associated (with) / Association	This term refers to a link of an application, an Executable Load File or a security domain to (another) security domain, which provides services to the former as defined in GlobalPlatform Card Specification [6] section 7.2.
Card Image Number / Card Identification Number (CIN)	An identifier for a specific GlobalPlatform card and that may be used by a Card Management System to uniquely identify a card within its card base.
Certified eUICC	An eUICC meeting the GSMA requirements for Remote SIM Provisioning and certified according to the GSMA compliance programme defined in [64]. Note: Unless stated otherwise, the word eUICC in this specification refers to a Certified eUICC.

Certificate Revocation List	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Connectivity Parameters	A set of data (for example SMSC address) required by the eUICC to open a communication channel (for example SMS, HTTPS) on a dedicated network.
Customer	A paying party, in particular a 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.
Disabled (Profile)	The state of a Profile where all files and applications (for example NAA) present in the Profile are not selectable over the eUICC-Terminal interface.
Discrete eUICC	An eUICC implemented on discrete hardware.
DNS Resolver Client	Client side on eUICC in charge of initiating the queries to the DNS server.
DNS Resolver Server	Server-side component in charge of providing the IP address(s) of the target server to the DNS Resolver Client
Domain Name System	An internet protocol for translating domain names (or hostnames) into IP addresses.
Embedded UICC	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the Device, and enables the secure changing of Profiles.
Emergency Profile	An Operational Profile with a Profile Attribute allocated, indicating that this Profile is an Emergency Profile. An Emergency Profile complies with regulatory requirements and only provides the capability to make Emergency Calls and receive calls from an Emergency centre (e.g. Public Safety Answering Point)
Emergency Profile Attribute	This is an attribute allocated to a Profile which, when set, identifies the Emergency Profile.
Enabled (Profile)	The state of a Profile when its files and/or applications (for example, NAA) are selectable over the UICC-Terminal interface.
Executable Load File	An on-card container of one or more application's executable code as defined in GlobalPlatform Card Specification [6].
Executable Module	The on-card executable code of a single application present within an Executable Load File as defined in GlobalPlatform Card Specification [6].
eUICC Certificate	A certificate issued by the EUM for a specific, individual, eUICC. This certificate can be verified using the EUM Certificate.

eUICC Manufacturer	Supplier of the eUICCs and resident software (for example firmware and operating system).
eUICC OS Update	Mechanism to correct existing features on an eUICC by the original OS Manufacturer when the eUICC is in the field.
EUM Certificate	A certificate issued to a GSMA accredited EUM which can be used to verify eUICC Certificates. This certificate can be verified using the Root Certificate.
Fall-Back Attribute	This is an attribute of a Profile which, when set, identifies the Profile to be enabled by the Fall-Back Mechanism or by the execution of the Disable Profile function on another Profile. Only one Profile on the eUICC can have the Fall-Back attribute set at a time.
Fall-Back Mechanism	eUICC-based mechanism which enables the Profile with Fall-Back Attribute set when the Enabled Profile loses network connectivity
Field-Test eUICC	A pre-production eUICC whose functional or security certifications are not yet completed by the EUM.
Integrated Circuit Card ID	Unique number to identify a Profile in an eUICC. Note: the ICCID throughout this specification is used to identify the Profile.
Integrated eUICC	An eUICC implemented on a Tamper Resistant Element (TRE) that is integrated into a System-on-Chip (SoC), optionally making use of remote volatile/non-volatile memory.
Integrated TRE	A TRE implemented inside a larger System-on-Chip (SoC)
International Mobile Subscriber Identity	Unique identifier owned and issued by Mobile Network Operators as defined in ETSI TS 123 003 [31].
Issuer Identification Number (IIN)	An identifier for a specific issuer that may be used by an off-card entity to associate the card with a specific Card Management System.
Issuer Security Domain	A security domain on the UICC as defined by GlobalPlatform Card Specification [6].
Local Disable	A function of the interface between a Device and an eUICC that provides the capability for a Device to locally disable the Emergency Profile or the Test Profile on the eUICC without involvement of an SM-SR and/or SM-DP.
Local Enable	A function of the interface between a Device and an eUICC that provides the capability for a Device to locally enable the Emergency Profile or the Test Profile on the eUICC without involvement of an SM-SR and/or SM-DP.
M2M Service Provider (M2M SP)	A Service Provider relying on an Operator providing the Profiles on the eUICC.
Mobile Network Operator	An entity providing access capability and communication services to its Customers through a mobile network infrastructure.

MNO-SD	Security domain part of the Profile, owned by the Operator, providing the Secured Channel to the Operator's OTA Platform. It is used to manage the content of a Profile once the Profile is enabled.
Network Access Application	An application residing on a UICC which provides authorisation to access a network for example a USIM application.
Operator	A Mobile Network Operator or Mobile Virtual Network Operator; a company providing wireless cellular network services.
Operator Notification Configuration (ONC)	Operator request to configure Operator specific status change notifications for Profiles owned by this Operator.
Orphaned Profile	A Profile whose Policy Rules have become unmanageable, for example due to the termination of the Customer's contract with the Operator.
OTA Keys	The credentials included in the Profile, used in conjunction with OTA Platforms.
OTA Platform	An Operator platform for remote management of UICCs and the content of Enabled Operator Profiles on eUICCs.
PIX	Proprietary application Identifier eXtension, the value of which is part of the AID.
Platform Management	A set of functions related to the enabling, disabling and deletion of a Profile on and the transport of Profile Management functions to an eUICC. Platform Management actions are protected by Platform Management Credentials shared between the SM-SR and the ISD-R. Platform Management does not affect the content of a Profile.
Profile Component	A Profile Component is an element of the Profile and may be one of the following: An element of the file system like an MF, EF or DF An Application, including NAA and Security Domain POL1 MNO-SD. Connectivity Parameters.
Platform Management Credentials	Data required within an eUICC so that a secured communication can be set up between an external entity and the eUICC in order to enable, disable and delete Profiles on the eUICC and to transport Profile Management functions.
Policy	Principles reflected in a set of rules that governs the behaviour of eUICC and/or entities involved in the remote management of the eUICC.
Policy Rule	Defines the atomic action of a Policy and the conditions under which it is executed.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC and which allows, when enabled, the access to a specific mobile network infrastructure.

Profile Lifecycle Management	Execution of certain Platform Management commands by the M2M SP on a Profile, based on prior Profile Lifecycle Management Authorisation from the Operator owning the Profile.
Profile Lifecycle Management Authorisation (PLMA)	Authorisation given by an Operator to an M2M SP to permit Profile Lifecycle Management. Such authorisations are managed by the SM-SR.
Profile Management	A set of functions related to the downloading, installation and content update of a Profile in a dedicated ISD-P on the eUICC. Download and installation are protected by Profile Management Credentials shared between the SM-DP and the ISD-P.
Profile Management Credentials	Data required within an eUICC so that a Profile downloaded from an external entity can be decrypted and installed on the eUICC.
Profile Owner	The entity that controls the operations that can be performed upon its Profile. With the exception of Test Profiles, this is always the Operator.
Profile Type	Operator specific defined type of Profile. This is equivalent to the "ProfileType" as described in 5.1.1.2.4 of this specification.
RID	Registered Application Provider IDentifier, the value of which is part of the AID.
Roles	Roles are representing a logical grouping of functions.
Root Certificate	Self-signed certificate of the CI, used to authenticate certificates issued to other entities.
Script Chaining	Indication that a command script is split over several secured messages. Script Chaining indicators will specify when to keep and restore the command context at the boundary of secure channels that transport the different parts of the command script
Security Domain Image Number (SDIN)	Identification number used by an Application Management System to uniquely identify an instance of a Security Domain on a card as specified in GlobalPlatform Card Specification [6].
Security Domain Provider Identification Number (SIN)	Identification number used by an off-card entity to associate the Security Domain with a specific Card Management System, as specified in GlobalPlatform Card Specification [6]. It is an IIN, typically contains the ISO 7812 [19] defined identification of the Security Domain provider.
Subscriber	An entity (associated with one or more users) that is engaged in a Subscription with a Telecommunication Service Provider. The Subscriber is allowed to subscribe and unsubscribe to services, to register a user or a list of users authorised to use those services, and also to set the limits relative to the use that associated users make of those services.
Subscription	Describes the commercial relationship between the Subscriber and the Telecommunication Service Provider.

Subscription Address	A unique network address, such as MSISDN, IMSI or SIP-URI, of a mobile Subscription within a mobile network. It is used to route messages, for example SMS, to the eUICC.
Subscription Manager Data Preparation	Role that prepares the Profiles to be securely provisioned on the eUICC and manages the secure download and installation of these Profiles onto the eUICC.
Subscription Manager Secure Routing	Role that securely performs functions of Platform Management commands and the transport of Profile Management commands.
Tamper Resistant Element	A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data.
Telecommunication Service Provider	An entity that provides Subscriptions to Subscribers either as part of an Operator or as a party with a wholesale agreement with an Operator. The Telecommunication Service Provider could also be the Operator.
Test Profile	A combination of data and applications to be provisioned on an eUICC to provide connectivity to test equipment for the purpose of testing the Device and the eUICC. A Test Profile does not allow access to an ITU-E.212 [16] network.

1.6 Abbreviations

Abbreviation	Description
AID	Application Identifier
AES	Advanced Encryption Standard
CASD	Controlling Authority Security Domain
CBC	Cipher Block Chaining
CC	Cryptographic Checksum
CERT.DP.ECDSA	Certificate of the SM-DP for its ECDSA key
CERT.SR.ECDSA	Certificate of the SM-SR for its ECDSA key
CERT.ECASD.ECKA	Certificate of the ECASD for its ECKA key
CI	Certificate Issuer
CIN	Card Image Number / Card Identification Number
CMAC	Cipher-based Message Authentication Code
CRL	Certificates Revocation List
ECASD	eUICC Controlling Authority Security Domain
ECDSA	Elliptic Curve cryptography Digital Signature Algorithm
ECKA	Elliptic Curve cryptography Key Agreement algorithm
DAP	Data Authentication Pattern
DGI	Data Grouping Identifier
DNS	Domain Name System
DR	Derivation Random

EUM	eUICC Manufacturer
EID	eUICC-ID
EIN	EUM Identification Number
EIS	eUICC Information Set
ESIN	EUM Specific Identification Number
ETSI	European Telecommunications Standards Institute
ePK.DP.ECKA	ephemeral Public Key of the SM-DP used for ECKA
ePK.SR.ECKA	ephemeral Public Key of the SM-SR used for ECKA
eSK.DP.ECKA	ephemeral Private Key of the SM-DP used for ECKA
eSK.SR.ECKA	ephemeral Private Key of the SM-SR used for ECKA
eUICC	Embedded UICC
FQDN	Fully Qualified Domain Name
GP	GlobalPlatform
GSMA	GSM Association
ICCID	Integrated Circuit Card ID
IIN	Issuer Identification Number
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
ISO	International Standards Organisation
ITU	International Telecommunications Union
LTE	Long Term Evolution
LV	Length Value
M2M SP	Machine to Machine Service Provider
MEP	Message Exchange Pattern
MNO	Mobile Network Operator
MO	Mobile Originated
MOC	Mandatory, Optional or Conditional
MT	Mobile Terminated
NAA	Network Access Application
ONC	Operator Notification Configuration
OTA	Over The Air
PIX	Proprietary application Identifier eXtension
PK.CI.ECDSA	Public Key of the CI in the ECASD for verifying certificate signatures
PK.DP.ECDSA	Public Key of the SM-DP, part of the CERT.DP.ECDSA, for verifying its signatures

PK.ECASD.ECKA	Public Key of the ECASD used for ECKA
PK.SR.ECDSA	Public Key of the SM-SR part of the CERT.SR.ECDSA, for verifying its signatures
PLMA	Profile Lifecycle Management Authorisation
POL1	Policy Rules within the Profile
POL2	Policy Rules associated to a Profile and stored in the relevant EIS at the SM-SR
PoR	Proof of Receipt
PPK-ENC	Profile Protection Key for message encryption/decryption
PPK-MAC	Profile Protection Key for command MAC generation/verification
PPK-RMAC	Profile Protection Key for response MAC generation/verification
SCP	Secure Channel Protocol
SD	Security Domain
SDIN	Security Domain Image Number
ShS	Shared Secret
SIN	Security Domain Provider Identification Number
SK.DP.ECDSA	Private Key of the of SM-DP for creating signatures
SK.ECASD.ECKA	Private Key of the ECASD used for ECKA
SK.SR.ECDSA	Private Key of the SM-SR for creating signatures
SK.CI.ECDSA	Private key of the CI for signing certificates
SM	Subscription Manager
SM-DP	Subscription Manager Data Preparation
SM-SR	Subscription Manager Secure Routing
SOA	Service-oriented Architecture
SOAP	Simple Object Access Protocol
TAR	Toolkit Application Reference
TLS	Transport Layer Security
TLV	Tag Length Value
TRE	Tamper Resistant Element
URI	Uniform Resource Identifier
URL	Uniform Resource locator
USIM	Universal Subscriber Identity Module
XML	Extensible Markup Language
W3C	World Wide Web Consortium

1.7 References

Ref	Document Number	Title
[1]	SGP.01	GSMA 'Remote Provisioning Architecture for Embedded UICC' Version 4.3
[2]	ETSI TS 101 220	Smart Cards; ETSI numbering system for telecommunication application providers; Release 9
[3]	ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT) ; Release 9
[4]	ETSI TS 102 225	Secured packet structure for UICC based applications; Release 12
[5]	ETSI TS 102 226	Remote APDU structure for UICC based applications; Release 9
[6]	GPC_SPE_034	GlobalPlatform Card Specification v.2.2.1
[7]	GPC_GUI_010	GlobalPlatform Card Specification v.2.2.1 UICC Configuration v1.0.1
[8]	GPC_SPE_011	GlobalPlatform Card Specification v.2.2 Amendment B: Remote Application Management over HTTP v1.1.3
[9]	GPC_SPE_025	GlobalPlatform Card Specification v.2.2 Amendment C: Contactless Services v1.1.1
[10]	GPC_SPE_014	GlobalPlatform Card Specification v.2.2 Amendment D: Secure Channel Protocol 03 v1.1.1
[11]	GPC_SPE_042	GlobalPlatform Card Specification v.2.2 Amendment E: Security Upgrade for Card Content Management v1.0.1
[12]	ITU E.212	The international identification plan for public networks and Subscriptions
[13]	3GPP TS 31.115	Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications Release 11
[14]	OMA Smartcard-Web-Server v1.0	OMA-TS-Smartcard_Web_Server-V1_0-20080421-A
[15]	RFC 5246	The TLS Protocol – Version 1.2
[16]	RFC 4279	Pre-Shared Key Cipher suites for Transport Layer Security (TLS)
[17]	RFC 5487	Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode
[18]	RFC 3629	Unicode Transformation Format 8-bit
[19]	ISO/IEC 7812	Identification Cards; Identification of issuers
[20]	ETSI TS 124 008	Mobile radio interface Layer 3 specification; Core network protocols; Release 9
[21]	ITU E.118	The international telecommunication charge card
[22]	ITU E.164	International Public Telecommunication Numbering Plan
[23]	GPS_SPE_002	"GlobalPlatform System": Messaging Specification for Management of Mobile NFC Services, Version 1.1.2
[24]	RFC 4051	Additional XML Security Uniform Resource Identifiers (URIs)

[25]	ETSI TS 102 127	Transport protocol for CAT applications; Release 6
[26]	XML DSIG-CORE	W3C XML Signature Syntax and Processing (Second Edition)
[27]	3GPP TS 31.111	Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) ; Release 9
[28]	3GPP TS 31.116	Remote APDU Structure for (U)SIM Toolkit applications; Release 9
[29]	3GPP TS 24.341	Support of SMS over IP networks; Release 9
[30]	GSMA Security Principles Related to Handset Theft	GSMA Doc Reference: Security Principles Related to Handset Theft 3.0.0 EICTA CCIG Doc Reference: EICTA Doc: 04cc100
[31]	ETSI TS 123 003	Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification; Release 9
[32]	RFC 768	User Datagram Protocol, Aug 1980.
[33]	RFC 793	Transmission Control Protocol, DARPA Internet Program, Protocol specification, Sept 1981.
[34]	GPC_GUI_049	GlobalPlatform Card, Secure Element Configuration Version 1.0, October 2012
[35]	3GPP TS 27.007	Technical Specification Group Core Network and Terminals; AT command set for User Equipment (UE) ; Release 9
[36]	NIST SP 800-57 Part 1	NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General (Revision 3), July 2012
[37]	BSI TR-02102	BSI – Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version: 2013.02
[38]	GSMA PRD IR.92	GSMA PRD IR.92: IMS Profile for Voice and SMS
[39]	3GPP TS 23.040	Technical Specification Group Core Network and Terminals; Technical realisation of the Short Message Service (SMS)
[40]	SOAP	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) http://www.w3.org/TR/soap12-part1/
[41]	WS-Addressing	Web Services Addressing 1.0, Core , 9th of May 2006 http://www.w3.org/TR/ws-addr-core/
[42]	WS-Addressing-SOAP-Binding	Web Services Addressing 1.0 - SOAP Binding, 9th of May 2006 http://www.w3.org/TR/2006/REC-ws-addr-soap-20060509/
[43]	WS-MakeConnection	Web Services Make Connection (WS-MakeConnection), 2nd February 2009, http://docs.oasis-open.org/ws-rx/wsmc/200702/wsmc-1.1-spec-os.html
[44]	WSS-SOAPMessageSecurity	Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), 1 February 2006, https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[45]	WSS-UserNameTokenProfile	Web Services Security UsernameToken Profile 1.1, February 2006, http://docs.oasis-open.org/wss/v1.1/
[46]	WSS-X509TokenProfile	Web Services Security X.509 Certificate Token Profile 1.1, February 2006, http://docs.oasis-open.org/wss/v1.1/
[47]	XML	Extensible Markup Language (XML) 1.0, W3C Recommendation 10-Feb-98, REC-xml-19980210
[48]	XML Signature	XML Signature Syntax and Processing (Second Edition),W3C Recommendation http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/
[49]	BSI TR-03111	BSI Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0
[50]	NIST SP 800-56A	NIST Special Publication SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revision 2), May 2013
[51]	ANSSI ECC FRP256V1	Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français. JORF n°0241 du 16 octobre 2011 page 17533. texte n° 30. 2011
[52]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application, Release 9
[53]	SIMAPP	SIMalliance: eUICC Profile Package - Interoperable Format Technical Specification v2.3.1, 28 November 2019, http://simalliance.org/euicc/euicc-technical-releases/
[54]	GPC_SPE_007	GlobalPlatform Card Specification v.2.2 Amendment A: Confidential Card Content Management v1.0.1
[55]	NIST SP 800-56C	NIST Special Publication 800-56C Recommendation for Key Derivation through Extraction-then-Expansion
[56]	SGP.14	GSMA eUICC PKI Certificate Policy v1.1
[57]	RFC 5280	Internet X.509 PKI Certificate and CRL Profile
[58]	RFC 1035	DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
[59]	RFC 3596	DNS Extensions to Support IP Version 6
[60]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels, S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[61]	FS.04	FS.04 - Security Accreditation Scheme for UICC Production – Standard v8
[62]	FS.08	FS.08 – Security Accreditation Scheme for Subscription Manager - Standard v3
[63]	SGP.05	SGP.05 - Embedded UICC Protection Profile v1.1
[64]	SGP.16	M2M Compliance Process v1.0
[65]	RFC 3987	Internationalized Resource Identifiers (IRIs). January 2005. http://www.ietf.org/rfc/rfc3987.txt

[66]	Java Card	Java Card Classic Platform Specification https://www.oracle.com/java/technologies/javacard-specs-downloads.html
[67]	3GPP TS 33.501	Security architecture and procedures for 5G system (Release 15)
[68]	3GPP TS 31.130	(U)SIM API for Java™ Card (Release 15)
[69]	GPC_SPE_095	GlobalPlatform Card - Digital Letter of Approval - Version 1.0
[70]	ETSI TS 102 221	Smart Cards; UICC-Terminal interface; Physical and logical characteristics
[71]	GSMA PRD AA.35	Procedures for Industry Specifications
[72]	SGP.22	GSMA RSP Technical Specification
[73]	SGP.29	GSMA EID Definition and Assignment Process
[74]	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax. January 2005. http://www.ietf.org/rfc/rfc3986.txt

1.8 Conventions

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document SHALL be interpreted as described in RFC 2119 [60].

2 General Parts of the Technical Specification

This section contains a technical description and architecture of the Remote Provisioning System for the Embedded UICC. It SHALL be compliant with the Remote Provisioning Architecture for Embedded UICC [1]. In addition, the statements in this section define the basic characteristics that need to be taken into account when realising this specification.

2.1 General Architecture

This section further specifies the Roles and interfaces associated with the Remote Provisioning and Management of the eUICC, building on GSMA Remote Provisioning Architecture for Embedded UICC [1].

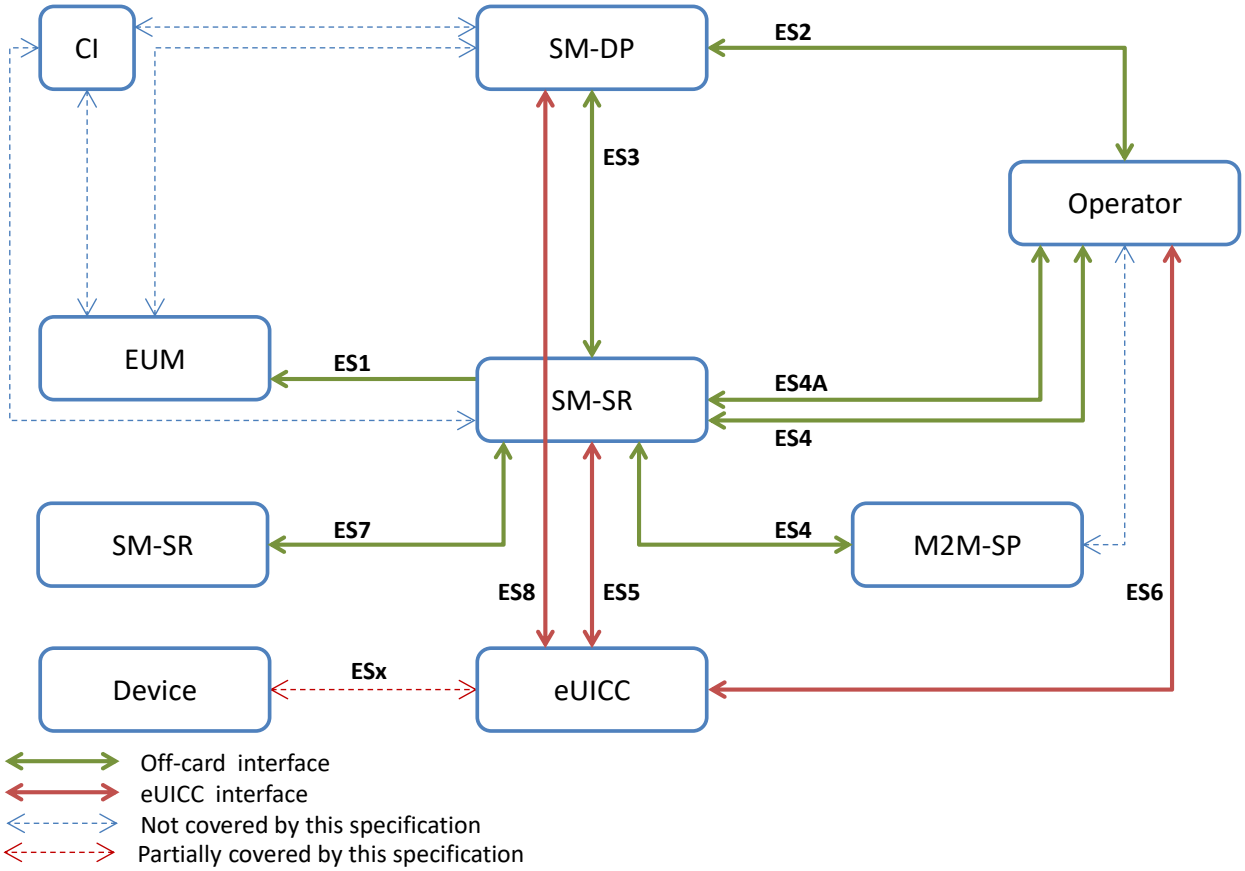


Figure 1: eUICC Remote Provisioning System

The above figure provides the complete description of the eUICC Remote Provisioning and Management system.

The ES5, ES6, ES8 and ESx interfaces are described in section 4.

The ES1, ES2, ES3, ES4 and ES7 interfaces are described in section 5.

NOTE: Functions of the ES2 interface related to Profile ordering and master delete are considered out of the scope of this specification as these functions may be based upon pre-existing Operator processes.

NOTE: The interface between the SM-DP and EUM and the related function for Profile Creation is out of the scope of this specification as this function is based upon proprietary mechanisms.

NOTE: The ES6 interface is based on the RAM and RFM mechanisms described in ETSI TS 102 225 [4] and ETSI TS 102 226 [5].

NOTE: As defined in GSMA Remote Provisioning Architecture for Embedded UICC [1], the Initiator Role is assumed to be played by the Operator and functions related to this Role are specified in the ES4 interface.

NOTE: ESx and its related operations for Emergency and Test Profiles (Local Enabling and Local Disabling), as well as the support of the Emergency Profile and Test Profile, are optional features.

2.2 eUICC Architecture

This section focuses on the eUICC architecture which widely leverages current telecommunication standards, as well as GlobalPlatform standards that are especially well adapted to establish Role separation and data isolation. In particular, each entity will have a dedicated Security Domain with different privileges and configuration.

2.2.1 Security Domains

The eUICC architecture comprises the following Security Domains for the purpose of Platform and Profile Management:

- The ISD-R is the representative of the off-card entity SM-SR
- The ECASD is the representative of the off-card entity CI
- An ISD-P is the representative of an off-card entity SM-DP. An eUICC can contain more than one ISD-P

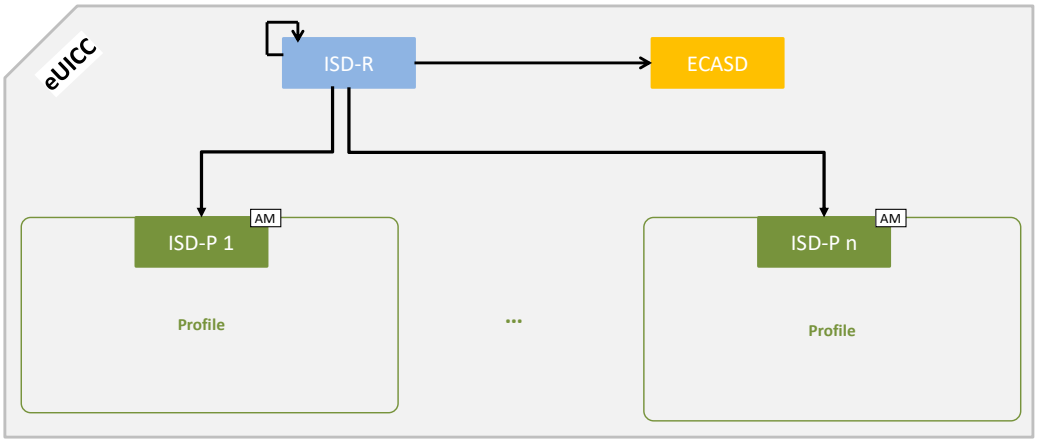


Figure 2: Security Domain Architecture Overview

An ISD, as specified in GlobalPlatform Card Specification [6], does not exist in the architecture of the eUICC.

2.2.1.1 ISD-R

There SHALL be only one ISD-R on an eUICC.

The ISD-R SHALL be installed and first personalized by the EUM during eUICC manufacturing. The ISD-R SHALL be Associated with itself.

After eUICC manufacturing, the ISD-R SHALL be in life-cycle state PERSONALIZED as defined in GlobalPlatform Card Specification [6], section 5.3. The LOCKED state SHALL NOT be supported by the ISD-R.

The ISD-R privileges SHALL be granted according to Annex C.

The ISD-R SHALL only be able to perform Platform Management functions on ISD-Ps.

2.2.1.2 ECASD

There SHALL be only one ECASD on an eUICC.

The ECASD SHALL be installed and personalized by the EUM during the eUICC manufacturing. The ECASD SHALL be Associated with the ISD-R.

After eUICC manufacturing, the ECASD SHALL be in life-cycle state PERSONALIZED as defined in GlobalPlatform Card Specification [6], section 5.3.

The ECASD is involved in the following functions:

- SM-DP key set establishment for Profile Download and Installation
- SM-SR key set establishment for SM-SR Change

The ECASD SHALL be personalized by the EUM during eUICC manufacturing with:

- PK.CI.ECDSA
- SK.ECASD.ECKA
- CERT.ECASD.ECKA for eUICC Authentication and key establishment
- EID

The ECASD SHALL comply with the requirements defined for the CASD in GlobalPlatform Card Specification UICC configuration [7] except:

- AIDs and TAR SHALL be allocated as defined in section 2.2.3
- Support of SCP 02 is not required
- Only the ISD-R and ISD-Ps SHALL be able to use the ECASD services

2.2.1.3 ISD-P

An ISD-P hosts a unique Profile.

Only one ISD-P SHALL be enabled on an eUICC at any point in time.

An ISD-P SHALL be installed by the ISD-R and then personalized by its related SM-DP (see section 3.1.1). At least one ISD-P with a Profile SHALL be installed and first personalized by the EUM during eUICC manufacturing to allow future eUICC connectivity.

The ISD-P SHALL be able to receive and process a Profile Package, wrapped in an SCP03t Secure Channel, as specified in section 4.1.3.3.

The eUICC SHALL support the SIMalliance: eUICC Profile Package - Interoperable Format Technical Specification [53] with the major version being 2 and the version being at least 2.3.1. The eUICC MAY in addition support higher major versions. The EUM SHALL indicate in the EIS the versions supported by the eUICC, as specified in section 5.1.1.2.10.

No component outside the ISD-P SHALL have visibility or access to any Profile component with the exception of the ISD-R, which SHALL have read access to POL1 and to the Connectivity Parameters as defined in section 4.1.3.4.

A Profile Component SHALL NOT have any visibility of, or access to, components outside its ISD-P. An ISD-P SHALL NOT have any visibility of, or access to, any other ISD-P.

It SHALL be possible to allocate the same AID within different Profiles. A Profile Component SHALL NOT use the reserved ISD-R, ISD-P and ECASD AIDs.

It SHALL be possible to allocate the same TAR within distinct Profiles. A Profile Component SHALL NOT use the reserved ISD-R, ISD-P and ECASD TARs.

An ISD-P SHALL remain associated to the ISD-R during all its life time in order for the ISD-R to be able to perform the Platform Management functions:

- ISD-P Creation: the Association between the ISD-R and an ISD-P SHALL be created at that time
- ISD-P Deletion and Master Delete
- Profile Enabling and Disabling
- Fall-Back Attribute setting
- Transport function: The Association SHALL allow SCP03/SCP03t establishment between the SM-DP and the ISD-P.

ISD-P SHALL follow the life-cycle illustrated in the Figure 3, based on the Security Domain life-cycle defined in GlobalPlatform Card Specification [6], section 5.3.

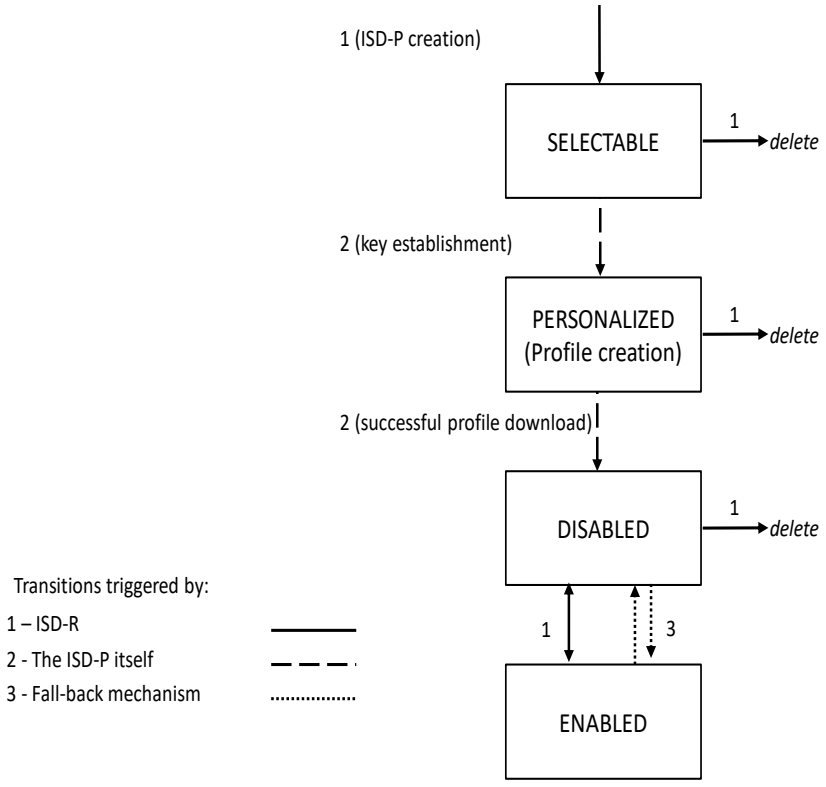


Figure 3: ISD-P Life-Cycle State Transitions

After execution of the procedure described in section 3.1.1, the ISD-P SHALL be in SELECTABLE state. After execution of the procedure described in section 3.1.2, the ISD-P SHALL be in PERSONALIZED state.

NOTE: The INSTALLED state for security domains defined in GlobalPlatform Card Specification [6] is skipped by the command for ISD-P creation defined in section 4.1.1.1.

After execution of the procedure described in section 3.1.3 or 3.4, the ISD-P SHALL be in the DISABLED state. The ISD-P can also transition to the DISABLED state as the result of the enabling of another ISD-P as described in section 3.2, or the activation of the Fall-Back Mechanism.

After execution of the procedure described in section 3.2, the ISD-P SHALL be in the ENABLED state. The ISD-P can also transition to the ENABLED state as the result of the activation of the Fall-Back Mechanism.

Deletion removes the ISD-P with its Profile from the eUICC.

The LOCKED state SHALL NOT be supported by an ISD-P.

For coding the states, table 11-5 of GlobalPlatform Card Specification [6] is modified as follows:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	1	1	(INSTALLED)
0	0	0	0	0	1	1	1	SELECTABLE
0	0	0	0	1	1	1	1	PERSONALIZED (Profile creation)
0	0	0	1	1	1	1	1	DISABLED
0	0	1	1	1	1	1	1	ENABLED

Table 1: ISD-P Coding States

These states can be mapped to the architectural states defined in GSMA Remote Provisioning Architecture [1] as shown below:

State (as defined in [1])	State (as defined above)
Created	(INSTALLED)
	SELECTABLE
	PERSONALIZED
Disabled	DISABLED
Enabled	ENABLED
Deleted	No explicit mapping; ISD-P no longer exists on the eUICC

Table 2: ISD-P State Mapping

ISD-P privileges SHALL be granted according to Annex C.

All Profile Components, in particular the MNO-SD, SHALL remain linked to the ISD-P in order to enable the following:

- Profile Download and Installation: the Profile Components, which are affiliated with the ISD-P, are created at that time
- ISD-P Deletion and Master Delete: the Profile Components SHALL be deleted at that time
- Profile Enabling and Disabling: Enable and Disable access to all the Profile Components
- Update of POL1
- Provide read access to POL1 when required for Platform Management functions.

The Application privileges (defined in GlobalPlatform Card Specification [6]) assigned to a Profile Component SHALL apply according to Annex C.

All Profile Components created by the ISD-P SHALL always remain affiliated with the ISD-P. In particular it is not possible to change the affiliation of any Profile Component.

When an ISD-P is not in enabled state, the eUICC SHALL ensure that:

- Remote management of any Profile Component is not possible via the ES6 interface;
- The file system within the Profile cannot be selected by the Device or any application on the eUICC;
- The applications (including NAAs and Security Domains) within the Profile cannot be selected, triggered or deleted.

2.2.2 Identification of eUICC: EID

The EID is the eUICC identifier used in the context of Remote Provisioning and Management of the eUICC.

The EID SHALL be stored within the ECASD and can be retrieved by the Device at any time using the standard GlobalPlatform GET DATA command by targeting the ECASD as specified in GlobalPlatform Card Specification [6] as follows:

- Select the ECASD using the SELECT command with the AID value defined in section 2.2.3
- Send a ‘GET DATA’ command to the ECASD with the data object tag '5A' to retrieve the EID

This version of the specification allows EIDs according to two formats:

- the IIN based format, and
- the EIN based format.

The versions up to version 4.2 of this specification only used the IIN based format defined below, where the IIN has a fixed length of 8 digits.

Starting from version 4.2.1 of this specification, EIDs MAY also be assigned according to the EIN based format as defined in SGP.29 [73], where the EIN is of variable length.

The EID SHALL uniquely identify an eUICC. The owner of the IIN or the EIN SHALL guarantee the uniqueness of the EID, also with respect to eUICCs produced according to previous versions of this specification and to all versions of SGP.22 [72].

The following rules will maximise the interoperability between the different versions:

- An EUM generating EIDs according to SGP.29 [73] SHOULD get an EUM certificate where the first 8 digits of the EIDs are fixed and listed as IIN in NameConstraints extension of the certificate.
- An EUM with an EIN longer than 8 digits SHOULD only generate EIDs if it is acceptable that the EIN is not uniquely identifiable in the NameConstraints extension of the certificate.

The EID according to the IIN based format SHALL have the following structure:

- The EID SHALL always be 32 digits long, with the first 8 digits representing the IIN.
- The EID SHALL always be built of
    - A Major Industry Identifier digit of 8 (1st digit), as defined in ISO/IEC 7812 [19].
    - An additional digit of 9 specifying telecommunications, as defined in ISO/IEC 7812 [19],
    - An additional three digits for country code (3rd to 5th digits).
        - If the country code is one digit long, its value SHALL be prefixed by two digits of 0,
        - If the country code is two digits long, its value SHALL be prefixed by one digit of 0.
    - An additional three digits for issuer identifier (6th to 8th digits)
        - If the issuer identifier is one digit long, its value SHALL be prefixed by two digits of 0,
        - If the issuer identifier is two digits long, its value SHALL be prefixed by one digit of 0.
    - An additional ten digits for issuer specific information (9th to 18th digits), of which the first five digits (9th to 13th) contain version information about the platform and OS, to be specified by the issuer and the last five digits (14th to 18th) contain additional issuer information,
    - An additional twelve digits for the individual identification number (19th to 30th digits),
    - A last two digits (31st to 32nd digits) containing check digits calculated over all 32 digits as specified below.
- The country code and issuer identifier SHALL be assigned as specified in ITU E.118 [21]
- The two check digits are calculated as follows:
    - 1. Replace the two check digits by two digits of 0,
    - 2. Using the resulting 32 digits as a decimal integer, compute the remainder of that number on division by 97,

    - 3. Subtract the remainder from 98, and use the decimal result for the two check digits,
        - If the result is one digit long, its value SHALL be prefixed by one digit of 0.
- When stored as a byte string, the first digit SHALL be put into the highest four bits of the first byte

Annex J provides a description of how the verification of an EID is performed.

2.2.3 Identification of Security Domains: AID and TAR

The ISD-P AID, the ISD-R AID and the ECASD AID SHALL follow the structure specified in ETSI TS 101 220 [2], with a RID and a PIX. The ISD-P AID, the ISD-R AID and the ECASD AID SHALL be 16 bytes long including the TAR.

The RID of the Executable Load File, the Executable Module and the Application of the ISD-R, the ISD-P and the ECASD SHALL be set to 'A000000559' (as defined in ISO/IEC 7816-5:2004).

The ISD-R application SHALL be installed by the EUM during eUICC manufacturing. The ISD-R Executable Load File AID and the ISD-R Executable Module AID can be freely selected by the EUM.

The ISD-R application AID SHALL be ‘A0 00 00 05 59 10 10 FF FF FF FF 89 00 00 01 00' as defined into Annex H.

The ECASD application SHALL be installed by the EUM during eUICC manufacturing. The ECASD Executable Load File AID and the ECASD Executable Module AID can be freely selected by the EUM.

The ECASD application AID SHALL be ‘A0 00 00 05 59 10 10 FF FF FF FF 89 00 00 02 00' as defined into Annex H.

The ISD-P application SHALL be installed by SM-SR during the first step of the “Profile Download and Installation” procedure in section 3.1.

The ISD-P Executable Load File AID SHALL be ‘A0 00 00 05 59 10 10 FF FF FF FF 89 00 00 0D 00' as defined into Annex H.

The ISD-P Executable Module AID SHALL be ‘A0 00 00 05 59 10 10 FF FF FF FF 89 00 00 0E 00' as defined into Annex H.

The ISD-P application AID SHALL be coded according to Annex H. The SM-SR SHALL allocate the ISD-P application AID in the range defined in Annex H.

NOTE: The choice of having the ISD-P AID allocated by the SM-SR is to avoid conflicts with other ISD-P AIDs used by already installed ISD-Ps; the SM-DP cannot have such visibility.

The MNO-SD application AID and TAR(s) can be freely allocated by the Operator during Profile definition.

2.2.4 Profile Structure

The Profile structure, composed of a set of Profile Components, is specified by, and under the full control of, the Operator. The full Profile structure SHALL be contained in a unique ISD-P.

The Profile structure SHALL contain a Profile Component, called MNO-SD, which performs an identical Role as the ISD for a UICC (see GlobalPlatform Card Specification [6]). This MNO-SD is the representative of the Operator owning the Profile, meaning it contains the Operator's OTA Key sets.

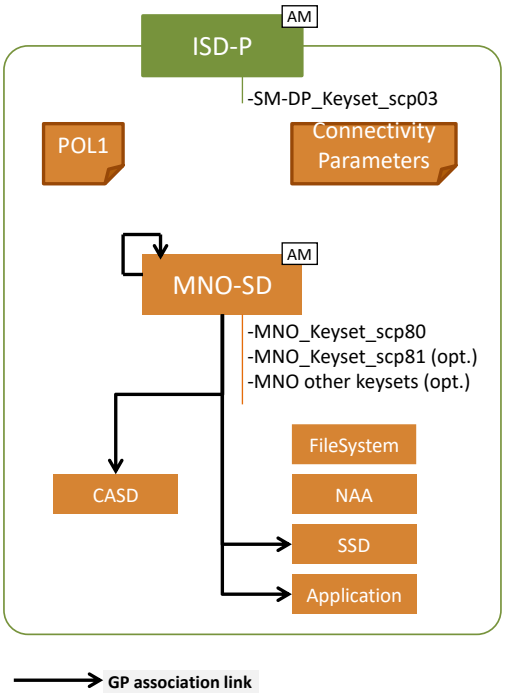


Figure 4: Profile Structure Overview

The Profile in the Figure 4 provides an example of a Profile structure.

The Profile structure SHALL include:

- The MNO-SD
- At least one NAA
- POL1, even if not used
- The file system
- Connectivity Parameters of the Profile

The Profile structure MAY contain:

- Several Applications (as defined in GlobalPlatform Card Specification [6]) in addition to the MNO-SD
- One CASD (as defined in GlobalPlatform Card Specification UICC Configuration [7])

The privileges that can be allocated to the MNO-SD and to applications SHALL comply with Annex C.

It SHALL be possible for the Operator to establish secure channels between the Operator OTA Platform and security domains of the Profile as specified in ETSI TS 102 225 [4] and ETSI TS 102 226 [5].

2.2.5 Secure Channel on Interfaces

2.2.5.1 Secure Channel on ES5 (SM-SR-eUICC)

The ES5 functions are addressed to the eUICC through a secure channel established between the SM-SR and the ISD-R. The eUICC SHALL support SCP80 and may support SCP81 (defined in ETSI 102 225 [4] and ETSI 102 226 [5]). See also section 2.4.

To enable SCP80, the ISD-R SHALL be personalized before issuance by the EUM with at least one key set, with a Key Version Number between ‘01’ to ‘0F’ following GlobalPlatform Card Specification UICC Configuration [7].

To enable SCP81, the ISD-R SHALL be personalized with at least one key set, with a Key Version Number between ‘40’ to ‘4F’ following GlobalPlatform Secure Element Configuration [34].

The key length and algorithm SHALL comply with section 2.3.3.

The key sets SHALL be loaded in the ISD-R, and provided to SM-SR, in the EIS, through ES1

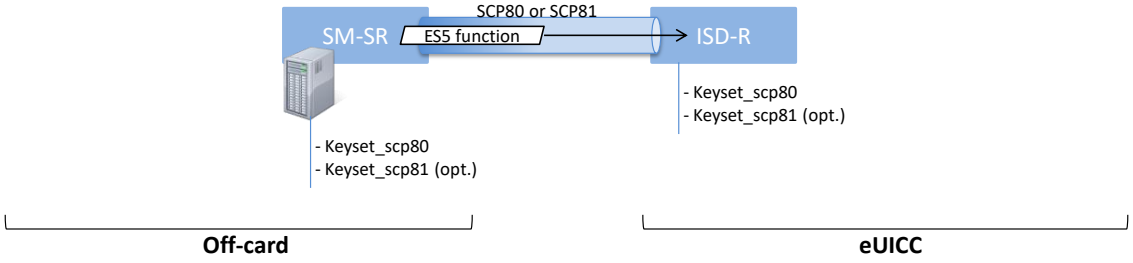


Figure 5: Secure Channel Between SM-SR and ISD-R

2.2.5.2 Secure Channel on ES8 (SM-DP - eUICC)

The ES8 functions are addressed to the eUICC through a secure channel established between the SM-DP and its ISD-P. The eUICC SHALL support SCP03 for ES8 (as defined in GlobalPlatform Card Specification Amendment D [10], as well as the variant SCP03t defined in this specification (see section 4.1.3.3).

NOTE: SCP03 is the only secure channel defined by GlobalPlatform that complies with requirements of the section 2.3.3.

To enable SCP03 and SCP03t, the ISD-P SHALL be personalized with at least one key set, with a Key Version number between '30' to '3F' (see GlobalPlatform Secure Element Configuration [34]).

The secure channel configuration, key length and algorithm to be used SHALL comply with section 2.5.

The first SCP03 key set is loaded into the ISD-P by its SM-DP as described in the procedure "Key Establishment with Scenario#3-Mutual Authentication", section 3.1.2.

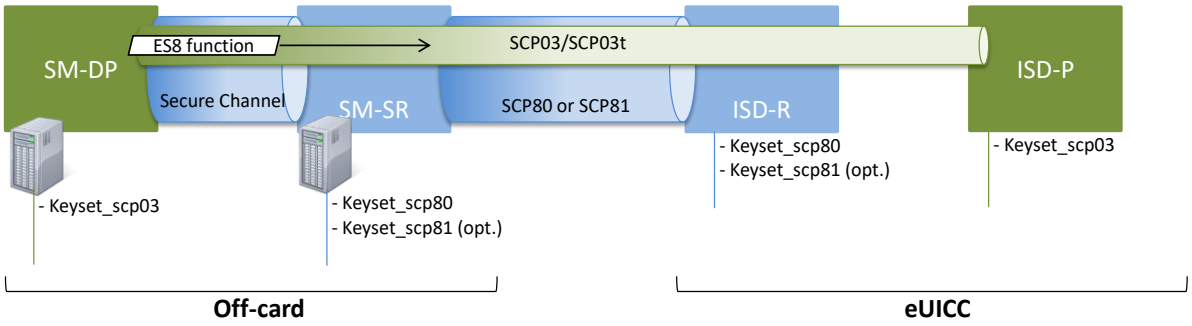


Figure 6: Secure Channel Between SM-DP and ISD-P

2.2.5.3 Secure Channel on ES6 (Operator-eUICC)

The ES6 functions are addressed to the eUICC through a secure channel (as defined in ETSI TS 102 225 [4] and ETSI TS 102 226 [5]) established between the Operator and the MNO-SD (as defined in section 2.2.3).

NOTE: The Operator can also communicate with any other SSD (of the Profile) belonging to the Operator. The Figure 7 only illustrates the secure channel with the MNO-SD.

The initial OTA Key sets are part of the Profile and are loaded by the SM-DP during the "Profile Download and Installation", see section 3.1, or loaded by the EUM before eUICC issuance.

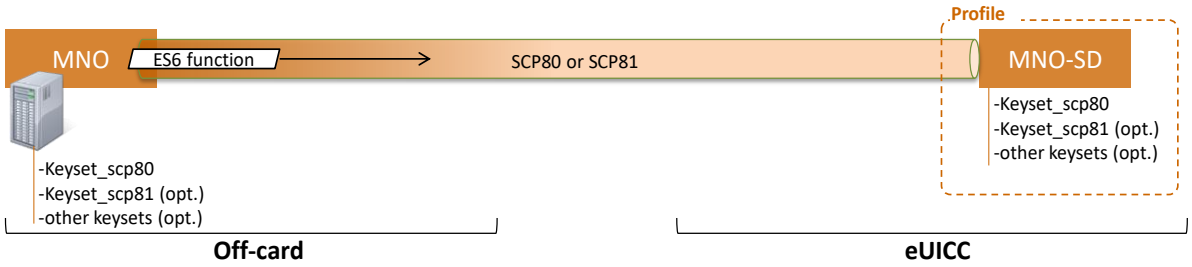


Figure 7: Secure Channel Between Operator and MNO-SD

2.2.6 eUICC OS Update

An eUICC should support a secure mechanism to allow the eUICC OS Update when the eUICC is in the field. Such mechanism allows the eUICC Manufacturer to correct errors in existing features on the eUICC. When an eUICC OS Update mechanism is supported, it SHALL be declared in the EIS through OSUpdateSupported in the AdditionalProperties field.

The process and mechanisms are EUM implementation specific and therefore out of scope of this specification.

In case an eUICC OS Update happens, the EUM SHALL ensure that:

- the resulting eUICC SHALL maintain, at least, the same level of security and functional compliance than the previous eUICC.
- The EIS additional property updatedPlatformVersion is updated to reflect the change of Operating System version

After an update of the EIS, the SM-SR SHOULD take implementation-dependent actions to also update the EIS field “remainingMemory”.

2.2.7 Java Card™ Support

The eUICC MAY support Java Card™. If Java Card™ is supported, the eUICC SHALL support at least version 3.0.4 of the Java Card Classic Platform Specification [66].

2.2.8 Hardware Characteristics of the eUICC

The following requirements apply:

- The eUICC SHALL be based on a Tamper Resistant Element.
- The eUICC SHALL be either a Discrete eUICC or an Integrated eUICC.
- A Discrete eUICC MAY either be removable or non-removable. A removable eUICC SHALL be packaged in a form factor specified in ETSI TS 102 221 [70].

2.3 Security Overview

This section provides an overview of the overall ecosystem security features.

The expectation 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.

The security requirements have to be applied to the different Actors and Roles (Customer, Operator, SM-DP, SM-SR, CI, eUICC and eUICC Manufacturer). Each Role is considered as elements which can belong to a security realm and has to fulfil the appropriate certification compliance criteria (see section 2.9).

In addition to the intrinsic security of each security realm, the data exchanged between these entities has to be protected. Any communication between two security realms of the eUICC ecosystem SHALL be origin authenticated, as well as integrity-Protected and, unless otherwise specified in detailed sections of this specification, confidentiality protected.

For all the procedures described in this specification the security realms are mutually authenticated and they have negotiated a minimal-acceptable common cryptographic suite for further communication.

For the eUICC interfaces, the Platform Management commands (ES5) and the OTA Platform commands (ES6) SHALL be protected by either a SCP80 or SCP81 secure channel with security level defined in section 2.4. The Profile Management commands (ES8) SHALL be at least protected by a SCP03 security level as detailed in section 2.5.

Off-card entities SHALL implement access control mechanisms for all function execution and data access requests. This access SHALL be authorised and any access SHALL be traced as defined in the GSMA certification schemes.

2.3.1 Certificate Issuer Role

The Certificate Issuer (CI) Role issues the certificates for the eUICC Remote Provisioning System and acts as a trusted third party for the purpose of mutual authentication of the entities of the system. The CI provides:

- A self-signed Root Certificate used to verify certificates issued and signed by the CI
- A public key (PK.CI.ECDSA), part of that Root Certificate, used on the eUICC to verify certificates issued by the CI
- A certificate (CERT.DP.ECDSA, signed by the CI) to authenticate the SM-DP. This certificate is used in the “Load and Install Profile” procedure
- A certificate (CERT.SR.ECDSA, signed by the CI) to authenticate the SM-SR. This certificate is used in the “SM-SR change” procedure
- A certificate, signed by the CI, to authenticate the EUM. This certificate is used in the "Download and Install Profile" and in the “SM-SR change” procedures.
- A Certificate Revocation List (CRL), issued periodically or on event, as specified in the GSMA eUICC PKI Certificate Policy SGP.14 [56]. This CRL lists identifiers of the certificates issued by the CI that have been revoked before their expiration date.

2.3.2 Certification Chains

The Certificate Issuer Role issues certificates for Embedded UICC remote provisioning system entities and acts as a trusted root for the purpose of authentication of the entities of the system.

The following certificates SHALL be signed and issued by the CI, according to the policies specified in SGP.14 [56]:

- Self-signed Root Certificate
- EUM Certificates
- SM-SR Certificates
- SM-DP Certificates

The EUM, SM-SR, and SM-DP certificates, SHALL be requested to the CI, following the procedures, and using the CSR formats, defined in SGP.14 [56].

The Self-signed Root certificate, and the EUM certificates, SHALL follow the format specified by SGP.14 [56], based on X.509, including in particular extensions SubjectAltName and SubjectKeyIdentifier.

The SM-SR, SM-DP, and eUICC certificates, SHALL follow the format specified by this document, in sections 4.1.1 and 4.1.3, based on Global Platform Amendment E [11]

The following certificates SHALL be signed and issued by the EUM:

- eUICC Certificates

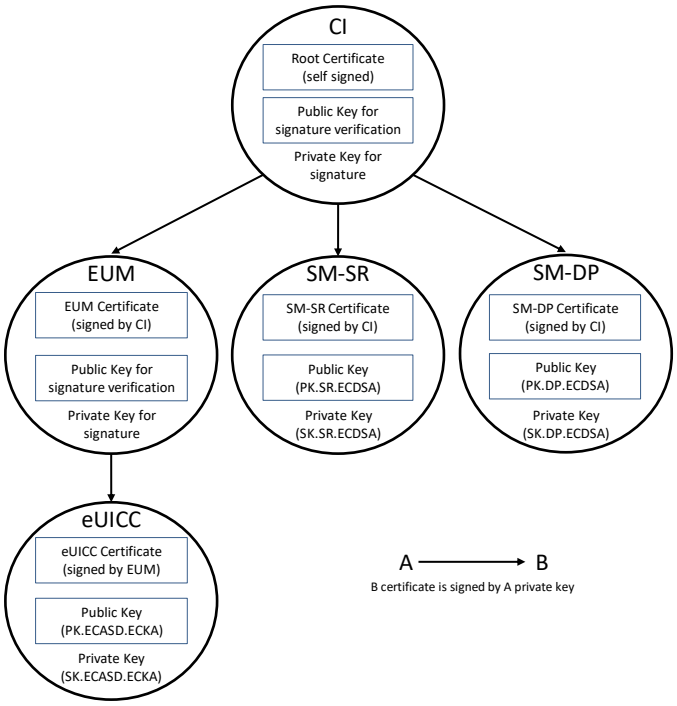


Figure 8: Certificate Chains

The certificate operational period and key pair usage period of all certificates SHALL be set to the time limits defined in SGP.14 [56] section 8.2.

2.3.2.1 Management of certificates on eUICC

The following certificates SHALL be checked by the eUICC:

- the SM-SR Certificate
- the SM-DP Certificate

The following certificate and key SHALL be stored in the eUICC:

- the eUICC Certificate
- the public key allowing to verify SM-SR and SM-DP certificates

The eUICC Certificate is part of the EIS (eUICC Information Set) which is stored in the SM-SR and/or at EUM level. This certificate contains:

- The PK.ECASD.ECKA used for ElGamal Elliptic Curves key agreement as defined in GlobalPlatform Card Specification Amendment E [11]
- The EID
- The technical reference of the product, which allows the Common Criteria (CC) certification report to be identified by Common Criteria certification body (for example BSI, ANSSI).

2.3.2.2 Identification of parent certificates

It is recognized that the CA-ID field (tag 42) in a GlobalPlatform certificate is usually filled with the identifier of the organization that issues the certificate. In case this organization has

more than one key pair that can be used to sign issued certificates, this tag alone is not sufficient to distinguish which parent key pair was used.

In the context of this specification, an additional identifier of the parent key pair SHALL therefore be provided in the parent certificate as an extension SubjectKeyIdentifier, (as described in RFC 5280 [57]).

This identifier SHALL be referenced in the child certificates as an extension Authority Key Identifier (as described in RFC 5280 [57]) in the EUM certificate, or as a tag C9 Authority Key Identifier within the discretionary data field (tag 73) for eUICC, SM-SR, and SM-DP certificates.

When the Authority Key Identifier extension or tag is present, its value SHALL match the value of the Subject Key Identifier extension of the parent certificate.

2.3.2.3 Certificate revocation management

The EUM Certificate, SM-DP Certificate, and SM-SR Certificate, can be revoked by the CI for a number of reasons, described in SGP.14 [56], and following procedures described in the same document for the triggering and evaluation of the revocation request, and for the information of relying parties after revocation.

The Operator SHOULD consider the revocation status of the EUM Certificate before downloading their Profile on an eUICC whose EIS and ECASD Certificate was signed by the EUM private key.

The Operator SHOULD consider the revocation status of the Certificate of the SM-DP and SM-SR which manage the Operator's Profiles.

NOTE: This can be achieved by retrieving regularly the most up-to-date CRL issued by the CI, and check if any Certificate of their EUM, SM-DP SM-SR supplier is listed. From this point the Operator can inspect the reason for revocation.

As a general recommendation, the Operator SHOULD NOT download a Profile on an eUICC whose EUM Certificate was revoked. And the Operator SHOULD avoid to manage its Profiles via an SM-DP or an SM-SR whose certificate has been revoked.

However, based on the revocation information, the Operator can make an informed decision as to whether it can continue to rely on the eUICC, SM-SR, SM-DP, at the Operator's own risk, as stipulated in SGP.14 [56]. The SM-DP and SM-SR SHALL obey the Operator's informed decision:

- When an Operator requests the SM-DP to download a Profile on an eUICC, the SM-DP SHALL NOT refuse to download the Profile for the sole reason that the EUM certificate has been revoked.
- When an Operator requests a Profile Management or Platform Management operation, the SM-DP SHALL NOT refuse to perform the operation for the sole reason that the SM-SR Certificate has been revoked.
- When receiving an EIS via ES1 or ES7, the SM-SR SHALL NOT refuse to register the eUICC for the sole reason that the EUM Certificate has been revoked.
- When an Operator requests a Profile Management or Platform Management operation, the SM-SR SHALL NOT refuse to perform the operation for the sole reason that the EUM Certificate has been revoked.

- When an M2M SP requests a Profile Lifecycle Management operation, the SM-SR SHALL NOT refuse to perform the operation for the sole reason that the EUM Certificate has been revoked.
- When an Operator requests a Profile Management or Platform Management operation via the SM-DP, the SM-SR SHALL NOT refuse to perform the operation for the sole reason that the EUM Certificate has been revoked.
- When transferring an eUICC to another SM-SR2 via SM-SR Change, the SM-SR1 SHALL NOT refuse to perform the operation for the sole reason that the SM-SR2 Certificate has been revoked.

NOTE The above ensures that the eUICC doesn't need to manage the revocation status of the SM-DP certificate or the SM-SR certificate that it receives.

2.3.2.4 EID impact on certificate verification

Due to the introduction of a second EID format (see section 2.2.2), special care is required when verifying certificates which make use of this format.

The SM-DP and SM-SR SHALL accept all EID formats defined in SGP.29 [73].

The SM-DP and SM-SR SHOULD verify the consistency of the IINs/EINs and EID as restricted in the EUM and eUICC Certificates, with the following considerations on SGP.29 [73].

- EIDs issued according to the EIN-based format do not have an 8-digit IIN. Instead, they have a variable-length EIN. Therefore:
  - If the EIN is 8 digits long, then the Name Constraint exactly matches the EIN.
  - If the EIN is longer than 8 digits, then the Name Constraint does not fully specify the EIN. In this case, the SM-DP and SM-SR SHOULD consider that the Name Constraint cannot fully ensure that EUMs assign values only within their ranges.
  - If the EIN is shorter than 8 digits, then the Name Constraint also includes the first few digits of the EUM Specific Identification Number (ESIN). This effectively reduces the number of digits available in the ESIN. The EUM SHOULD take care that these digits are assigned the same values in all EIDs.

2.3.3 General Consideration on Algorithm and Key Length

Following the recommendations of several security agencies (for example NIST: SP 800-57 Part 1: Recommendation for Key Management [36], which was last revised in 2012; BSI: TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen [37], which was updated in 2013. For an overview see also http://www.keylength.com/en/2/), the following table provides an overview of the key lengths and hashing methods that SHALL be applied in the context of this specification to ensure a good level of security up to the horizon 2030:

Algorithm	Minimum Key Length
Symmetric (AES)	128 bits, block size of 128 bits
Asymmetric (RSA)	3072 bits
Elliptic curve	256 bits

Hashing for Digital signatures and hash-only applications	SHA-256
Hashing for HMAC, Key Derivation Functions and Random Number Generation	SHA-256

Table 3: Algorithm and Key Length

2.4 OTA Communication on ES5 (SM-SR-eUICC)

2.4.1 General OTA Requirements

In the eUICC Remote Provisioning and Management system the OTA communication is exclusively handled by the SM-SR. The SM-SR can use SMS, CAT_TP and HTTPS for remote OTA communication with the eUICC.

- The eUICC SHALL support SMS and either CAT_TP or HTTPS or both.
- Device requirements are stated in Annex G.
- The SM-SR SHALL support SMS, HTTPS and CAT_TP.
- In HTTPS case, the SM-SR and eUICC MAY support DNS resolution to resolve the IP address of the SM-SR
- For LTE network deployments the system SHALL support SMS as defined in GSMA PRD IR.92 [38].
- The SM-SR is free to select the most relevant protocol according to the eUICC and Device capabilities and the platform or Profile Management operation to execute.
- The eUICC SHALL support the RAM and RFM as defined in ETSI TS 102 226 [5], in particular Expanded Remote Application data format and Script Chaining.

2.4.2 Void

2.4.3 SMS

The usage of the SMS protocol may be relevant in several situations:

- SMS for HTTPS session triggering, as defined in ETSI TS 102 226 [5], and also in OMA-Smart Card Web Server [14] (section “Remote Administration Request sent using a MT-SMS”)
- SMS for CAT_TP session triggering as defined in ETSI TS 102 226 [5].
- When a command to be sent to the eUICC can fit into a few SMS; such a solution can be more efficiently handled via SMS, as compared to HTTPS.

The eUICC SHALL support the sending of secure packet over SMS as defined in 3GPP TS 31.115 [13]

The eUICC SHALL support RAM over SMS as defined in ETSI TS 102 226 [5].

The eUICC SHALL comply with 3GPP TS 31.111 [27] and 3GPP TS 31.116 [28].

Except for the notification described in section 3.15.1, concerning the security level, the SMS (MT or MO) SHALL make use of a CC with a length of 64 bits using AES CMAC mode, ciphering using AES in CBC mode and counter value higher (SPI1=’16’). Minimum key lengths are defined in section 2.3.3.

- Procedures for the PoR SHALL follow ETSI TS 102 225 [4] and 3GPP TS 31.115 [13] with the following precisions: in the case that an incoming SMS for the ISD-R does not meet this security level, it must be rejected by the eUICC and no PoR SHALL be sent back
- When the eUICC cannot authenticate the SM-SR, it SHALL NOT send any PoR and discard the command packet with no further action being taken.

SPI2 SHALL be set to:

- '00': no PoR (this value SHALL only be used for the notification described in section 3.15.1 and optionally for the SMS for HTTPS session triggering described in section 2.4.3.1),
- or to '39': PoR with CC and encryption.

When a PoR is returned, the SMS SHALL make use of a CC with a length of 64 bits using AES CMAC mode , ciphering using AES in CBC mode and SHALL be sent using SMS-SUBMIT mode. Minimum key lengths are defined in section 2.3.3.

The SM-SR SHALL verify that the counter value of the PoR is the same as the counter value sent in the command packet.

All these security requirements SHALL apply also for the SCP80 secured packets exchanged during a CAT_TP session.

2.4.3.1 SMS for HTTPS Session Triggering

The SM-SR SHALL make use of a special SMS for triggering the opening of an HTTPS session to the eUICC.

This SMS SHALL be addressed to the ISD-R. The necessary TAR information SHALL be included in the EIS. The SMS SHALL comply with the format described in GlobalPlatform Card Specification Amendment B [8], section "Administration session triggering parameters".

The SM-SR MAY choose to request a PoR or not for this special SMS, and set the SPI2 byte of the SMS accordingly.

NOTE: Normally the SM-SR will close the session. However, if needed, the eUICC MAY close the session.

2.4.3.2 SMS for CAT_TP Session Triggering

The SM-SR SHALL make use of a special SMS for triggering the opening of a CAT_TP session to the eUICC.

This SMS SHALL be addressed to the ISD-R. The necessary TAR information SHALL be included in the EIS. The SMS SHALL comply with the format described in:

- ETSI TS 102 226 [5], using the parameter "Request for BIP channel opening" and "Request for CAT_TP link establish". These parameters and the corresponding "Data for BIP channel opening" and "Data for CAT_TP link establishment" are separated in two different commands sent in the same push SMS.

NOTE: Normally the SM-SR will close the session. However, if needed, the eUICC MAY close the session.

2.4.3.3 Command Format in SMS

The commands sent to the eUICC within a secure script in SMS SHALL be formatted as an expanded remote command structure as defined in ETSI TS 102 226 [5]. As a consequence, the eUICC SHALL provide the answer as an expanded remote response structure.

2.4.4 HTTPS

If HTTPS is used, the following sections SHALL apply.

2.4.4.1 PSK-TLS

2.4.4.1.1 Cipher Suites

The eUICC SHALL support the Transport Layer Security (TLS) protocol v1.2 [15] and SHALL support at least one of the following Pre-Shared Key Cipher suites as defined in RFC 5487 [17]:

- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_CBC_SHA256

The Pre-Shared Keys SHALL have an entropy of at least 128 bits.

The eUICC ISD-R SHALL be configured with ‘i’ = ‘04’ to indicate only TLS 1.2 supported as defined in GlobalPlatform Amd B [8].
The SM-SR SHALL select a cipher suite of the same or higher security compared to the two listed above.

2.4.4.1.2 PSK-ID Value for TLS Handshake

The PSK-ID specified in this section defines a format suited for PSK random keys. However, a SM-SR MAY use a dedicated PSK-ID format in particular to be able to manage PSK derived from master key. In this case the derivation algorithm used SHALL be robust and follow the NIST recommendation SP800-56C [55], the derived Pre-Shared Keys SHALL have an entropy of at least 128 bits.

As specified in RFC 4279 [16], the PSK Identity SHALL be first converted to a character string, and then sent encoded in octets using UTF-8 [18] by the eUICC.

In the context of this specification, the PSK Identity before conversion is a sequence of Tag/Length/Value (TLV) objects in hexadecimal string representation.

NOTE: As the PSK Identity is expected to be as short as possible, all lengths are coded in one byte. BER-TLV coding is unnecessary in this case.

Description	Length (bytes)	Value
Tag for identifying PSK-ID format	1	‘80’
Length	1	‘01’

Identification of the PSK-ID format.	1	Expected value is ‘02’ indicating a full qualified format for random PSK.
Tag for indicator of EID	1	‘81’
Length of EID	1	‘10’
EID value	16	The EID value. The value SHALL be coded in hexadecimal string representation.
Tag for security domain AID	1	‘4F’
Length of security domain AID	1	‘10’
Security domain AID value	16	The AID value of the ISD-R. The value SHALL be coded in hexadecimal string representation.
Tag for key identifier	1	‘82’
Length	1	‘01’
Key identifier	1	The key identifier value. The value SHALL be coded in hexadecimal representation.
Tag for Key version	1	‘83’
Length	1	‘01’
Key version	1	The key version value. The value SHALL be coded in hexadecimal representation. Key version number range reserved for SCP81 is '40' to '4F'.

Table 4: PSK-ID Format

Example of PSK-ID before conversion to an UTF-8 string:

‘80010281100102030405060708090102030405060 74F10000102030405060708090A0B0C0D0E0F820101830140’

2.4.4.1.3 Other restrictions on TLS session management

In addition to restrictions to the TLS protocol specified in GP Amendment B [8], the ISD-R and SM-SR SHALL NOT support TLS Session resumption (RFC 4507 or RFC 5077) nor several parallel TLS sessions.

2.4.4.2 HTTP POST Request of ISD-R

The POST request is used by the ISD-R to fetch remote APDU strings and to transmit response strings. The ISD-R SHALL strictly follow GlobalPlatform Card Specification Amendment B [8] for the format of the POST request. The content of the HTTP POST header field X-Admin-From SHALL be filled with the “Agent Id” information standardised in GlobalPlatform Card Specification Amendment B [8], section “Administration Session Triggering Parameters” (the format of this field is not standardised).

“Agent Id” information SHALL include two parts:

- the eUICC identifier (EID)
- the identifier of the Security Domain representing the Admin Agent function

Each part is built using the following format:

```
//<part-id>/<part-id-type>/<part-id-value>
```

Where:

- `<part-id>` is the tag that specifies which part is defined: “se-id” or “aa-id”
- `<part-id-type>` specifies the type of the identifier that is provided: “eid” or “aid”
- `<part-id-value>` provides the identifier value itself.

Format of the “X-Admin-From” field:

```
//se-id/eid/<EID>;//aa-id/aid/<RID ISD-R AID>/<PIX ISD-R AID>
```

Note that this representation of AID in the format /aid/<RID>/<PIX> is already used in GlobalPlatform for other purposes than the “Agent Id”.

Example of Agent Id field:

“//se-id/eid/89001012012341234012345678901224;//aa-id/aid/A000000559/1010FFFF8900000100”
The eUICC SHALL use the Chunked mode [Transfer-Encoding: chunked CRLF] for the POST request message.

The SM-SR SHALL use Chunked mode [Transfer-Encoding: chunked CRLF] for the POST response.

First request sent by the ISD-R:

POST <initial uri> **HTTP/1.1** CRLF

Host: <SM-SR ip> CRLF

X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF

X-Admin-From://se-id/eid/<value>;//aa-id/aid/ <RID ISDR-AID >/<PIX ISDR-AID> CRLF

CRLF

Return of a command response (no error case) sent by the ISD-R:

POST <uri contained in the previous POST response> **HTTP/1.1** CRLF

Host: <SM-SR ip> CRLF

X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF

X-Admin-From://se-id/eid/<value>;//aa-id/aid/ <RID ISDR-AID value>/<PIX ISDR-AID> CRLF

Content-Type: application/vnd.globalplatform.card-content-mgt-response;version=1.0 CRLF

Transfer-Encoding: chunked CRLF

X-Admin-Script-Status: ok CRLF

CRLF

[response-string]

2.4.4.3 HTTP POST Response of SM-SR

The POST response is used by the SM-SR to transmit the next remote APDU format string to the ISD-R and possibly to provide the next URI that must be used to request the following admin command.

The POST response SHALL strictly follow the GlobalPlatform Card Specification Amendment B [8].

POST response sent by the SM-SR containing commands that SHALL be executed by the ISD-R:

HTTP/1.1 200 CRLF

X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF

Content-Type : application/vnd.globalplatform.card-content-mgt;version=1.0 CRLF

X-Admin-Next-URI: <uri of the next POST> CRLF

CRLF

[Command script]

POST response sent by the SM-SR containing commands that SHALL be executed by the ISD-P:

HTTP/1.1 200 CRLF

X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF

Content-Type : application/vnd.globalplatform.card-content-mgt;version=1.0 CRLF

X-Admin-Next-URI: <uri of the next POST> CRLF

X-Admin-Targeted-Application://aid/<rid>/<pix> (of the ISD-P-AID) CRLF

CRLF

[Command script]

Intermediate POST response sent by the SM-SR containing no command to execute but instructing to not close the HTTP session: the eUICC SHALL accordingly send a POST on the next URI provided, with no response body.

HTTP/1.1 204 CRLF

X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF

X-Admin-Next-URI: <uri of the next POST> CRLF

CRLF

Last POST response sent by the SM-SR with nothing to do, communication SHALL be closed:

HTTP/1.1 204 CRLF
X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF
CRLF

2.4.4.4 Command Format in HTTP Message

The commands sent to the eUICC within a secure script in HTTP messages SHALL be formatted in an expanded remote command structure with indefinite length coding as defined in ETSI TS 102 226 [5]. As a consequence, the eUICC will provide the answer as an expanded remote response structure with indefinite length coding.

2.4.4.5 Sequence for HTTPS Session Triggering

Except if specified differently for a specific procedure, an HTTPS session with the eUICC is always triggered by the SM-SR by sending a MT-SMS as defined in section 2.4.3.1.

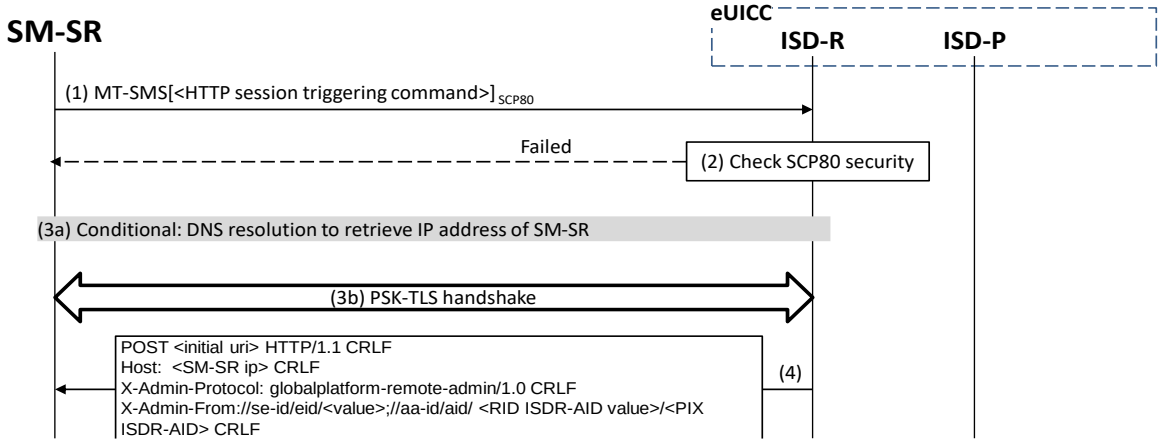


Figure 9: Sequence for HTTPS Session Triggering

(1) The SM-SR sends a MT-SMS to the ISD-R for HTTPS session triggering as defined in section 2.4.3.1.

(2) The ISD-R checks the security of the MT-SMS. The figure assumes the security is ok as defined in [13], otherwise section 2.4.3.1 applies.

(3) Opening of TLS socket

a) If supported and if correctly configured by SM-SR and eUICC, the ISD-R MAY request a DNS resolution to retrieve the IP Address of the SM-SR. See section 2.4.5

b) The PSK-TLS handshake is performed as defined in [16] and [17]. The figure assumes the security is ok. In case of a temporary or fixable error, the SM-SR SHALL retry or fix the error.

(4) The first POST request is sent to the SM-SR as defined in section 2.4.4.2.

Then the SM-SR can continue with the procedure to execute.

2.4.5 DNS Resolution

DNS resolution is an optional feature that is triggered only when:

- The eUICC includes a DNS resolver Client configured to initiate the DNS queries to server
- The SM-SR relies upon a DNS Resolver Server able to provide the IP address associated to the domain name sent by the client query.
- The eUICC determines that it has to resolve the IP address of the SM-SR server

2.4.5.1 Criteria to determine whether DNS resolution is needed

If:

- the eUICC is requested to open an HTTPS session and
- the eUICC supports DNS resolution and
- the ISD-R has no IP address configured in the Connection Parameters of its Administration Session Triggering Parameters nor in the Administration Session Triggering SMS that may have triggered the session (as defined by Global Platform Amendment B [8]) and
- the ISD-R has a FQDN, and IP addresses of DNS servers, configured in DNS parameters as defined in section 4.1.1.10 and
- the ISD-R has not already resolved the FQDN to an IP address, or has resolved it but has reasons to consider the resolved value is stale

then the eUICC SHALL perform a DNS resolution as described in the procedure 2.4.5.3 to retrieve the IP address(es) of the SM-SR server.

The eUICC MAY also support other heuristics to determine that DNS resolution is needed and to which DNS servers to send the DNS queries. For example it MAY obtain the IP addresses of DNS servers from the device as specified in ETSI TS 102 223 release 12.

2.4.5.2 DNS protocol features

The DNS resolver of SM-SR and eUICC SHALL:

- Be compliant to RFC 1035 and RFC 3596 defining the Domain Name System and protocol
- Support Query type A (IPv4) and AAAA (IPv6)
- Use UDP protocol
- Support only Recursive mode: the DNS resolver Server SHALL recursively resolve the given FQDN query, meaning that the answer SHALL contain all the available IP addresses
- Send short responses: any response returned by DNS Server must fit in one UDP packet

2.4.5.3 Procedure flow for DNS resolution

The sequence flow in the Figure 10 describes the basic exchange for DNS resolution

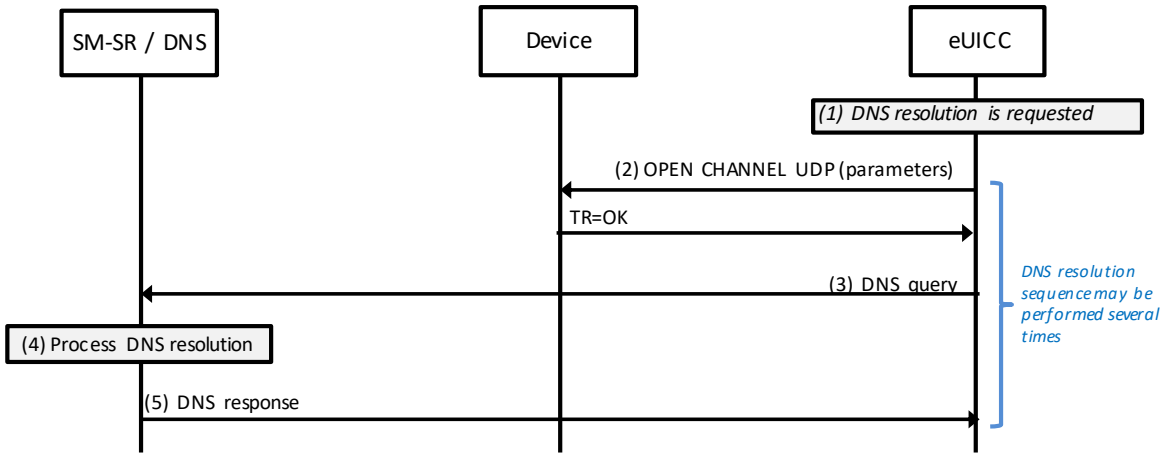


Figure 10: Sequence for Basic DNS resolution

(1) The eUICC determines that DNS resolution of SM-SR IP address is needed (as per section 2.4.5.1)

(2) if the device supports providing DNS IP addresses, the eUICC MAY obtain one or more IP addresses from the device; otherwise the eUICC SHALL use the IP addresses configured in the DNS parameters of the ISD-R's SMSR addressing parameters (as defined in section 4.1.1.10)
The eUICC opens an UDP channel to the DNS server

(3) The eUICC sends the DNS Query to the DNS Resolver Server

(4) The DNS Resolver Server of SM-SR processes this query, and retrieves the IP address(es) of the SM-SR server

(5) The DNS Resolver Server of the SM-SR send the DNS response including all the resolved IP addresses of the SM-SR server

NOTE: The eUICC MAY implement proprietary mechanisms to leverage more than one IP addresses of DNS server, and more than one IP addresses of SM-SR server, such as retry procedures, load balancing procedures. The technical solution of these mechanisms is out of scope.

2.5 Communication on ES8 (SM-DP - eUICC)

The ES8 interface is between the SM-DP and its ISD-P and goes through the SM-SR.

The ES8 is realised by a SCP03 or SCP03t secure channel that is tunnelled through the secure channel between the SM-DP and the SM-SR (ES3) and on through into the SCP80 or SCP81 secure channel between the SM-SR and the ISD-R (ES5). It is then provided by the ISD-R to the ISD-P. This is shown in the Figure 6.

The eUICC SHALL support the Secure Channel Protocol 03 (SCP03) as defined in GlobalPlatform Card Specification Amendment D [10], as well as the variant SCP03t defined in this specification (see section 4.1.3.3), with:

- AES in CBC mode with key length of 128 bits, referred as AES-128
- Use of C-MAC, C-DECRYPTION R-MAC and R-ENCRYPTION for SCP03 (set in reference control parameter P1 of the EXTERNAL AUTHENTICATE command) and for SCP03t.

- Use of mode i='70', meaning use of pseudo-random card challenge, R-MAC and R-ENCRYPTION support

As a result the SM-DP and its ISD-P are mutually authenticated, all commands sent from the SM-DP to the ISD-P are signed and encrypted, and all responses sent by the ISD-P to the SM-DP are also signed and encrypted.

2.6 **SM-DP to SM-SR** Link Establishment (ES3)

The link between the SM-DP and the SM-SR (ES3) may have to be established during a procedure. For the "Profile Download and Installation" procedure, the Operator may ask to the SM-DP to contact an SM-SR that may be unknown to the SM-DP. The SM-DP will have to establish a connection with this new SM-SR.

It is assumed in this specification that:

- The Operator, requesting an action of an SM-DP through the ES2 interface, is able to provide the identification of the SM-SR in charge of the management of the eUICC targeted by the function.
- The SM-DP, based on the SM-SR identification provided through the ES2 interface, is able to retrieve the SM-SR address.
- The SM-DP, based on the SM-SR identification and address, is able to establish a new link to the identified SM-SR during any procedure requiring this step.

The procedure describing how the SM-DP establishes a link to the SM-SR (for example: business agreement or technical solution) is not covered by this specification.

2.7 OTA Platform Communication on ES6 (Operator-eUICC)

The ES6 is the interface between the Operator OTA Platform and a Profile inside an eUICC (see also section 2.2.5.3) through a secure channel as defined in ETSI TS 102 225 [4] and ETSI TS 102 226 [5]. This interface is the same as the one used with UICCs.

This specification recommends that OTA Platform communication on ES6 makes use of at least a minimum security settings defined for ES5 in section 2.4.

2.8 Communication on ES1 (EUM - SM-SR)

ES1 is the interface between the EUM and the first SM-SR that will manage the eUICC, to send to the SM-SR the EIS describing the eUICC or to update the EIS. The EIS contains the ISD-R keysets that SM-SR will use to secure the ES5 communication as described in section 2.4. Those keysets SHALL be protected by a mechanism agreed by the two parties. The agreement SHALL cover at least the following features. The default value specified SHALL be supported to ensure that an agreement can be reached:

- Ciphering algorithm: AES
- Size of the transport key: at least the size of the transported keys (keys in the keysets being themselves at least as per section 2.3.3)

- Padding: no padding if the length of the key being ciphered is already aligned with the AES block size, otherwise PKCS#7
- Cipher mode: CBC mode, with an initialization vector of '00…00'.

2.9 Compliance

The elements of the ecosystem (SM-DP, SM-SR and eUICC) SHALL be certified according to section 5 of the GSMA Remote Provisioning Architecture for Embedded UICC [1]. SM-SR, SM-DP and eUICC SHALL be compliant with SGP.16 [64].

3 Detailed Procedure Specifications

This section contains the detailed specifications of the procedures that realise the Remote Provisioning and Management system for the eUICC.

The order of sending or reception of the responses of the functions and notifications defined across this procedures section MAY differ from it in the real implementations.

3.1 Profile Download and Installation

The Profile Download and Installation procedure is sub-divided into four main steps:

1. ISD-P creation on the eUICC
2. Personalization of the ISD-P with a first key set, called the key establishment procedure
3. Download and installation of the Profile onto the eUICC
4. Optional: Enabling of the newly installed Profile.

Optionally the SM-SR MAY send a command ES5.UpdateSMSRAddressingParameters to update the list of TP-DestinationAddress and define a specific TP-DA for this newly loaded Profile. The command can be sent anytime after step 1 (ISD-P creation) but before step 4 (enabling of the Profile).

3.1.1 ISD-P Creation

The next figure describes the call flow for the first step which is the ISD-P creation. The procedure illustrates the usage of RAM over HTTP as an example of the transport protocol, assuming that the sequence will be followed by a key establishment procedure and the full download of the Profile.

NOTE: CAT_TP could be used as transport protocol and would have an equivalent procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 160
hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
endbox

OP->>DP: (1) downloadProfile(srid, eid, iccid, final state, profileType)
DP->SR: (2) getEIS(eid)

Rnote over SR #FFFFF
(3) Retrieve EIS
Endrnote

SR-->DP: Failed
DP-->>OP:

SR-->DP: (4) Return EIS

Rnote over DP #FFFFFF
(5) Check eUICC eligibility
Endrnote
DP-->>OP: Failed

DP->>SR: (6) createISDP(eid, iccid, mno-id,…)

Rnote over SR #FFFFFF
(7) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP:

Hnote over SR, ISDR #C0C0C0
HTTPS session opening
Endhnote


SR->>ISDR: (9)
note over SR, ISDR
**HTTP/1.1 200 CRLF**
Headers
CRLF
<Body with ES5.createISD-P function>
End note

ISDR->ISDP: (10) New              .

ISDR->>SR: (11)
note over SR, ISDR
**POST /<next-uri> HTTP/1.1 CRLF**
Headers
X-Admin-Script-Status: <script-status> CRLF
CRLF
<Body with ES5.createISD-P response>
End note



Rnote over SR #FFFFFF
(12) EIS update
```

```
Endrnote

SR->>DP: (13) create ISDP function response
@enduml
```

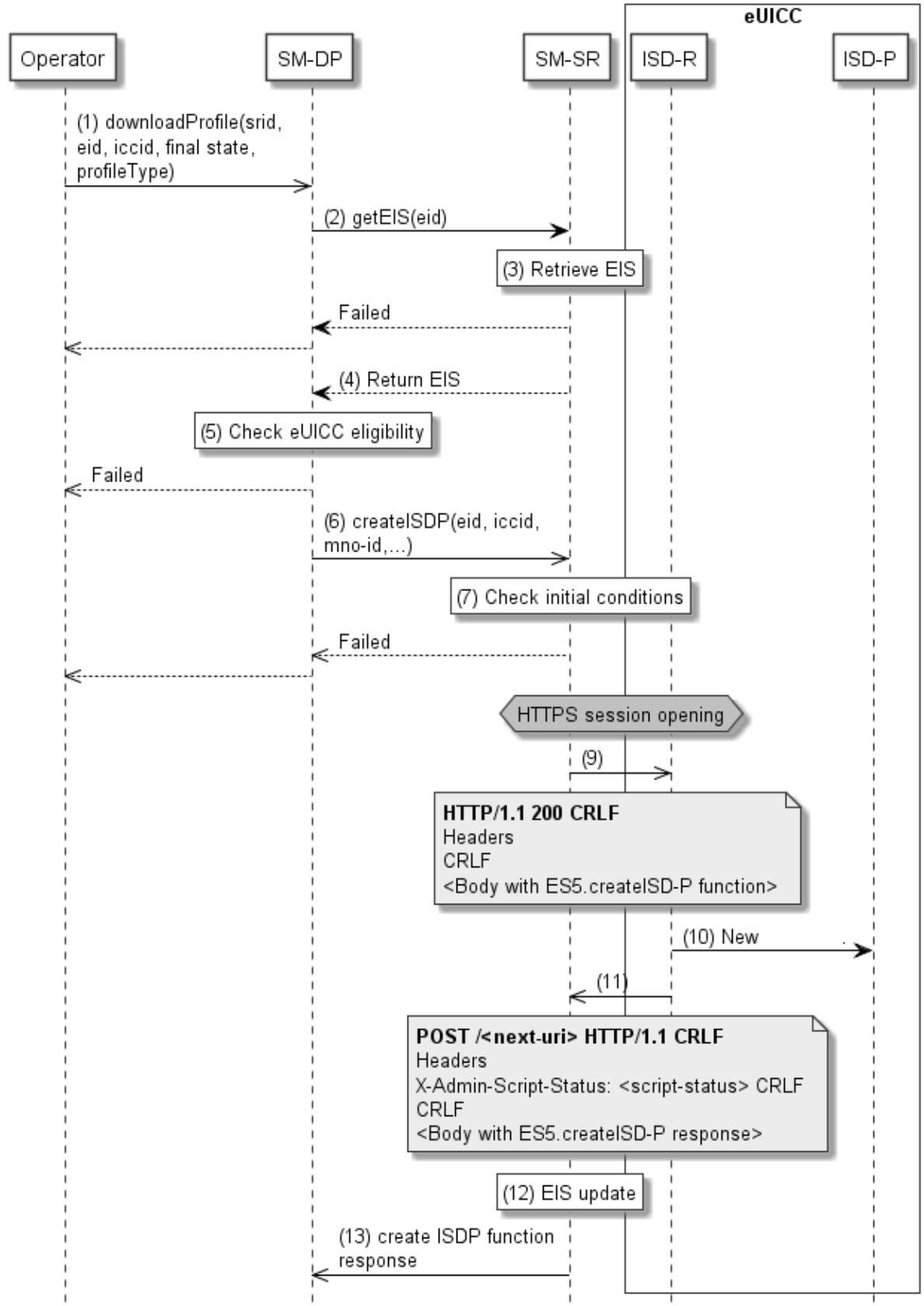


Figure 11: ISD-P creation

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Operator owning the Profile to download SHALL call the "**ES2.DownloadProfile**" function with its relevant input data (the Operator has to provide the SM-SR identification and address). By providing the required final state, the Operator MAY ask the SM-DP to enable the newly downloaded Profile at the end of the procedure. Else, by default, the Profile will be in the DISABLED state.

(2) The SM-DP on reception of this request SHALL call the "**ES3.GetEIS**" function with its relevant input data.

(3) The SM-SR SHALL retrieve the EIS of the eUICC based on the EID. At this stage the SM-SR MAY return an error indicating that the eUICC is unknown in its system. The error SHALL be finally returned to the Operator and the procedure SHALL end.

(4) The SM-SR SHALL return the EIS of the eUICC.

a. In case the EIS indicates an ISD-P in state 'Created' with the 'smdp-id' associating it to the calling SM-DP, the SM-DP SHALL delete this Profile, whether it has the same or a different ICCID, as described in section 3.1.5 before attempting to install a new Profile.

(5) The SM-DP SHALL check the eligibility of the eUICC against the characteristics of the Profile to be downloaded. Although the exact checks performed by the SM-DP are out of scope for this specification, some examples might include:

a. Is the target Profile compatible with and validated against this type of eUICC? (including the fact that the SM-DP is able to generate the Profile for this type of eUICC).

b. Is there enough memory? In case of uncertainty of the information contained within the EIS, the SM-DP could request an online audit.

c. Is the eUICC certified? In case of a non-certified eUICC, the SM-DP MAY stop the procedure.

d. If the Profile Owner has disallowed Profile download to Field-Test eUICCs: if the target eUICC indicates it's a Field-Test eUICC, the SM-DP SHALL stop the procedure.

The SM-DP SHALL verify the ECASD certificate, which was received as part of the EIS, using the EUM Certificate and the CI's Root Certificate and SHALL extract PK.ECASD.ECKA from the ECASD certificate.

If any of these conditions is not satisfied or if the certificate verification fails, the SM-DP SHALL return a response indicating a failure.

(6) The SM-DP SHALL call the "**ES3.CreateISDP**" function with its relevant input data.

(7) The SM-SR SHALL verify that the SM-DP request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.4.3).

If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating a failure, and the procedure SHALL stop.

Otherwise the SM-SR, SHALL create a new Profile entry for the EIS having a state “In-Creation”. The Profile with this state SHALL NOT appear in the EIS returned on ES3.GetEIS and ES4.GetEIS

(8) If there is no existing HTTPS session with the eUICC, the SM-SR SHALL trigger the HTTPS session as defined in section 2.4.4.5.

(9) The SM-SR SHALL return the HTTP POST response containing the “**ES5.CreateISDP**” with its relevant input data. The X-Admin-Targeted-Application parameter SHALL be omitted as the command is targeting the ISD-R.

(10) The ISD-R SHALL create the ISD-P. In case of an error, the ISD-R SHALL return the error within the next POST request to the SM-SR. The SM-SR SHALL delete the new Profile entry having the state “In-Creation“ from the EIS. The error SHALL be finally returned to the SM-DP and the procedure MAY end depending on the error.

(11) The eUICC SHALL return the “**ES5.CreateISDP**” function execution response within the POST request to the SM-SR.

(12) Assuming a successful ISD-P creation, the SM-SR SHALL update the state of the Profile in the EIS to “Created“.

(13) The SM-SR SHALL return to the SM-DP the “**ES3.CreateISDP**” function execution response.

(13a) In case the SM-SR does not receive a function execution response from the eUICC (e.g. due to a disrupted connection), the SM-SR SHALL trigger ES5.DeleteISDP function on the targeted ISD-P and update the EIS by removing the new Profile entry with status "In Creation" from the EIS accordingly.

In this sample procedure, it is assumed that the SM-DP has indicated “more to do” in the “ES5.CreateISDP” call. In case the SM-DP did not indicate “more to do”, the SM-SR MAY end the HTTPS session.

3.1.2 Key Establishment with Scenario#3-Mutual Authentication

The next figure describes the second step in the Profile Download and Installation procedure.

This sequence defines a new scenario called “Scenario#3-Mutual Authentication”. This sequence uses Scenario#3 based on ECKA EG (ElGamal) scheme as defined in GlobalPlatform Card Specification Amendment E [11] complemented by an SM-DP authentication step.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 160


hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
participant ECASD #FFFFFF
endbox

DP->>SR: (1) sendData(eid, sd-aid, ES8.EstablishISDPKeySet(CERT.DP.ECDSA))
Rnote over SR
(2) Check initial
 conditions
End rnote

SR-->>DP: Failed
DP-->>OP:

Hnote over SR, ISDR #C0C0C0
(2a) Conditional:
 HTTPS Session opening
Endhnote


SR->>ISDR: (3)
note over SR, ISDR
**HTTP/1.1 200 CRLF**
…
CRLF
<Body with ES8.EstablishISDPKeySet(CERT.DP.ECDSA)>
End note

ISDR->ISDP: (3a) CERT.DP.ECDSA

rnote over ISDP
(3b) Verifies that it is
 an SM-DP certificate
End rnote

ISDP->ECASD: (4) CERT.DP.ECDSA

Rnote over ECASD
5) verifies CERT.DP.ECDSA
 using PK.CI.ECDSA.
Continue if successful:
- extracts PK.DP.ECDSA
 from CERT.DP.ECDSA.
- generates RC
End rnote
ECASD-->ISDP:(6) RC or error
ISDP-->ISDR: (7)

ISDR->>SR:
note over SR, ISDR
**POST /<next-uri> HTTP/1.1 CRLF**
…
**X-Admin-Script-Status:** <script-status> CRLF
CRLF
<Body with ES8.EstablishISDPKeySet response: RC or error>
```

```
End note

SR->>DP:(8) sendData response with ES8.EstablishISDPKeySet response: RC or error

Hnote over OP, ISDP #C0C0C0
(8a) Conditional: Error manageent, see 3.1.4
Endhnote

rnote right of OP
(9) Generates (eSK.DP.ECKA, ePK.DP.ECKA)
 Signs RC and ePK.DP.ECKA with SK.DP.ECDSA
End rnote

DP->>SR: (10) sendData( eid, sd-aid, ES8.keyEstablishISDPKeySet(ePK.DP.ECKA,
signature))
SR->>ISDR: (11)
Note over SR
**HTTP/1.1 200 CRLF**
 …
CRLF
 <Body with ES8.EstablishISDPKeySet(ePK.DP.ECKA, RC, signature)>
End note

ISDR->ISDP:(12) ePK.DP.ECKA, signature
ISDP->ECASD
rnote over ECASD
13) verifies signature
 using PK.DP.ECDSA.
Continue if successful:
 - calculates ShS from
 ePK.DP.ECKA and
 SK.ECASD.ECKA.
End rnote

ECASD-->ISDP: (14) ShS or error

rnote over ISDP
(15) (Opt.) Generates DR
 Derives keyset from ShS (and DR)
 Calculates receipt.
End rnote

ISDP-->ISDR: (16) Receipt (Opt. DR) or error

ISDR->>SR:(17)
Note over SR, ISDR
**POST** /<next-uri> **HTTP/1.1** CRLF
 …
**X-Admin-Script-Status:** <script-status> CRLF
CRLF
 <Body with ES8.EstablishISDPKeySet response: Receipt (Opt. DR) or error>
End note

SR->>DP:(18) sendData response with ES8.keyEstablishISDPKeySet response: Receipt
(Opt. DR) or error

hnote over OP, ISDP #C0C0C0
(18a) Conditional: Error management see 3.1.4
end hnote

rnote right of OP
(19) Calculates ShS from eSK.DP.ECKA
 and PK.ECASD.ECKA.
 Derives keyset from ShS (and DR)
 Verifies receipt
End rnote
@enduml
```

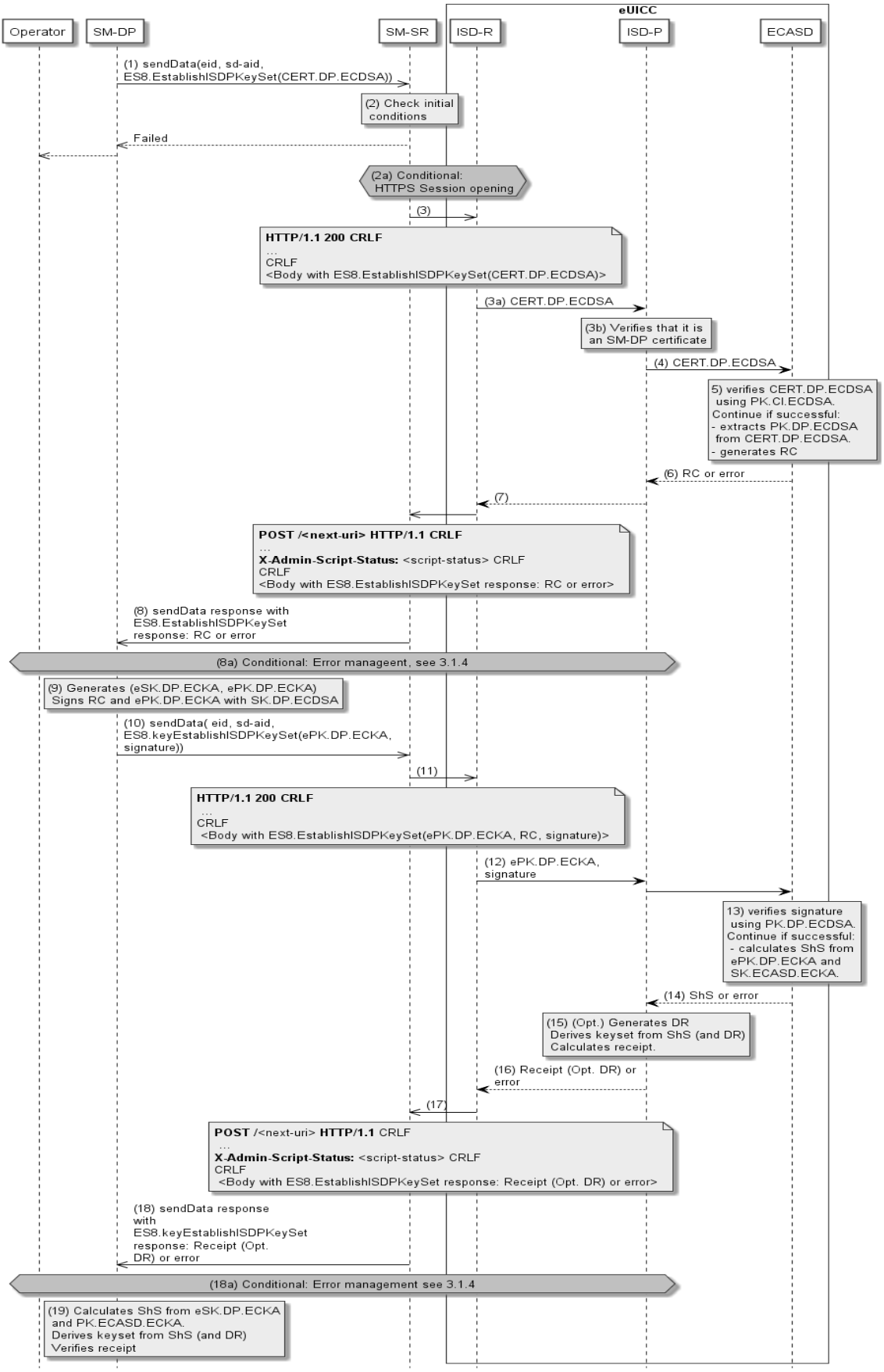

eUICC
Operator
SM-DP
SM-SR
ISD-R
ISD-P
ECASD
(1) sendData(eid, sd-aid, ES8.EstablishISDPKeySet(CERT.DP.ECDSA))
(2) Check initial conditions
Failed
(2a) Conditional: HTTPS Session opening
(3)
HTTP/1.1 200 CRLF
...
CRLF
<Body with ES8.EstablishISDPKeySet(CERT.DP.ECDSA)>
(3a) CERT.DP.ECDSA
(3b) Verifies that it is an SM-DP certificate
(4) CERT.DP.ECDSA
5) verifies CERT.DP.ECDSA using PK.CI.ECDSA. Continue if successful:
- extracts PK.DP.ECDSA from CERT.DP.ECDSA.
- generates RC
(6) RC or error
(7)
POST /<next-uri> HTTP/1.1 CRLF
...
X-Admin-Script-Status: <script-status> CRLF
CRLF
<Body with ES8.EstablishISDPKeySet response: RC or error>
(8) sendData response with ES8.EstablishISDPKeySet response: RC or error
(8a) Conditional: Error manageent, see 3.1.4
(9) Generates (eSK.DP.ECKA, ePK.DP.ECKA) Signs RC and ePK.DP.ECKA with SK.DP.ECDSA
(10) sendData(eid, sd-aid, ES8.keyEstablishISDPKeySet(ePK.DP.ECKA, signature))
(11)
HTTP/1.1 200 CRLF
...
CRLF
<Body with ES8.EstablishISDPKeySet(ePK.DP.ECKA, RC, signature)>
(12) ePK.DP.ECKA, signature
13) verifies signature using PK.DP.ECDSA. Continue if successful:
- calculates ShS from ePK.DP.ECKA and SK.ECASD.ECKA.
(14) ShS or error
(15) (Opt.) Generates DR Derives keyset from ShS (and DR) Calculates receipt.
(16) Receipt (Opt. DR) or error
(17)
POST /<next-uri> HTTP/1.1 CRLF
...
X-Admin-Script-Status: <script-status> CRLF
CRLF
<Body with ES8.EstablishISDPKeySet response: Receipt (Opt. DR) or error>
(18) sendData response with ES8.keyEstablishISDPKeySet response: Receipt (Opt. DR) or error
(18a) Conditional: Error management see 3.1.4
(19) Calculates ShS from eSK.DP.ECKA and PK.ECASD.ECKA. Derives keyset from ShS (and DR) Verifies receipt

Figure 12: Key Establishment, Scenario #3

Start Conditions:

As a pre-condition, the ISD-P SHALL be created as defined in section 3.1.1, the eUICC/ECASD SHALL support the scenario#3-Mutual Authentication and SHALL be provisioned with the SK.ECASD.ECKA, PK.CI.ECDSA.

Procedure:

(1) The SM-DP SHALL call the "**ES3.SendData**" function specifying the targeted eUICC, the ISD-R, and the data containing the "**ES8.EstablishISDPKeySet**" function with the certificate identifying the SM-DP. The certificate SHALL be issued by the SM-DP Certificate Issuer.

(2) The SM-SR SHALL verify that the SM-DP request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.4.4).

If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating a failure, and the procedure SHALL stop.

(2a) The SM-SR SHALL trigger the HTTPS session with the ISD-R if not already opened as defined in section 2.4.4.5.

(3) The SM-SR SHALL return the HTTP POST response with a body containing the "**ES8.EstablishISDPKeySet**" function as provided by the SM-DP in (1). The X-Admin-Targeted-Application parameter SHALL be omitted as the command is targeting the ISD-R

(3a) The ISD-R SHALL forward the content of the STORE DATA command contained in the HTTP response to the ISD-P.
(3b) The ISD-P SHALL verify that it is an SM-DP certificate.

(4) The ISD-P SHALL forward the CERT.DP.ECDSA to the ECASD for verification.

(5) ECASD SHALL verify the provided CERT.DP.ECDSA with the PK.CI.ECDSA; if CERT.DP.ECDSA is valid, ECASD SHALL extract and store the PK.DP.ECDSA and generate a random challenge (RC). The length of the Random Challenge SHALL 16 or 32

(6) The Random Challenge (or error if any) SHALL be returned to the ISD-P which forwards it to the ISD-R.

(7) The ISD-R SHALL return the execution response (RC or error) within a new HTTP POST request addressed to the SM-SR.

(8) The SM-SR SHALL return the content of the received HTTP POST (RC or error) to the SM-DP.

(8a) In case of failure during the key establishment procedure, error management procedure describes in section 3.1.4 SHALL be executed and the procedure SHALL stop.

(9) The SM-DP SHALL generate an ephemeral key pair (related to the targeted ICCID), called ePK.DP.ECKA and eSK.DP.ECKA. The SM-DP signs the received Random Challenge(RC) and the generated ePK.DP.ECKA with the SK.DP.ECDSA.

(10) The SM-DP SHALL call the "**ES3.SendData**" function specifying the targeted eUICC, the ISD-R and the data containing the "**ES8.EstablishISDPKeySet**" function with the

ePK.DP.ECKA and the previously computed signature on Random Challenge (RC) and ePK.DP.ECKA using SK.DP.ECDSA.

(11) The SM-SR SHALL return the HTTP POST response with a body containing the "**ES8.EstablishISDPKeySet**" function as provided by the SM-DP in (10). The X-Admin-Targeted-Application parameter SHALL be omitted as the command is targeting the ISD-R.

(12) The ISD-P SHALL forward the content of the STORE DATA command, containing the ePK.DP.ECKA and signature to the ISD-P, which SHALL forward them to the ECASD for verification.

(13) The ECASD SHALL verify the signature using the previously stored PK.DP.ECDSA. If the signature is not verified, an error SHALL be returned. Else the ECASD SHALL calculate the ShS using the ePK.DP.ECKA and the SK.ECASD.ECKA.

(14) The ShS or an error SHALL be returned to the ISD-P.

(15) The ISD-P:

- MAY optionally compute a Derivation Random (DR, if requested by the SM-DP in the function call).
- Derives the key set from ShS (and optionally DR).
- Calculates the receipt to be returned to SM-DP.
- In case of error at this step, the length of the returned receipt SHALL be 0.

(16) The ISD-P SHALL return the calculated receipt (and optionally the DR) or the error to the ISD-R.

(17) The ISD-R SHALL return the execution response to the ISD-P (receipt (opt. DR) or error) within a new HTTP POST request addressed to the SM-SR.

(18) The SM-SR SHALL return the content of the received HTTP POST (receipt (opt. DR) or error) to the SM-DP.

(18a) In case of failure during the Key Establishment procedure, the error management procedure described in section 3.1.4 SHALL be executed and the procedure SHALL stop.

(19) The SM-DP symmetrically SHALL:

- Calculate the ShS using the eSK.DP.ECKA and the PK.ECASD.ECKA,
- Derive the key set from ShS (and optionally DR), and
- Verify the receipt received in the response to ensure that key set derivation is consistent with what has been performed by the ISD-P.

The eUICC SHALL support key establishment with and without the DR. The SM-DP decides which option to use.

BSI TR-03111 [49] contains recommendations and requirements on the generation and validation of ephemeral keys. In addition, NIST SP 800-56A [50] provides requirements on the destruction of ephemeral keys and other intermediate secret data after their use.

3.1.3 Download and Installation of the Profile

This section describes the third part of the procedure for the Profile Download and Installation step. The procedure illustrates the usage of RAM over HTTP as an example of the transport protocol.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 160
hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
endbox

DP->SR: (1) sendData(eid, isd-p-aid, [<data1>]<sub>scp03t</sub>, moreTodo)
Rnote over SR #FFFFF
(2) Check initial
 conditions
Endrnote

Hnote over SR, ISDR #C0C0C0
(2b) Conditional: HTTPS
 session opening
End hnote

SR->>ISDR: (3)
note over SR,ISDR
**HTTP/1.1 200 CRLF**
 …
**X-Admin-Targeted-Application:**//aid/<rid>/<pix> (of ISD-P-AID)CRLF
CRLF
<Body with [<data1>]<sub>scp03t</sub> >
End note

ISDR->ISDP: (4)
rnote over ISDP
(5) Unwrap
SCP03t security
End rnote

rnote over ISDP
(6) Process
Profile data
End rnote

ISDP-->ISDR: (6a)
ISDR->>SR: (7)

Note left of ISDP
**POST** /<next-uri> **HTTP/1.1** CRLF
 …
**X-Admin-Script-Status:** <script-status> CRLF
CRLF
 <Body with [data1 execution response] <sub>scp03t</sub> >
End note

SR->>DP: (8) SendData response + [data1 execution response]<sub>scp03t</sub>
Hnote over DP, ISDP #C0C0C0
(9) Optional: new data sending
End hnote

Hnote over OP, ISDP #C0C0C0
(9a) Conditional: Error management see 3.1.4
End hnote
```

```
DP->SR: (10) profileDownloadCompleted(eid, iccid, subdAddress, POL2)

rnote over SR
(11) Update
EIS
End rnote

SR-->DP

Hnote over SR, ISDP #C0C0C0
(12) Optional: : Enable Profile see 3.3
End hnote

DP->>OP: (13) Profile download &installation success
SR->>M2MSP: (14) Cond: HandleProfileDownloadedNotification (eid, iccid, enabled)

@enduml
```

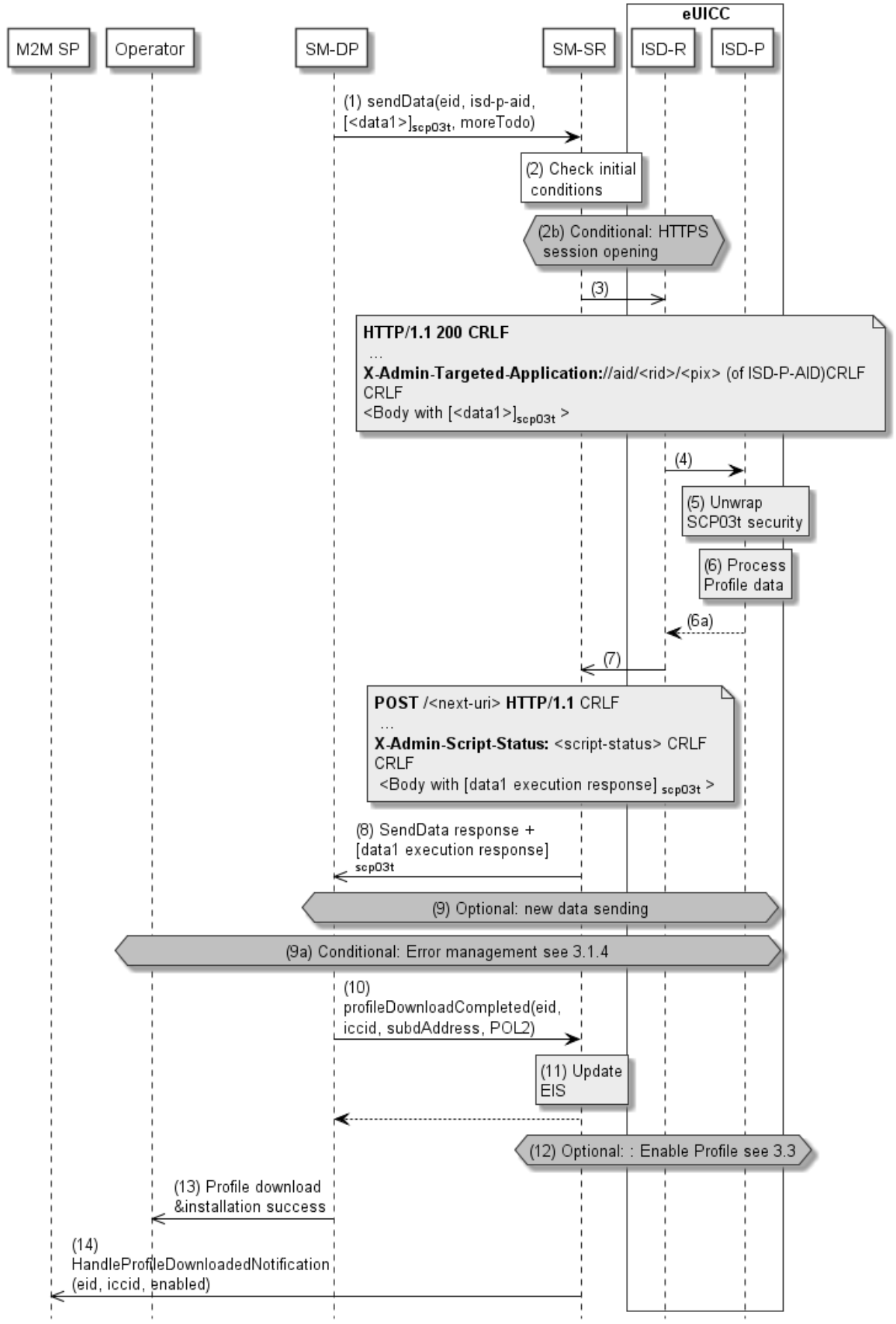


Figure 13: Download and Installation of the Profile

Start Conditions:

As a pre-condition, the ISD-P SHALL be created and personalized as defined in section 3.1.1 and section 3.1.2.

Procedure:

(1) The SM-DP SHALL call the "**ES3.SendData**" function specifying the targeted eUICC, the ISD-P, and providing the Profile data to download as input data. The Profile data has to be given as specified in section 4.1.3.1 and 5.4.4.

(2) The SM-SR SHALL verify that the SM-DP request is acceptable (the verifications that the SM-SR SHALL perform are described in section 5.4.4).

(2a) Depending on the error, the procedure MAY stop and a global failure message SHALL be returned to the Operator.

(2b) The SM-SR SHALL trigger the HTTPS session opening with the ISD-R if not already opened, as defined in section 2.4.4.5.

(3) The SM-SR SHALL return the HTTP POST response containing the secure data as provided by the SM-DP. The X-Admin-Targeted-Application field SHALL contain the ISD-P-AID.

(4) The ISD-R SHALL forward the received secure data to the ISD-P identified by the X-Admin-Targeted-Application field.

(5) The ISD-P SHALL process the security of the received data. The figure illustrates a success case; in case of security failure the error SHALL be returned within the next POST request to the SM-SR and finally returned to the SM-DP; and the procedure MAY end depending on the error.

(6) The ISD-P SHALL process the received command TLV(s).

(6a) The ISD-P SHALL return the response to the command TLV(s) to the ISD-R.

(7) The ISD-R SHALL return the ISD-P's response within the next POST request to the SM-SR.

(8) The SM-SR SHALL return to the SM-DP the execution status of the "**ES3.SendData**" function.

(9) Optionally the SM-DP MAY call the same "**ES3.SendData**" function again if the download and installation of the Profile requires several steps. This optional step MAY be repeated as many times as required.

(9a) In case of failure during the Download and Installation procedure, the SM-DP SHALL execute the error management procedure described in section 3.1.4. If this error management procedure fails to delete the ISD-P because the POL1 of the Profile prevented the deletion, the SM-DP shall consider that the profile installation succeeded on the eUICC, and SHALL continue at step 10 below. Otherwise the SM-DP SHALL return the result as specified in section 3.1.4 and the procedure SHALL stop.

(10) When Profile download is completed the SM-DP SHALL call the "**ES3.ProfileDownloadCompleted**" function. This basically indicates to the SM-SR that the Profile is downloaded and installed. The SM-DP MAY take the opportunity to define a POL2 on the Profile. The Operator SHALL be able to specify the POL2 content even if it is empty.

As requested by the Operator, after Profile installation the SCP03 key set of the ISD-P MAY:

i. Be retained by the SM-DP. In this case the Operator can instruct the SM-DP to hand over or delete the key set at a later point in time;
ii. Be handed over to the Operator. The keys MAY be replaced by the Operator;
iii. Be deleted from the eUICC by the SM-DP (using the GlobalPlatform DELETE command).

(11) The SM-SR SHALL update the EIS reflecting that the Profile is in "DISABLED" state, and POL2 if present.

(12) If the Operator has initially requested the Profile to be enabled, the SM-DP SHALL request the SM-SR to enable the newly installed Profile following the procedure in section 3.3 with the following modifications:

- The procedure SHALL start with step (1)

For the Normal Case, described in section 3.3.1 the following modification SHALL apply:

- The SM-DP SHALL NOT perform step 17

For the Failure Case, described in section 3.3.2 the following modification SHALL apply:

- The SM-DP SHALL NOT perform step (14)

NOTE When a M2M SP has a PLMA set to receive "Profile Download Notifications", as described in section 5.7.1, it has to be considered that the M2M SP may receive the information of a successful Profile download, based on a notification sent by the SM-SR, earlier than the Operator who has initiated the Profile Download. The Operator does not receive the result of a Profile download until the Profile Enable procedure, as described in section 3.3, has been executed. The result of Profile Download, including the result of Profile Enabling, is sent as described by step (13) of this procedure.

(13) The SM-DP SHALL return the response to the "**ES2.DownloadProfile**" function call to the Operator. In case the Profile has been downloaded successfully but the optional step 12 failed or expired before completion of the Profile enabling, the function execution response SHALL include the execution status "Executed-WithWarning" indicating that the Profile has been downloaded.

(14) If the profile has been successfully downloaded and installed, the SM-SR SHALL send the "**ES4.HandleProfileDownloadedNotification**" to a M2M SP, if authorised by the Operator owning the Profile, and SHALL indicate if the profile has been enabled as described in the optional step 12.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileDownloadedNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileDownloadedNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileDownloadedNotification**".

At the end of this procedure, if the Profile has been enabled, the Operator owning of the Profile is able to perform any remote management operation to the Profile using its own Remote Administration Server.

3.1.4 Error Management Sub-Routine

The next figure describes the flow for error management. This procedure is called when an error occurs during the key-establishment procedure or during the steps 1 to 11 of the Profile Download and Installation procedure (before the optional enabling of the Profile). The procedure illustrates the usage of RAM over HTTP as an example of the transport protocol.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 160
hide footbox

participant “Operator” as OP #FFFFFF
participant “SM-DP” as DP #FFFFFF
participant “SM-SR” as SR #FFFFFF
box “eUICC” #FFFFFF
participant “ISD-R” as ISDR #FFFFFF
participant “ISD-P” as ISDP #FFFFFF
participant ECASD #FFFFFF
endbox

DP->>SR: (1) In case of failure, deleteISDP(iccid) function

Hnote over SR, ISDR #C0C0C0
(1a) Conditional:
HTTPS session
opening
end hnote

SR->>ISDR: (2)
Note left of ISDP
**HTTP/1.1 200** CRLF
 …
CRLF
 <Body with ES5.DeleteProfile(isd-p-aid)>
End note

Rnote over ISDR #FFFFFF
(3) Enforce POL1
Endrnote
|||

Alt Unless POL1 rejects deletion
Rnote over ISDR: (4) Delete ISD-P
End

ISDR->>SR: (5)
Note left of ISDP
**POST** /<next-uri> **HTTP/1.1** CRLF
 …
**X-Admin-Script-Status:** <script-status> CRLF
CRLF
 <Body with ES5.DeleteProfile response >
End note

SR->>DP: (6) ISD-P deletion result

Alt Deletion failed due to POL1
Hnote over OP, SR #C0C0C0
(7a) Complete Download and Installation
     procedure, see 3.1.3
End hnote

Else Otherwise
DP->>OP: (7) Download failed
End

@end uml
```

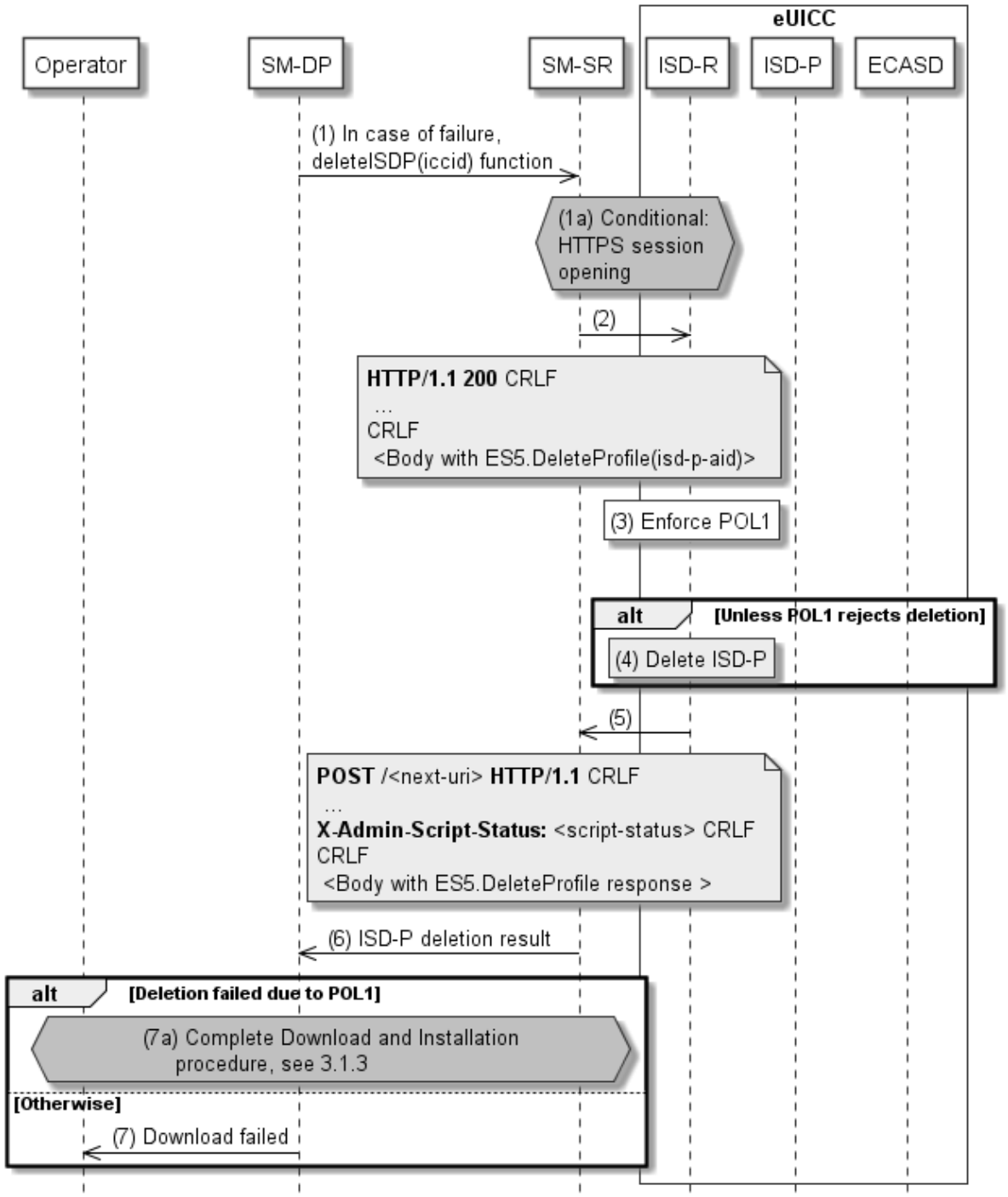


Figure 14: Error Management Sub-Routine

Procedure:

(1) In case of failure during the key establishment procedure or the Download Profile procedure, the SM-DP SHALL call the **"ES3.DeleteISDP"** function with its relevant input data.

(1a) The SM-SR SHALL trigger the HTTP session with the ISD-R if not already opened as defined in section 2.4.4.5.

(2) The SM-SR SHALL return the HTTP POST response with a body containing the "**ES5.DeleteProfile**" function with the ICCID. The X-Admin-Targeted-Application parameter SHALL be omitted as the command is targeting the ISD-R.

(3) If the Profile is already completely installed, the ISD-R SHALL enforce POL1. If POL1 prevents the deletion of the target Profile, the ISD-R SHALL skip step 4.

(4) The ISD-R SHALL delete the targeted ISD-P.

(5) The ISD-R SHALL return the execution response to the ISD-P deletion "**ES5.DeleteProfile**" within a new HTTP POST request addressed to the SM-SR.

(6) The SM-SR SHALL forward the status of the "**ES3.DeleteISDP**"to the SM-DP.

(7) If the deletion of the ISD-P was successful, the response message indicating the failure of the download SHALL be returned to the Operator. In case of a timeout of the "**ES5.DeleteProfile**", the status of the download SHALL be reported as 'Expired'.

a. If the deletion of the ISD-P was prevented by POL1, the SM-DP shall consider that the profile download and installation succeeded on the eUICC, and SHALL continue the procedure 3.1.3.

NOTE: In case the deletion of the ISD-P fails or expires (e.g. because the eUICC is out of coverage), or in case the SM-DP does not receive confirmation of the deletion (e.g. because sending the result (5) failed), the SM-DP will get a chance to delete the ISD-P and the potentially incomplete profile at the beginning of a subsequent Profile Download on the same eUICC, as described in section 3.1.5.

3.1.5 ISD-P Cleanup Sub-Routine

The next figure describes the alternate flow that an SM-DP SHALL follow to delete an ISD-P that it formerly failed to delete.

NOTE 1: The case where a Cleanup fails due to POL1 is not covered here.

NOTE 2: The case where a Profile with the same ICCID was incompletely downloaded to a different eUICC is not covered here.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 160
hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
endbox

OP->>DP: (1) downloadProfile(srid, eid, iccid, final state, profileType)
DP->SR: (2) getEIS(eid)

Rnote over SR #FFFFF
(3) Retrieve EIS
Endrnote

SR-->DP: (4) Return EIS

Alt [If the SM-DP detects an ISD-P that it created and still in an incomplete
state]

DP->>SR: (5alt) DeleteProfile(eid, iccid)
Rnote over SR #FFFFF
(6alt) Check initial conditions
Endrnote
SR-->>DP: Failed
SR->>ISDR: (7alt) MT-SMS [ES5.DELETE command]SCP80

Rnote over ISDR #FFFFFF
(8alt) Delete ISD-P
Endrnote

ISDR-->>SR: (9alt) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(10alt) Update EIS
Endrnote
SR-->>DP: (11alt) Profile deletion result

End

Rnote over DP #FFFFFF
(5) Check eUICC eligibility
Endrnote
DP-->>OP: Failed

DP->>SR: (6) createISDP(eid, iccid, mno-id,…)

@enduml
```

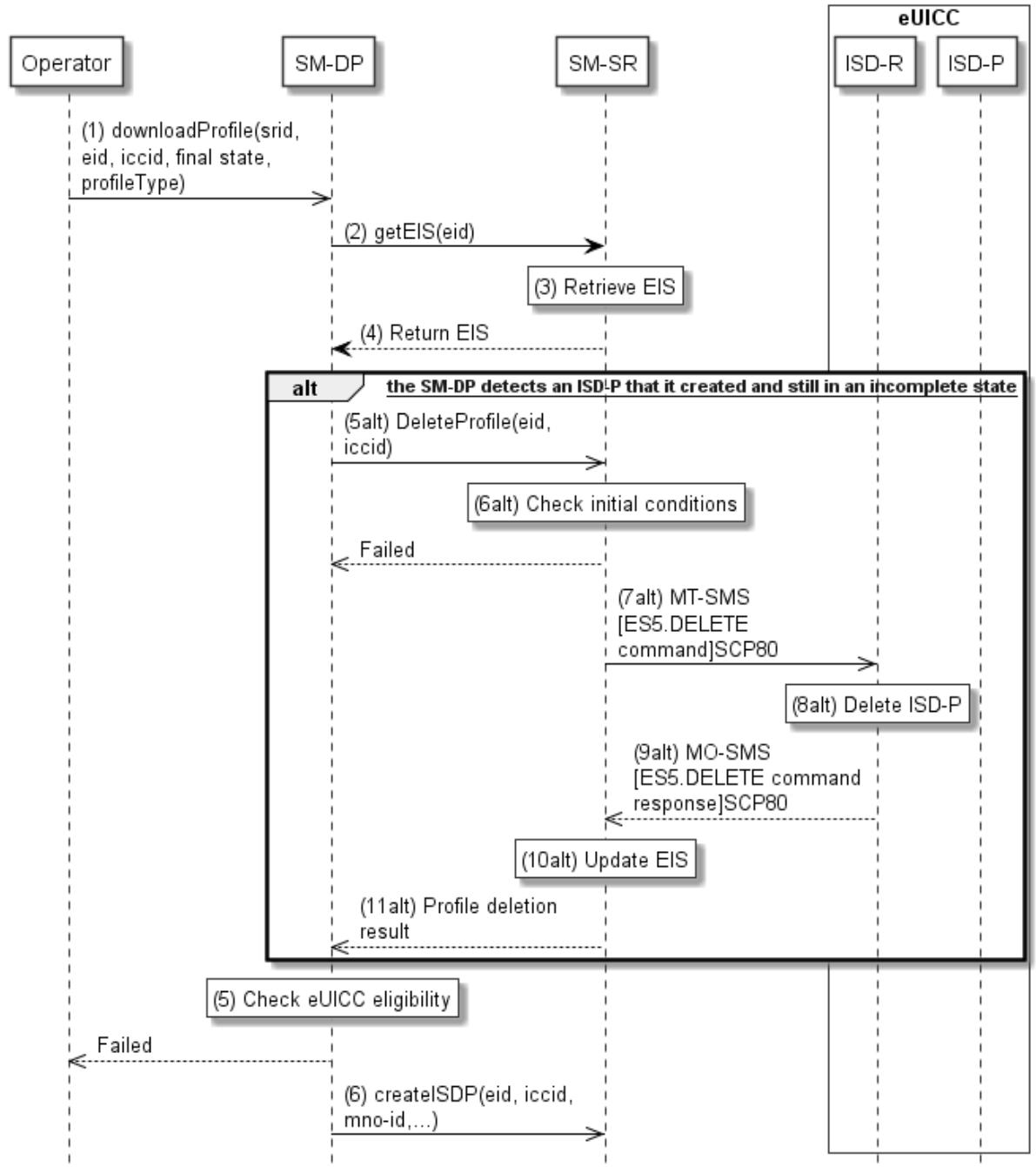


Figure 315-A: ISD-P cleanup at the beginning of a subsequent profile download

Procedure:

(1) 2) (3) (4) See section 3.1.1.

(5alt) As per the EIS, or by comparing the EIS with its own records, the SM-DP determines that an ISD-P associated to this SM-DP is in an incomplete state (the profile download procedure did not complete nominally). The SM-DP SHALL then send a request "**ES3.DeleteISDP**" to the SM-SR to delete the incomplete ISD-P.

(6alt) The SM-SR SHALL verify if the SM-DP request is acceptable (the verifications that the SM-SR SHALL perform are described in section5.4.9). If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating a failure, and the procedure SHALL end.

(7alt) The SM-SR SHALL send an MT-SMS containing the "**ES5.DELETE**" command with its relevant input data (see section 4.1.1.4) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.DELETE**" command.

(8alt) The ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(9alt) The ISD-R SHALL return the MO-SMS to the SM-SR containing the execution status of the "**ES5.DELETE**" command.

(10alt)In case of successful execution, the SM-SR SHALL update the EIS to reflect the newly deleted Profile.

(11alt) The SM-SR SHALL return the response to the "**ES3.DeleteISDP**" function to the SM-DP.

(5)(6)… The SM-DP and SM-SR SHALL resume the procedure described in section 3.1.1

3.2 Profile Enabling

The Profile Enabling procedure between the Operator and the SM-SR is used to enable a Profile previously downloaded and installed on an eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.5). The procedure is initiated by the Operator owning the Profile to be enabled. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can also be performed using other transport protocols.

3.2.1 Normal Case

The sequence flow in the Figure 15 describes the normal case where the target Profile can successfully be enabled.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator2" as OP2 #FFFFFF
participant "Operator1" as OP1 #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

OP1->>SR: (1) EnableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP1: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>OP1: Failed
Rnote over ISDR #FFFFFF
(5) Enable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>OP1: (6a) Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment with the enabled profile
Endrnote
|||
Hnote right of SR #FFFFFF
(9)                  Notification procedure over SMS
Endhnote
|||
Rnote over SR #FFFFFF
(10) Check POL2
Endrnote
SR->>ISDR: (11) Cond.:  MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(11a) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.DELETE command FAILED response]SCP80
SR-->>OP1: Failed
Rnote over ISDR #FFFFFF
(11b) Delete disabled ISD-P
and contained profile
Endrnote
ISDR-->>SR: (11c) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(12) Update EIS
Endrnote
SR-->>OP1: (13) Profile enabling result
SR->>OP2: (14) HandleProfileDisabledNotification(eid, iccid2)
SR->>M2MSP: (15) HandleProfileEnabledNotification (eid, iccid)
SR->>M2MSP: (16) HandleProfileDisabledNotification (eid, iccid2)

@enduml
```

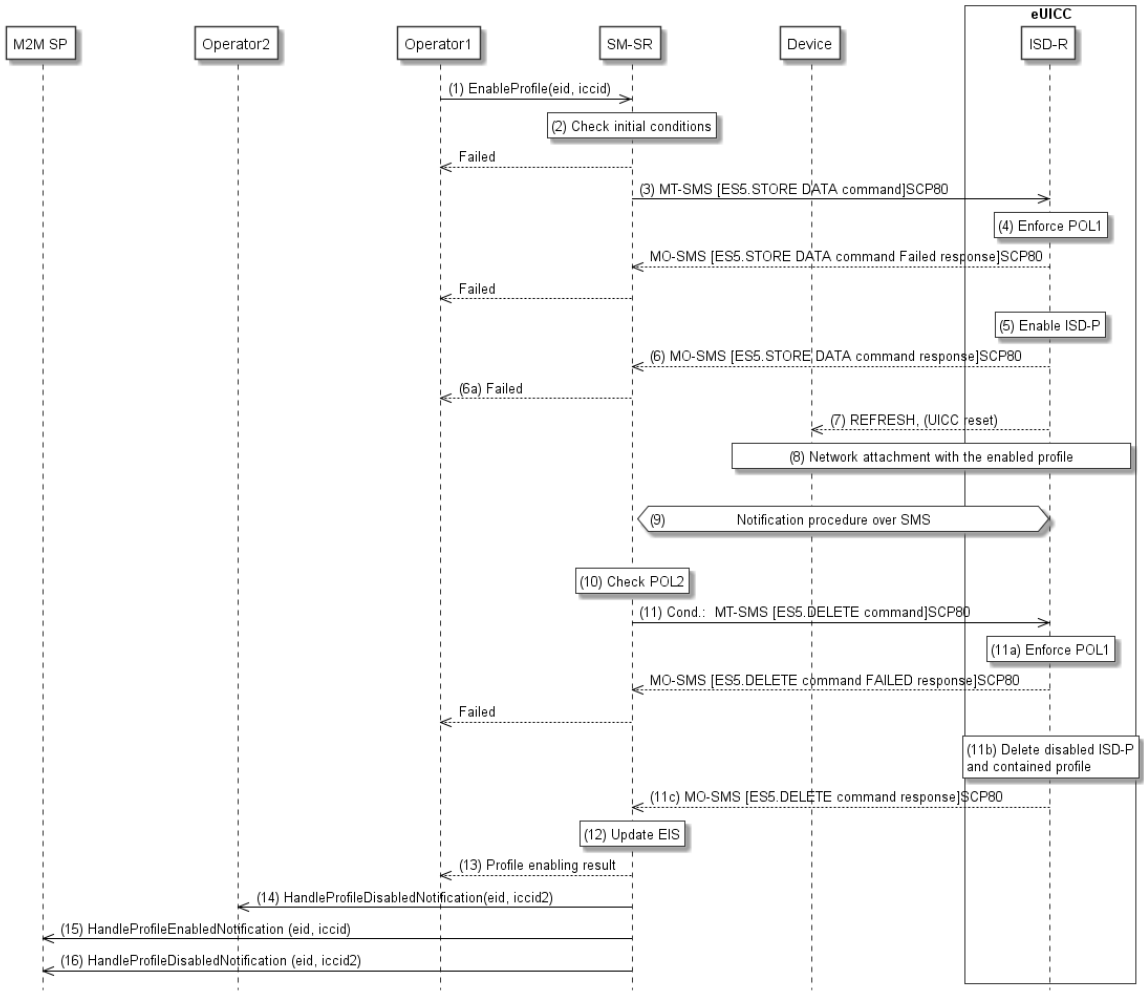


Figure 15: Profile Enabling, Success Case

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) Operator1, of the target Profile SHALL call the **"ES4.EnableProfile"** function with its relevant input data.

(2) The SM-SR SHALL verify that the Operator1 request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.5.5), and in particular evaluates POL2 of the currently Enabled Profile. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR SHALL send an MT-SMS containing the "**ES5.STORE DATA**" command for Profile enabling with its relevant input data (see section 4.1.1.2) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.STORE DATA**" command.

(4) The ISD-R SHALL enforce POL1 of the currently Enabled Profile. If POL1 rejects enabling of the target Profile, the ISD-R SHALL return directly the MO-SMS containing the response indicating a failure, and the procedure SHALL end.

(5) If POL1 allows, the ISD-R SHALL disable the currently enabled ISD-P and enable the targeted ISD-P.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective after the terminal executes the REFRESH command.

(6) The ISD-R SHALL return the MO-SMS containing the execution status of the "**ES5.STORE DATA**" command to the SM-SR.

(6a) If the response to the "**ES5.STORE DATA**" command indicates a failure, the SM-SR SHALL return a response indicating the failure to Operator1, and the procedure SHALL end.

(7) The ISD-R SHALL send a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

NOTE: In case of any error after this step, indicating that the currently Enabled Profile cannot provide connectivity, the ISD-R SHALL re-enable the previously Enabled Profile as described in section 3.2.2.

(8) The eUICC and the Device SHALL perform a network attach procedure with the newly Enabled Profile.

(9) The eUICC SHALL perform the notification procedure as described in section 4.1.1.11. During this procedure, if the ISD-R doesn't succeed in sending the SMS notification (after having exhausted all possible retries), or doesn't receive the SM-SR notification confirmation ("**ES5.HandleNotificationConfirmation**" command), the ISD-R SHALL consider this as an error, and the previous note SHALL apply. After successfully verifying the content of the notification confirmation received from the SM-SR (which confirms that the newly Enabled Profile provides connectivity), the eUICC SHALL no longer attempt to re-enable the previously Enabled Profile.
After this verification, if POL1 of the now Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", and this Profile does not have the Fall-Back Attribute set, the ISD-R SHALL delete the disabled ISD-P and the contained Profile. The eUICC SHALL send the response to the notification confirmation indicating whether the disabled ISD-P has been deleted or not.

NOTE: If the SM-SR receives the notification after the expiration of the Validity Period (which was provided to the SM-SR for this function call), it will not send the notification confirmation (see section 3.15.1).

(9a) If the previously Enabled Profile (now Disabled) has the Fall-Back Attribute, and its POL1 contains the rule "Profile deletion is mandatory when its state is changed to disabled", this rule SHALL be ignored according to Sections 2.4 and 3.6.3.2 in GSMA Remote Provisioning Architecture for the Embedded UICC [1], and the procedure SHALL continue at step 10.

(10) On reception of the "**ES5.HandleNotificationConfirmation**" response, and if this response indicates that the Disabled Profile has not been deleted, the SM-SR SHALL evaluate POL2 of the Disabled Profile. If POL2 of the Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", the SM-SR SHALL perform step (11), else it SHALL jump to step (12).

(11) The SM-SR SHALL send an MT-SMS containing the "**ES5.DELETE**" command with its relevant input data (see section 4.1.1.4) to the ISD-R, targeting the Disabled Profile. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.DELETE**" command.

(11a) The ISD-R SHALL enforce POL1 of the target Profile. If POL1 rejects the deletion of the target Profile, the ISD-R SHALL return the MO-SMS containing the response indicating the corresponding failure, and the procedure SHALL end.

(11b) If POL1 allows its deletion, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(11c) The ISD-R SHALL return the MO-SMS to the SM-SR containing the execution status of the "**ES5.DELETE**" command.

(12) According to the executed sequence and the eUICC responses, the SM-SR SHALL update the EIS to reflect that:

- The target Profile has been enabled
- The previously Enabled Profile has been disabled or deleted.

NOTE: POL1 and POL2 MAY have different content. As a consequence, both the eUICC and the SM-SR have to ensure the ISD-P deletion based on their respective Policy.

(13) The SM-SR SHALL return the response to the "**ES4.EnableProfile**" function to Operator1, indicating that the Profile has been enabled.

(14) Unless Operator2 has set an ONC (Operator Notifications Configuration) to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" or "**ES4.HandleProfileDeletedNotification**" (if deletion was triggered by the evaluation of POL1 and POL2) to Operator2, the owner of the Profile that was enabled at the beginning of the procedure. In case Operator2 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such a situation based on its own database), the SM-SR SHALL send this notification to the SM-DP authorised by Operator2 by calling the "**ES3.HandleProfileDisabledNotification**" or the "**ES3.HandleProfileDeleted**Notification". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator2 by calling the "**ES2.HandleProfileDisabledNotification**" or the "**ES2.HandleProfileDeletedNotification**".

(15) The SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to a M2M SP, if authorised by Operator1 the owner of the Profile that was Disabled at the beginning of the procedure.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileEnabledNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileEnabledNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileEnabledNotification**".

(16) The SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" or "**ES4.HandleProfileDeletedNotification**" (if deletion was triggered by the evaluation of

POL1 and POL2) to a M2M SP, if authorised by Operator2 the owner of the Profile that was Enabled at the beginning of the procedure.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileDisabledNotification**" or "**ES4.HandleProfileDeletedNotification**"

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileDisabledNotification**" or "**ES3.HandleProfileDeletedNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileDisabledNotification**" or "**ES2.HandleProfileDeletedNotification**"

NOTE: This M2M SP might be the same M2M SP as for Operator1 or any other M2M SP.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.2.2 Connectivity Failure Case

The sequence flow in the Figure 16 describes the case where the target Profile cannot provide connectivity after it is enabled, and when roll-back to the previously Enabled Profile occurs.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator1" as OP1 #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

OP1->>SR: (1) EnableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP1: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>OP1: Failed
Rnote over ISDR #FFFFFF
(5) Enable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>OP1: (6a) Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment with the enabled profile **fails**
                                OR
                  Notification procedure **fails**
Endrnote
|||
Hnote over ISDR #FFFFFF
(9) Enable previous ISD-P
Endhnote
ISDR-->>DEV: (10) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(11) Network attachment with the enabled profile
Endrnote
|||
Hnote right of SR #FFFFFF
(12)                Notification procedure over SMS
Endhnote
|||
SR-->>OP1: (13) Profile enabling failure
@enduml
```

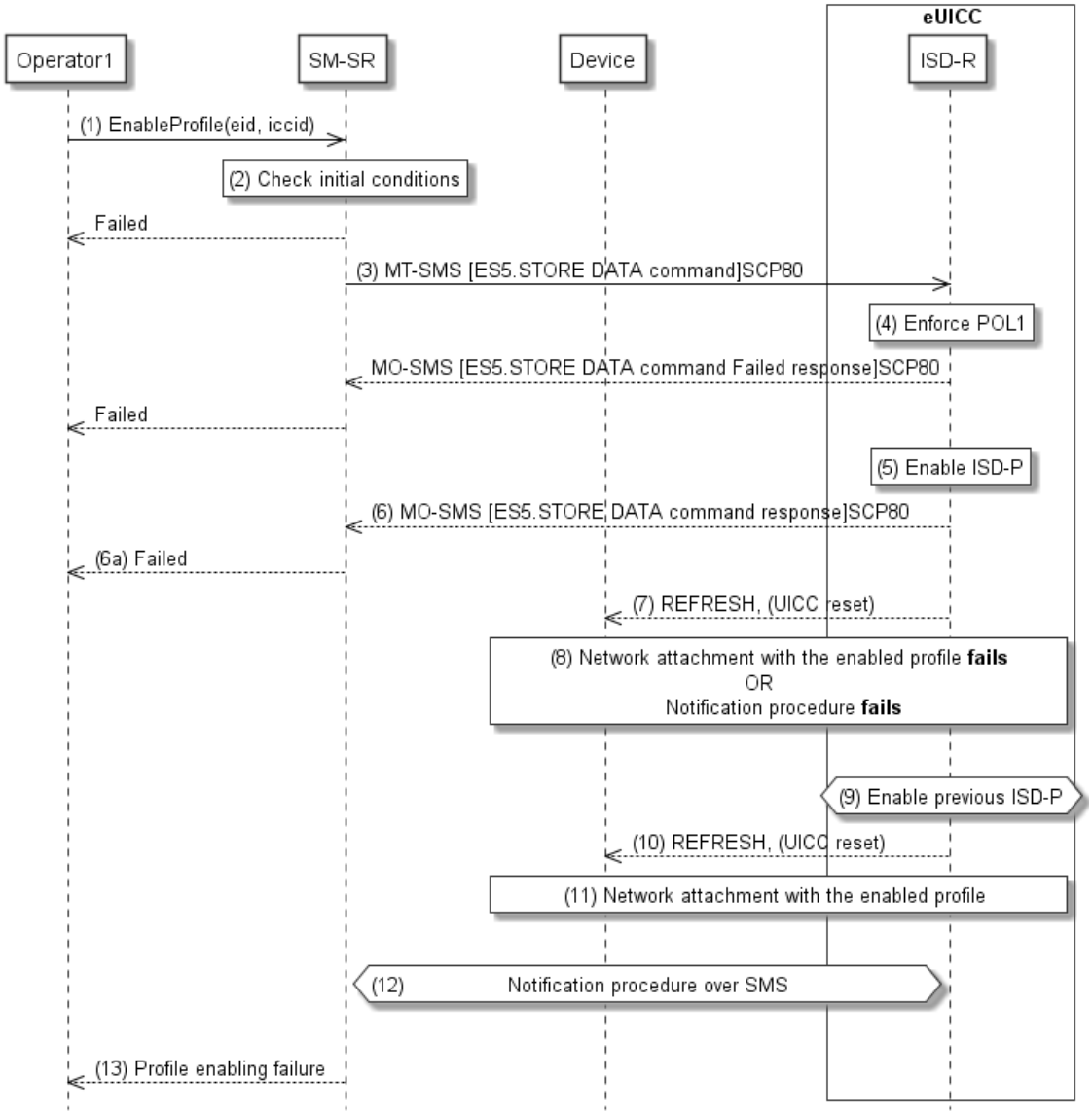


Figure 16: Profile Enabling failure, with roll-back

Start Conditions:

The start conditions are identical to section 3.2.1.

Procedure:

Steps (1), (2), (3), (4), (5), (6), (6a) and (7) are also identical to section 3.2.1.

(8) A network attach failure occurs indicating that the Enabled Profile cannot provide connectivity, or the eUICC doesn't succeed to send the SMS notification (after having exhausted all possible retries), or doesn't receive the SM-SR notification confirmation.

(9) The ISD-R SHALL enable the Profile that was previously enabled before the reception of the command, to re-establish connectivity.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective only after the terminal executes the REFRESH command.

(10) The ISD-R sends a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a new network attach procedure.

(11) The eUICC and the Device SHALL perform a new network attach procedure with the Profile Enabled before the start of the procedure.

(12) The eUICC SHALL perform the notification procedure as described in section 4.1.1.11. On reception of the SMS notification, the SM-SR is informed that the target Profile has not been enabled. In order to minimize the notification retries on eUICC side, the SM-SR SHALL send the "**ES5.HandleNotificationConfirmation**" command defined in section 4.1.1.12 even if the Validity Period specified in the "**ES4.EnableProfile**" command has expired.

(13) Finally, the SM-SR SHALL return the response to the "**ES4.EnableProfile**" function to Operator1; indicating a failure, the target Profile didn't succeed to provide the connectivity.

3.3 Profile Enabling Via SM-DP

The Profile Enabling procedure between the Operator and the SM-DP is used to enable a Profile previously downloaded and installed on an eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.5). The procedure is initiated by the Operator owning the Profile to be enabled. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can be also performed using other transport protocols.

This procedure is similar to the procedure "Enable Profile" described in section 3.2.

3.3.1 Normal Case

The sequence flow in the 0 describes the normal case where the targeted Profile can successfully be enabled.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator2" as OP2 #FFFFFF
participant "Operator1" as OP1 #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

OP1->>DP: (0) Cond.: EnableProfile(eid, smsr-id, iccid)
DP->>SR: (1) EnableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP1: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>DP: Failed
DP-->>OP1: Failed
Rnote over ISDR #FFFFFF
(5) Enable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>DP: (6a) Failed
DP-->>OP1: Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment with the enabled profile
Endrnote
|||
Hnote right of SR #FFFFFF
(9)                 Notification procedure over SMS
Endhnote
|||
Rnote over SR #FFFFFF
(10) Check POL2
Endrnote
SR->>ISDR: (11) Cond.:  MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(11a) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.DELETE command FAILED response]SCP80
SR-->>DP: Failed
DP-->>OP1: Failed
Rnote over ISDR #FFFFFF
(11b) Delete disabled ISD-P
and contained profile
Endrnote
ISDR-->>SR: (11c) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(12) Update EIS
Endrnote
SR-->>DP: (13) Profile enabling result
```

```
SR->>OP2: (14) HandleProfileDisabledNotification(eid, iccid2)
SR->>M2MSP: (15) HandleProfileEnabledNotification (eid, iccid)
SR->>M2MSP: (16) HandleProfileDisabledNotification (eid, iccid2)
DP-->>OP1: (17) Cond.: Profile enabling result

@enduml
```

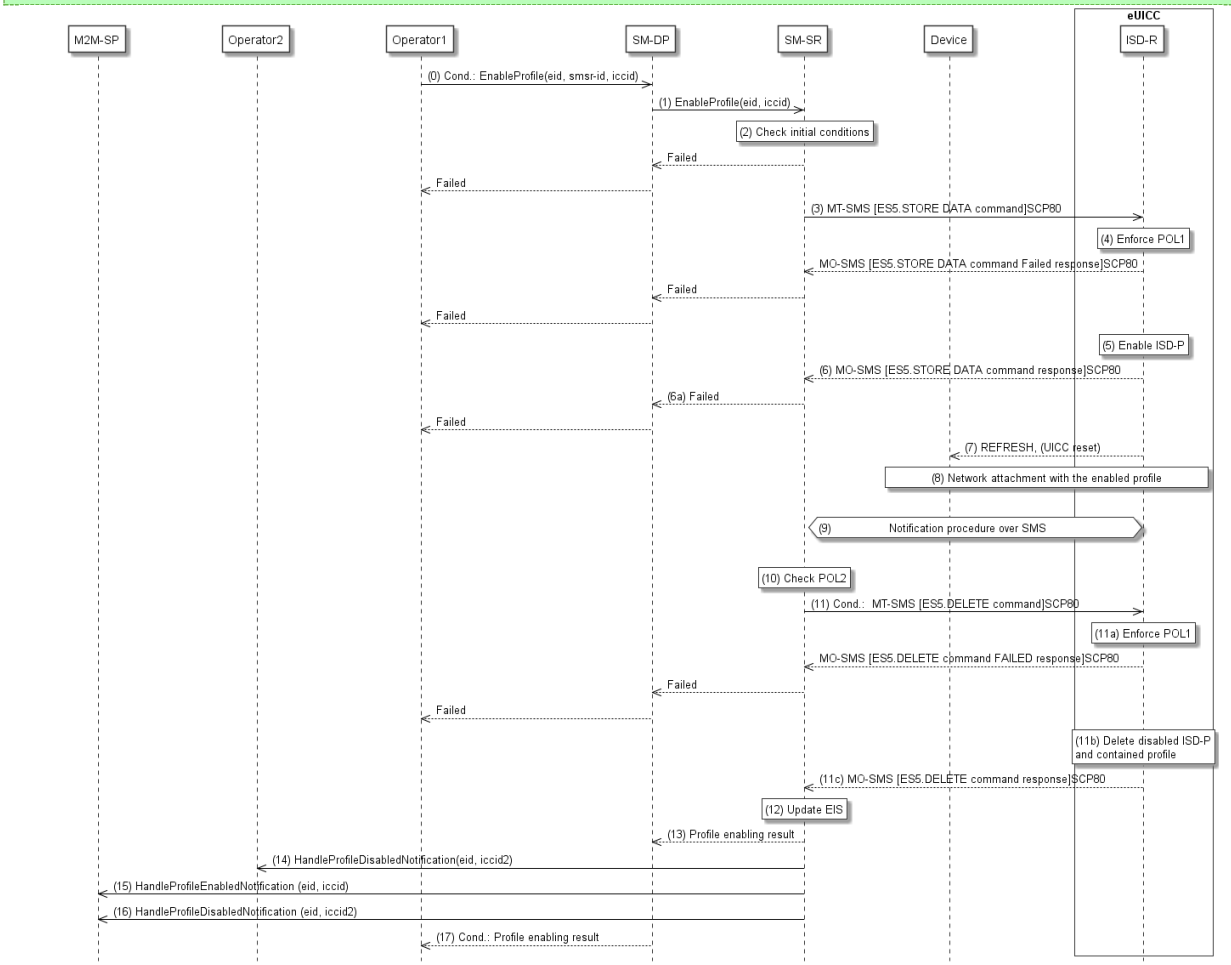


Figure 17: Profile Enabling, Success Case

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(0) Operator1, the owner of the target Profile, SHALL call the **"ES2.EnableProfile"** function with its relevant input data, see section 5.3.5, in particular the identification of the SM-SR in charge of the management of the target eUICC. If the Profile Enabling procedure has been requested during a Profile Download (see section 3.1.3), this step is not applicable.

(1) The SM-DP SHALL forward the request to the SM-SR provided by the Operator and SHALL call the function "**ES3.EnabledProfile**". During this step the SM-DP may have to establish a link to the SM-SR (see section 2.6).

Steps (2) to (12) are the same as in the procedure "Profile Enabling" described in section 3.2.1.

(13) The SM-SR SHALL return the response to the "**ES3.EnableProfile**" function to the SM-DP, indicating that the Profile has been enabled.

(14) Unless Operator2 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" or "**ES4.HandleProfileDeletedNotification**" (if deletion was triggered by the evaluation of POL1 and POL2) to Operator2, the owner of the Profile that was enabled at the beginning of the procedure. In case Operator2 has no direct connection with the SM-SR, the SM-SR SHALL apply the same process as described in point (14) of section 3.2.1.

(15) The SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to a M2M SP, if authorised by Operator1 the owner of the Profile that was disabled at the beginning of the procedure.

(16) The SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" or "**ES4.HandleProfileDeletedNotification**" (if deletion was triggered by the evaluation of POL1 and POL2) to a M2M SP, if authorised by Operator2 the owner of the Profile that was enabled at the beginning of the procedure.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileEnabledNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileEnabledNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileEnabledNotification**".

NOTE: This M2M SP might be the same M2M SP as for Operator1 or any other M2M SP.

(17) Finally, the SM-DP SHALL return the response to the "**ES2.EnableProfile**" function call to Operator1. If the Profile Enabling procedure has been requested during a Profile Download (see section 3.1.3), then the SM-DP SHALL NOT execute this step.

3.3.2 Connectivity Failure Case

The sequence flow in the Figure 18 describes the case where the targeted Profile cannot provide connectivity after it is enabled, and when roll-back to the previously Enabled Profile occurs.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator1" as OP1 #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

OP1->>DP: (0) Cond.: EnableProfile(eid, smsr-id, iccid)
DP->>SR: (1) EnableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP1: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>DP: Failed
DP-->>OP1: Failed
Rnote over ISDR #FFFFFF
(5) Enable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>DP: (6a) Failed
DP-->>OP1: Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment with the enabled profile **fails**
                            OR
                Notification procedure **fails**
Endrnote
|||
Hnote over ISDR #FFFFFF
(9) Enable previous ISD-P
Endhnote
ISDR-->>DEV: (10) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(11) Network attachment with the enabled profile
Endrnote
|||
Hnote right of SR #FFFFFF
(12)                Notification procedure over SMS
Endhnote
|||
SR-->>DP: (13) Profile enabling failure
DP-->>OP1: (14) Cond.: Profile enabling failure
@enduml
```

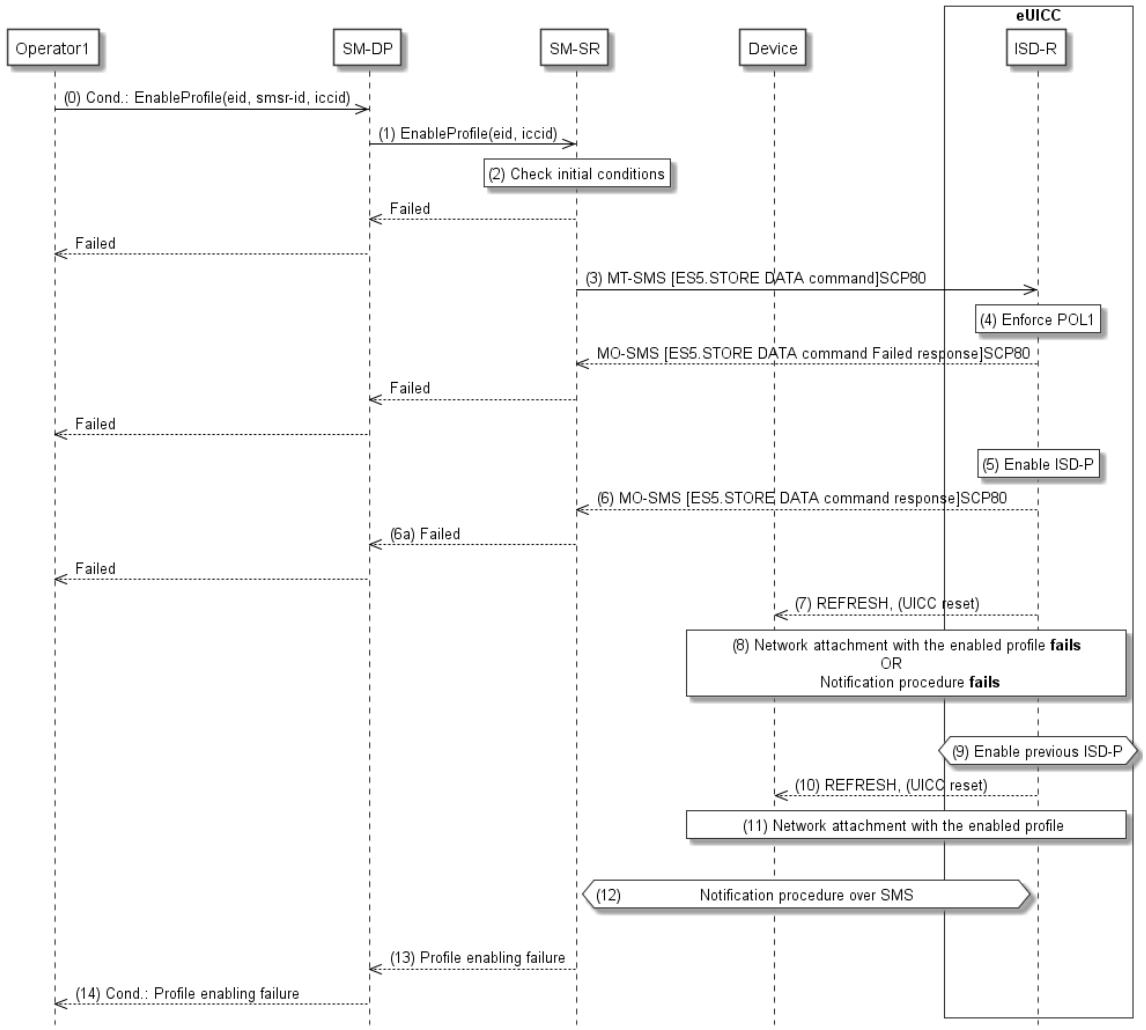


Figure 18: Profile Enabling, With Roll-Back

Start Conditions:

The start conditions are the same as in section 3.3.1.

Procedure:

Steps (0) and (1) are the same as in section 3.3.1. If the Profile Enabling procedure has been requested during a Profile Download (see section 3.1.3), the step (0) is not applicable.

Steps (2) to (12) are the same as in procedure “Connectivity failure case” as described in section 3.2.2.

(13) The SM-SR SHALL return the response to the “**ES3.EnableProfile**” function to the SM-DP, indicating a failure, the target Profile didn’t succeed to provide the connectivity.

(14) Finally, the SM-DP SHALL return the response to the “**ES2.EnableProfile**” function to Operator1, indicating a failure, the target Profile didn’t succeed to provide the connectivity. If the Profile Enabling procedure has been requested during a Profile Download (see section 3.1.3), then the SM-DP SHALL NOT execute this step.

NOTE: In case the previously Enabled Profile can also not provide connectivity, the eUICC SHALL activate the Fall-Back Mechanism.

3.4 Profile Disabling

The Profile Disabling procedure is initiated by the Operator owning the Profile to be disabled. The procedure illustrated using SMS as a possible transport protocol between the SM-SR and the eUICC, but can be also performed using other transport protocols.

The sequence flow in the 0 describes the case where the targeted Profile can successfully be disabled.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator2" as OP2 #FFFFFF
participant "Operator1" as OP1 #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

OP1->>SR: (1) DisableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP1: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>OP1: Failed
Rnote over ISDR #FFFFFF
(5) Disable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>OP1: (6a) Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment using profile with Fall-Back Attribute
Endrnote
|||
Hnote right of SR #FFFFFF
(9)                  Notification procedure over SMS
Endhnote
|||
Rnote over SR #FFFFFF
(10) Check POL2
Endrnote
SR->>ISDR: (11) Cond.:  MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(11a) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.DELETE command FAILED response]SCP80
SR-->>OP1: Failed
Rnote over ISDR #FFFFFF
(11b) Delete disabled ISD-P
and contained profile
Endrnote
ISDR-->>SR: (11c) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(12) Update EIS
Endrnote
SR-->>OP1: (13) Profile disabling result
SR->>OP2: (14) HandleProfileEnabledNotification(eid, iccid2)
SR->>M2MSP: (15) HandleProfileDisabledNotification (eid, iccid)
SR->>M2MSP: (16) HandleProfileEnabledNotification (eid, iccid2)

@enduml
```

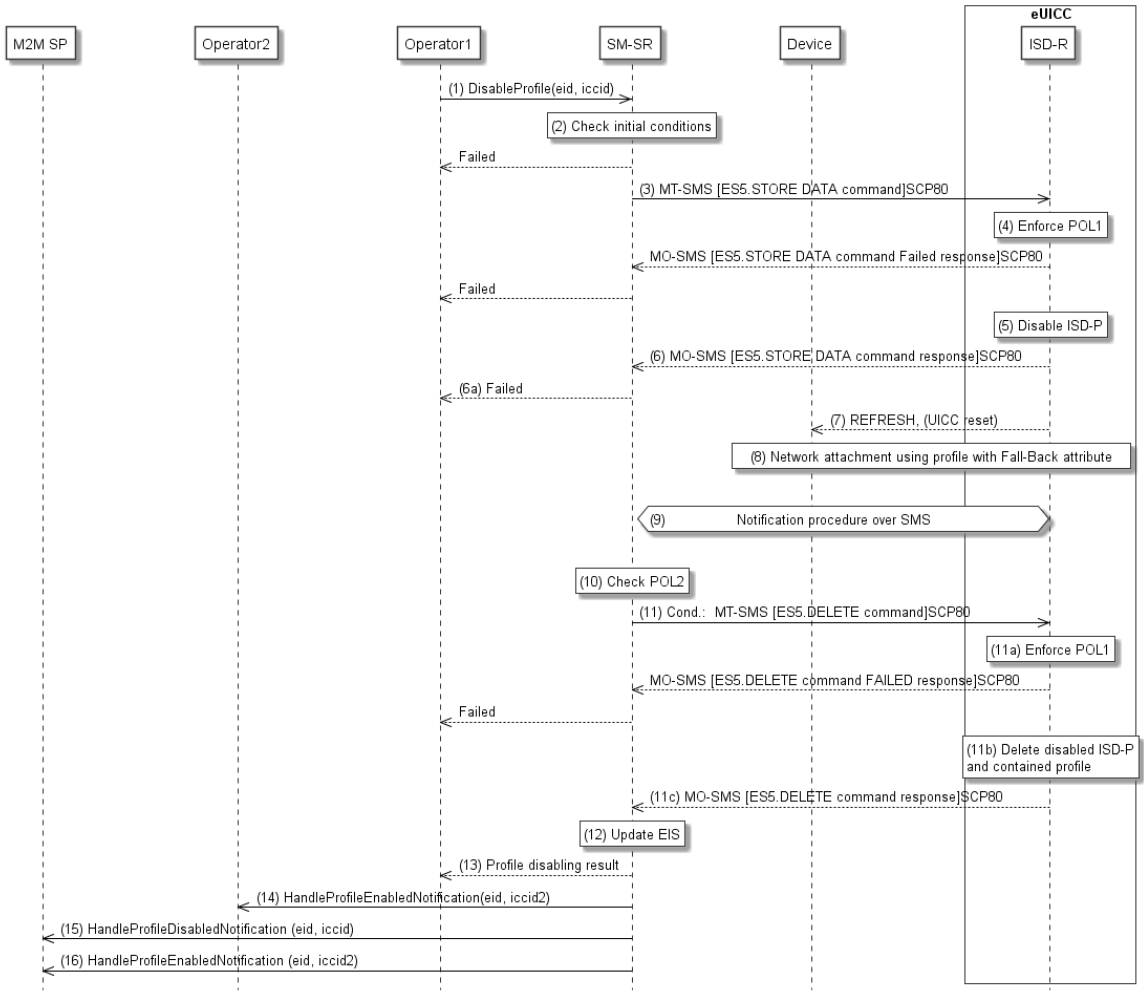


Figure 19: Profile Disabling

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) Operator1, the owner of the target Profile SHALL call the "**ES4.DisableProfile**" function with its relevant input data.

(2) The SM-SR SHALL verify that the Operator1 request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.5.6, and in particular checks that Profile is enabled and Profile disabling is allowed in POL2. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR SHALL send an MT-SMS containing the "**ES5.STORE DATA**" command for Profile disabling with its relevant input data (see section 4.1.1.3) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.STORE DATA**" command.

(4) The ISD-R SHALL enforce POL1 of the currently Enabled Profile. In case POL1 rejects disabling, the ISD-R SHALL return PoR containing the response indicating a failure, and the procedure SHALL end.

(5) The ISD-R SHALL disable the targeted ISD-P and the contained Profile and SHALL enable the Profile with the Fall-Back Attribute set.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective only after the terminal executes the REFRESH command.

(6) The ISD-R SHALL return the MO-SMS containing the execution status of the "**ES5.STORE DATA**" command to the SM-SR.

(6a) If the response to the "**ES5.STORE DATA**" command indicates a failure, the SM-SR SHALL return a response indicating the failure to Operator1, and the procedure SHALL end.

(7) The ISD-R sends a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

NOTE: In case of any error after this step indicating that the current Enabled Profile cannot provide connectivity, the ISD-R SHALL re-enable the previously Enabled Profile as described in section 3.2.2.

(8) The eUICC and the Device SHALL perform a new network attach procedure with the Profile with the Fall-Back Attribute set.

(9) The eUICC SHALL perform the notification procedure as described in section 4.1.1.11. During this procedure, if ISD-R doesn't succeed to send the SMS notification, or doesn't receive the SM-SR notification confirmation ("**ES5.HandleNotificationConfirmation**" command), the ISD-R SHALL consider this as an error, and the previous note SHALL apply.

After successfully verifying the content of the notification confirmation received from the SM-SR (which confirms that the newly Enabled Profile provides connectivity), the eUICC SHALL no longer attempt to re-enable the previously Enabled Profile.
After this verification, if POL1 of the Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", the ISD-R SHALL delete the disabled ISD-P and the contained Profile. The eUICC SHALL send the response to the notification confirmation indicating whether the disabled ISD-P has been deleted or not.

NOTE: If the SM-SR receives the notification after the expiration of the Validity Period (which was provided to the SM-SR for this function call), it will not send the notification confirmation (see section 3.15.1).

(10) On reception of the **ES5.HandleNotificationConfirmation** response, and if the **ES5.HandleNotificationConfirmation** response indicates that the Disabled Profile has not been deleted, the SM-SR SHALL evaluate POL2 of the Disabled Profile. If POL2 of the Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", the SM-SR SHALL perform step (11), else it SHALL jump to step (12).

(11) The SM-SR SHALL send an MT-SMS containing the "**ES5.DELETE**" command with its relevant input data (see section 4.1.1.4) to the ISD-R, targeting the Disabled Profile. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.DELETE**" command.

(11a) The ISD-R SHALL enforce POL1 of the target Profile. If POL1 rejects the deletion of the target Profile, the ISD-R SHALL return the MO-SMS containing the response indicating the corresponding failure, and the procedure SHALL end.

(11b) If POL1 allows its deletion, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(11c) The ISD-R SHALL return the MO-SMS to the SM-SR containing the execution status of the "**ES5.DELETE**" command.

(12) According to the executed sequence and the eUICC responses, the SM-SR SHALL update the EIS to reflect that:

- The Profile having the Fall-Back Attribute has been enabled
- The previously Enabled Profile has been disabled or deleted.

NOTE: POL1 and POL2 MAY have different content. As a consequence, both the eUICC and the SM-SR have to ensure the ISD-P deletion based on their respective Policy.

(13) The SM-SR SHALL return the response to the "**ES4.DisableProfile**" function to Operator1, indicating that the Profile has been disabled. In case the Profile has also been deleted because of POL1 or POL2, the function execution response SHALL include an execution status "Executed-WithWarning" indicating that the Profile has also been deleted.

(14) Unless Operator2 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to Operator2, the owner of Profile with Fall-Back Attribute set that is now enabled. In case Operator2 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such situation based on its own database), the SM-SR SHALL send this notification to the SM-DP authorised by Operator2 by calling the "**ES3.HandleProfileEnabledNotification**". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator2 by calling the "**ES2.HandleProfileEnabledNotification**".

(15) The SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" to a M2M SP, if authorised by Operator1 the owner of the Profile that was enabled at the beginning of the procedure.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileDisabledNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileDisabledNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileDisabledNotification**"

(16) The SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to a M2M SP, if authorised by Operator2 the owner of Profile with Fall-Back Attribute set that is now enabled.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileEnabledNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileEnabledNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileEnabledNotification**".

NOTE: This M2M SP might be the same M2M SP as for Operator1 or any other M2M SP.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.5 Profile Disabling Via SM-DP

The Profile Disabling procedure is initiated by the Operator owning the Profile to be disabled through the SM-DP. The procedure illustrated using SMS as a possible transport protocol between SM-SR and eUICC, but can be also performed using other transport protocols.

This procedure is similar to the procedure "Disable Profile" described in section 3.4.

The sequence flow in the Figure 20 describes the case where the targeted Profile can successfully be disabled.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator2" as OP2 #FFFFFF
participant "Operator1" as OP1 #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

OP1->>DP: (0) DisableProfile(eid, smsr-id, iccid)
DP->>SR: (1) DisableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP1: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>DP: Failed
DP-->>OP1: Failed
Rnote over ISDR #FFFFFF
(5) Disable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>DP: (6a) Failed
DP-->>OP1: Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment using profile with Fall-Back attribute
Endrnote
|||
Hnote right of SR #FFFFFF
(9)                 Notification procedure over SMS
Endhnote
|||
Rnote over SR #FFFFFF
(10) Check POL2
Endrnote
SR->>ISDR: (11) Cond.:  MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(11a) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.DELETE command FAILED response]SCP80
SR-->>DP: Failed
DP-->>OP1: Failed
Rnote over ISDR #FFFFFF
(11b) Delete disabled ISD-P
and contained profile
Endrnote
ISDR-->>SR: (11c) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(12) Update EIS
Endrnote
SR-->>DP: (13) Profile disabling result
```

```
SR->>OP2: (14) HandleProfileEnabledNotification(eid, iccid2)
SR->>M2MSP: (15) HandleProfileDisabledNotification (eid, iccid)
SR->>M2MSP: (16) HandleProfileEnabledNotification (eid, iccid2)
DP-->>OP1: (17) Profile disabling result
@enduml
```

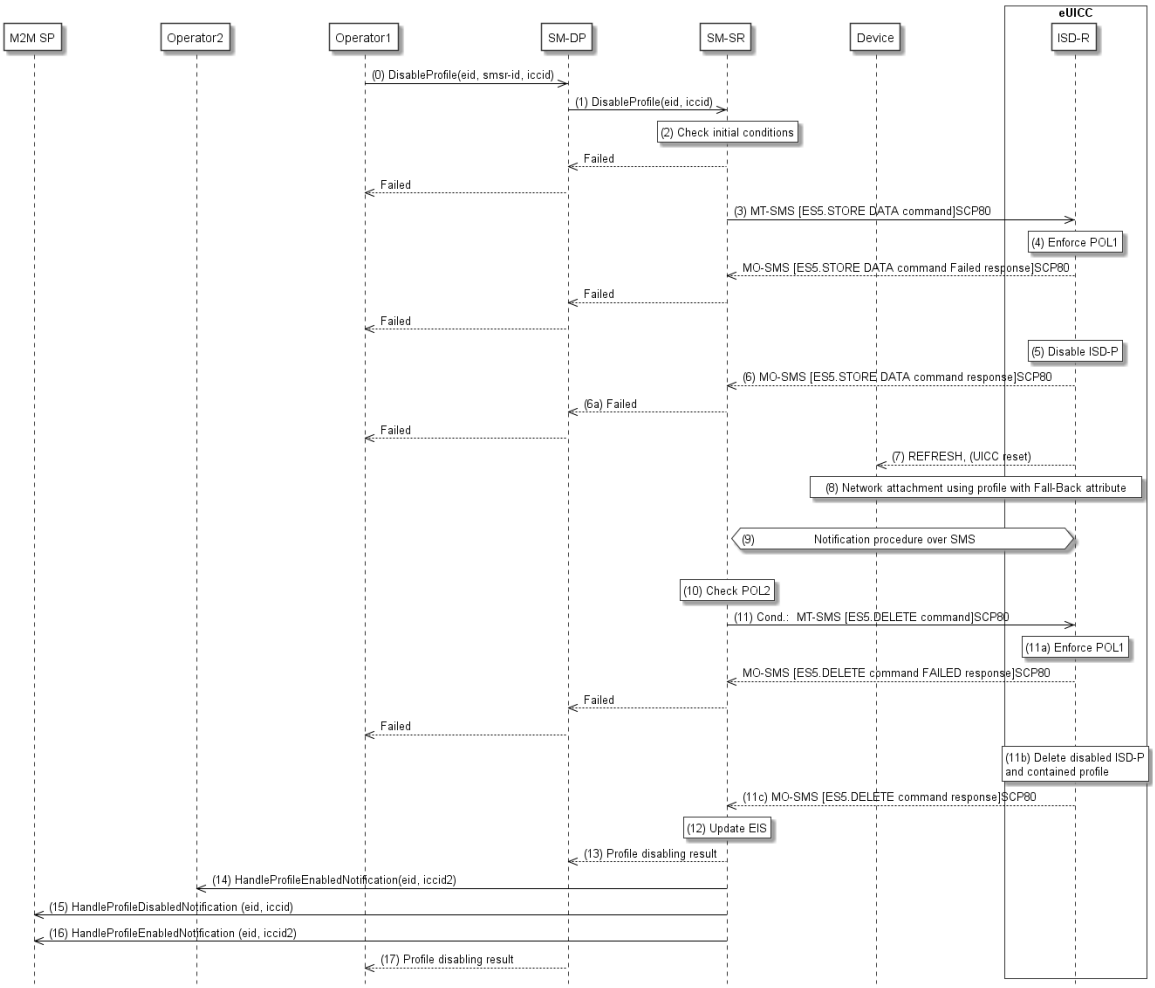


Figure 20: Profile Disabling Via SM-DP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(0) Operator1, the owner of the target Profile, SHALL call the "**ES2.DisableProfile**" function with its relevant input data, see section 5.3.6, in particular the identification of the SM-SR in charge of the management of the target eUICC.

(1) The SM-DP SHALL forward the request to the SM-SR identified by the Operator and SHALL call the "**ES3.DisableProfile**" function with its relevant input data.

Steps (2) to (12) are the same as in the procedure "Profile Disabling" described in section 3.4.

(13) The SM-SR SHALL return the response to the "**ES3.DisableProfile"** function to the SM-DP, indicating that the Profile has been disabled. In case the Profile has also been deleted because of POL1 or POL2, the function execution response SHALL include an

execution status “Executed-With Warning” indicating that the Profile has also been deleted.

(14) Unless Operator2 has set an ONC to not receive those notifications, the SM-SR SHALL send the “**ES4.HandleProfileEnabledNotification**” to Operator2, the owner of the Profile with Fall-Back Attribute set that is now enabled.

(15) The SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" to a M2M SP, if authorised by Operator1 the owner of the Profile that was enabled at the beginning of the procedure.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the “**ES4.HandleProfileDisabledNotification**”.

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the “**ES3.HandleProfileDisabledNotification**”.

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the “**ES2.HandleProfileDisabledNotification**”

(16) The SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to a M2M SP, if authorised by Operator2 the owner of Profile with Fall-Back Attribute set that is now enabled.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the “**ES4.HandleProfileEnabledNotification**”.

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the “**ES3.HandleProfileEnabledNotification**”.

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the “**ES2.HandleProfileEnabledNotification**”.

NOTE: This M2M SP might be the same M2M SP as for Operator1 or any other M2M SP.

(17) Finally, the SM-DP SHALL return the response to the “**ES2.DisableProfile**” function call to Operator1.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.6 Profile and ISD-P Deletion

The Profile and ISD-P deletion procedure between the Operator and the SM-SR is used to delete the target ISD-P with its Profile on the eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.4). The procedure is initiated by the Operator owning the Profile to be deleted. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can be also performed using other transport protocols.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

OP->>SR: (1) DeleteProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP: Failed
Rnote over SR, ISDR #ADD1B2
(3) Optional: If targeted profile is enabled, then
execute function "ES4.DisableProfile"
Endrnote
SR-->>OP: Failed
SR->>ISDR: (4) MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(5) Enforce POL1
Endrnote
|||
Rnote over ISDR #FFFFFF
(6) Delete ISD-P
Endrnote
ISDR-->>SR: (7) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(8) Update EIS
Endrnote
SR-->>OP: (9) Profile deletion result
SR->>M2MSP: (10) Cond: HandleProfileDeletedNotification (eid, iccid)
@enduml
```

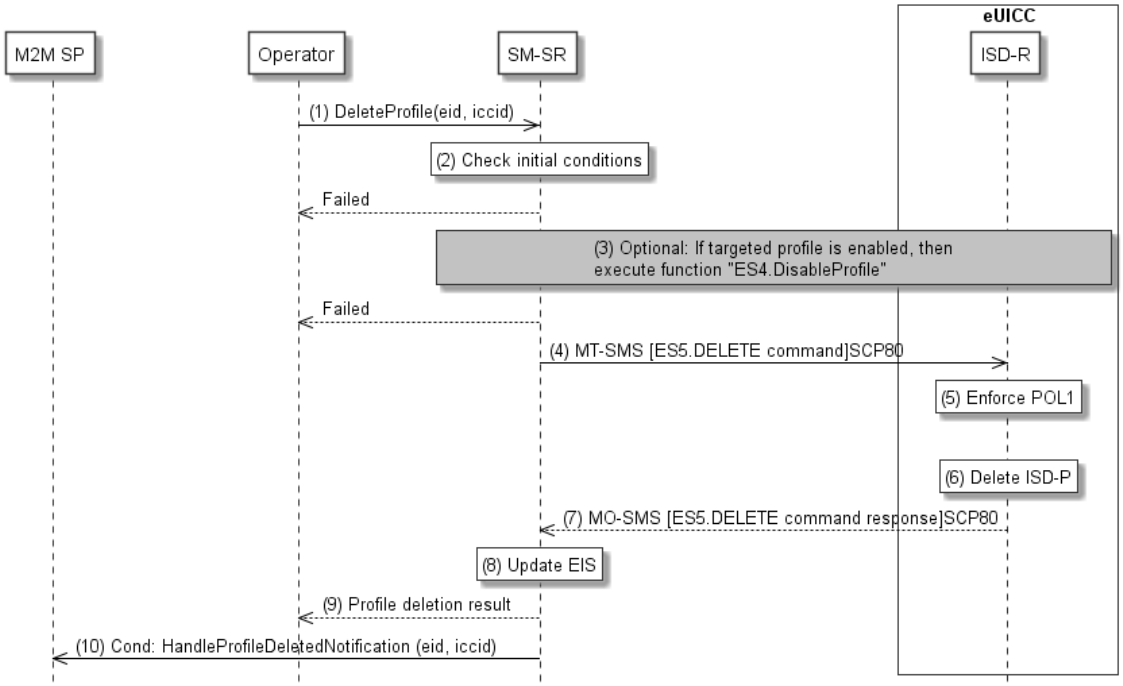


Figure 21: Profile and ISD-P Deletion

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Operator owning the target Profile SHALL call the "**ES4.DeleteProfile**" function with its relevant input data.

(2) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.4.7), and in particular SHALL evaluate POL2 of the target Profile. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR SHALL check the state of the target Profile. If the target Profile is enabled and if POL2 of the target Profile allows it to be disabled, then the SM-SR SHALL execute the "**ES4.DisableProfile**" function to first disable the target Profile (and thus enable the Profile having the Fall-Back Attribute). In case of error, a response indicating the failure is returned to the Operator, and the procedure SHALL end.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective only after the terminal executes the REFRESH command.

(4) The SM-SR SHALL send an MT-SMS containing the "**ES5.DELETE**" command with its relevant input data (see section 4.1.1.4) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.DELETE**" command.

(5) The ISD-R, SHALL enforce POL1. If POL1 rejects deletion of the target Profile, the ISD-R SHALL return directly the MO-SMS containing the response indicating a failure, and the procedure SHALL end.

(6) If POL1 allows, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(7) The ISD-R SHALL return the MO-SMS containing the execution status of the "**ES5.DELETE**" command to the SM-SR.

(8) In case of successful execution, the SM-SR SHALL update the EIS to reflect the newly deleted Profile.

(9) Finally, the SM-SR SHALL return the response to the "**ES4.DeleteProfile**" function to the caller Operator.

(10) The SM-SR SHALL send the "**ES4.HandleProfileDeletedNotification**" to a M2M SP, if authorised by the Operator who owns the Profile, indicating that the profile has been deleted.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileDeletedNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileDeletedNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileDeletedNotification**"

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.7 Profile and ISD-P Deletion Via SM-DP

The Profile and ISD-P deletion procedure is used between the Operator and the SM-DP to delete the target ISD-P with its Profile on the eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.4). The procedure is initiated by the Operator owning the target Profile and is actually performed by the SM-SR in charge of the eUICC management. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can be also performed using other transport protocols.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox
OP->>DP: (1) DeleteProfile(eid, iccid, smsr-id)
DP->>SR: (2) DeleteProfile(eid, iccid)
Rnote over SR #FFFFF
(3) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP: Failed
Rnote over SR, ISDR #ADD1B2
(4) Optional: If targeted profile is enabled, then
execute function "ES4.DisableProfile"
Endrnote
SR-->>DP: Failed
DP-->>OP: Failed
SR->>ISDR: (5) MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(6) Enforce POL1
Endrnote
|||
Rnote over ISDR #FFFFFF
(7) Delete ISD-P
Endrnote
ISDR-->>SR: (8) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(9) Update EIS
Endrnote
SR-->>DP: (10) Profile deletion result
SR->>M2MSP: (11) Cond: HandleProfileDeletedNotification (eid, iccid)
DP-->>OP: (12) Profile deletion result
@enduml
```

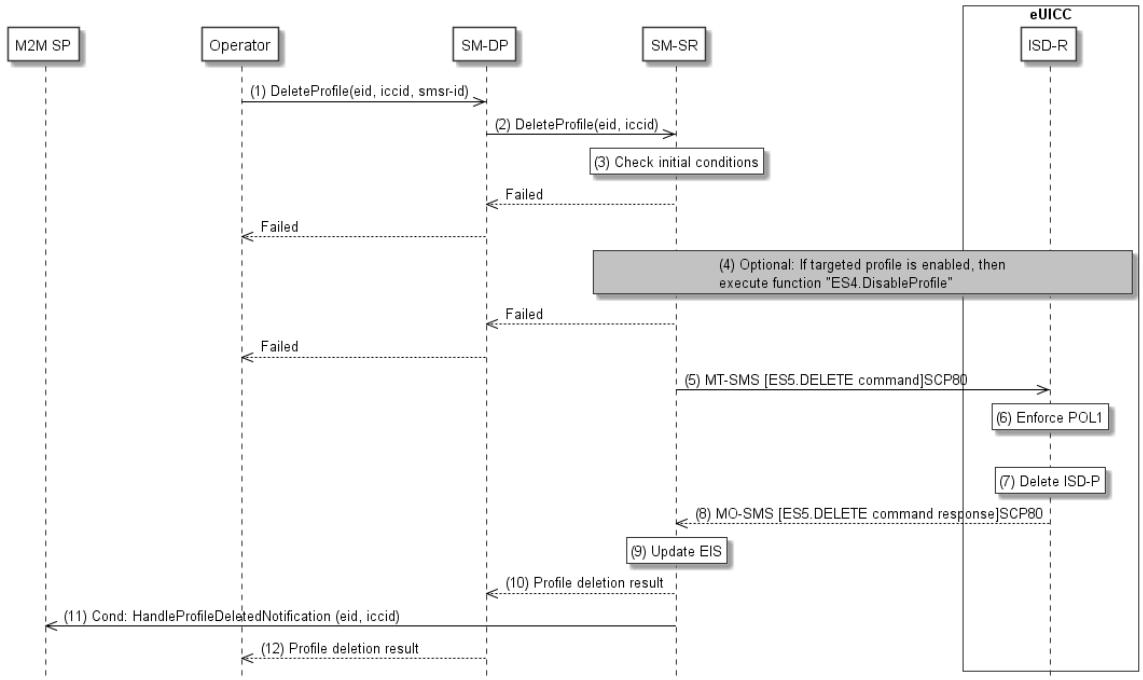


Figure 22: Profile and ISD-P Deletion via SM-DP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Operator owning the Profile which is to be deleted SHALL call the "**ES2.DeleteProfile**" function with its relevant input data (we assume that the Operator knows the identification and the address of the SM-SR, as the Operator has a Profile on the eUICC managed by this SM-SR). The identification and address of the SM-SR in charge of the management of the eUICC SHALL be provided at that time to the SM-DP.

(2) The SM-DP SHALL forward the Operator request to the relevant SM-SR.

(3) The SM-SR SHALL verify if the SM-DP request is acceptable (the verifications that the SM-SR SHALL perform are described in section 5.4.9), and, in particular, SHALL evaluate POL2 of the target Profile. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating a failure, and the procedure SHALL end.

(4) The SM-SR SHALL check the state of the target Profile. If the target Profile is enabled and if POL2 of the target Profile allows it to be disabled, then the SM-SR SHALL execute the "**ES4.DisableProfile**" function to first disable the target Profile (and thus enable the Profile having the Fall-Back Attribute). In case of error, a response indicating the failure SHALL be returned to the SM-DP, who forwards it to the Operator, and the procedure SHALL end.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective only after the terminal executes the REFRESH command.

(5) The SM-SR SHALL send an MT-SMS containing the "**ES5.DELETE**" command with its relevant input data (see section 4.1.1.4) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.DELETE**" command.

(6) The ISD-R SHALL enforce POL1. If POL1 rejects the deletion of the target Profile, the ISD-R SHALL return the MO-SMS containing the response indicating a failure, and the procedure SHALL end.

(7) If POL1 allows its deletion, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(8) The ISD-R SHALL return the MO-SMS to the SM-SR containing the execution status of the "**ES5.DELETE**" command.

(9) In case of successful execution, the SM-SR SHALL update the EIS to reflect the newly deleted Profile.

(10) The SM-SR SHALL return the response to the "**ES3.DeleteISDP**" function to the SM-DP.

(11) The SM-SR SHALL send the "**ES4.HandleProfileDeletedNotification**" to a M2M SP, if authorised by the Operator owning the Profile, indicating that the profile has been deleted.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileDeletedNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileDeletedNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileDeletedNotification**"

(12) Finally, the SM-DP SHALL forward the received response to the Operator.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.8 SM-SR Change

The SM-SR Change procedure is used between the Initiator Operator (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 2.3.1) and the SM-SRs to change the SM-SR for the target eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.11) from SM-SR1 to SM-SR2.

This sequence uses the same key establishment mechanism as section 3.1.2.

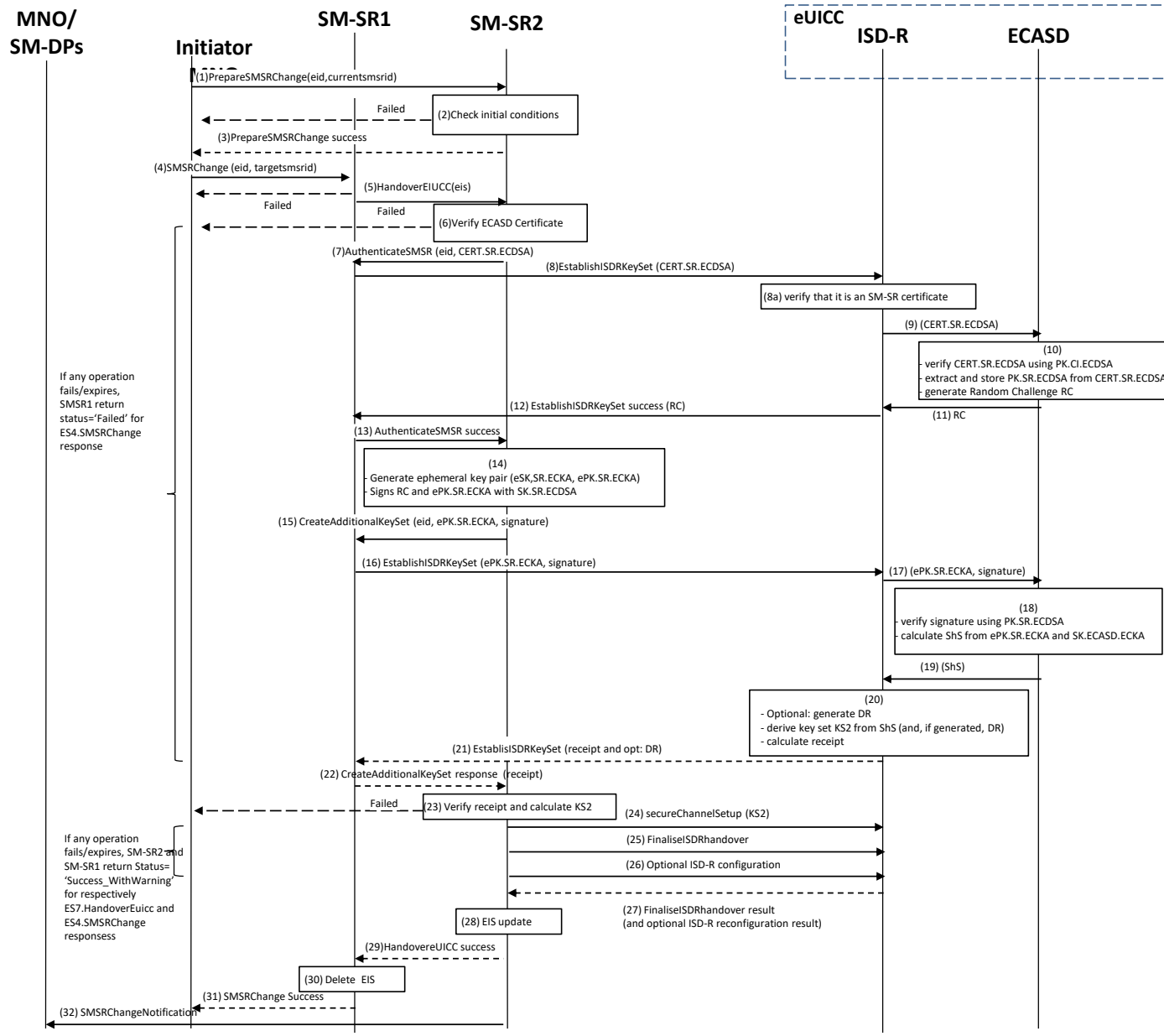


Figure 23: SM-SR Change

NOTE1: The same ISD-R is used by both SM-SRs.

NOTE2: The actions to perform in relationship to the Operator before the SM-SR change are out of scope of this specification.

NOTE3: The settings of the secure connections between the Operators and the SM-SRs are out of scope of this specification.

NOTE4: The interaction between CI and SM-SR2 is out of the scope of this procedure.

NOTE5: Profile Lifecycle Management Authorisations (PLMA, see chapter 3.20 for further details), on SM-SR1 SHALL NOT be taken into account during the change procedure to SM-SR2. If necessary, the operator SHALL perform

the procedures defined in 3.20.1 or 3.20.2 to configure PLMAs on the SM-SR2.

NOTE6: In this procedure, the Initiator should be the Operator1 as it is the one requesting the transfer from SM-SR1 to SM-SR2.

Start Conditions:

a) The EID of the eUICC is known to the Initiator Operator.
a) The two OIDs of the SM-SR1 and SM-SR2 are known to the Initiator Operator.
b) The ISD-R is personalised with the keys of SM-SR1.
c) The change of SM-SR is allowed.
d) SM-SR2 has a certificate signed by the Certificate Issuer (CI).
e) The public key of the CI is stored in the ECASD.

Procedure:

(1) The Initiator Operator SHALL call the "**ES4.PrepareSMSRChange**" function addressing the new SM-SR with the EID as input data.

(2) SM-SR2 SHALL verify that it is prepared to manage this eUICC. A failure at this step will stop the procedure and the error information SHALL be returned to the Initiator Operator.

(3) SM-SR2 SHALL return a response indicating a success.

(4) The Initiator Operator SHALL call the SM-SR1 "**ES4.SMSRChange**" function with its relevant input. SM-SR1 SHALL verify that there is no pending action for the eUICC. SM-SR1 SHALL also reject any new management requests for the target eUICC as long as the procedure is on-going. In case of pending action(s), SM-SR1 SHALL stop the SM-SR Change procedure and indicate that other actions are pending..

(5) SM-SR1 SHALL call the SM-SR2 "**ES7.HandoverEUICC**" function with its relevant input data.

(6) SM-SR2 SHALL verify that:
- It has the capabilities to manage this eUICC.
- The ECASD certificate is valid, using the EUM Certificate and the CI's Root Certificate. The ECASD certificate is part of the EIS and is provided in the HandoverEUICC function. SM-SR2 SHALL extract PK.ECASD.ECKA from the ECASD certificate.

(7) SM-SR2 SHALL call the "**ES7.AuthenticateSMSR**" function specifying the targeted eUICC and providing the certificate identifying SM-SR2, CERT.SR.ECDSA.

a. In case SM-SR1 does not receive call 7 before the expiration of the Validity Period specified by the Initiator Operator at step 4, SM-SR1 SHALL send an error ('Execution Status' indicating 'Failed') to the Operator.

(8) SM-SR1 SHALL call the "**ES5.EstablishISDRKeySet**" function with CERT.SR.ECDSA as input data to authenticate SM-SR2.

(8a) The ISD-R SHALL verify that it is an SM-SR certificate.

(9) The ISD-R SHALL forward the CERT.SR.ECDSA to ECASD.

(10) The ECASD SHALL:
- Verify CERT.SR.ECDSA using PK.CI.ECDSA;
- Extract and store PK.SR.ECDSA from CERT.SR.ECDSA;

- Generate a Random Challenge(RC). The length of the Random Challenge SHALL be 16 or 32.

(11) The ECASD SHALL return the Random Challenge (RC) to the ISD-R.

(12) The ISD-R SHALL return a response indicating a success with the generated Random Challenge RC.

(13) SM-SR1 r SHALL forward the Random Challenge to SM-SR2.

b. In case of failure or expiration in steps 8 to 13, the SM-SR2 SHALL abort the procedure and return an error in ES7.HandoverEuicc response. The SM-SR1 SHALL abort the procedure too and propagate the error to the Initiator Operator.

(14) SM-SR2 SHALL generate an ephemeral key pair (eSK.SR.ECKA, ePK.SR.ECKA) and sign the received Random Challenge (RC) and ePK.SR.ECKA with SK.SR.ECDSA.

(15) SM-SR2 SHALL call the "**ES7.CreateAdditionalKeyset**" function specifying the targeted eUICC and providing the ePK.SR.ECKA and the previously generated signature.

c. In case the Validity Period specified by SM-SR2 does not fit within the time remaining out of the Validity Period specified by the Initiator Operator in step 4, the SM-SR1 SHALL return an error to SM-SR2 indicating that the Validity Period is refused.SM-SR2 MAY then retry call 15 with an acceptable Validity Period

d. In case SM-SR1 does not receive an acceptable call 15 before the expiration of the Validity Period specified by the Initiator Operator at step 4, SM-SR1 SHALL send an error ('Execution Status' indicating 'Failed') to the Operator.

(16) SM-SR1 SHALL call the "**ES5.EstablishISDRKeySet**" function with ePK.SR.ECKA and the signature as input data to request generation of an additional key set KS2.

(17) The ISD-R SHALL forward ePK.SR.ECKA and the signature to ECASD

(18) The ECASD SHALL:

- Verify the signature using PK.SR.ECDSA. If unsuccessful an error SHALL be returned; else
- Calculate ShS from ePK.SR.ECKA and SK.ECASD.ECKA.

(19) The ECASD SHALL return the ShS to the ISD-R

(20) The ISD-R SHALL:

- Optional: generates DR;
- Derive key set from ShS (and, if generated, DR);
- Calculate receipt.

(21) The ISD-R SHALL return a response indicating a success with the calculated receipt and optionally the DR.

(22) SM-SR1 receives and SHALL forward the response to SM-SR2.

NOTE: By checking the consistency of the Validity Period at step 15b, SM-SR1 ensures that its own Validity Period does not expire before step 22.

(23) SM-SR2 SHALL:

- Calculate the ShS from eSK.SR.ECKA and PK.ECASD.ECKA,
- Derive key set KS2 from ShS (and optional DR), and

- Verify the receipt.
- If the verification of the receipt fails, SM-SR2 SHALL send an error to SM-SR1 and SM-SR1 SHALL forward the error to the Initiator Operator.
- If for any reason the procedure fails or expires on SM-SR2 before starting step 24, SM-SR2 SHALL delete the EIS from its database and send an error to SM-SR1, and SM-SR1 SHALL forward the error to the Initiator Operator.

(24) SM-SR2 SHALL open a secure channel (section 2.2.5.1) using the newly created key set KS2.

(25) SM-SR2 SHALL call the "**ES5.FinaliseISDRhandover**" to delete the keys of SM-SR1.

(26) Optionally, SM-SR2 MAY send other commands to update the ISD-R configuration (see NOTE below)

- Personalise other key sets to have the capability to use other secure channels using the PUT KEY command as specified in GlobalPlatform Card Specification v.2.2.1 [6]
- Update the HTTPS parameters of the admin agent in the ISD-R, as specified in GlobalPlatform Card Specification Amendment B [8]
- Update the DNS parameters if this feature is supported by the eUICC and SM-SR2
- Erase the DNS parameters if this feature is not supported by SM-SR2.
- Update the SM-SR addressing parameters of the ISD-R using the function ES5.
- UpdateSMSRAddressingParameters defined in section 4.1.1.10 This update is necessary before the eUICC sends a profile change notification, so SM-SR2 SHALL perform this update before sending any enable or disable profile command, and it SHOULD perform this update as soon as possible (to cover the activation of the Fall-Back Mechanism).

NOTE: SM-SR2 SHOULD perform steps 25 and 26 in a single command script. SM-SR2 MAY provide the corresponding commands in any order.

(27) The ISD-R SHALL return the result of the keys deletion (and the result of optional operations that have been sent at step 26) to SM-SR2.

(28) SM-SR2 SHALL update the EIS to reflect that it now manages the eUICC.

(29) SM-SR2 SHALL return to SM-SR1 that it has successfully registered the eUICC.

e. If SM-SR2 has not received the result of the keys deletion at step 26, or if any of the optional operations failed or expired, SM-SR2 SHALL still return to SM-SR1 that it has registered the eUICC, but SHALL indicate a warning (status "Executed-WithWarning").

(30) SM-SR1 SHALL remove the EIS for the target eUICC, even if SM-SR2 indicated a warning at step 29-a.

(31) SM-SR1 SHALL return the result of the SM-SR change function to the Initiator Operator.

f. If SM-SR2 returned a warning at step 29, SM-SR1 SHALL also return a warning to the Operator

(32) SM-SR2 SHALL call the "**ES4.HandleSMSRChangeNotification**" function, with its relevant input data, to notify the Operators owning the Profiles on the eUICC. In case an Operator has no direct connection with SM-SR2 (SM-SR2 SHALL be able to detect such

situation based on its own database), SM-SR2 SHALL send this notification to the SM-DP authorised by such an Operator by calling the "**ES3.HandleSMSRChangeNotification**" function. SM-SR2 can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to the Operator by calling the "**ES2.HandleSMSRChangeNotification**".

The eUICC SHALL support key establishment with and without the DR. The SM-SR decides which option to use.

BSI TR-03111 [49] contains recommendations and requirements on the generation and validation of ephemeral keys. In addition, NIST SP 800-56A [50] provides requirements on the destruction of ephemeral keys and other intermediate secret data after their use.

End Conditions:

b) The ISD-R is personalised with only the key set of SM-SR2
f) The eUICC is registered within SM-SR2
g) The EIS and EID reside within SM-SR2
h) SM-SR1 is no longer related to the eUICC and its EIS record has been erased
i) The Operator(s) owning the Profile(s) are aware of the change
j) The Initiator Operator is aware of the SM-SR change

Whatever the result and timing of these optional operations, successful completion of the ISD-R key establishment (steps 5 to 23 above), proven by successful verification of the receipt, ensures SM-SR2 is now able to manage the eUICC.

As soon as SM-SR2 has verified the receipt (step23 above), the management of the eUICC is ensured by the new SM-SR2. From this point, SM-SR2 SHALL only return a status "Executed-Success" or "Executed-WithWarning", and SM-SR1 SHALL forward this status to the Initiator Operator and SHALL remove the EIS from its database, so that the Initiator Operator knows with no ambiguity which SM-SR is now managing the eUICC.

In case the deletion of SM-SR1 keys fails or does not complete (which only SM-SR2 knows), SM-SR2 is still responsible for the management of the eUICC.

In case the procedure expires on SM-SR1 side after step 22, even before the procedure completes or expires on SM-SR2, SM-SR1 SHALL inform the Initiator Operator. The Operator MAY then retry the procedure from step 1 or from step 4.

When retrying the procedure, if SM-SR2 had indeed completed step (23) on its side during the first attempt:

- SM-SR2 SHALL skip the steps (7) to (23)
- SM-SR2 SHALL perform steps (24) to (28) (if not already done during the first attempt)
- SM-SR2 SHALL return the response (29) with an indication that the eUICC is already managed

The SM-SR1 SHALL then delete the EIS, and return the response (31) indicating a Success_WithWarning to the Initiator.

3.9 eUICC Registration at SM-SR: Register a New EIS

This procedure is used by the EUM to register an EIS representing an eUICC at the SM-SR. The EIS is required by the SM-SR to perform Platform Management functions and enable Profile Management functions on the eUICC.

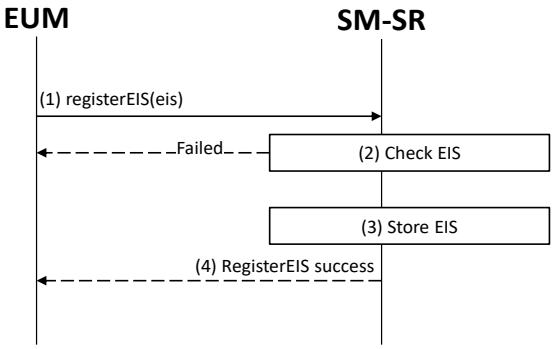


Figure 24: EIS Registration at SM-SR

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

It is assumed that the EUM has been given the SM-SR identity and address by the entity that has ordered the eUICC.

Procedure:

(1) The EUM that has manufactured the eUICC SHALL call the "**ES1.RegisterEIS**" function with the EIS data. The EIS SHALL include the data according to Annex E. The EIS SHALL be signed by the EUM.

(2) The SM-SR SHALL verify that the EUM request is acceptable (the verifications that the SM-SR SHALL perform are described in the section5.2.1). If any of the conditions to be verified is not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR SHALL store the new EIS in its database.

(4) The SM-SR SHALL return the successful response to the "**ES1.RegisterEIS**" function to the caller EUM.

3.10 Master Delete Procedure

This procedure deletes an Orphaned Profile regardless of the Profile's Policy Rules. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can be also performed using other transport protocols.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox
participant "Initiator" as INI #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "Operator" as OP #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
endbox
INI->>SR: (1) Request for Master Delete\n(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>INI: Failed
|||
SR->>DP: (3) Request for Master Delete Authorisation

group Authorisation
Hnote over DP, OP #FFFFF
Requests authorisation
(out of scope)
Endhnote
Rnote over DP  #FFFFF
(4) Check if the request is
authorised and authenticated
Endrnote
end
DP-->>SR: Refuse
SR-->>INI: Refuse
DP->>SR: (5) Master Delete Authorisation response\n (Delete Token)
SR->>ISDR: (6) MT-SMS [ES5.MasterDelete command](Delete Token)
Rnote over ISDR #FFFFF
(7) Check conditions
Endrnote
ISDR-->>SR: Failed
SR-->>INI: Failed
Rnote over ISDR, ISDP #FFFFF
(8) ISD-P verifies the Token
and ISD-R deletes ISD-P and contained profile
Endrnote
ISDR-->>SR: (9) MO-SMS [ES5.MasterDelete command response]
Rnote over SR #FFFFFF
(10) Update EIS
Endrnote
SR-->>INI: (11) Profile deletion result
@enduml
```

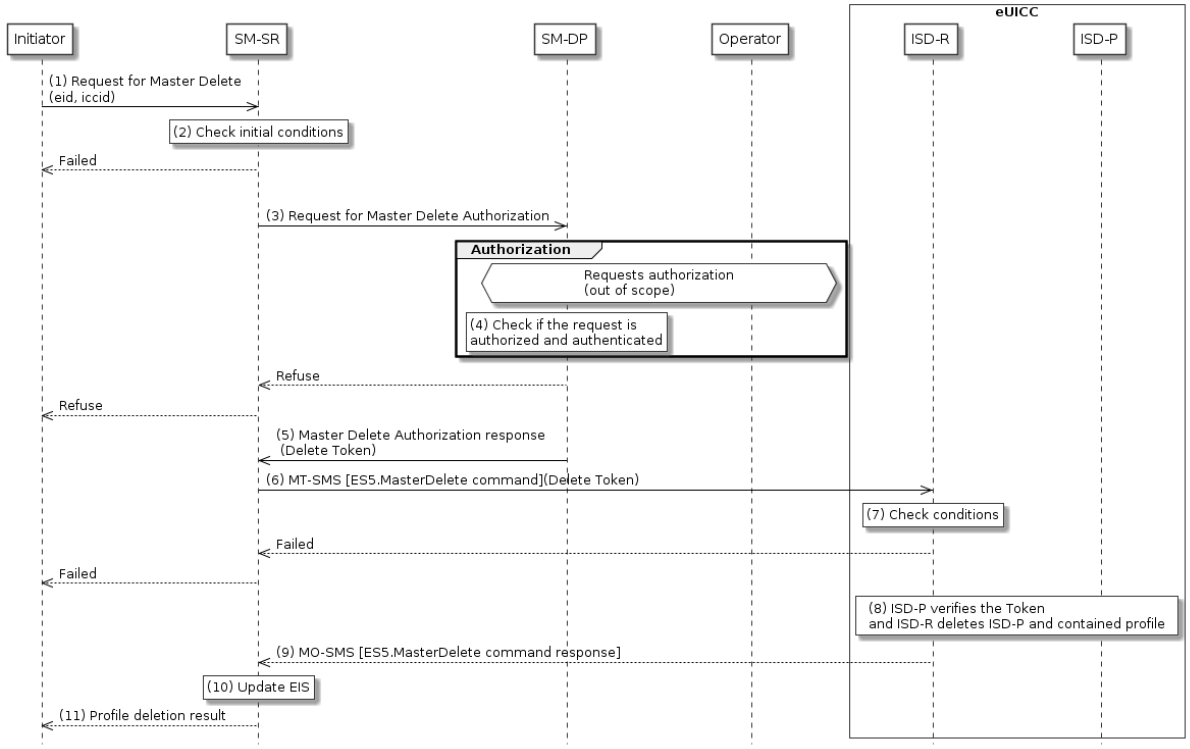


Figure 25: Master Delete

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1], plus:

c) The target Profile has been verified not to be the Profile which has the Fall-Back Attribute set.

Procedure:

(1) The Initiator SHALL send a Master Delete request to the SM-SR containing at least ICCID and EID (the function used in this step is not covered in this specification).

(2) The SM-SR SHALL verify that the request is acceptable (at least the preconditions are satisfied). If any of the verifications fails, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) SM-SR SHALL send a request for Master Delete authorisation to the SM-DP, which is associated with the target Profile (the function used in this step is not covered in this specification).

(4) SM-DP SHALL verify that the request is authenticated and authorised.

The SM-DP also requests authorisation from the Operator owner of the target Profile.

NOTE: The definition of this interface is out of the scope of this document.

If the verification of the request from the SM-SR fails, or if the Operator does not give its authorisation, the SM-DP SHALL return that the deletion of target Profile is not allowed, and the procedure SHALL end.

(5) If deletion of the Profile is allowed, a delete token as defined in section 4.1.1.6, SHALL be returned to the SM-SR.

(6) The SM-SR SHALL send an MT-SMS containing the "**ES5.MasterDelete**" command with its relevant input data (see section 4.1.1.6) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.MasterDelete**" command.

(7) The ISD-R SHALL execute the function as described in section 4.1.1.6. In case of an error, a response indicating the failure SHALL be returned (step 9) to the SM-SR and the procedure SHALL end.

(8) The ISD-P SHALL verify the token and if successful, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(9) The ISD-R SHALL return the MO-SMS containing the execution status of the "**ES5.MasterDelete**" command to the SM-SR.

(10) In case of successful execution, the SM-SR SHALL update the EIS to reflect the deleted Profile.

(11) Finally, the SM-SR SHALL return the response to the Master Delete request to the Initiator (the function used in this step is not covered in this specification).

NOTE 1: The MT SMS and MO-SMS SHALL be secured according to section 2.4.

NOTE 2: The token SHALL be usable only once.

3.11 POL2 Update Via SM-DP

This procedure is used by the Operator to update POL2 via the SM-DP.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox
participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>DP: (1) UpdatePolicyRules(POL2)
DP->>SR: (2) UpdatePolicyRules(POL2)
Rnote over SR #FFFFF
(3) Update POL2
Endrnote
SR-->>DP: (4) UpdatePolicyRules Result
SR->>M2MSP: (5) Cond: HandleProfilePOL2UpdatedNotification (eid, iccid, POL2)
DP-->>OP: (6) UpdatePolicyRules Result
@enduml
```

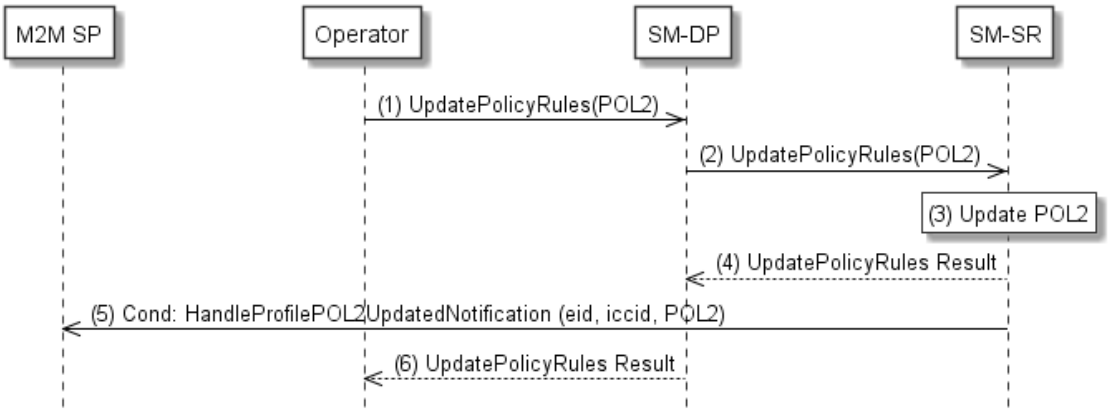


Figure 26: **POL2 Update Via SM-DP**

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Operator owner of the target Profile SHALL call the "**ES2.UpdatePolicyRules**" function with its relevant input data, as described in section 5.3.3, in particular the identification of the SM-SR in charge of the management of the target eUICC.

(2) The SM-DP SHALL forward the request to the SM-SR identified by the Operator and SHALL call the "**ES3.UpdatePolicyRules**" function with its relevant input data, as described in section 5.4.6

(3) The SM-SR SHALL update the POL2 of the targeted eUICC's EIS.

(4) The SM-SR SHALL return the execution status of the "**ES3.UpdatePolicyRules**" to the SM-DP.

(5) The SM-SR SHALL send the "**ES4.HandleProfilePOL2UpdatedNotification**" to a M2M SP, if authorised by Operator owning the Profile, indicating the updated POL2 rules according to chapter 5.1.1.2.2.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfilePOL2UpdatedNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfilePOL2UpdatedNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfilePOL2UpdatedNotification**"

(6) Finally, the SM-DP SHALL return the execution status of the "**ES2.UpdatePolicyRules**" command to the Operator.

3.12 POL1Update by Operator

This procedure allows the Update of POL1 by the Operator via the ES6 interface. For updating the POL1, the Operator SHALL use its OTA Keys hosted in the MNO-SD.

The procedure illustrates the usage of SMS as a possible transport protocol between the Operator and eUICC, but can be also performed using other transport protocols.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox
participant "Operator" as OP #FFFFFF
box "eUICC" #FFFFFF
participant "MNO-SD" as MNO #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
endbox
OP->>MNO: (1) MT-SMS [POL1UpdateByMNO command]SCP80 (POL1)
|||
MNO->>ISDP: (2) POL1 Update command (POL1)
Rnote over ISDP #FFFFF
(3) ISD-P Update POL1
Endrnote
ISDP-->>MNO: (4) POL1 Update command response
|||
MNO-->>OP: (5) MO-SMS [POL1UpdateByMNO command response]SCP80
@enduml
```

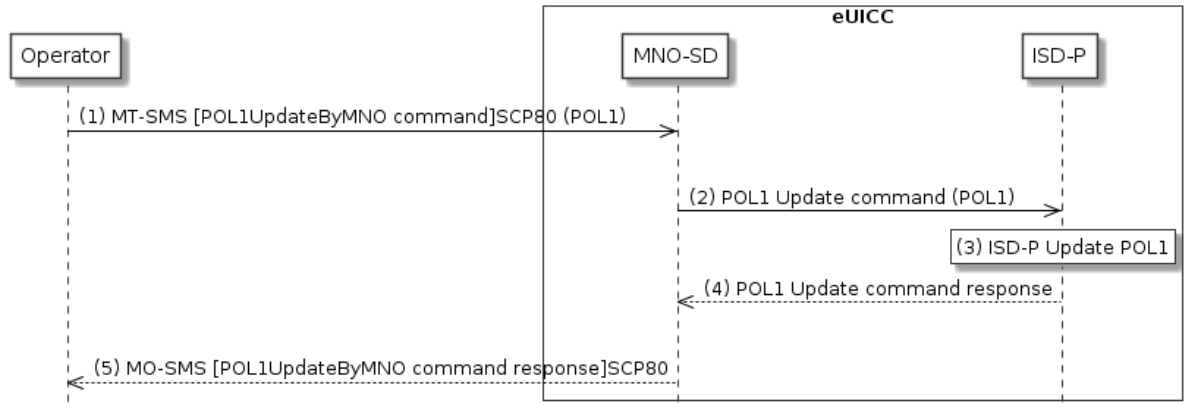


Figure 27: POL1 Update Via Operator

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Operator owning the target Profile SHALL send a MT-SMS containing the "**ES6.UpdatePOL1byMNO**" function with its relevant input data (as described in section 4.1.2.1).

(2) The MNO-SD receives this request and SHALL transfer it to the ISD-P with POL1 as input data.

(3) The ISD-P SHALL process POL1 update of the target profile.

(4) The ISD-P SHALL return the execution status of the "**ES6.UpdatePOL1byMNO**" to MNO-SD.

(5) Finally, the MNO-SD SHALL return the MO-SMS containing the execution status of the "**ES6.UpdatePOL1byMNO**" command to the Operator.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.7.

NOTE2: If the ISD-P and its target profile has the Fall-Back Attribute set, POL1 with "Profile deletion is mandatory when it is disabled" set in this profile, then this POL1 rule will be ignored according to Sections 2.4 and 3.6.3.2 in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

3.13 Connectivity Parameters Update by Operator

This procedure allows the update of the Connectivity Parameters by the Operator on the ES6 interface.

The procedure illustrates the usage of SMS as a possible transport protocol between the Operator and eUICC, but can be also performed using other transport protocols.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox
participant "Operator" as OP #FFFFFF
box "eUICC" #FFFFFF
participant "MNO-SD" as MNO #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
endbox
OP->>MNO: (1) MT-SMS [Connectivity Parameters]SCP80
|||
MNO->>ISDP: (2) Connectivity Parameters Update command
Rnote over ISDP #FFFFF
(3) ISD-P Update
Connectivity Parameters
Endrnote
ISDP-->>MNO: (4)  Connectivity Parameters Update response
|||
MNO-->>OP: (5) MO-SMS [Connectivity Parameters Update command response]SCP80
@enduml
```

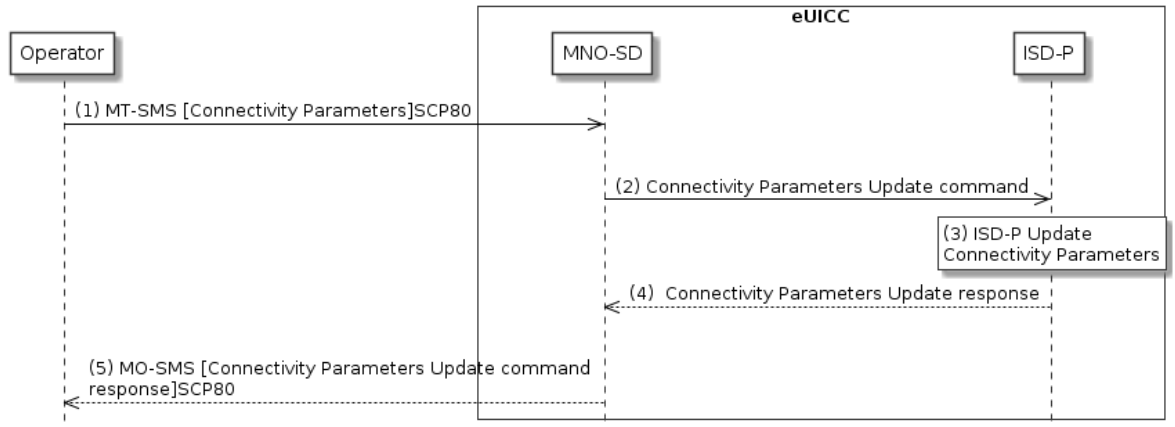


Figure 28: Connectivity Parameters Update by Operator

Start condition:

The Operator wants to update the Connectivity Parameters in their Profile

Procedure:

(1) The Operator owning the target Profile SHALL send a MT-SMS containing the Connectivity Parameters to the MNO-SD.

(2) The MNO-SD SHALL transfer the Connectivity Parameters to the ISD-P.

(3) The ISD-P SHALL update the Connectivity Parameters.

(4) The ISD-P SHALL return the execution status to the MNO-SD.

(5) The MNO-SD SHALL send the MO-SMS containing the execution status to the Operator.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.7.

3.14 Connectivity Parameters Update Using SCP03

This procedure allows the update of the Connectivity Parameters using SCP03by the SM-DP on the ES8 interface.

The procedure illustrates the usage of SMS as a possible transport protocol between the SM-SR and eUICC, where ISD-R is in charge of encapsulating the data in SCP80,. Other transport protocols such as HTTPS or CAT-TP can be used.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox
participant "Operator/SM-DP" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
participant "ISD-P" as ISDP #FFFFFF
endbox
OP->>SR: (1) UpdateConnectivityParametersSCP03\nCommand(Connectivity Parameters
SCP03)
SR->>ISDR: (2)  MT-SMS [Connectivity Parameters SCP03]SCP80
ISDR->>ISDP: (3) (Connectivity Parameters SCP03)
Rnote over ISDP #FFFFF
(4) ISD-P Update
Connectivity Parameters
Endrnote
ISDP-->>ISDR: (5) Connectivity Parameters Update response
|||
ISDR-->>SR: (6) MO-SMS [Connectivity Parameters Update command response]SCP80
SR-->>OP: (7) UpdateConnectivityParametersSCP03 Result
@enduml
```

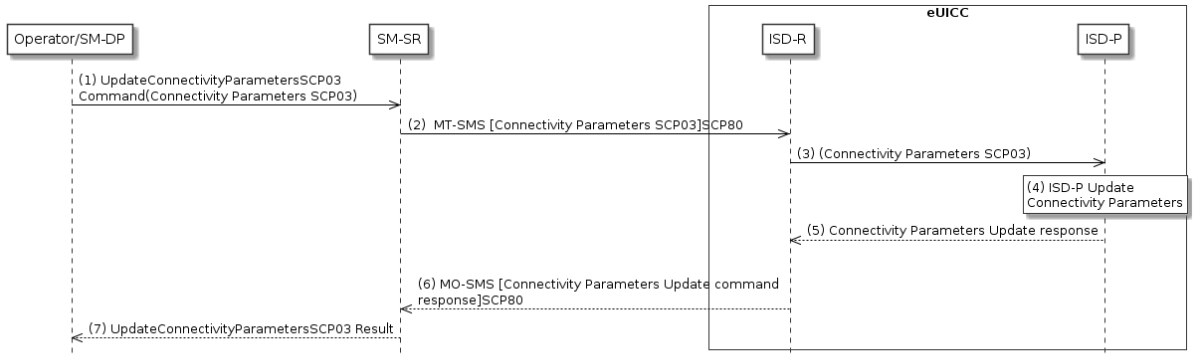


Figure 29: Connectivity Parameters Update Using SCP03

The start conditions are described in [1].

(1) The Operator, or the SM-DP, on behalf of the Operator owning the target Profile, SHALL send a request containing "**ES3.UpdateConnectivityParameters**" function with its relevant input data (as described in section 5.4.6). The <data> parameter SHALL contain an SCP03 script as defined in section 4.1.3.2 including the command "**ES8.UpdateConnectivityParametersSCP03**"

(2) The SM-SR SHALL send a ciphered MT-SMS using SCP80 containing the ciphered data provided by the SM-DP, to the ISD-P TAR according to section 2.5.

(3) The ISD-R SHALL transfer the <data> to the ISD-P.

(4) The ISD-P SHALL update the Connectivity Parameters.

(5) The ISD-P SHALL return the execution status of the "**ES8.UpdateConnectivityParametersSCP03**" to ISD-R.

(6) The ISD-R SHALL send the ciphered MO-SMS containing the execution status of the "**ES8.UpdateConnectivityParametersSCP03**" command to the SM-SR. This execution status is sent from the ISD-P TAR and the ISD-R SHALL apply the security through the SCP80 to this MO-SMS.

(7) Finally, the SM-SR SHALL return the execution status of the "**ES3.UpdateConnectivityParameters**" command to the SM-DP.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.2.5

3.15 Default Notification Procedure

This section provides a default notification procedure from the eUICC to the SM-SR. This default notification carries information about the eUICC and the Device.

This notification is initiated by the eUICC in some conditions:

- First network attachment of the Device: this indicates to the SM-SR in charge of managing of the eUICC that the eUICC has been deployed on the field. The notification of "First network attachment" happens only once in the eUICC's lifetime. It is triggered when the eUICC is network attached the very first time. Nevertheless, note that this notification will be retried until the effective reception by the SM-SR, including further network attachments if not succeeded during the first network attachment session.
- After an explicit new Profile Enabling request: this indicates to the SM-SR which is the Profile which is currently enabled. This notification happens right after the network attachment:
  - With the newly Enabled Profile in case of successful attachment
  - Or with the previously Enabled Profile or with the Profile having the Fall-Back Attribute, after the attachment with the requested Profile has failed.
- After activation of the Fall-Back Mechanism: this indicates to the SM-SR that the Profile with the Fall-Back Attribute has been enabled. This notification happens right after the network attachment.

The notification may happen either on SMS, CAT_TP or HTTPS. The content of the notification message is the same whatever protocol is used. The eUICC is free to select the most relevant protocol according to the Device's capabilities.

The notification has to be confirmed by the SM-SR. The confirmation will depend on the protocol used for notification.

On reception of the SM-SR notification confirmation, the eUICC may perform any operation as specified in one of the procedures including the notification sequence (like for instance deletion of an ISD-P after its disabling, see section 3.6). After the eUICC has performed the follow-up activities, the eUICC SHALL respond to the SM-SR notification confirmation function, including the identification of the operation performed if any.

3.15.1 Notification Using SMS

This figure describes the notification sequence over SMS. It is applicable either for first “power on” of the Device, or the enabling of a Profile (after explicit request or Fall-Back Mechanism).

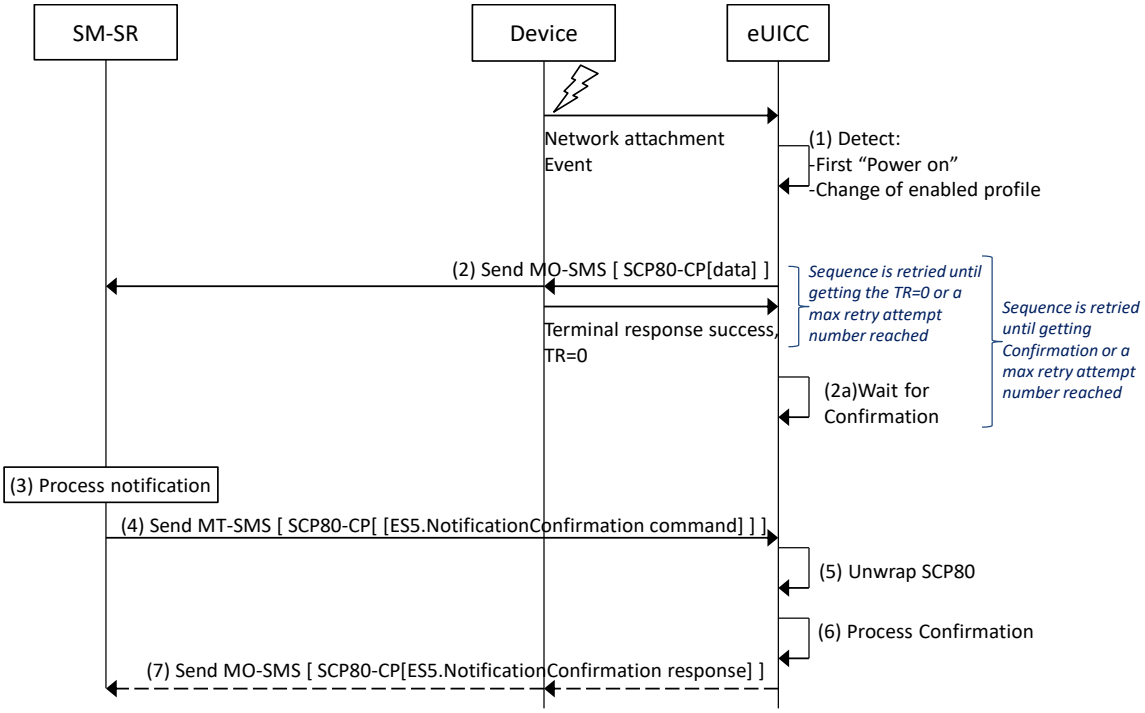


Figure 30: Sequence Flow of Notification Over SMS

(1) At the end of the start-up sequence, the eUICC detects a first “power on” or a situation where the Enabled Profile has changed compared to the previous eUICC reset.

(2) The eUICC sends an MO-SMS envelop. The SMS contains a secure SCP 80 Command Packet (MO-SMS SHALL be formatted as defined in section 2.4.3 with security set to cryptographic checksum and no ciphering, the counter value of the Command Packet SHALL be set to ‘0000000000’ and SPI set to “No counter available”) using the SCP80 keys of the ISD-R, and containing the notification data structure described in section 4.1.1.11. The secured data SHALL be coded as described in section 4.1.1.11.

NOTE: This deviates from the typical secured packets generation defined in ETSI TS 102 225 [4].

The eUICC SHALL use the network information of the Enabled Profile, and the addressing information configured for this profile in ISD-R. If there is no addressing information configured for this profile in ISD-R, the global addressing information configured in ISD-R SHALL be used.

NOTE: This allows using an internal address (network specific number) for the connection of the SM-SR Platform to the SMSC.

The eUICC SHALL retry sending until getting a successful response of the Device (‘0X’). Note, that the eUICC SHALL implement a mechanism to avoid attempting an infinite number of retries. Finally the eUICC SHALL use another protocol in case of final failure for sending the notification using SMS.

(2a) The eUICC SHALL wait for the SM-SR confirmation. If no confirmation is received by the eUICC after a certain amount of time (dependent on the configuration), eUICC SHALL restart from step (2) (with the same sequence number).

(3) The SM-SR processes the notification. If the notification type indicates “Profile change succeeded” but the Validity Period of the corresponding function call has already expired on the SM-SR, the SM-SR SHALL NOT send the “**ES5.HandleNotificationConfirmation**” command defined in section 4.1.1.12.

NOTE: If the eUICC does not receive the confirmation from the SM-SR, the eUICC may retry sending the notification. After having exhausted all possible retries, the eUICC will roll-back to the previously Enabled Profile.

(4) The SM-SR sends an MT-SMS containing the “**ES5. HandleNotificationConfirmation**” command defined in section 4.1.1.12 in a SCP80 command packet. This MT-SMS SHALL target the entity on the eUICC that has sent the notification.

(5) The ISD-R un-wraps the SCP80 security layer

(6) The eUICC processes the notification confirmation data; this may include follow-up activities as required by the procedure where this sequence is used.

(7) The eUICC SHALL return the MO-SMS containing the response of the “**ES5.HandleNotificationConfirmation**” command. The MO-SMS SHALL be secured according to section 2.4.3. The eUICC SHALL retry sending until getting a successful response of the Device (‘0X’). Note, that the eUICC SHALL implement a mechanism to avoid attempting an infinite number of retries.

3.15.2 Notification Using HTTPS

This figure describes the notification sequence over HTTPS. It is applicable either for first “power on” of the Device, or the enabling of a Profile (after explicit request or Fall-Back Mechanism).

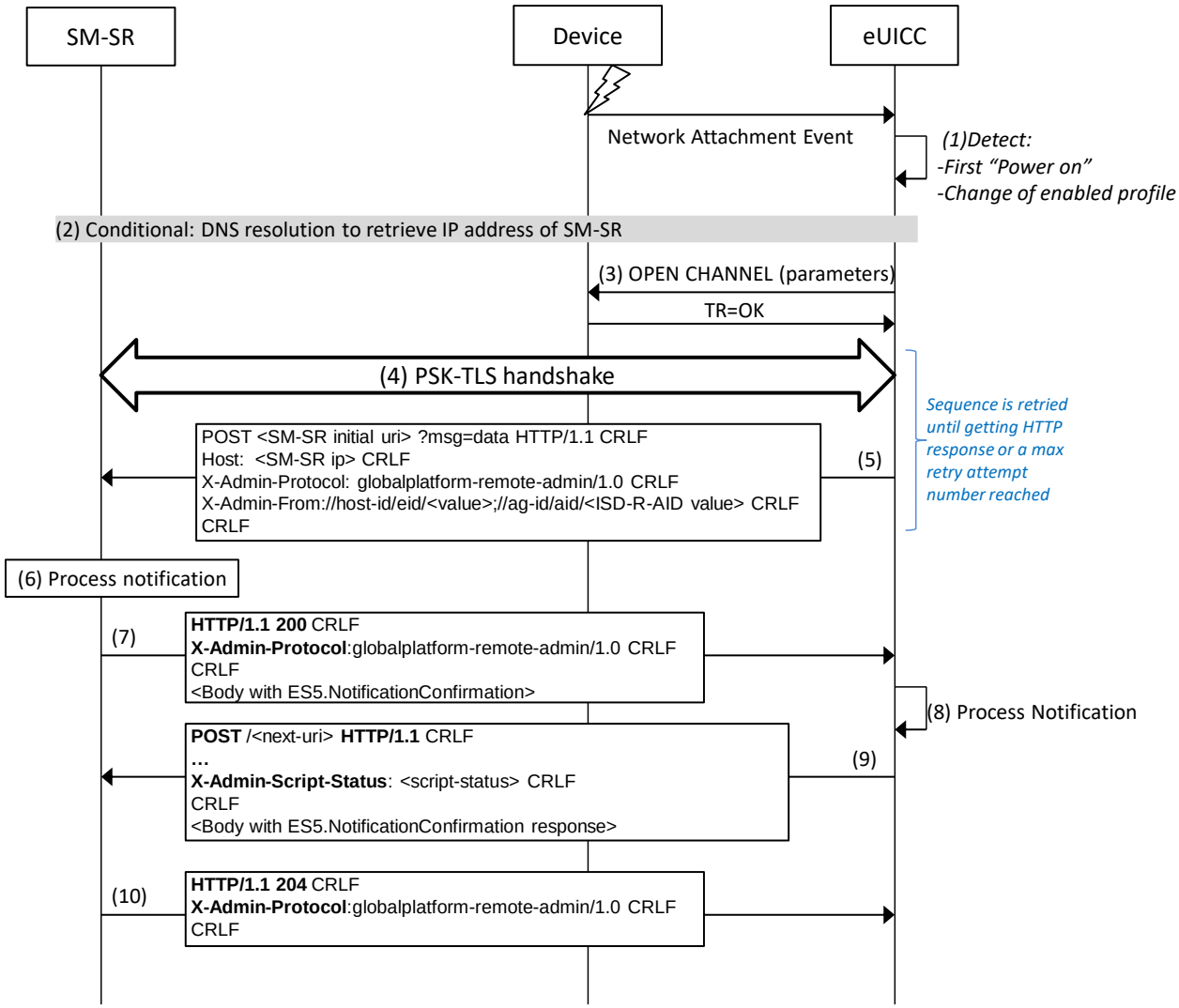


Figure 31: Sequence Flow of Notification Over HTTPS

(1) At the end of the start-up sequence, the eUICC detects a first "power on" or a situation where the Enabled Profile has changed compared to the last eUICC reset.

(2) If DNS resolution is supported and correctly configured on the eUICC, the ISD-R MAY request a DNS resolution first to retrieve the IP Address(es) of the SM-SR, as defined in section 2.4.5.

(3) The eUICC opens a BIP channel with the relevant parameters to address the SM-SR. This includes having access to the Network Access Name, User Login and User Password of the Enabled Profile.

(4) The ISD-R of the eUICC negotiates the PSK-TLS handshake with the SM-SR. The TLS session SHALL be opened as defined in section 2.4.3. The ISD-R SHALL apply the retry Policy as defined in GlobalPlatform Card Specification Amendment B [8].

(5) The eUICC sends the first HTTP POST. The notification contains the SM-SR URL with the special query parameter "?msg" containing the data for eUICC notification defined in section 4.1.1.11. The data of the notification SHALL be coded as hexadecimal string (see section 5.1.1.1) with no spaces.

a. The ISD-R SHALL apply the retry Policy as defined in GlobalPlatform Card Specification Amendment B [8].

(6) The SM-SR processes the notification. If the notification type indicates “Profile change succeeded” but the Validity Period of the corresponding function call has already expired on the SM-SR, the SM-SR SHALL NOT send the “**ES5.HandleNotificationConfirmation**” command defined in section 4.1.1.12.

NOTE: If the eUICC does not receive the confirmation from the SM-SR, the eUICC may retry sending the notification. After having exhausted all possible retries, the eUICC will roll-back to the previously Enabled Profile.

(7) The SM-SR SHALL return an HTTP response with a body containing the “**ES5. HandleNotificationConfirmation**” command acknowledging the reception of the notification.

(8) The eUICC processes the notification confirmation; this may include follow-up activities as required by the procedure where this sequence is used.

(9) The eUICC SHALL return the execution response of the “**ES5. HandleNotificationConfirmation**” command within a new HTTP POST request addressed to the SM-SR.

(10) The SM-SR SHALL return an HTTP response “204 No content”.

3.16 Fall-Back Activation Procedure

The Fall-Back Mechanism SHALL be activated in case of loss of network connectivity by the current Enabled Profile. The eUICC SHALL disable the current Enabled Profile and enable the Profile with Fall-Back Attribute set.

If the current enabled Profile is the Emergency Profile or the Test Profile, the eUICC SHALL NOT activate the Fall-Back Mechanism, until the Local Disable command is called.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator1" as OP1 #FFFFFF
participant "Operator2" as OP2 #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant Device #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

rnote over ISDR
(1) Triggering Fall-Back Mechanism
End rnote

rnote over ISDR
(2) Disable current Profile.
 Enable Fall-Back Profile.
End rnote

ISDR->>Device: (3) REFRESH (UICC reset)

Hnote right of Device #C0C0C0
(4) Network attach
 with the
 enabled profile
End hnote

Hnote over SR, ISDR #C0C0C0
(5) Notification procedure
End hnote

Rnote over SR
(6) EIS Update
End rnote

SR->OP2: (7) Cond: handleProfileEnabledNotification(eid, iccid2)
SR->OP1: (8) Cond: handleProfileDisabledNotification(eid, iccid)
SR->>M2MSP: (9) Cond: HandleProfileEnabledNotification (eid, iccid2)
SR->>M2MSP: (10) Cond: HandleProfileDisabledNotification (eid, iccid)

@enduml
```

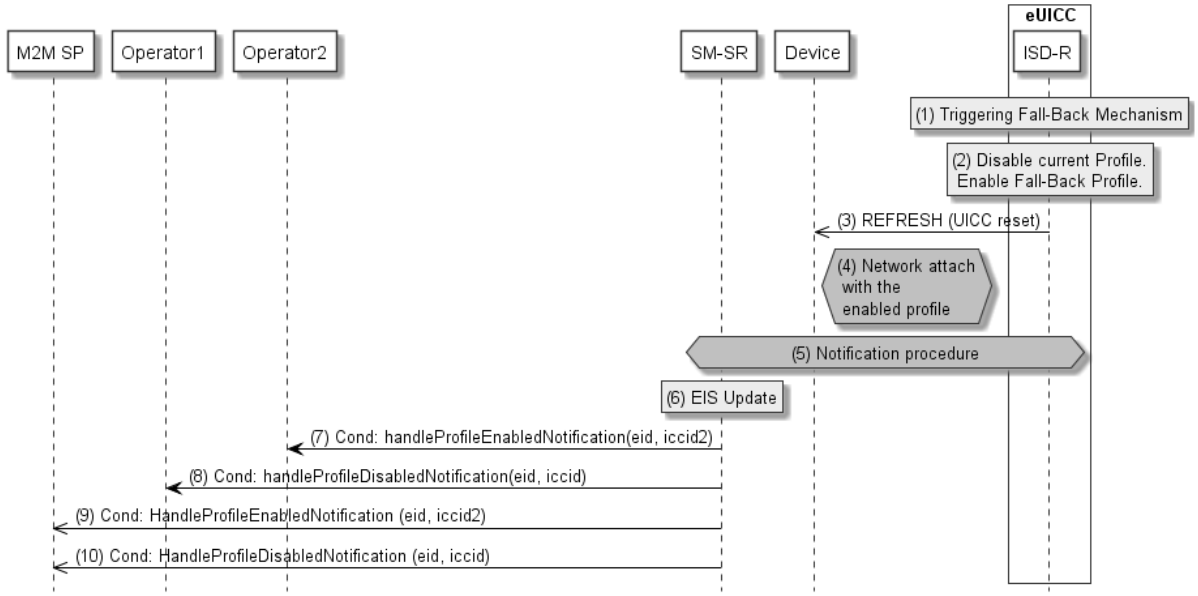


Figure 32: Fall-Back Activation Procedure

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1]

The profile with Fall-Back Attribute set has already been installed and is in disabled state.

Procedure:

(1) The Fall-Back Mechanism is triggered in accordance with the Start Conditions.

(2) Ignoring POL1 of the Enabled Profile, the ISD-R SHALL disable the currently Enabled Profile and SHALL enable the Profile with the Fall-Back Attribute set.

(3) The ISD-R SHALL request the Device to perform the toolkit REFRESH command in UICC Reset mode. This will trigger the execution of the network attach procedure.

(4) The eUICC and the Device SHALL perform a new network attach procedure.

(5) The eUICC SHALL perform the notification procedure as described in section 4.1.1.11. The ISD-R SHALL ensure that all supported Default Notification mechanism will be used to inform SM-SR about the activation of the Fall-Back Mechanism. After having exhausted all possible retries to inform the SM-SR, the eUICC SHALL stay in this state and continue trying to notify the SM-SR. On reception of the notification, the SM-SR is informed that the Fall-Back Mechanism was triggered and the last Enabled Profile has been disabled.

a. If the previously Enabled Profile contains the rule "Profile deletion is mandatory when its state is changed to disabled", the eUICC SHALL NOT automatically delete this Profile.

(6) The SM-SR SHALL update the EIS to reflect that:

- The Profile having the Fall-Back Attribute set has been enabled
- The previously Enabled Profile has been disabled

(7) Unless Operator1 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to Operator2, the owner of Profile with the Fall-Back Attribute set that is now enabled. In case Operator2 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such situation based on its own database), the SM-SR SHALL send this notification to the SM-DP that acts on behalf of

Operator2 by calling the "**ES3.HandleProfileEnabledNotification**". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator2 by calling the "**ES2.HandleProfileEnabledNotification**".

(8) Unless Operator1 has set an ONC to not receive those notifications, thehe SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" to Operator1, the owner of the Profile that was enabled at the beginning of the procedure. In case Operator1 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such a situation based on its own database), the SM-SR SHALL send this notification to the SM-DP that acts on behalf of Operator1 by calling the "**ES3.HandleProfileDisabledNotification**". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator1 by calling the "**ES2.HandleProfileDisabledNotification**".

(9) The SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to an M2M SP, if authorised by Operator2 who owns the Profile with Fall-Back Attribute set that is now enabled.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileEnabledNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileEnabledNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileEnabledNotification**".

(10) The SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" to an M2M SP, if authorised by Operator1 who owns the Profile that was enabled at the beginning of the procedure.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileDisabledNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileDisabledNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileDisabledNotification**".

NOTE: This M2M SP might be the same M2M SP as for Operator1 or any other M2M SP.

If the previously Enabled Profile has the POL1 rule "disable not allowed" or "Profile deletion is mandatory when its state is changed to disabled" set, then:

- the eUICC SHALL only switch back to this Profile
- The eUICC SHALL prevent the execution of the function "Set Fall-Back Attribute"
- it SHALL only be possible to delete this Profile by the Master Delete function.

NOTE: A mechanism MAY permit to request to the eUICC to switch back to the previously enabled profile once the network connectivity has been restored. In this case, after network attachment to the previously Enabled profile succeeds, the eUICC SHALL perform the notification procedure as described in section 4.1.1.11. The ISD-R SHALL ensure that all supported Default Notification mechanism will be used to inform SM-SR that the previously enabled profile has been enabled again. After having exhausted all possible retries to inform the SM-SR, the eUICC SHALL continue trying to notify the SM-SR. On reception of the notification, the SM-SR is informed that the Fall-Back Mechanism is cancelled, and SHALL update the EIS to reflect the new Enabled and Disabled profiles.

The technical solution of the cancellation of the Fall-Back Mechanism mentioned above is out of scope.

3.17 Profile Enabling via M2M SP

The Profile Enabling procedure between the M2M SP and the SM-SR is used to enable a Profile previously downloaded and installed on an eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.16). The procedure is initiated by the M2M SP, based on prior authorisation of the Operator owning the Profile to be enabled, as defined in section 3.20. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can also be performed using other transport protocols.

3.17.1 Normal Case

The sequence flow in the figure below describes the normal case where the target Profile can successfully be enabled.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator2" as OP2 #FFFFFF
participant "Operator1" as OP1 #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

M2MSP->>SR: (1) EnableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->> M2MSP: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->> M2MSP: Failed
Rnote over ISDR #FFFFFF
(5) Enable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->> M2MSP: (6a) Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment with the enabled profile
Endrnote
|||
Hnote right of SR #FFFFFF
(9)                  Notification procedure over SMS
Endhnote
|||
Rnote over SR #FFFFFF
(10) Check POL2
Endrnote
SR->>ISDR: (11) Cond.:  MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(11a) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.DELETE command FAILED response]SCP80
SR-->>M2MSP: Failed
Rnote over ISDR #FFFFFF
(11b) Delete disabled ISD-P
and contained profile
Endrnote
ISDR-->>SR: (11c) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(12) Update EIS
Endrnote
SR-->>M2MSP: (13) Profile enabling result
SR->>OP1: (14) Cond: HandleProfileEnabledNotification (eid, iccid)
SR->>OP2: (15) Cond: HandleProfileDisabledNotification(eid2, iccid2)
SR->>M2MSP: (16) Cond: HandleProfileDisabledNotification(eid2, iccid2)

@enduml
```

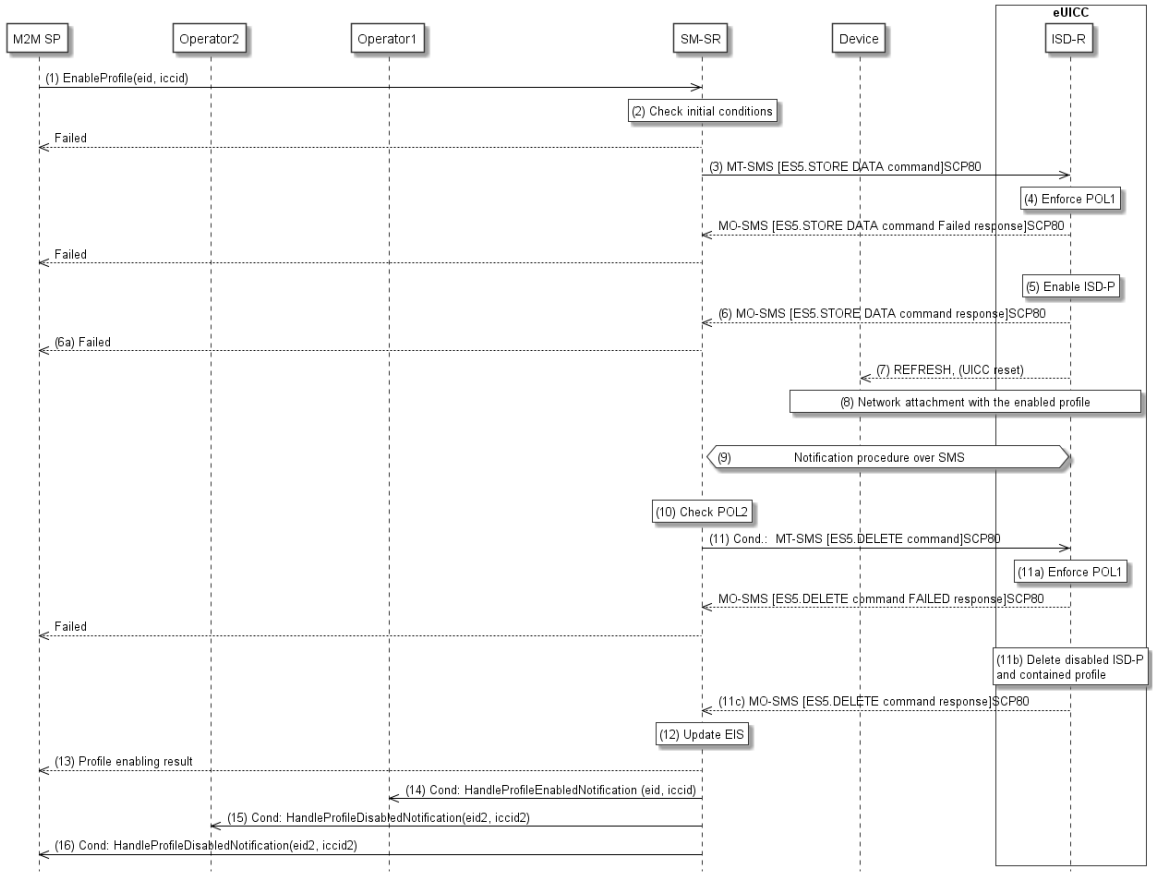


Figure 33: Profile Enabling via M2M SP, Success Case

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To enable the targeted Profile of Operator1 the M2M SP SHALL call the **"ES4.EnableProfile"** function with its relevant input data.

(2) The SM-SR SHALL verify that the M2M SP request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.5.5), and in particular checks that the M2M SP has the authorisation to enable the targeted profile, and evaluates POL2 of the currently Enabled Profile. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR SHALL send an MT-SMS containing the "**ES5.STORE DATA**" command for Profile enabling with its relevant input data (see section 4.1.1.2) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.STORE DATA**" command.

(4) The ISD-R SHALL enforce POL1 of the currently Enabled Profile. If POL1 rejects enabling of the target Profile, the ISD-R SHALL return directly the MO-SMS containing the response indicating a failure, and the procedure SHALL end.

(5) If POL1 allows, the ISD-R SHALL disable the currently enabled ISD-P and enable the targeted ISD-P.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective after the terminal executes the REFRESH command.

(6) The ISD-R SHALL return the MO-SMS containing the execution status of the "**ES5.STORE DATA**" command to the SM-SR.

(6a) If the response to the "**ES5.STORE DATA**" command indicates a failure, the SM-SR SHALL return a response indicating the failure to M2M SP, and the procedure SHALL end.

(7) The ISD-R SHALL send a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

NOTE: In case of any error after this step, indicating that the currently Enabled Profile cannot provide connectivity, the ISD-R SHALL re-enable the previously Enabled Profile as described in section 3.2.2.

(8) The eUICC and the Device SHALL perform a network attach procedure with the newly Enabled Profile.

(9) The eUICC SHALL perform the notification procedure as described in section 4.1.1.11. During this procedure, if the ISD-R doesn't succeed in sending the SMS notification (after having exhausted all possible retries), or doesn't receive the SM-SR notification confirmation ("**ES5.HandleNotificationConfirmation**" command), the ISD-R SHALL consider this as an error, and the previous note SHALL apply.
After successfully verifying the content of the notification confirmation received from the SM-SR (which confirms that the newly Enabled Profile provides connectivity), the eUICC SHALL no longer attempt to re-enable the previously Enabled Profile.
After this verification, if POL1 of the now Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", and this Profile does not have the Fall-Back Attribute set, the ISD-R SHALL delete the disabled ISD-P and the contained Profile. The eUICC SHALL send the response to the notification confirmation indicating whether the disabled ISD-P has been deleted or not.

NOTE: If the SM-SR receives the notification after the expiration of the Validity Period (which was provided to the SM-SR for this function call), it will not send the notification confirmation (see section 3.15.1).

(9a) If the previously Enabled Profile (now Disabled) has the Fall-Back Attribute, and its POL1 contains the rule "Profile deletion is mandatory when its state is changed to disabled", this rule SHALL be ignored according to Sections 2.4 and 3.6.3.2 in GSMA Remote Provisioning Architecture for the Embedded UICC [1], and the procedure SHALL continue at step 10.

(10) On reception of the "**ES5.HandleNotificationConfirmation**" response, and if this response indicates that the Disabled Profile has not been deleted, the SM-SR SHALL evaluate POL2 of the Disabled Profile. If POL2 of the Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", the SM-SR SHALL perform step (11), else it SHALL jump to step (12).

(11) The SM-SR SHALL send an MT-SMS containing the "**ES5.DELETE**" command with its relevant input data (see section 4.1.1.4) to the ISD-R, targeting the Disabled Profile.

The SM-SR SHALL request a PoR to get the execution status of the "**ES5.DELETE**" command.

(11a) The ISD-R SHALL enforce POL1 of the target Profile. If POL1 rejects the deletion of the target Profile, the ISD-R SHALL return the MO-SMS containing the response indicating the corresponding failure, and the procedure SHALL end.

(11b) If POL1 allows its deletion, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(11c) The ISD-R SHALL return the MO-SMS to the SM-SR containing the execution status of the "**ES5.DELETE**" command.

(12) According to the executed sequence and the eUICC responses, the SM-SR SHALL update the EIS to reflect that:

- The target Profile has been enabled
- The previously Enabled Profile has been disabled or deleted.

NOTE: POL1 and POL2 MAY have different content. As a consequence, both the eUICC and the SM-SR have to ensure the ISD-P deletion based on their respective Policy.

(13) The SM-SR SHALL return the response to the "**ES4.EnableProfile**" function to the M2M SP, indicating that the Profile has been enabled.

(14) Unless Operator1 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to Operator1, the owner of the Profile that was disabled at the beginning of the procedure. In case Operator1 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such a situation based on its own database), the SM-SR SHALL send this notification to the SM-DP authorised by Operator1 by calling the "**ES3.HandleProfileEnabledNotification**". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator1 by calling the "**ES2.HandleProfileEnabledNotification**".

(15) Unless Operator1 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileDisabledNotification**" or "**ES4.HandleProfileDeletedNotification**" (if deletion was triggered by the evaluation of POL1 and POL2) to Operator2, the owner of the Profile that was enabled at the beginning of the procedure. In case Operator2 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such a situation based on its own database), the SM-SR SHALL send this notification to the SM-DP authorised by Operator2 by calling the "**ES3.HandleProfileDisabledNotification**" or the "**ES3.HandleProfileDeleted**Notification". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator2 by calling the "**ES2.HandleProfileDisabledNotification**" or the "**ES2.HandleProfileDeletedNotification**".

(16) The SM-SR SHALL send the **"ES4.HandleProfileDisabledNotification"** or **"ES4.HandleProfileDeletedNotification"** (if deletion was triggered by the evaluation of POL1 and POL2) to a M2M SP, if authorised by Operator2 the owner of the Profile that was enabled at the beginning of the procedure.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileDisabledNotification**" or "**ES4.HandleProfileDeletedNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileDisabledNotification**" or "**ES3.HandleProfileDeletedNotification**".
Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileDisabledNotification**" or "**ES2.HandleProfileDeletedNotification**".

NOTE: This M2M SP might be the same M2M SP as for Operator1 or any other M2M SP.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.17.2 Connectivity Failure Case

The sequence flow in the figure below describes the case where the target Profile cannot provide connectivity after it is enabled, and when roll-back to the previously Enabled Profile occurs.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP1 #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

M2MSP->>SR: (1) EnableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>M2MSP: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>M2MSP: Failed
Rnote over ISDR #FFFFFF
(5) Enable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>M2MSP: (6a) Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment with the enabled profile **fails**
                              OR
                  Notification procedure **fails**
Endrnote
|||
Hnote over ISDR #FFFFFF
(9) Enable previous ISD-P
Endhnote
ISDR-->>DEV: (10) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(11) Network attachment with the enabled profile
Endrnote
|||
Hnote right of SR #FFFFFF
(12)                Notification procedure over SMS
Endhnote
|||
SR-->>M2MSP: (13) Profile enabling failure
@enduml
```

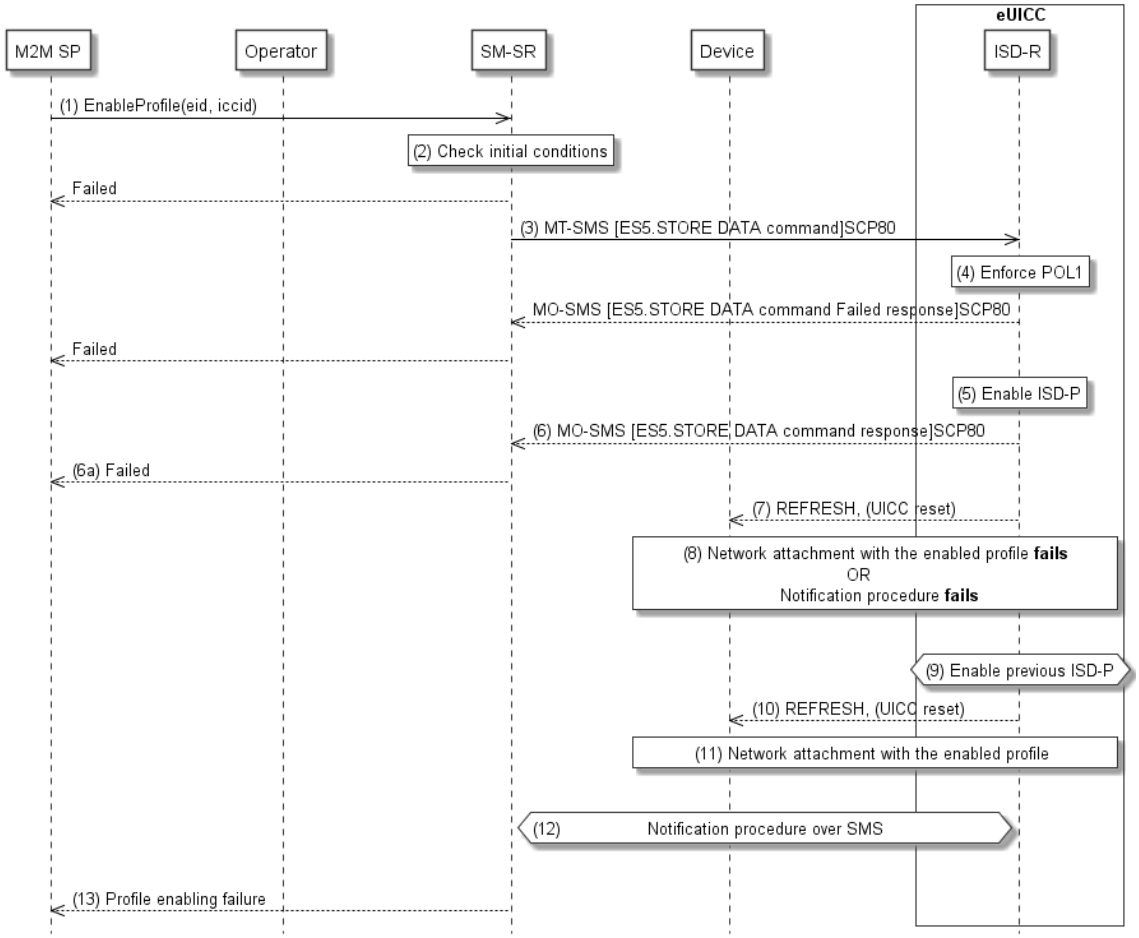


Figure 34: Profile Enabling via M2M SP, Failure Case with roll-back

Start Conditions:

The start conditions are identical to section 3.17.1

Procedure:

Steps (1), (2), (3), (4), (5), (6), (6a) and (7) are also identical to section 3.17.1.

(8) A network attach failure occurs indicating that the Enabled Profile cannot provide connectivity, or the eUICC doesn't succeed to send the SMS notification (after having exhausted all possible retries), or doesn't receive the SM-SR notification confirmation.

(9) The ISD-R SHALL enable the Profile that was previously enabled before the reception of the command, to re-establish connectivity.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective only after the terminal executes the REFRESH command.

(10) The ISD-R sends a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a new network attach procedure.

(11) The eUICC and the Device SHALL perform a new network attach procedure with the Profile Enabled before the start of the procedure.

(12) The eUICC SHALL perform the notification procedure as described in section 4.1.1.11. On reception of the SMS notification, the SM-SR is informed that the target Profile has not been enabled. In order to minimize the notification retries on eUICC side, the SM-SR SHALL send the "**ES5.HandleNotificationConfirmation**" command defined in section 4.1.1.12 even if the Validity Period specified in the "**ES4.EnableProfile**" command has expired.

(13) Finally, the SM-SR SHALL return the response to the "**ES4.EnableProfile**" function to the M2M SP, indicating a failure, the target Profile didn't succeed to provide the connectivity.

3.18 Profile Disabling via M2M SP

The Profile Disabling procedure between the M2M SP and the SM-SR is used to disable a Profile previously downloaded and installed on an eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.17). The procedure is initiated by the M2M SP, based on prior authorisation of the Operator owning the Profile to be disabled, as defined in section 3.20. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can also be performed using other transport protocols.

The sequence flow in the figure below describes the normal case where the target Profile can successfully be disabled.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator2" as OP2 #FFFFFF
participant "Operator1" as OP1 #FFFFFF
participant "SM-SR" as SR #FFFFFF
participant "Device" as DEV #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

M2MSP->>SR: (1) DisableProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>M2MSP: Failed
SR->>ISDR: (3) MT-SMS [ES5.STORE DATA command]SCP80
Rnote over ISDR #FFFFFF
(4) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.STORE DATA command Failed response]SCP80
SR-->>M2MSP: Failed
Rnote over ISDR #FFFFFF
(5) Disable ISD-P
Endrnote
ISDR-->>SR: (6) MO-SMS [ES5.STORE DATA command response]SCP80
SR-->>M2MSP: (6a) Failed
ISDR-->>DEV: (7) REFRESH, (UICC reset)
Rnote over DEV, ISDR #FFFFFF
(8) Network attachment using profile with Fall-Back attribute
Endrnote
|||
Hnote right of SR #FFFFFF
(9)                  Notification procedure over SMS
Endhnote
|||
Rnote over SR #FFFFFF
(10) Check POL2
Endrnote
SR->>ISDR: (11) Cond.:  MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(11a) Enforce POL1
Endrnote
ISDR-->>SR: MO-SMS [ES5.DELETE command FAILED response]SCP80
SR-->>M2MSP: Failed
Rnote over ISDR #FFFFFF
(11b) Delete disabled ISD-P
and contained profile
Endrnote
ISDR-->>SR: (11c) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(12) Update EIS
Endrnote
SR-->>M2MSP: (13) Profile disabling result
SR->>OP1: (14) Cond: HandleProfileDisabledNotification(eid, iccid)
SR->>OP2: (15) Cond: HandleProfileEnabledNotification(eid, iccid2)
SR->>M2MSP: (16) Cond: HandleProfileEnabledNotification(eid, iccid2)
@enduml
```

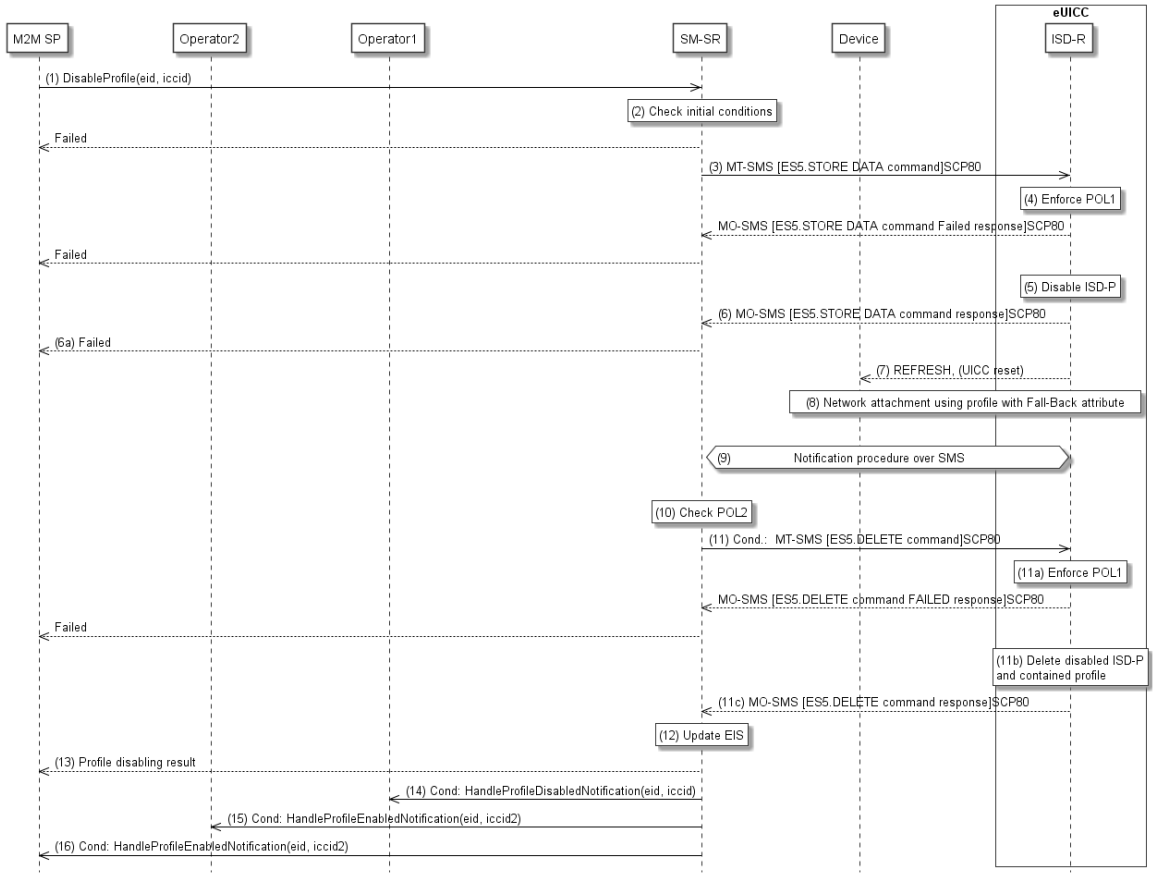


Figure 35: Profile Disabling via M2M SP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To disable the targeted Profile of Operator1 the M2M SP SHALL call the **"ES4.Disable.Profile"** function with its relevant input data.

(2) The SM-SR SHALL verify that the M2M SP request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.5.6, and in particular checks that the targeted Profile is enabled, that the M2M SP has the authorisation to disable the targeted profile, and that Profile disabling is allowed in POL2. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR SHALL send an MT-SMS containing the "**ES5.STORE DATA**" command for Profile disabling with its relevant input data (see section 4.1.1.3) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the "**ES5.STORE DATA**" command.

(4) The ISD-R SHALL enforce POL1 of the currently Enabled Profile. In case POL1 rejects disabling, the ISD-R SHALL return PoR containing the response indicating a failure, and the procedure SHALL end.

(5) The ISD-R SHALL disable the targeted ISD-P and the contained Profile and SHALL enable the Profile with the Fall-Back Attribute set.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective only after the terminal executes the REFRESH command.

(6) The ISD-R SHALL return the MO-SMS containing the execution status of the "**ES5.STORE DATA**" command to the SM-SR.

(6a) If the response to the "**ES5.STORE DATA**" command indicates a failure, the SM-SR SHALL return a response indicating the failure to M2M SP, and the procedure SHALL end.

(7) The ISD-R sends a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

NOTE: In case of any error after this step indicating that the current Enabled Profile cannot provide connectivity, the ISD-R SHALL re-enable the previously Enabled Profile as described in section 3.2.2.

(8) The eUICC and the Device SHALL perform a new network attach procedure with the Profile with the Fall-Back Attribute set.

(9) The eUICC SHALL perform the notification procedure as described in section 4.1.1.11. During this procedure, if ISD-R doesn't succeed to send the SMS notification, or doesn't receive the SM-SR notification confirmation ("**ES5.HandleNotificationConfirmation**" command), the ISD-R SHALL consider this as an error, and the previous note SHALL apply.
After successfully verifying the content of the notification confirmation received from the SM-SR (which confirms that the newly Enabled Profile provides connectivity), the eUICC SHALL no longer attempt to re-enable the previously Enabled Profile.
After this verification, if POL1 of the Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", the ISD-R SHALL delete the disabled ISD-P and the contained Profile. The eUICC SHALL send the response to the notification confirmation indicating whether the disabled ISD-P has been deleted or not.

NOTE: If the SM-SR receives the notification after the expiration of the Validity Period (which was provided to the SM-SR for this function call), it will not send the notification confirmation (see section 3.15.1).

(10) On reception of the **ES5.HandleNotificationConfirmation** response, and if the **ES5.HandleNotificationConfirmation** response indicates that the Disabled Profile has not been deleted, the SM-SR SHALL evaluate POL2 of the Disabled Profile. If POL2 of the Disabled Profile contains the rule "Profile deletion is mandatory when it is disabled", the SM-SR SHALL perform step (11), else it SHALL jump to step (12).

(11) The SM-SR SHALL send an MT-SMS containing the "**ES5.DELETE**" command with its relevant input data (see section 4.1.1.4) to the ISD-R, targeting the Disabled Profile.

The SM-SR SHALL request a PoR to get the execution status of the "**ES5.DELETE**" command.

(11a) The ISD-R SHALL enforce POL1 of the target Profile. If POL1 rejects the deletion of the target Profile, the ISD-R SHALL return the MO-SMS containing the response indicating the corresponding failure, and the procedure SHALL end.

(11b) If POL1 allows its deletion, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(11c) The ISD-R SHALL return the MO-SMS to the SM-SR containing the execution status of the "**ES5.DELETE**" command.

(12) According to the executed sequence and the eUICC responses, the SM-SR SHALL update the EIS to reflect that:

- The Profile having the fall-back attribute has been enabled
- The previously Enabled Profile has been disabled or deleted.

NOTE: POL1 and POL2 MAY have different content. As a consequence, both the eUICC and the SM-SR have to ensure the ISD-P deletion based on their respective Policy.

(13) The SM-SR SHALL return the response to the "**ES4.DisableProfile**" function to M2M SP, indicating that the Profile has been disabled. In case the Profile has also been deleted because of POL1 or POL2, the function execution response SHALL include an execution status "Executed-WithWarning" indicating that the Profile has also been deleted.

(14) Unless Operator1 has set an ONC to not receive those notifications, the SM-SR SHALL send the "ES4.HandleProfileDisabledNotification" to Operator1, the owner of the Profile that was enabled at the beginning of the procedure. In case the Profile has also been deleted because of POL1 or POL2, the function execution response SHALL include an execution status "Executed-WithWarning" indicating that the Profile has also been deleted. In case Operator1 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such a situation based on its own database), the SM-SR SHALL send this notification to the SM-DP authorised by Operator1 by calling the "ES3.HandleProfileEnabledNotification". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator1 by calling the "ES2.HandleProfileEnabledNotification".

(15) Unless Operator2 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileEnabledNotification**" to Operator2, the owner of Profile with Fall-Back Attribute set that is now enabled. In case Operator2 has no direct connection with the SM-SR (SM-SR SHALL be able to detect such situation based on its own database), the SM-SR SHALL send this notification to the SM-DP authorised by Operator2 by calling the "**ES3.HandleProfileEnabledNotification**". The SM-SR can retrieve the SM-DP identity based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to Operator2 by calling the "**ES2.HandleProfileEnabledNotification**".

(16) The SM-SR SHALL also send the **"ES4.HandleProfileEnabledNotification"** to a M2M SP, if authorised by Operator2 the owner of Profile with Fall-Back Attribute set that is now enabled.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileEnabledNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileEnabledNotification**".

Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileEnabledNotification**".

NOTE: This M2M SP might be the same M2M SP as for Operator1 or any other M2M SP.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.19 Profile and ISD-P Deletion via M2M SP

The Profile and ISD-P deletion procedure between the M2M SP and the SM-SR is used to delete the target ISD-P with its Profile on the eUICC (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.18). The procedure is initiated by the M2M SP, based on prior authorisation of the Operator owning the Profile to be deleted, as defined in section 3.20. The procedure illustrates the usage of SMS as a possible transport protocol between SM-SR and eUICC, but can be also performed using other transport protocols.

The sequence flow in the figure below describes the normal case where the target Profile can successfully be deleted.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF
box "eUICC" #FFFFFF
participant "ISD-R" as ISDR #FFFFFF
endbox

M2MSP->>SR: (1) DeleteProfile(eid, iccid)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>M2MSP: Failed
Rnote over SR, ISDR #ADD1B2
(3) Optional: If targeted profile is enabled, then
execute function "ES4.DisableProfile"
Endrnote
SR-->>M2MSP: Failed
SR->>ISDR: (4) MT-SMS [ES5.DELETE command]SCP80
Rnote over ISDR #FFFFFF
(5) Enforce POL1
Endrnote
|||
Rnote over ISDR #FFFFFF
(6) Delete ISD-P
Endrnote
ISDR-->>SR: (7) MO-SMS [ES5.DELETE command response]SCP80
Rnote over SR #FFFFFF
(8) Update EIS
Endrnote
SR-->>M2MSP: (9) Profile deletion result
SR->>OP: (10) HandleProfileDeletedNotification(eid, iccid)
@enduml
```

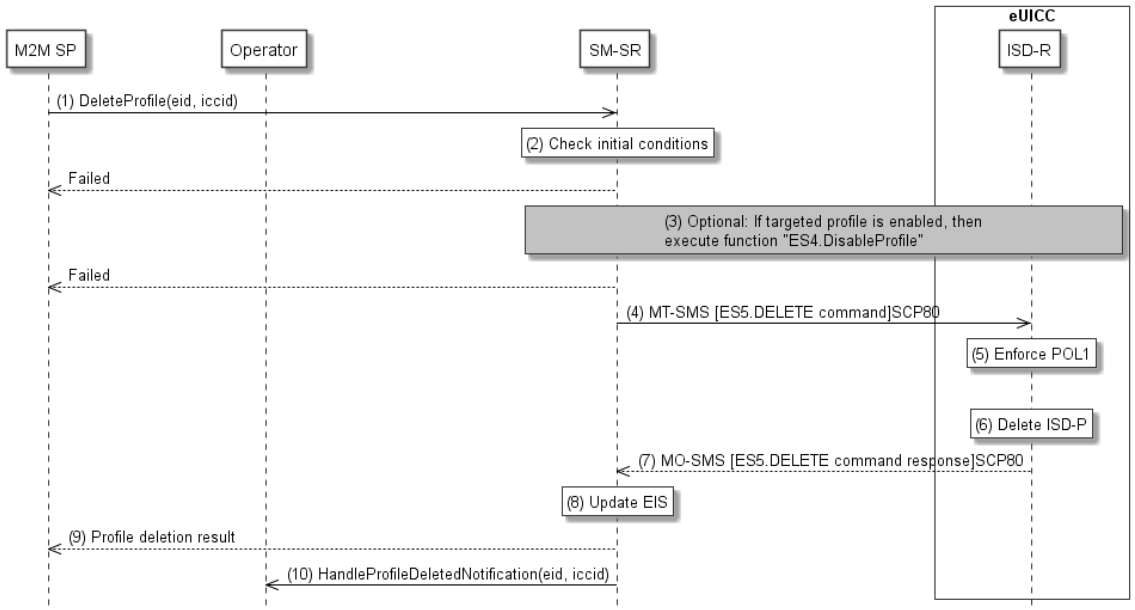


Figure 36: Profile and ISD-P Deletion via M2M SP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To delete the targeted Profile of the Operator the M2M SP SHALL call the "**ES4.DeleteProfile**" function with its relevant input data.

(2) The SM-SR SHALL verify that the M2M SP request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.4.7), and in particular checks that the M2M SP has the authorisation to enable the targeted profile, and evaluates POL2 of the target Profile. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR SHALL check the state of the target Profile. If the target Profile is enabled and if POL2 of the target Profile allows it to be disabled, then the SM-SR SHALL execute the **"ES4.DisableProfile"** function to first disable the target Profile (and thus enable the Profile having the Fall-Back Attribute). In case of error, a response indicating the failure is returned to the M2M SP, and the procedure SHALL end.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the targeted ISD-P is marked as enabled in this step, it MAY actually become effective only after the terminal executes the REFRESH command.

(4) The SM-SR SHALL send an MT-SMS containing the **"ES5.delete"** command with its relevant input data (see section 4.1.1.4) to the ISD-R. The SM-SR SHALL request a PoR to get the execution status of the **"ES5.delete"** command.

(5) The ISD-R, SHALL enforce POL1. If POL1 rejects deletion of the target Profile, the ISD-R SHALL return directly the MO-SMS containing the response indicating a failure, and the procedure SHALL end.

(6) If POL1 allows, the ISD-R SHALL delete the targeted ISD-P and the contained Profile.

(7) The ISD-R SHALL return the MO-SMS containing the execution status of the "ES5.DELETE" command to the SM-SR.

(8) In case of successful execution, the SM-SR SHALL update the EIS to reflect the newly deleted Profile.

(9) The SM-SR SHALL return the response to the **"ES4.DeleteProfile"** function to the M2M SP, indicating that the Profile has been deleted.

(10) Unless the Operator has set an ONC to not receive those notifications, the SM-SR SHALL send the **"ES4.HandleProfileDeletedNotification"** to the Operator, the owner of the Profile. In case the Operator has no direct connection with the SM-SR (SM-SR SHALL be able to detect such a situation based on its own database), the SM-SR SHALL send this notification to the SM-DP authorised by the Operator by calling the **"ES3.HandleProfileDeletedNotification"**. The SM-SR can retrieve the SM-DP identity

based on the EIS content. Then the SM-DP, on reception of this notification, SHALL forward it to the Operator by calling the **"ES2.HandleProfileDeletedNotification"**.

NOTE: The MT-SMS and MO-SMS SHALL be secured according to section 2.4.

3.20 Profile Lifecycle Management Authorisation (PLMA)

The Profile Lifecycle Management Authorisation (PLMA) mechanisms described in this section allows the Operator and owner of Profiles to grant authorisations to an M2M SP to perform certain operations, or receive certain notifications, related to a set of Profiles, identified by a Profile Type. A list of available operations and notification for the M2M SP can be found in section 5.1.1.2.14.

The Operator can manage the PLMA for its own Profiles through a dedicated Operator / SM-SR interface, as described in section 5.7 or through its Operator / SM-DP interface as described in sections 5.3.13 and 5.3.14.

A "PLMA" is a combination of identifiers and authorised actions:

- **Identifiers**: List of identifiers to identify the Operator, M2M SP and Profile Type; see section 5.1.1.2.14 for details

- **Authorised actions:** List of operations and notifications; see section 5.1.1.2.14 for details

NOTE: It should be considered that the role of a M2M SP can also be played by a partner Operator or affiliate from the Operator, who is responsible to provide Profile Lifecycle Management Authorisations to its own profile(s).

3.20.1 Set Profile Lifecycle Management Authorisation

The Set Profile Lifecycle Management Authorisation (PLMA) procedure between the Operator and the SM-SR is used to authorise the M2M SP for the profile lifecycle management of the Operator owned Profile installed on an eUICC, and to authorise the reception of notifications when the status of the authorised Profile on the eUICC has changed (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15.1). The PLMA contains the authorised operations and notifications and will be provided as input parameters by the Operator owning the Profile to the SM-SR, see section 5.1.1.2.14.

NOTES:

- The management of POL2 cannot be authorised to a M2M SP
- If no PLMA is configured in the SM-SR for a given set of identifiers, then no authorisations SHALL be granted to any other function caller apart from the Operator who is owning the targeted Profiles.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>SR: (1) SetPLMA(identifiers, PLMA)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP: Failed
Rnote over SR #FFFFFF
(3) Store PLMA
Endrnote
SR-->>OP: (4) SetPLMA result
SR->>M2MSP: (5) HandlePLMAChangedNotification (identifiers)

@enduml
```

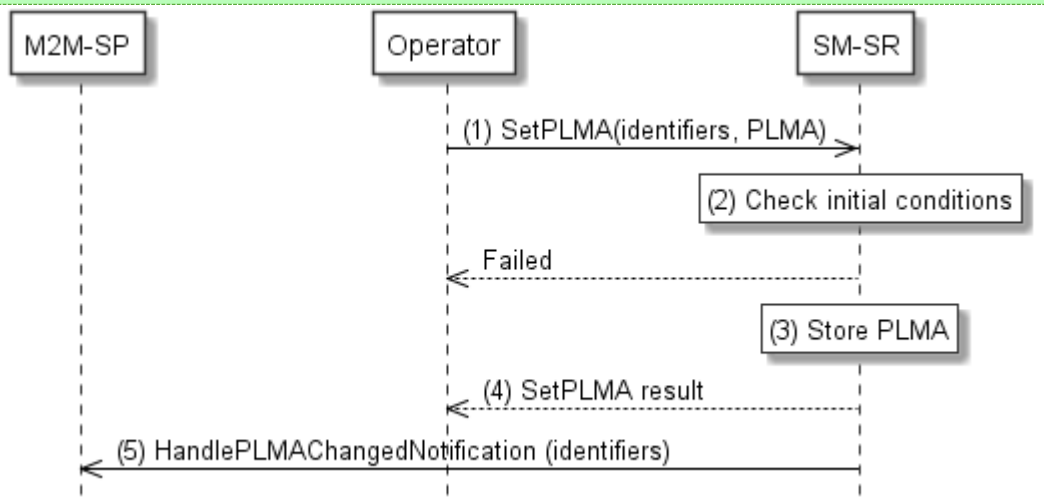


Figure 37: Set PLMA

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To set a PLMA for a M2M SP, an Operator SHALL call the "**ES4A.SetPLMA**" function with its relevant input parameters, see section 5.7.1, and the list of authorised operations and notifications, see section 5.1.1.2.14.

(2) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.7.1, and in particular checks that the function caller is the Operator owning the targeted Profile Type. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR creates and stores the PLMA based on the input parameters provided in the function call by the Operator. In case a PLMA already exists for the set of identifiers provided as input parameters, the PLMA is overwritten with new authorisations and the SM-SR SHALL indicate a success but with warning.

It SHALL be possible to set a PLMA for a given Profile Type even if this Profile Type is not referenced in an EIS in the SM-SR. In that case, the PLMA referencing this Profile Type SHALL become applicable as soon as the Profile Type reference is added to any EIS and the SM-SR SHALL indicate a success and optionally with warning.

(4) The SM-SR SHALL return the response to the **"ES4A.SetPLMA"** function to the Operator, indicating that the PLMA have been set.

(5) The SM-SR SHALL send the "**ES4.HandlePLMAChangedNotification**" to the M2M SP indicating the identifiers and the applied authorisations of the "**ES4A.SetPLMA**" function.

If the M2M SP is another Operator connected through its SM-DP, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandlePLMAChangedNotification**".
Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandlePLMAChangedNotification**"

Once the PLMA is set in the SM-SR, the M2M SP is able to call authorised Profile Lifecycle Management functions and to receive authorised notifications on Profile status changes for the Profiles addressed by this PLMA via the SM-SR. When the M2M SP is an Operator, it is also able to call authorised Profile Lifecycle Management functions and to receive authorised notifications on Profile status changes for the Profiles addressed by this PLMA via its SM-DP. The list of authorised operations and notifications can be found in Table 511214-B: List of Operation Eligible to PLMA.

3.20.2 Set Profile Lifecycle Management Authorisation rules via SM-DP

The Set Profile Lifecycle Management Authorisation procedure between the Operator and the SM-SR is done through the SM-DP (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15.1). The procedure is initiated by the Operator owning the targeted Profile Type and is similar to the procedure "Set Profile Lifecycle Management Authorisation rules" described in section 3.20.1.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>DP: (1) SetPLMA(identifiers, PLMA)
DP->>SR: (2) SetPLMA(identifiers, PLMA)
Rnote over SR #FFFFF
(3) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP: Failed
Rnote over SR #FFFFFF
(4) Store PLMA
Endrnote
SR-->>DP: (5) SetPLMA result
SR->>M2MSP: (6) HandlePLMAChangedNotification (identifiers)
DP-->>OP: (7) SetPLMA result

@enduml
```

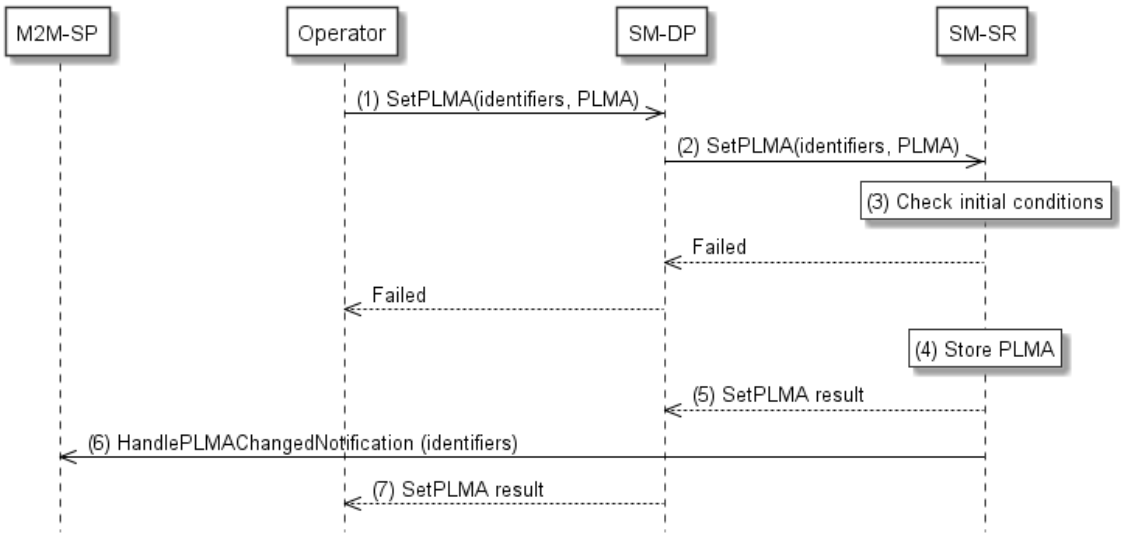


Figure 38: Set PLMA via SM-DP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To set a PLMA for a M2M SP, an Operator SHALL call the "**ES2.SetPLMA**" function with its relevant input parameters, see section and the list of authorised operations and notifications

(2) The SM-DP SHALL forward the request to the SM-SR identified by the Operator and SHALL call the "**ES3.SetPLMA**" function with its relevant input data.

(3) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.4.16), and in particular checks that the function calling SM-DP is belonging to the Operator owning the targeted Profile Type. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(4) The SM-SR creates and stores the PLMA based on the input parameters provided in the function call by the Operator. In case a PLMA already exists for the set of identifiers provided as input parameters, the PLMA is overwritten with new authorisations and the SM-SR SHALL indicate a success but with warning.

It SHALL be possible to set a PLMA for a given Profile Type even if this Profile Type is not referenced in an EIS in the SM-SR. In that case, the PLMA referencing this Profile Type SHALL become applicable as soon as the Profile Type reference is added to any EIS and the SM-SR SHALL indicate a success and optionally with warning.

(5) The SM-SR SHALL return the response to the "**ES3.SetPLMA"** function to the SM-DP, indicating that the PLMA have been set.

(6) The SM-SR SHALL send the "**ES4.HandlePLMAChangedNotification**" to the M2M SP indicating the identifiers and the applied authorisations of the "**ES2.SetPLMA**" function. If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandlePLMAChangedNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandlePLMAChangedNotification**".
Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandlePLMAChangedNotification**".

(7) Finally, the SM-DP SHALL return the response to the "**ES2.SetPLMA**" function call to the Operator.

Once the PLMA is set in the SM-SR, the M2M SP is able to call authorised Profile Lifecycle Management functions and to receive authorised notifications on Profile status changes for the Profiles addressed by this PLMA via the SM-SR. When the M2M SP is an Operator, it is also able to call authorised Profile Lifecycle Management functions and to receive authorised notifications on Profile status changes for the Profiles addressed by this PLMA via its SM-DP. The list of authorised operations and notifications can be found in Table 511214-B: List of Operation Eligible to PLMA.

3.20.3 Retrieve Profile Lifecycle Management Authorisation by Operator

The Retrieve PLMA procedure between the Operator and the SM-SR is used to retrieve the list of PLMA granted by the Operator to a M2M SP or the PLMA granted by the Operator for a Profile Type or the PLMA for a dedicated Operator owned single Profile, (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15.2). The result of the function call provides back the granted PLMA(s) based on the provided input parameters.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>SR: (1) GetPLMA(identifiers)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP: Failed
Rnote over SR #FFFFFF
(3) Retrieve PLMA
Endrnote
SR-->>OP: (4) GetPLMA result (PLMA)
@enduml
```

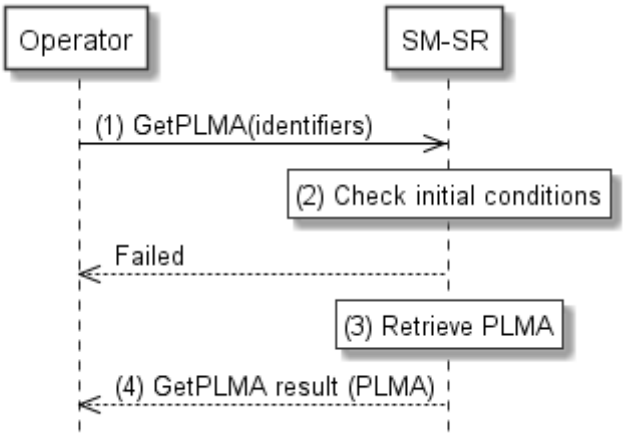


Figure 39: Retrieve PLMA by Operator

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To retrieve the PLMA(s) an Operator SHALL call the "**ES4A.GetPLMA**" or the "**ES4.GetPLMA**" function with its relevant input parameters, see section 5.7.2 and 5.5.17.

(2) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.7.2). If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

NOTE If the function caller is an Operator that is not the owner of the targeted Profile or Profile Type, the call may still be valid, but in this case the calling Operator is merely acting as an M2M SP, similar to the procedure described in section 3.20.5. The checks the SM-SR shall perform in this case are described in section 5.5.17.

(3) The SM-SR retrieves the PLMA(s) matching with the identifiers set as input parameters by the Operator. In case no PLMA exists for the provided identifier, the SM-SR SHALL return an empty result.

(4) The SM-SR SHALL return the response to the **"ES4.GetPLMA"** function call to the Operator.

3.20.4 Retrieve Profile Lifecycle Management Authorisation by Operator via SM-DP

The Retrieve Profile Lifecycle Management Authorisation procedure between the Operator and the SM-SR is done through the SM-DP (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15.2). The procedure is initiated by the Operator is similar to the procedure "Set Profile Lifecycle Management Authorisation Rules" described in section 3.20.3. The result of the function call provides back the granted PLMA (s) based on the provided input parameters

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>DP: (1) GetPLMA(identifiers)
DP->>SR: (2) GetPLMA(identifiers)
Rnote over SR #FFFFF
(3) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP: Failed
Rnote over SR #FFFFFF
(4) Retrieve PLMA
Endrnote
SR-->>DP: (5) GetPLMA result (PLMA)
DP-->>OP: (6) GetPLMA result (PLMA)
@enduml
```

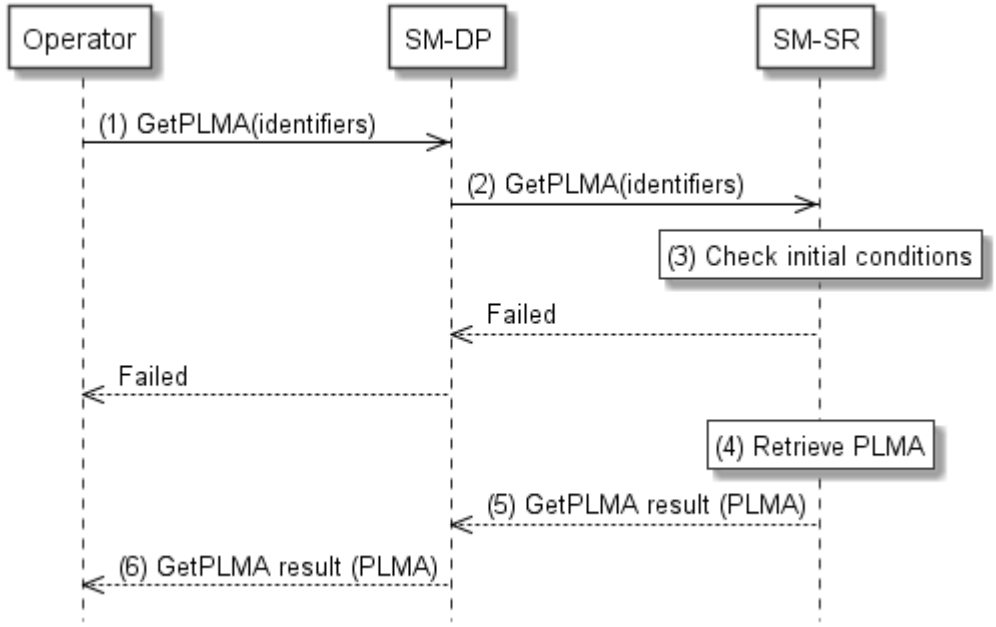


Figure 40: Retrieve PLMA by Operator via SM-DP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To retrieve the PLMA(s) an Operator SHALL call the "**ES2.GetPLMA**" function of its SM-DP with its relevant input parameters, see section 5.3.14.

(2) The SM-DP SHALL forward the request to the SM-SR identified by the Operator and SHALL call the "**ES3.GetPLMA**" function with its relevant input data.

(3) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.4.17). If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

NOTE If the SM-DP has sent the request on behalf of an Operator that is not the owner of the targeted Profile or Profile Type, the call may still be valid, but in this case this Operator is merely acting as an M2M SP. The checks the SM-SR shall perform are described in section 5.4.17.

(4) The SM-SR retrieves the PLMA(s) matching with the identifiers set as input parameters by the Operator. In case no PLMA exists for provided identifier, the SM-SR SHALL return an empty result.

(5) The SM-SR SHALL return the response to the **"ES3.RetrivePLMA"** function to the SM-DP.

(6) Finally, the SM-DP SHALL return the response to the "**ES2.GetPLMA**" function call to the Operator.

3.20.5 Retrieve Profile Lifecycle Management Authorisation by M2M SP

The Retrieve PLMA procedure between the M2M SP and the SM-SR is used to retrieve the list of PLMA granted by an Operator to a M2M SP or the PLMA granted by an Operator for a Profile Type or the PLMA for a dedicated Operator owned single Profile (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15.2). The result of the function call provides back the granted PLMA (s) based on the provided input parameters.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "M2M SP" as M2MSP #FFFFFF
participant "SM-SR" as SR #FFFFFF

M2MSP->>SR: (1) GetPLMA(identifiers)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>M2MSP: Failed
Rnote over SR #FFFFFF
(3) Retrieve PLMA
Endrnote
SR-->>M2MSP: (4) GetPLMA result (PLMA)
@enduml
```

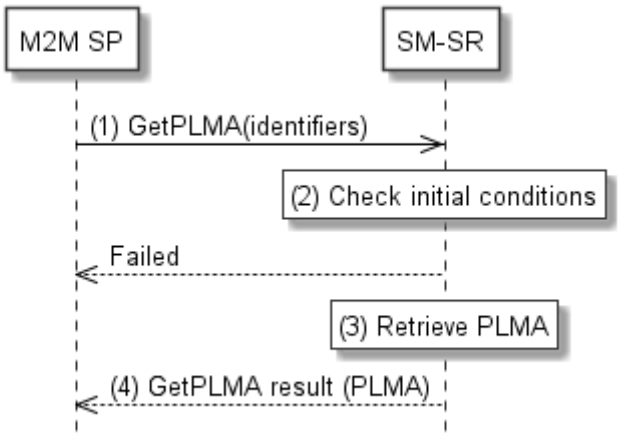


Figure 41: Retrieve PLMA by M2M SP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To retrieve the PLMA(s) the M2M SP SHALL call the "**ES4.GetPLMA**" function with its relevant input parameters, see section 5.5.17.

(2) The SM-SR SHALL verify that the M2M SP request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.5.17. If a Profile Type or a single Profile is indicated in the input parameters, the SM-SR SHALL check that the M2M SP is authorised for the targeted Profile Type or single Profile. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR retrieves the PLMA(s) for the requesting M2M SP matching with the identifiers set as input parameters by the M2M SP. In case no PLMA(s) exists for the provided identifier, the SM-SR SHALL return an empty result.

(4) The SM-SR SHALL return the response to the "**ES4.GetPLMA**" function call to the M2M SP.

3.21 Operator Notifications Configuration (ONC)

The Operator Notifications Configuration (ONC) mechanisms described in this section allows the Operator and owner of Profiles to define which notifications it would like to receive or not for a dedicated set of its Profiles, whenever the status of its Profiles has changed; whatever the origin of the status change is.

The support of this functionality by the SM-SR is optional:

- If the SM-SR supports this functionality, the SM-SR SHALL implement it as specified in this section and its subsections, and following the specification of the related functions SetONC and GetONC of the off-card interfaces.
- If the SM-SR does not support this functionality, the SM-SR SHALL NOT accept calls to setONC, and the SM-SR SHALL send the notifications to the Operator owning a Profile as specified in the procedures of sections 3.2 to 3.19, considering that the Operator has not set an ONC.

The Operator can manage the Operator Notifications Configuration for its own Profiles through a dedicated Operator / SM-SR interface, as described in section 5.7.3 and 5.7.4 or through its Operator / SM-DP interface as described in section 5.3.18 and 5.3.19.

An ONC is a combination of identifiers and discarded notifications:

- **Identifiers**: List of identifiers to identify the Operator and Profile Type; see section 5.1.1.2.15 for details

- **Discarded notifications:** List of notifications which SHALL NOT be sent to the Operator; see section 5.1.1.2.15 for details

3.21.1 Set Operator Notifications Configuration

The Set Operator Notification Configuration procedure between the Operator and the SM-SR is used to configure Profile status change notifications received by the Operator for its Profiles; whatever the origin of the status change is. The procedure provides to the SM-SR a Profile Type and a list of notifications to indicate which notifications SHALL be send to the Operator in case of any Profile status change of the targeted Profile Type.

NOTE: If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the Operator will receive all notifications for status changes for its own Profiles, associated with this Profile Type.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>SR: (1) SetONC (identifiers, notifications list)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP: Failed
Rnote over SR #FFFFFF
(3) Store Operator Notification Configuration
Endrnote
SR-->>OP: (4) SetONC result
@enduml
```

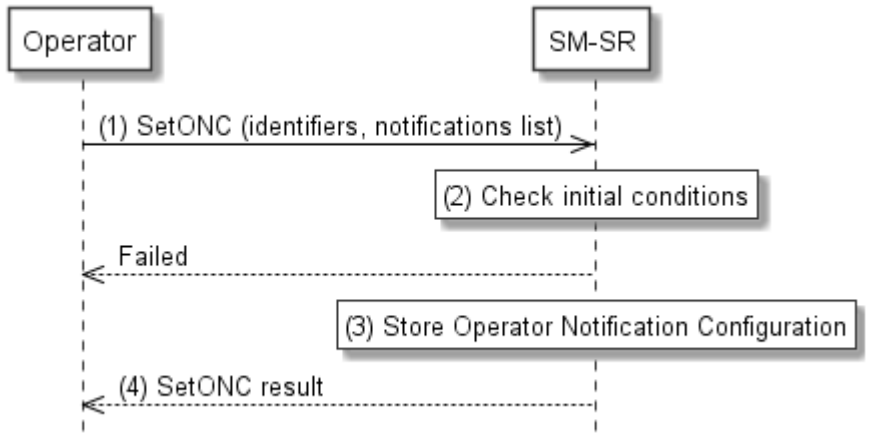


Figure 3211-A: Set Operator Notification Configuration

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To set its own Operator Notification Configuration, an Operator SHALL call the "**ES4A.SetONC**" function with its relevant input parameters, in particular the targeted Profile Type and the list of notifications, see in detail section 5.7.3.

(2) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.7.3). If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR creates and store the Operator Notification Configurations based on the input parameters provided in the function call by the Operator. In case a configuration already exists for the Operator and the targeted Profile Type, the configuration is overwritten with

the new configuration provided as input parameters and the SM-SR SHALL indicate a success but with warning.

It SHALL be possible to set the Operator Notification Configurations for a given Profile Type even if this Profile Type is not referenced in an EIS in the SM-SR. In that case, the Operator Notification Configuration referencing this Profile Type SHALL become applicable as soon as the Profile Type reference is added to any EIS and the SM-SR SHALL indicate a success and optionally with warning.

(4) The SM-SR SHALL return the response to the "**ES4A.SetONC**" function to the Operator, indicating that the Notification Configuration has been set.

3.21.2 Set Operator Notifications Configuration via SM-DP

The Set Operator Notification Configuration procedure between the Operator and the SM-SR is done through the SM-DP (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15.1). The procedure is initiated by the Operator owning the targeted Profile Type and is similar to the procedure "Set Operator Notification Configuration" described in section 3.21.1.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>DP: (1) SetONC (identifiers, notifications list)
DP->>SR: (2) SetONC(identifiers, notifications list)
Rnote over SR #FFFFF
(3) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP: Failed
Rnote over SR #FFFFFF
(4) Store Operator Notification Configuration
Endrnote
SR-->>DP: (5) SetONC result
DP-->>OP: (6) SetONC result
@enduml
```

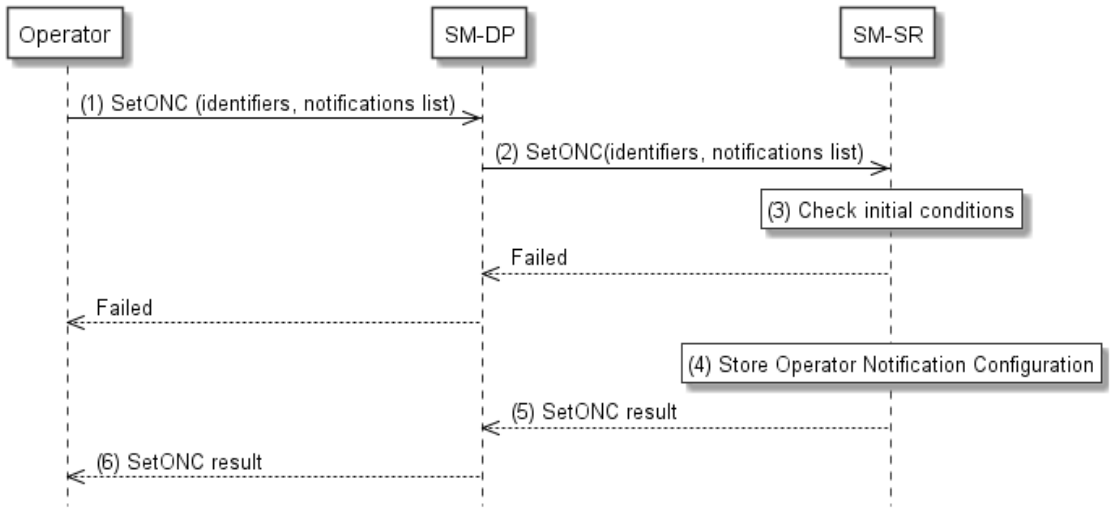


Figure 42: Set Operator Notification Configuration via SM-DP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To set its own Operator Notification Configuration, an Operator SHALL call the **"ES2.SetONC"** function of its SM-DP with its relevant input parameters, in particular the targeted Profile Type and the list of notifications, see in detail section 5.3.18.

(2) The SM-DP SHALL forward the request to the SM-SR identified by the Operator and SHALL call the **"ES3.SetONC"** function with its relevant input data.

(3) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.3.18). If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(4) The SM-SR creates and store the Operator Notification Configurations based on the input parameters provided in the function call by the Operator. In case a configuration already exists for the Operator and the targeted Profile Type, the configuration is overwritten with the new configuration provided as input parameters and the SM-SR SHALL indicate a success but with warning.
It SHALL be possible to set the Operator Notification Configurations for a given Profile Type even if this Profile Type is not referenced in an EIS in the SM-SR. In that case, the Operator Notification Configuration referencing this Profile Type SHALL become applicable as soon as the Profile Type reference is added to any EIS and the SM-SR SHALL indicate a success and optionally with warning.

(5) The SM-SR SHALL return the response to the "**ES3.SetONC"** function to the SM-DP, indicating that the Notification Configuration has been set.

(6) Finally, the SM-DP SHALL return the response to the "**ES2.SetONC**" function call to the Operator.

3.21.3 Retrieve Operator Notifications Configuration

The Retrieve Operator Notification Configuration procedure between the Operator and the SM-SR is used to retrieve the list of notifications an Operator would like not to receive for a dedicated Operator owned Profile Type (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15). The result of the function call provides back the discarded notifications based on the provided input parameters.

NOTE: If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the output data of this function will return an empty result, as all notifications will be sent for Profiles assigned with this Profile Type, see also section 5.7.4 for details.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>SR: (1) GetONC (identifiers, notifications list)
Rnote over SR #FFFFF
(2) Check initial conditions
Endrnote
SR-->>OP: Failed
Rnote over SR #FFFFFF
(3) Retrieve Operator Notification Configuration
Endrnote
SR-->>OP: (4) GetONC result
@enduml
```

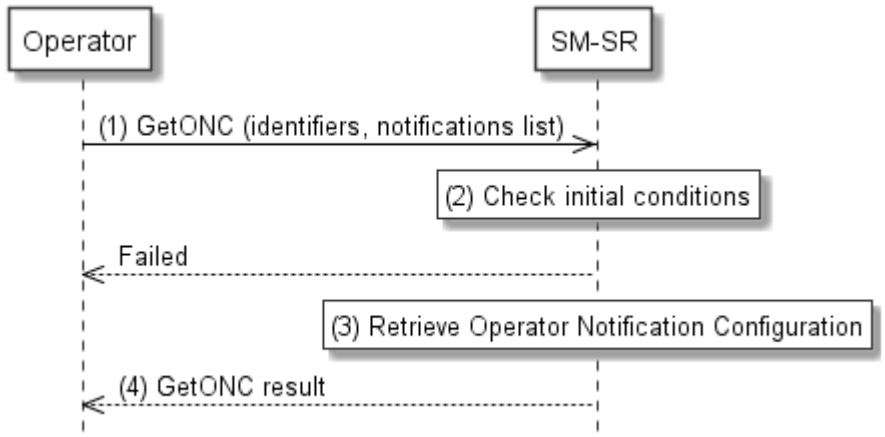


Figure 43: Retrieve Operator Notification Configuration

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To retrieve the Operator Notifications Configuration list, an Operator SHALL call the **"ES4A.GetONC"** function with its relevant input parameters, see section 5.7.4.

(2) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.7.4), and in particular checks that the function caller is the Operator owning the targeted Profile Type. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The SM-SR retrieves the list of Operator Notifications Configuration matching with the identifiers set as input parameters by the Operator. In case no ONC exists for the provided identifier, the SM-SR SHALL return an empty result.

(4) The SM-SR SHALL return the response to the **"ES4.GetONC"** function call to the Operator, indicating the list of notifications for the targeted profile.

3.21.4 Retrieve Operator Notifications Configuration via SM-DP

The Retrieve Operator Notification Configuration procedure between the Operator and the SM-SR is done through the SM-DP (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.15.1). The procedure is initiated by the Operator owning the targeted Profile Type and is similar to the procedure "Retrieve Operator Notification Configuration" described in section 3.21.1. The result of the function call provides back the discarded notifications based on the provided input parameters.

NOTE: If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the output data of this function will return an empty result, as all notifications will be sent for Profiles assigned with this Profile Type, see also section 5.7.4 for details.

The sequence flow in the figure below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox

participant "Operator" as OP #FFFFFF
participant "SM-DP" as DP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>DP: (1) GetONC (identifiers, notifications list)
DP->>SR: (2) GetONC (identifiers, notifications list)
Rnote over SR #FFFFF
(3) Check initial conditions
Endrnote
SR-->>DP: Failed
DP-->>OP: Failed
Rnote over SR #FFFFFF
(4) Retrieve Operator Notification Configuration
Endrnote
SR-->>DP: (5) GetONC result
DP-->>OP: (6) GetONC result
@enduml
```

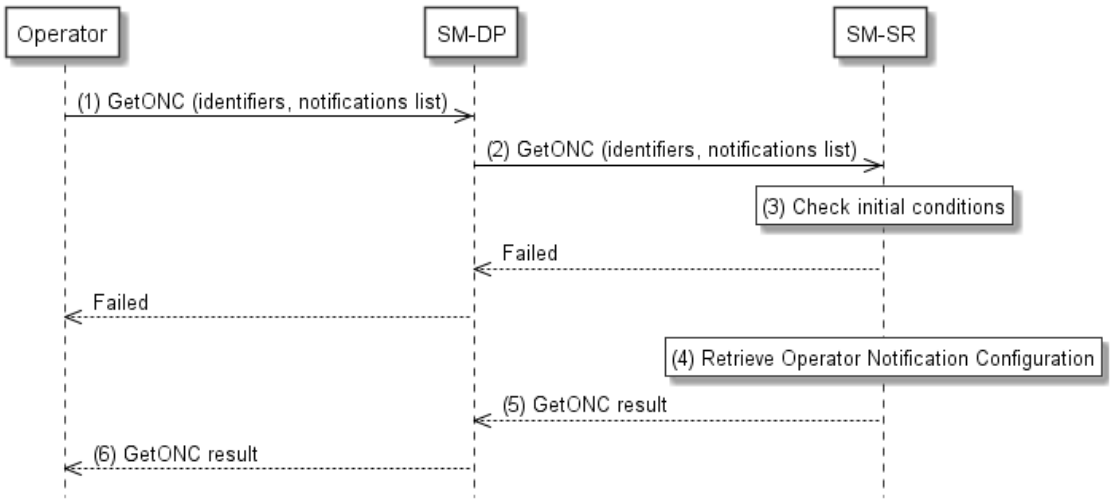


Figure 44: Retrieve Operator Notification Configuration via SM-DP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) To retrieve the Operator Notifications Configuration list, an Operator SHALL call the **"ES2.GetONC"** function of its SM-DP with its relevant input parameters, see section 5.3.19.

(2) The SM-DP SHALL forward the request to the SM-SR identified by the Operator and SHALL call the **"ES3.GetONC"** function with its relevant input data.

(3) The SM-SR SHALL verify that the Operator request is acceptable (the verifications that the SM-SR SHALL perform are described in the section 5.4.22), and in particular checks that the function calling SM-DP is belonging to the Operator owning the targeted Profile Type. If any of the conditions to be verified are not satisfied, the SM-SR SHALL return a response indicating the failure, and the procedure SHALL end.

(4) The SM-SR retrieves Operator Notifications Configuration list matching with the identifiers set as input parameters by the Operator. In case no ONC exists for the provided identifier, the SM-SR SHALL return an empty result.

(5) The SM-SR SHALL return the response to the "**ES3.GetONC"** function to the SM-DP, indicating the list of notifications for the targeted profile.

(6) Finally, the SM-DP SHALL return the response to the "**ES2.GetONC**" function call to the Operator.

3.22 Local Enable for Test Profile

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 120
skinparam sequenceArrowThickness 1

hide footbox

participant "Device" as DEV #FFFFFF
participant "eUICC" as eUICC #FFFFFF


DEV->>eUICC : (1) ESx.LocalEnableTestProfile
Rnote over eUICC #FFFFF
(2) Verify that the Test Profile exists
Endrnote
eUICC-->>DEV : Error
Rnote over eUICC #FFFFF
(3) Verify that the currently Enabled Profile
     is NOT the Emergency Profile
Endrnote
eUICC-->>DEV : Error

Rnote over eUICC #FFFFF
 (4) Verify that the currently Enabled Profile
     is NOT the Test Profile
Endrnote
eUICC-->>DEV : Error

Group Profile switch
Rnote over eUICC #FFFFF
(5) Enable Test Profile
Endrnote
eUICC-->>DEV : (6) Success
|||
eUICC-->>DEV: (7) REFRESH, (UICC reset)
|||
Rnote over DEV, eUICC #FFFFFF
(8) Network attachment with the Enabled Profile
Endrnote
end
@enduml
```

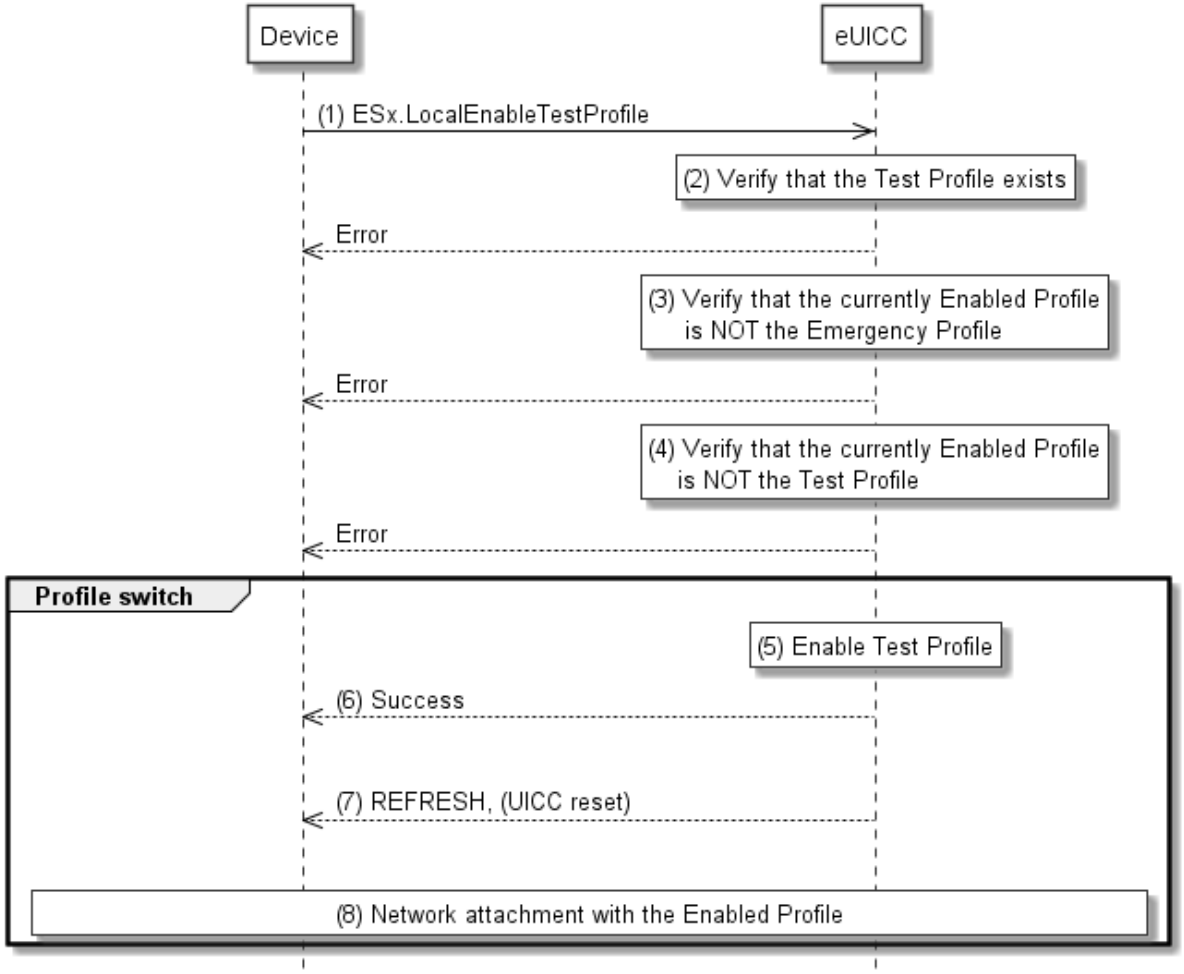


Figure 322: Local Enable of Test Profile

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Device SHALL call the **"ESx.LocalEnableTestProfile"** function.

(2) The eUICC SHALL verify that the Test Profile exists (including Flag and NAA keys as described in EUICC23 in SGP.01 [1]). If any of the conditions to be verified are not satisfied, the eUICC SHALL return a response indicating the failure, and the procedure SHALL end.

(3) The eUICC SHALL verify that the current enabled Profile is NOT the Emergency Profile. If the condition to be verified is not satisfied, the eUICC SHALL return a response indicating the failure, and the procedure SHALL end.

(4) The eUICC SHALL verify that the currently enabled Profile is NOT the Test Profile. If the condition to be verified is not satisfied, the eUICC SHALL return a response indicating that the Test Profile is already Enabled, and the procedure SHALL end.

(5) The eUICC SHALL NOT enforce POL1 of the currently Enabled Profile, and SHALL disable the currently enabled Profile, and enable the Test Profile.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the Profile is marked as enabled in this step, it MAY actually become effective after the terminal executes the REFRESH command.

(6) The eUICC SHALL return the execution status of the "**ESx. LocalEnableTestProfile**" command to the Device.

(7) The eUICC SHALL send a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

(8) The Device SHALL perform a network attach procedure with the newly enabled Profile.

NOTE: Whether the Test Profile provides connectivity to a test network or not, the eUICC will not attempt to enable automatically the previously Enabled Profile. This is in contrast to the remote enable procedures (for example in section 3.2.2).

3.23 Local Disable for Test Profile

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 100
skinparam sequenceArrowThickness 1

hide footbox

participant "Device" as DEV #FFFFFF
participant "eUICC" as ISDR #FFFFFF

DEV->>ISDR : (1) ESx.LocalDisableTestProfile
Rnote over ISDR  #FFFFF
(2) Verify that the currently Enabled Profile
     is the Test Profile
Endrnote
ISDR-->>DEV : Error

group Profile switch
Rnote over ISDR  #FFFFF
(3) Disable Test Profile and
      enable previously Enabled Profile
Endrnote
ISDR-->>DEV : (4) Success
|||
ISDR-->>DEV: (5) REFRESH, (UICC reset)
|||
Rnote over DEV, ISDR #FFFFFF
(6) Network attachment with the Enabled Profile
Endrnote
End
@enduml
```

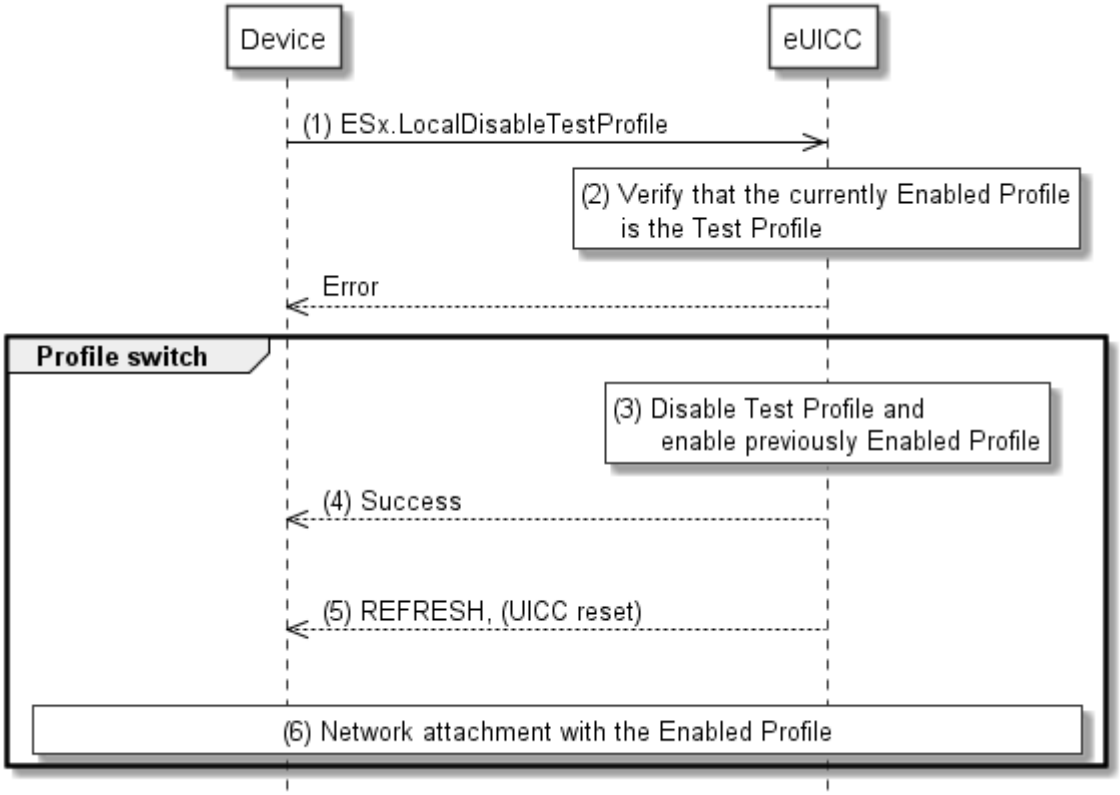


Figure 323: Local Disable of Test Profile

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Device SHALL call the **"ESx.LocalDisableTestProfile"** function.

(2) The eUICC SHALL verify that the currently Enabled Profile is the Test Profile (including Flag and NAA keys as described in EUICC23 in SGP.01[1]). If any of the conditions to be verified are not satisfied, the eUICC SHALL return a response indicating that the currently Enabled Profile is not the Test Profile, and the procedure SHALL end.

(3) The eUICC SHALL disable the Test Profile and enable the previously enabled Profile.

(4) The eUICC SHALL return the execution status of the "**ESx.LocalDisableTestProfile**" command to the Device.

(5) The eUICC SHALL send a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

NOTE: In case of any error after this step, indicating that the currently Enabled Profile cannot provide connectivity, the eUICC will trigger the Fall-Back Mechanism and will ensure that the previously enabled Profile is the Profile that was enabled before the Local Enable.

(6) The eUICC and the Device SHALL perform a network attach procedure with the newly Enabled Profile.

Dependent on the configuration of the eUICC, the eUICC MAY send a Notification about the Profile change after Test Profile disabling to the SM-SR.

3.24 POL2 Update

This procedure is used by the Operator to update POL2 via the SM-SR.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 400
skinparam ParticipantPadding 50
skinparam sequenceArrowThickness 1

hide footbox
participant "M2M SP" as M2MSP #FFFFFF
participant "Operator" as OP #FFFFFF
participant "SM-SR" as SR #FFFFFF

OP->>SR: (1) UpdatePolicyRules(POL2)
Rnote over SR #FFFFF
(2) Update POL2
Endrnote
SR-->>OP: (3) UpdatePolicyRules Result
SR->>M2MSP: (4) Cond: HandleProfilePOL2UpdatedNotification (eid, iccid, POL2)
@enduml
```

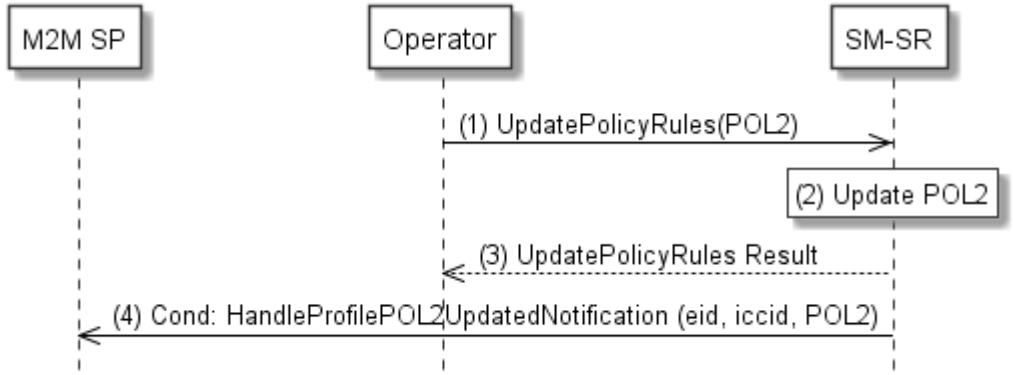


Figure 324: POL2 Update

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Operator owner of the target Profile SHALL call the "**ES4.UpdatePolicyRules**" function with its relevant input data, as described in section 5.3.3.

(2) The SM-SR SHALL update the POL2 of the targeted eUICC's EIS.

(3) The SM-SR SHALL return the execution status of the "**ES4.UpdatePolicyRules**" to the Operator.

(4) The SM-SR SHALL send the **"ES4.HandleProfilePOL2UpdatedNotification"** to a M2M SP, if authorised by the Operator owning the Profile, indicating the updated POL2 rules according to chapter 5.1.1.2.2.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfilePOL2UpdatedNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by the Operator owning the Profile, the SM-SR SHALL send this notification to the SM-DP

associated to this other Operator by calling the "**ES3.HandleProfilePOL2UpdatedNotification**".
Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfilePOL2UpdatedNotification**"

3.25 Emergency Profile Attribute Management

This procedure specifies setting the Emergency Profile Attribute for a Profile when no other Profile has the Emergency Profile Attribute set (case 1), or, a change regarding the Profile that has the Emergency Profile Attribute set (case 2). For case 2, the Operator1 owning the Profile that currently has the Emergency Profile Attribute set and the Operator2 that wants to set the Emergency Profile Attribute on its own Profile SHALL have an agreement. This agreement is materialized by the Operator1 setting a PLMA where it MAY grant Operator2 the authorisation to unset the Emergency Profile Attribute on this Operator1 Profile.

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

For case 1 the procedure below applies:

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox

Participant “M2M SP” as SP #FFFFFF
Participant “Operator 1\n<size:10>(owning Profile A)</size>” as OP1 #FFFFFF
Participant “Operator 2\n<size:10>(owning Profile B)</size>” as OP2 #FFFFFF
Participant “SM-DP” as DP #FFFFFF
Participant “SM-SR” as SR #FFFFFF
Participant “eUICC” as EUICC #FFFFFF

Alt [via SM-SR]
OP2->SR: [1.a] ES4.SetEmergencyProfileAttribute(EID,ICCID)\non Profile B Request

Else [via SM-DP]
OP2->DP: [1.b] ES2.SetEmergencyProfileAttribute(EID,SMSR-ID,ICCID)\non Profile B
Request

Rnote over DP #FFFFFF
Identify SM-SR
Endrnote

DP<->SR: Mutual Authentication

DP->SR: [1.c] ES3.SetEmergencyProfileAttribute(EID,ICCID)\non Profile B Request

end

SR->EUICC: [2] ES5.SetEmergencyProfileAttribute(ISD-P AID)\non Profile B

Rnote over EUICC #FFFFFF
[3a] Verify if Profile B has not set Fall-Back Attribute
Endrnote
EUICC-->SR: [3.a] Send STORE DATA response indicating an error

Rnote over EUICC #FFFFFF
[3b] Set Emergency Profile Attribute on Profile B
Endrnote

EUICC->SR: [4] SetEmergencyProfileAttribute response

Rnote over SR #FFFFFF
[5] EIS Update(AdditionalProperty)
Endrnote

Alt [via SM-SR]
SR->OP2: 6.a] ES4.HandleEmergencyProfileAttributeSetNotification\non Profile B
Request
SR->OP1

Else [via SM-DP]

SR->DP: [6.b] ES3.SetEmergencyProfileAttribute(EID,ICCID)\non Profile B Request

DP->OP2: [6.c] ES2.HandleEmergencyProfileAttributeSetNotification\non Profile B
Request

end

Opt [If if requested by Operator 2]
SR->SP: [7] HandleEmergencyProfileAttributeSetNotification of Profile B
end
@enduml
```

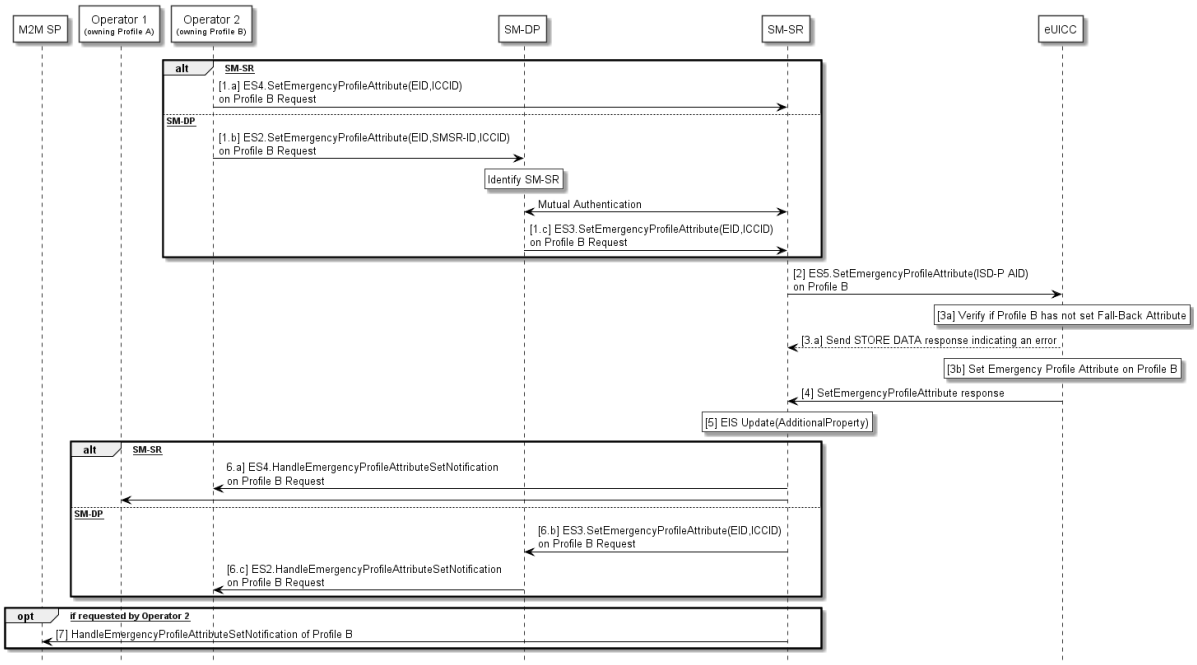


Figure 325-A: Emergency Profile Attribute Management (case 1: first Emergency Profile)

Start Conditions (case 1):

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

Procedure (case 1):

(1) The Operator2 owning Profile B requests setting of the Emergency Profile Attribute on Profile B to the SM-SR, either directly (1.a) by calling the "**ES4.SetEmergencyProfileAttribute"** function with the relevant input parameters or through its SM-DP (1.b) by calling the "**ES2.SetEmergencyProfileAttribute"** function with the relevant input parameters and the SM-DP forwarding the request to the SM-SR (1c) by calling the "**ES3.SetEmergencyProfileAttribute"** function with the relevant input parameters.

(2) The SM-SR, by calling the "**ES5.SetEmergencyProfileAttribute"** function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.

(3) The eUICC SHALL verify that Profile B does not have the Fall-Back Attribute set (3a) and SHALL then set the Emergency Profile Attribute to Profile B (3b).
    a. If the conditions (3a) is not true, the eUICC SHALL abort the procedure and SHALL send an error response to the SM-SR as detailed in the "**ES5.SetEmergencyProfileAttribute"** function.

(4) The eUICC SHALL send the "**ES5.SetEmergencyProfileAttribute"** response to the SM-SR

(5) The SM-SR SHALL update the EIS accordingly by adding the information that the Emergency Profile has been set on Profile B in the AdditionalProperty field.

(6) Based on ONC, the SM-SR SHALL notify to all Operators, having a Profile on this eUICC, either directly (6a) by calling the

"**ES4.HandleEmergencyProfileAttributeSetNotification"**, or via the SM-DP (6b) by calling the "**ES3.HandleEmergencyProfileAttributeSetNotification"** and the SM-DP SHALL forward the notification (6c) by calling the "**ES2.HandleEmergencyProfileAttributeSetNotification"**, that a Profile now has the Emergency Profile Attribute set. This notification MAY include the Profile ID.

(7) The SM-SR SHALL notify the M2M SP by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification"**, that the Profile B has the Emergency Profile Attribute set, if requested by the Operator2 during Platform Lifecycle Management Authorisation registration (see section 3.20).

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleEmergencyProfileAttributeSetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleEmergencyProfileAttributeSetNotification**".

End Conditions (case 1):

The Profile B has the Emergency Profile Attribute set.

For case 2 the procedure below applies

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox

Participant “M2M SP” as SP #FFFFFF
Participant “Operator 1\n<size:10>(owning Profile A)</size>” as OP1 #FFFFFF
Participant “Operator 2\n<size:10>(owning Profile B)</size>” as OP2 #FFFFFF
Participant “SM-DP” as DP #FFFFFF
Participant “SM-SR” as SR #FFFFFF
Participant “eUICC” as EUICC #FFFFFF

Alt [via SM-SR]
OP2->SR: [1.a] ES4.SetEmergencyProfileAttribute(EID,ICCID)\non Profile B Request

Else [via SM-DP]
OP2->DP: [1.b] ES2.SetEmergencyProfileAttribute(EID,SMSR-ID,ICCID)\non Profile B
Request

Rnote over DP #FFFFFF
Identify SM-SR
Endrnote

DP<->SR: Mutual Authentication

DP->SR: [1.c] ES3.SetEmergencyProfileAttribute(EID,ICCID)\non Profile B Request

end

Rnote over SR #FFFFFF
[2] Check PLMA for SetmergencyProfileAttribute for Operator 2
Endrnote

SR-->OP2: [2.a] Send error response with authorisation conflict
SR->EUICC: [3] ES5.SetEmergencyProfileAttribute(ISD-P AID)\non Profile B

Rnote over EUICC #FFFFFF
[4a] Verify if Profile B has not set Fall-Back Attribute
Endrnote
EUICC-->SR: [4.a] send STORE DATA error response

Rnote over EUICC #FFFFFF
[4b] Unset Emergency Profile Attribute on Profile A
by Setting Emergency Profile Attribute on Profile B
Endrnote

EUICC->SR: [5] SetEmergencyProfileAttribute response

Rnote over SR #FFFFFF
[6] EIS Update(AdditionalProperty)
Endrnote

SR->OP1: [7] ES4.HandleEmergencyProfileAttributeUnsetNotification\non Profile A

Alt [via SM-SR]
SR->OP2: [8.a] ES4.HandleEmergencyProfileAttributeSetNotification\non Profile B
SR->OP1

Else [via SM-DP]

SR->DP: [8.b] ES3.HandleEmergencyProfileAttributeSetNotification\non Profile B

DP->OP2: [8.c] ES2.HandleEmergencyProfileAttributeSetNotification\non Profile B

end
```

```
Opt [If if requested by Operator 1]
SR->SP: [9] HandleEmergencyProfileAttributeUnsetNotification of Profile A
End

Opt [If if requested by Operator 2]
SR->SP: [10] HandleEmergencyProfileAttributeSetNotification of Profile B
end
@enduml
```

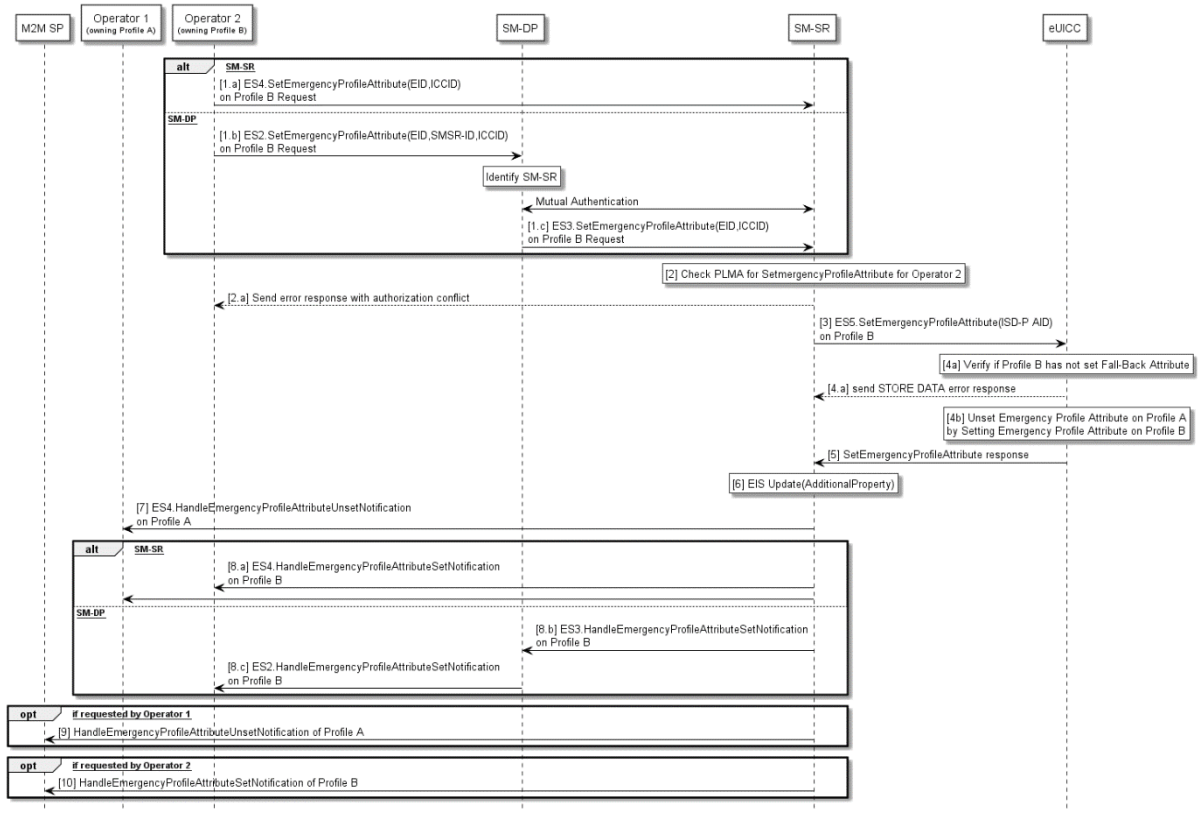


Figure 325-B: Emergency Profile Attribute Management (case 2: change of Emergency Profile)

Start Conditions (case 2):

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

Procedure (case 2):

(1) The Operator2 owning Profile B requests setting of the Emergency Profile Attribute on Profile B to the SM-SR, either directly (1.a) by calling the **"ES4.SetEmergencyProfileAttribute"** function with the relevant input parameters or through its SM-DP (1.b) by calling the "**ES2.SetEmergencyProfileAttribute"** function with the relevant input parameters and the SM-DP forwarding the request to the SM-SR (1c) by calling the "**ES3.SetEmergencyProfileAttribute"** function with the relevant input parameters.

(2) The SM-SR checks if Operator2 has PLMA configured to unset the Emergency Profile Attribute from the Operator1 owning the Profile that currently has the Emergency Profile Attribute set.

a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the Operator 2.

(3) The SM-SR, by calling the "**ES5.SetEmergencyProfileAttribute"** function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.

(4) The eUICC verifies that Profile B does not have the Fall-Back Attribute set (4a) and performs the operation (4b). This will remove the Emergency profile Attribute from Profile A.

b. If the conditions (4a) is not true, the eUICC aborts the procedure and return an error to the SM-SR as detailed in the "**ES5.SetEmergencyProfileAttribute"** function.

(5) The eUICC SHALL send the "**ES5.SetEmergencyProfileAttribute"** response to the SM-SR.

(6) The SM-SR updates the EIS accordingly by adding the information that the Emergency Profile has been set on Profile B in the AdditionalProperty field.

(7) Based on ONC, the SM-SR notifies Operator1, whose Profile has the Emergency Profile Attribute Unset, by calling the "**ES4.HandleEmergencyProfileAttributeUnsetNotification**" that its Profile now has the Emergency Profile Attribute unset.

(8) Based on ONC, the SM-SR notifies all Operators, having a Profile on this eUICC either directly (8a) by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification"**, or via the SM-DP (8b) by calling the "**ES3.HandleEmergencyProfileAttributeSetNotification"** and the SM-DP SHALL forward the notification (8c) by calling the "**ES2.HandleEmergencyProfileAttributeSetNotification"**, that a Profile now has the Emergency Profile Attribute set. This notification MAY include the Profile ID.

(9) The SM-SR SHALL notify the M2M SP that the Profile A has the Emergency Profile Attribute unset by calling the "**ES4.HandleEmergencyProfileAttributeUnsetNotification"**, if requested by the Operator1 during Platform Lifecycle Management Authorisation registration (see section 3.20).

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4. HandleEmergencyProfileAttributeUnsetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3. HandleEmergencyProfileAttributeUnsetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2. HandleEmergencyProfileAttributeUnsetNotification**".

(10) The SM-SR SHALL notify the M2M SP that the Profile B has the Emergency Profile Attribute set by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification"**, if requested by the Operator2 during Platform Lifecycle Management Authorisation registration (see section 3.20).
If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleEmergencyProfileAttributeSetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleEmergencyProfileAttributeSetNotification**".

End Conditions (case 2):

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

3.26 Emergency Profile Attribute Management via the M2M SP

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

This procedure specifies setting the Emergency Profile Attribute for a Profile when no other Profile has the Emergency Profile Attribute set (case 1), or, a change regarding the Profile that has the Emergency Profile Attribute set (case 2).

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

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

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

For case 1 the procedure below applies:

```
startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox

Participant "M2M SP" as SP #FFFFFF
Participant "Operator 1\n<size:10>(owning Profile A)</size>" as OP1 #FFFFFF
Participant "Operator 2\n<size:10>(owning Profile B)</size>" as OP2 #FFFFFF
Participant "SM-SR" as SR #FFFFFF
Participant "eUICC" as EUICC #FFFFFF

SP->SR: [1] ES4.SetEmergencyProfileAttribute(EID,ICCID)\non Profile B Request

Rnote over SR #FFFFFF
[2] Check PLMA for Setting Emergency Profile
Attribute from Operator 2
Endrnote
SR-->SP: [2.a] Send response indicating authorisation conflict

SR->EUICC: [3] ES5.SetEmergencyProfileAttribute(ISD-P AID)\non Profile B

Rnote over EUICC #FFFFFF
[4a] Verify if Profile B has not set Fall-Back Attribute
Endrnote
EUICC-->SR: [4.a] send STORE DATA response with herror

Rnote over EUICC #FFFFFF
[4b] Set Emergency Profile Attribute on Profile B
Endrnote

EUICC->SR: [5] SetEmergencyProfileAttribute response

Rnote over SR #FFFFFF
[6] EIS Update(AdditionalProperty)
Endrnote

SR->OP2: [7] ES4.HandleEmergencyProfileAttributeSetNotification of Profile B

SR->OP1

SR->SP: [8] ES4.HandleEmergencyProfileAttributeSetNotification of Profile B
@enduml
```

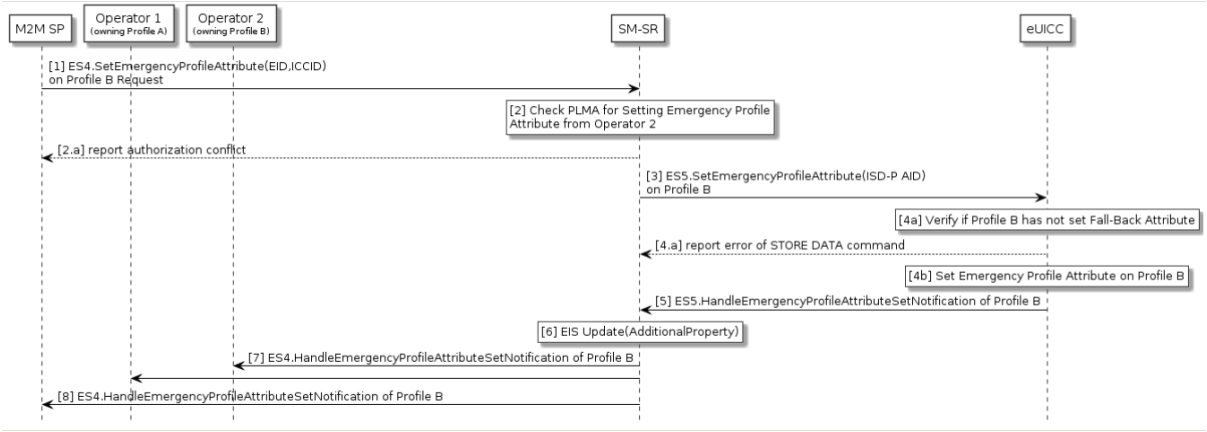


Figure 326-A: Emergency Profile Attribute Management by M2M SP (case 1: first Emergency Profile)

Start Conditions:

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

Procedure:

(1) The M2M SP requests setting of the Emergency Profile Attribute on Profile B to the SM-SR by calling the "**ES4.SetEmergencyProfileAttribute"** function with the relevant input parameters.

(2) The SM-SR checks if a PLMA from Operator2 that authorises the M2M SP to set the Emergency Profile Attribute on Profile B is configured
    a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the M2M SP.

(3) The SM-SR, by calling the "**ES5.SetEmergencyProfileAttribute"** function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.

(4) The eUICC verifies that Profile B does not have the Fall-Back Attribute set (4a) and then sets the Emergency Profile Attribute to the Profile B (4b).
    b. If the conditions (4a) is not true, the eUICC aborts the procedure and sends an error to the SM-SR as detailed in the "**ES5.SetEmergencyProfileAttribute"** function.

(5) The eUICC SHALL send the "**ES5.SetEmergencyProfileAttribute"** response to the SM-SR.

(6) The SM-SR updates the EIS accordingly by adding the information that the Emergency Profile has been set on Profile B in the AdditionalProperty field.

(7) Based on ONC, the SM-SR notify all Operators, having a Profile on this eUICC, by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification"** that a Profile now has the Emergency Profile Attribute set. This notification MAY include the Profile ID.

(8) The SM-SR notifies the M2M SP by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification"** that the Emergency Profile Attribute is now set for Profile B.

    If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification**".

    If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleEmergencyProfileAttributeSetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleEmergencyProfileAttributeSetNotification**"

End Conditions:

The Profile B has the Emergency Profile Attribute set.

For case 2 the procedure below applies:

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox

Participant "M2M SP" as SP #FFFFFF
Participant "Operator 1\n<size:10>(owning Profile A)</size>" as OP1 #FFFFFF
Participant "Operator 2\n<size:10>(owning Profile B)</size>" as OP2 #FFFFFF
Participant "SM-DP" as DP #FFFFFF
Participant "SM-SR" as SR #FFFFFF
Participant "eUICC" as EUICC #FFFFFF

SP->SR: [1] ES4.SetEmergencyProfileAttribute(EID,ICCID)\non Profile B Request

Rnote over SR #FFFFFF
[2] Check PLMA for Setting Emergency Profile
Attribute from Operator 2
Endrnote
SR-->SP: [2.a] Send response indicating authorisation conflict
Rnote over SR #FFFFFF
[3] Check PLMA for Unsetting Emergency Profile
Attribute from Operator 1
Endrnote
SR-->SP: [3.a] Send response indicating authorisation conflict

SR->EUICC: [4] ES5.SetEmergencyProfileAttribute(ISD-P AID)\non Profile B

Rnote over EUICC #FFFFFF
[5a] Verify if Profile B has not set Fall-Back Attribute
Endrnote
EUICC-->SR: [5.a] send error response

Rnote over EUICC #FFFFFF
[5b] Unset Emergency Profile Attribute on Profile A
by Setting Emergency Profile Attribute on Profile B
Endrnote

EUICC->SR: [6] SetEmergencyProfileAttribute response

Rnote over SR #FFFFFF
[7] EIS Update(AdditionalProperty)
Endrnote

SR->OP1: [8] ES4.HandleEmergencyProfileAttributeUnsetNotification\non Profile A

Alt [via SM-SR]
SR->OP2: [9.a] ES4.HandleEmergencyProfileAttributeSetNotification\non Profile B
SR->OP1

Else [via SM-DP]

SR->DP: [9.b] ES3.HandleEmergencyProfileAttributeSetNotification\non Profile B

DP->OP2: [9.c] ES2.HandleEmergencyProfileAttributeSetNotification\non Profile B

end

Opt [If if requested by Operator 1]
SR->SP: [10] HandleEmergencyProfileAttributeUnsetNotification of Profile A
End

Opt [If if requested by Operator 2]
SR->SP: [11] HandleEmergencyProfileAttributeSetNotification of Profile B
end
```

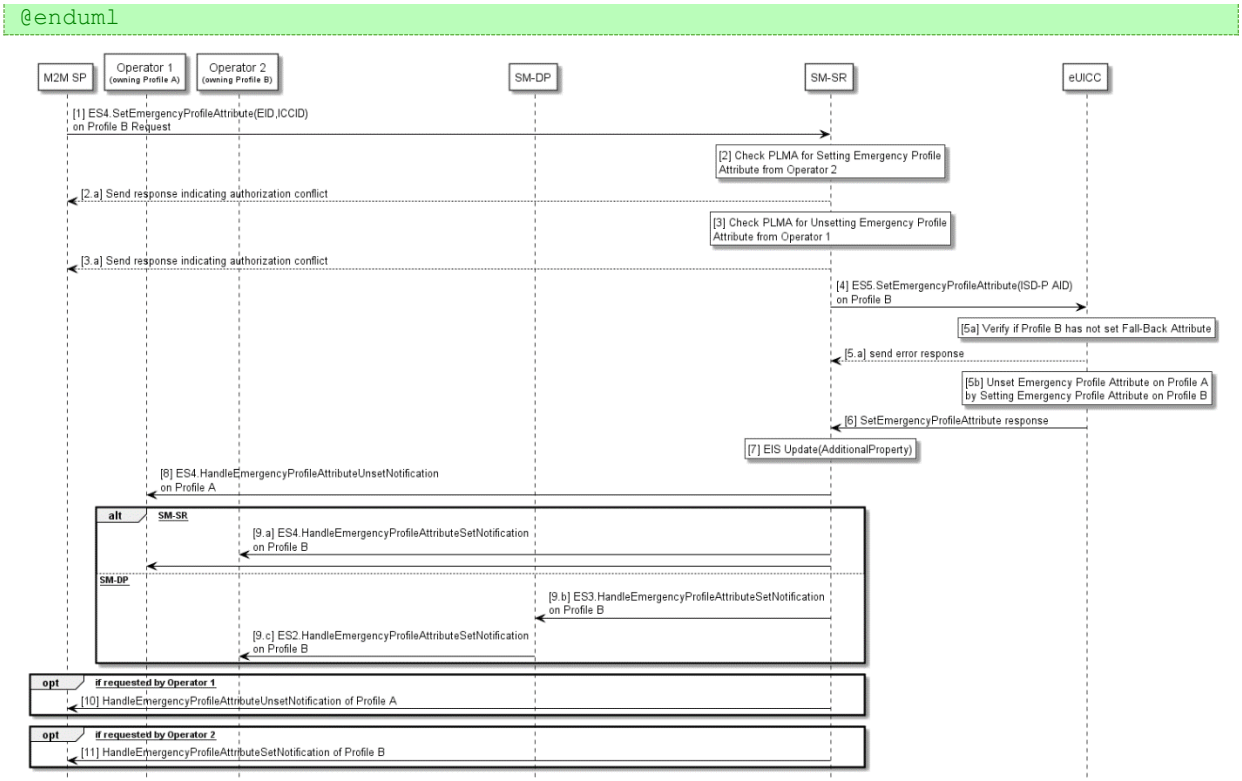


Figure 326-B: Emergency Profile Attribute Management by M2M SP (case 2: change of Emergency Profile)

Start Conditions:

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

Procedure:

(1) The M2M SP requests setting of the Emergency Profile Attribute on Profile B to the SM-SR by calling the "**ES4.SetEmergencyProfileAttribute"** function with the relevant input parameters.

(2) The SM-SR checks if a PLMA from Operator2 that authorises the M2M SP to set the Emergency Profile Attribute on Profile B is configured.
   a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the M2M SP.

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

(4) The SM-SR, by calling the "**ES5.SetEmergencyProfileAttribute"** function, requests the eUICC to set the Emergency Profile Attribute to the Profile B.

(5) The eUICC verifies that Profile B does not have the Fall-Back Attribute set (5a) and then sets the Emergency Profile Attribute to the Profile B (5b). This will remove the Emergency Profile Attribute from Profile A.
    c. If the conditions (5a) is not true, the eUICC aborts the procedure and returns an error to the SM-SR.

(6) The eUICC SHALL send the "**ES5.SetEmergencyProfileAttribute"** response to the SM-SR.

(7) The SM-SR updates the EIS accordingly by adding the information that the Emergency Profile has been set on Profile B in the AdditionalProperty field.

(8) Based on ONC, the SM-SR notifies Operator1, whose Profile has the Emergency Profile Attribute Unset, by calling the "**ES4.HandleEmergencyProfileAttributeUnsetNotification**" that its Profile now has the Emergency Profile Attribute unset.

(9) Based on ONC, the SM-SR notifies all Operators, having a Profile on this eUICC, by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification"** that a Profile now has the Emergency Profile Attribute set. This notification MAY include the Profile ID.

(10) The SM-SR notifies the M2M SP by calling the "**ES4.HandleEmergencyProfileAttributeUnsetNotification**" that the Emergency Profile Attribute is now unset for Profile A.
If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleEmergencyProfileAttributeUnsetNotification**".
If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleEmergencyProfileAttributeUnsetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleEmergencyProfileAttributeUnsetNotification**"

(11) The SM-SR notifies the M2M SP by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification"** that the Emergency Profile Attribute is now set for Profile B.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleEmergencyProfileAttributeSetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleEmergencyProfileAttributeSetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleEmergencyProfileAttributeSetNotification**"

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

3.27 Fall-Back Attribute Management

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

The Operator1 needs to grant PLMA for Operator2 in order to authorise to set the Fall-Back Attribute in Operator1 owned Profile, as a consequence, Operator2 owned Profile has the Fall-Back Attribute un-set (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.19).

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

The sequence flow below describes the procedure.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox

Participant "M2M SP" as SP #FFFFFF
Participant "Operator 1\n<size:10>(owning Profile A)</size>" as OP1 #FFFFFF
Participant "Operator 2\n<size:10>(owning Profile B)</size>" as OP2 #FFFFFF
Participant "SM-SR" as SR #FFFFFF
Participant "eUICC" as EUICC #FFFFFF

OP2->SR: [1] ES4.SetFallBackAttribute(EID, ICCID) \non Profile B Request

Rnote over SR #FFFFFF
[2] Check PLMA for un-setting Fall-Back
Attribute from Operator1
Endrnote

SR-->OP2: [2.a] Return response indicating the PLMA conflict

SR->EUICC: [3] ES5.SetFallBackAttribute on Profile B request

Rnote over EUICC #FFFFFF
[4] Unset Fall-Back Attribute on Profile A
by Setting Fall-Back Attribute on Profile B
Endrnote

EUICC->SR: [5] ES5.SetFallBackAttribute response (euiccResponseData)

Rnote over SR #FFFFFF
[6] Update EIS
Endrnote

SR->OP2: [7] ES4.SetFallBackAttribute response

SR->OP1: [8] Cond: ES4.HandleProfileFallBackAttributeUnSetNotification Report

SR->SP: [9] Cond: HandleProfileFallBackAttributeUnsetNotification of Profile A

SR->OP2: [10] Cond: ES4.HandleProfileFallBackAttributeSetNotification Report

SR->SP: [11] Cond: HandleProfileFallBackAttributeSetNotification of Profile B

@enduml
```

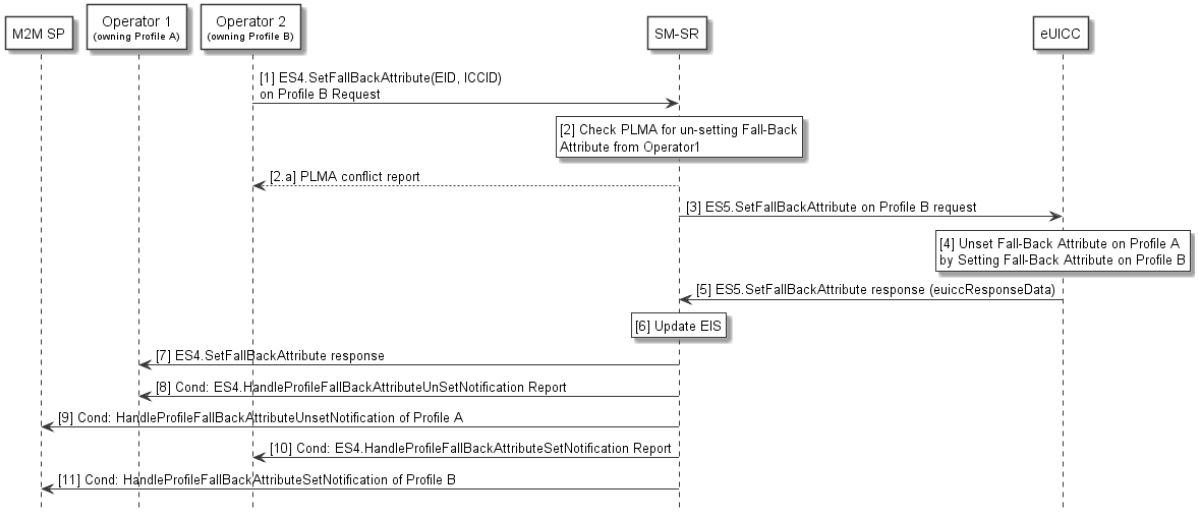


Figure 327: Fall Back Attribute Management Procedure

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for Embedded UICC [1].

Procedure:

(1) The Operator2 owning Profile B call "**ES4.SetFallBackAttribute"** function, providing the eid and the iccid of the targeted Profile, in order to set the Fall-Back Attribute to its Profile.

(2) The SM-SR checks if Operator1 has configured a PLMA authorising Operator2 to unset the Fall-Back Attribute on Profile A.

a. If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the Operator 2.

(3) The SM-SR, by calling "**ES5.SetFallBackAttribute"** function (see section 4.11.7), requests the eUICC to set the Fall-Back Attribute to the Profile B.

(4) The eUICC performs the operation. This will remove the Fall-Back Attribute from Profile A.

(5) The eUICC sends the "**ES5.SetFallBackAttribute**" response to the SM-SR by providing the euiccResponseData.

(6) According to the execution status provided by the eUICC, the SM-SR SHALL update the EIS to reflect that the Fall-Back Attribute is now set for Profile B.

(7) The SM-SR SHALL send the "**ES4.SetFallBackAttribute**" response to the Operator2.

(8) Unless Operator1 has set an ONC to not receive those notifications, the SM-SR SHALL call the "**ES4.HandleProfileFallBackAttributeUnsetNotification"** to notify the un-setting of the Fall-Back Attribute to the Operator1. In case Operator1 has no direct connection with the SM-SR, the SM-SR SHALL send this notification to the SM-DP authorised by Operator1 by calling the "**ES3.HandleProfileFallBackAttributeUnsetNotification"**. Then the SM-DP, on reception of this notification, SHALL forward it to Operator1 by calling the "**ES2.HandleProfileFallBackAttributeUnsetNotification"**.

(9) Unless Operator2 has set an ONC to not receive those notifications, the SM-SR sends the response back to Operator2

(10) The SM-SR SHALL send the "**ES4.HandleProfileFallBackAttributeUnsetNotification**" to an M2M SP, if authorised by Operator1 owning the Profile A.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileFallBackAttributeUnsetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileFallBackAttributeUnsetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileFallBackAttributeUnsetNotification**".

(11) The SM-SR SHALL send the "**ES4.HandleProfileFallBackAttributeSetNotification**" to an M2M SP, if authorised by Operator2 owning the Profile B.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileFallBackAttributeSetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileFallBackAttributeSetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileFallBackAttributeSetNotification**".

End Conditions:
The Profile B has the Fall-Back Attribute set. The Profile A has the Fall-Back Attribute un-set.

3.28 Fall-Back Attribute Management via SM-DP

This procedure contains the steps needed to change the Fall-Back Attribute from one Profile to another via SM-DP (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.19).

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox

Participant "M2M SP" as SP #FFFFFF
Participant "Operator 1\n<size:10>(owning Profile A)</size>" as OP1 #FFFFFF
Participant "Operator 2\n<size:10>(owning Profile B)</size>" as OP2 #FFFFFF
Participant "SM-DP" as DP #FFFFFF
Participant "SM-SR" as SR #FFFFFF
Participant "eUICC" as EUICC #FFFFFF

OP2->DP: [1] ES2.SetFallBackAttribute on Profile B\nRequest (SMSR-ID, EID, ICCID)

Rnote over DP #FFFFFF
[2] Identify SM-SR
Endrnote

DP->SR: [3] ES3.SetFallBackAttibute on Profile B Request (EID, ICCID)

Rnote over SR #FFFFFF
[4] Check PLMA for unsetting Fall-Back
Endrnote

SR-->DP: [4.a] Return response indicating PLMA conflict

DP->OP2: [4.b] Return response indicating PLMA conflict

SR->EUICC: [5] ES5.SetFallBackAttribute on Profile B request

Rnote over EUICC #FFFFFF
[6] Unset Fall-Back Attribute on Profile A
by Setting Fall-Back Attribute on Profile B
Endrnote

EUICC->SR: [7] ES5.SetFallBackAttribute response (euiccResponseData)

Rnote over SR #FFFFFF
[8] Update EIS
Endrnote

SR→DP: [9] ES3.SetFallBackAttibute response

DP→OP2: [10] ES2.SetFallBackAttribute response


SR->OP1: [11] Cond: ES4.HandleProfileFallBackAttributeUnsetNotification Report

SR->SP: [12] Cond: ES4.HandleProfileFallBackAttributeUnsetNotification of Profile A


SR->DP: [13] Cond: ES4.HandleProfileFallBackAttributeSetNotification\nof Profile B

SR->SP: [14] Cond: ES4.HandleProfileFallBackAttributeSetNotification of Profile B

@enduml
```

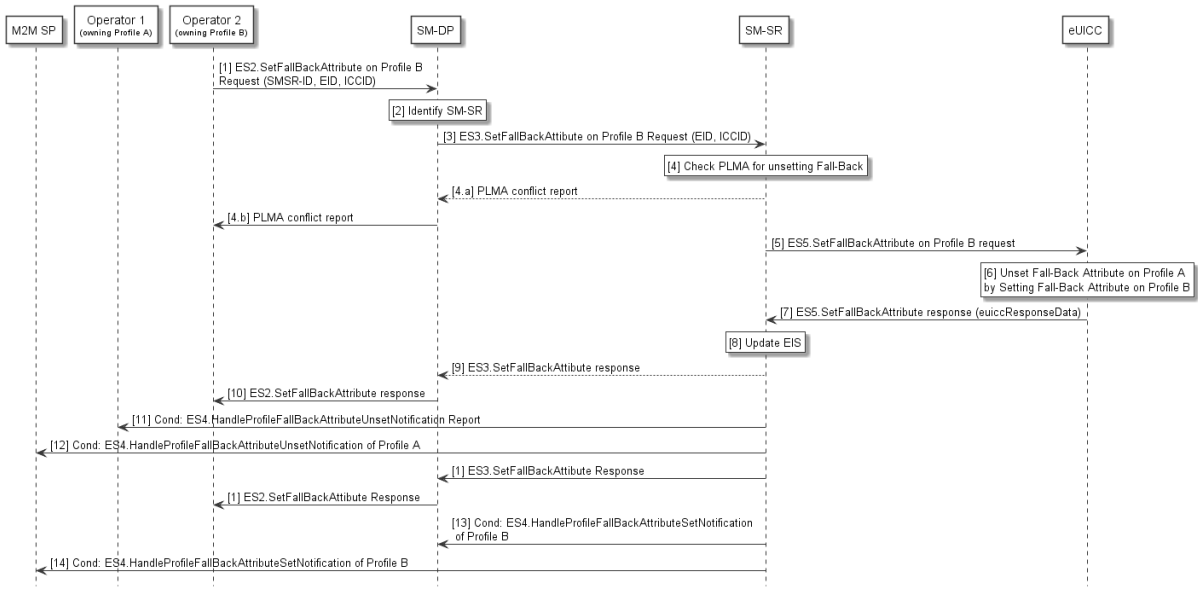


Figure 328: Fall-Back Attribute Management via SM-DP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for Embedded UICC [1].

Procedure:

(1) The Operator2 owning Profile B calls **"ES2.SetFallBackAttribute"** function providing the smsr-id of the SM-SR which will manage the operation and the eid and iccid of the targeted Profile.

(2) The SM-DP identifies the SM-SR.

(3) The SM-DP calls "**ES3.SetFallBackAttribute"** function providing the eid and the iccid of the targeted Profile.

(4) The SM-SR checks if Operator1 has configured a PLMA authorising Operator2 to unset the Fall-Back Attribute on Profile A.
   - **a.** If there is a conflict with the authorisation, the SM-SR aborts the procedure and informs the SM-DP.
   - **b.** The SM-DP informs the Operator2 accordingly

(5) The SM-SR, by calling "**ES5.SetFallBackAttribute"** function (see section 4.11.7), requests the eUICC to set the Fall-Back Attribute to the Profile B.

(6) The eUICC performs the operation. This will remove the Fall-Back Attribute from Profile A.

(7) The eUICC sends the "**ES5.SetFallBackAttribute**" response to the SM-SR by providing the euiccResponseData.

(8) According to the execution status provided by the eUICC, the SM-SR SHALL update the EIS to reflect that the Fall-Back Attribute is now set for Profile B.

(9) The SM-SR SHALL send the "**ES3.SetFallBackAttibute**" response to the SM-DP.

(10) The SM-DP SHALL send the "**ES2.SetFallBackAttibute**" response to the Operator2, informing that the Profile B has the Fall-Back Attribute set.

(11) Unless Operator1 has set an ONC to not receive those notifications, the SM-SR SHALL call the "**ES4.HandleProfileFallBackAttributeUnsetNotification"** function to notify the Fall-Back Attribute un-setting in Profile A to the Operator1. In case Operator1 has no direct connection with the SM-SR, the SM-SR SHALL send this notification to the SM-DP authorised by Operator1 by calling the "**ES3.HandleProfileFallBackAttributeUnsetNotification"**. Then the SM-DP, on reception of this notification, SHALL forward it to Operator1 by calling the **ES2.HandleProfileFallBackAttributeUnsetNotification**.

(12) The SM-SR SHALL send the "**ES4.HandleProfileFallBackAttributeUnsetNotification**" to an M2M SP, if authorised by Operator1 owning the Profile A.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileFallBackAttributeUnsetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileFallBackAttributeUnsetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileFallBackAttributeUnsetNotification**".

(13) Unless Operator2 has set an ONC to not receive those notifications, the SM-SR SHALL call the "**ES4.HandleProfileFallBackAttributeSetNotification"** function to notify the Fall-Back Attribute un-setting in Profile B to the Operator1. In case Operator1 has no direct connection with the SM-SR, the SM-SR SHALL send this notification to the SM-DP authorised by Operator2 by calling the "**ES3.HandleProfileFallBackAttributeSetNotification"**. Then the SM-DP, on reception of this notification, SHALL forward it to Operator2 by calling the **ES2.HandleProfileFallBackAttributeSetNotification**.

(14) The SM-SR SHALL send the "**ES4.HandleProfileFallBackAttributeSetNotification**" to an M2M SP, if authorised by Operator2 owning the Profile B.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileFallBackAttributeSetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileFallBackAttributeSetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileFallBackAttributeSetNotification**".

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

3.29 Fall-Back Attribute Management via M2M SP

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

The Operator1 SHALL authorise the M2M SP the un-setting of the Fall-Back Attribute on its Profile. Operator2 SHALL authorise the M2M SP the setting of the Fall-Back Attribute on its Profile. Such authorisations are granted via PLMA (see GSMA Remote Provisioning Architecture for Embedded UICC [1] section 3.5.20).

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox

Participant "M2M SP" as SP #FFFFFF
Participant "Operator 1\n<size:10>(owning Profile A)</size>" as OP1 #FFFFFF
Participant "Operator 2\n<size:10>(owning Profile B)</size>" as OP2 #FFFFFF
Participant "SM-SR" as SR #FFFFFF
Participant "eUICC" as EUICC #FFFFFF

SP->SR: [1] ES4.SetFallBackAttribute (EID, ICCID) on Profile B Request

Rnote over SR #FFFFFF
[2] Check PLMA for Setting Fall-Back
Attribute from Operator 2
Endrnote
SR-->SP: [2.a] Send response indicating authorisation conflict

Rnote over SR #FFFFFF
[3] Check PLMA for Unsetting Fall-Back
Attribute from Operator 1
Endrnote
SR-->SP: [3.a] Send response indicating authorisation conflict

SR->EUICC: [4] ES5.SetFallBackAttribute on Profile B request

Rnote over EUICC #FFFFFF
[5] Unset Fall-Back Attribute on Profile A
by Setting Fall-Back Attribute on Profile B
Endrnote

EUICC->SR: [6] ES5.SetFallBackAttribute response (euiccResponseData)

Rnote over SR #FFFFFF
[7] EIS Update
Endrnote

SR->SP: [8] ES4.SetFallBackAttribute response

SR->OP1: [9] Cond: ES4.HandleProfileFallBackAttributeUnsetNotification of Profile A

SR->SP: [10] Cond: ES4.HandleProfileFallBackAttributeUnsetNotification of Profile A

SR->OP2: [11] Cond: ES4.HandleProfileFallBackAttributeSetNotification of Profile B

SR->SP: [12] Cond: ES4.HandleProfileFallBackAttributeSetNotification of Profile B

@enduml
```

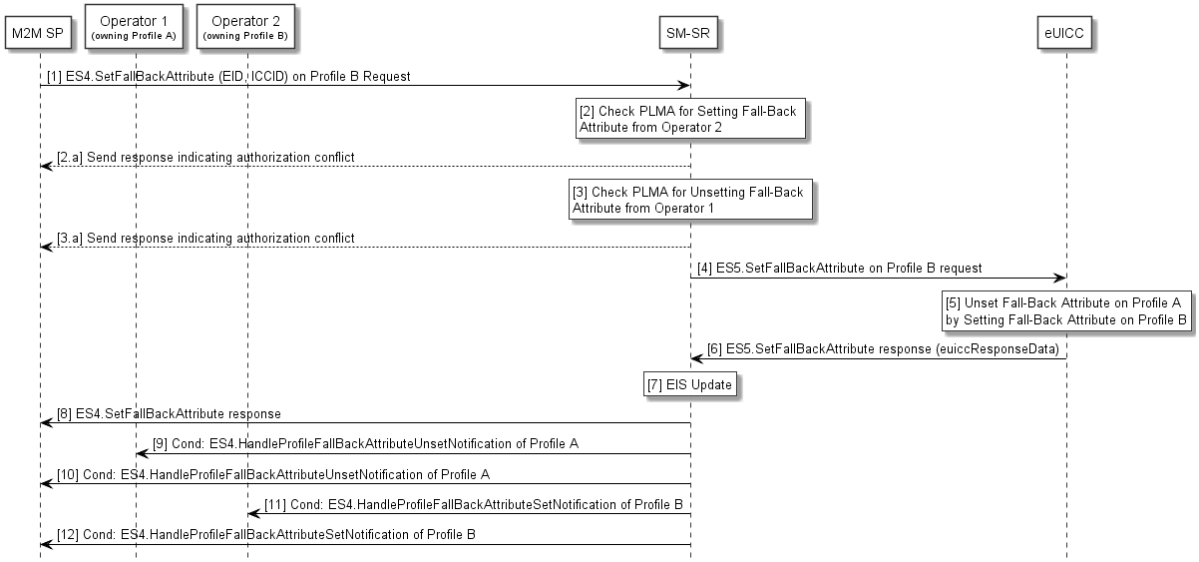


Figure 329: Fall-Back Attribute Management via M2M SP

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for Embedded UICC [1].

Procedure:

(1) The M2M SP calls the "**ES4.SetFallBackAttribute"** on Profile B to the SM-SR, by providing the eid and iccid of the targeted Profile.

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

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

(4) The SM-SR, by calling "**ES5.SetFallBackAttribute"** function, requests the eUICC to set the Fall-Back Attribute to the Profile B.

(5) The eUICC Sets the Fall-Back Attribute on the Profile B. This will remove the Fall-Back Attribute from Profile A.

(6) The eUICC sends the "**ES5.SetFallBackAttribute"** response to the SM-SR by providing the euiccResponseData.

(7) The SM-SR update the EIS accordingly.

(8) The SM-SR SHALL send the "**ES4.SetFallBackAttribute"** response to the M2M SP.

(9) Unless Operator1 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileFallBackAttributeUnsetNotification"** to inform the Operator1 that the Profile A now has the Fall-Back Attribute unset. In case Operator1 has no direct connection with the SM-SR, the SM-SR SHALL send this notification to the SM-DP authorised by Operator1 by calling the "**ES3.HandleProfileFallBackAttributeUnsetNotification"**. Then the SM-DP, on

reception of this notification, SHALL forward it to Operator1 by calling the "**ES2.HandleProfileFallBackAttributeUnsetNotification"**.

(10) If configured by the Operator1, the SM-SR SHALL call the "**ES4.HandleProfileFallBackAttributeUnsetNotification"** to inform the M2M SP.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator1, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileFallBackAttributeUnsetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator1, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileFallBackAttributeUnsetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileFallBackAttributeUnsetNotification**".

(11) Unless Operator2 has set an ONC to not receive those notifications, the SM-SR SHALL send the "**ES4.HandleProfileFallBackAttributeSetNotification"** to inform the Operator2 that the Profile B now has the Fall-Back Attribute set. In case Operator2 has no direct connection with the SM-SR, the SM-SR SHALL send this notification to the SM-DP authorised by Operator2 by calling the "**ES3.HandleProfileFallBackAttributeSetNotification"**. Then the SM-DP, on reception of this notification, SHALL forward it to Operator2 by calling the "**ES2.HandleProfileFallBackAttributeSetNotification"**.

(12) If configured by the Operator2, the SM-SR SHALL call the "**ES4.HandleProfileFallBackAttributeSetNotification"** to inform the M2M SP.

If the M2M SP is another Operator directly connected to the SM-SR and it is authorised by Operator2, the SM-SR SHALL send this notification to this other Operator by calling the "**ES4.HandleProfileFallBackAttributeSetNotification**".

If the M2M SP is another Operator connected through its SM-DP and it is authorised by Operator2, the SM-SR SHALL send this notification to the SM-DP associated to this other Operator by calling the "**ES3.HandleProfileFallBackAttributeSetNotification**". Then the SM-DP, on reception of this notification, SHALL forward it to the Operator, acting as the M2M SP, by calling the "**ES2.HandleProfileFallBackAttributeSetNotification**".

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

3.30 Local Enable for Emergency Profile

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 120
skinparam sequenceArrowThickness 1

hide footbox

participant "Device" as DEV #FFFFFF
participant "eUICC" as eUICC #FFFFFF


DEV->>eUICC : (1) ESx.LocalEnableEmergencyProfile
Rnote over eUICC #FFFFF
(2) Verify that the Emergency Profile exists
Endrnote
eUICC-->>DEV : Error
Rnote over eUICC #FFFFF
(3) Verify that the currently Enabled Profile
     is NOT the Emergency Profile
Endrnote
eUICC-->>DEV : Error

group Profile switch
Rnote over eUICC #FFFFF
(4) Enable Emergency Profile
Endrnote
eUICC-->>DEV : (5) Success
|||
eUICC->>DEV: (6) REFRESH, (UICC reset)
|||
Rnote over DEV, eUICC #FFFFFF
(7) Network attachment with the Emergency Profile
Endrnote
end

@enduml
```

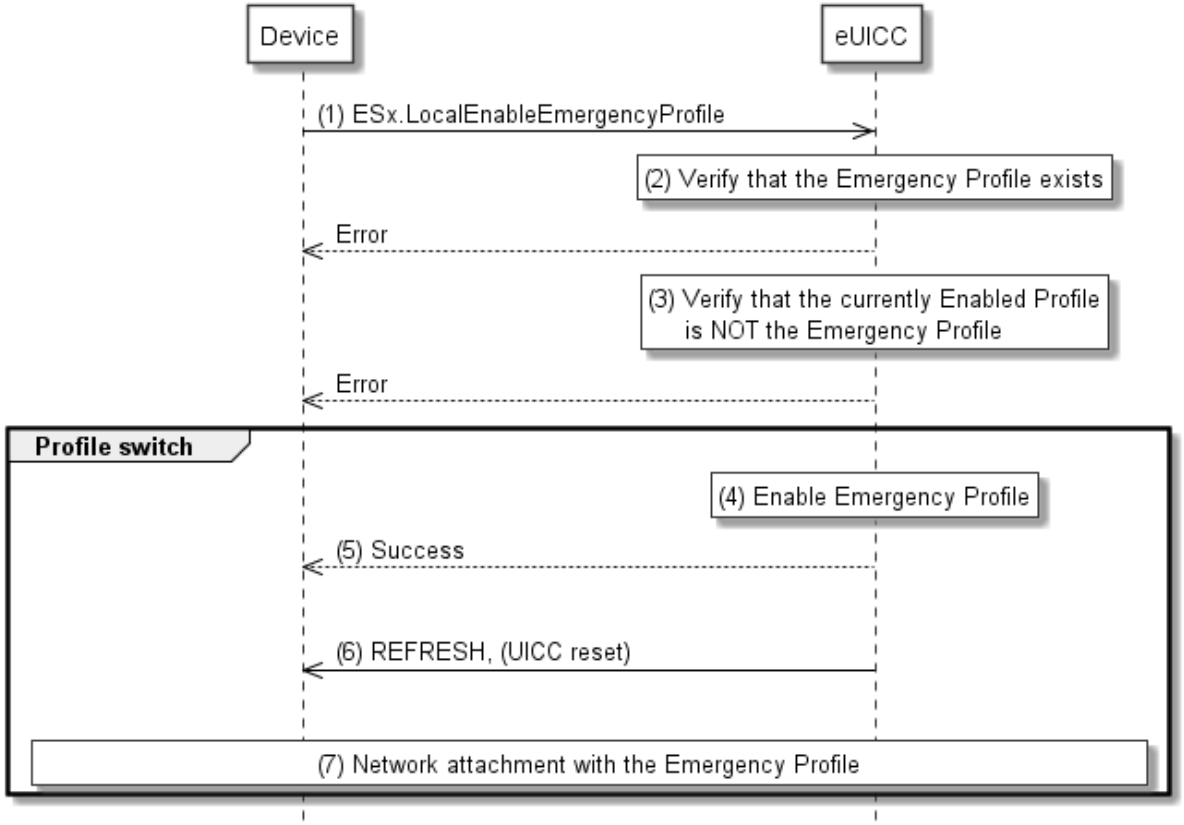


Figure 330: Local Enable of Emergency Profile

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

The Device SHALL call the **"ESx.LocalEnableEmergencyProfile"** function.

The eUICC SHALL verify that the Emergency Profile (Profile with the Emergency Profile Attribute set) exists on this eUICC. If the condition to be verified is not satisfied, the eUICC SHALL return a response indicating the failure, and the procedure SHALL end.

The eUICC SHALL verify that the current Enabled Profile is NOT already the Emergency Profile. If the condition to be verified is not satisfied, the eUICC SHALL return a response indicating that the Emergency Profile is already Enabled, and the procedure SHALL end.

The eUICC SHALL NOT enforce POL1 of the currently Enabled Profile, and SHALL disable the currently Enabled Profile and enable the Emergency Profile.

NOTE: Profile change includes a change of the IMSI that is used to attach to the network. As indicated in 3GPP TS 31.102 [52], such a change requires special caution and should always be accompanied by a REFRESH command to avoid inconsistent information being read by the terminal. So while the Profile is marked as enabled in this step, it MAY actually become effective after the terminal executes the REFRESH command.

The eUICC SHALL return the successful execution status of the "**ESx. LocalEnableEmergencyProfile**" command to the Device.

The eUICC SHALL send a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

The Device SHALL perform a network attach procedure with the newly enabled Profile.

NOTE: Whether the Emergency Profile provides connectivity to a test network or not, the eUICC will not attempt to enable automatically the previously Enabled Profile. This is in contrast to the remote enable procedures (for example in section 3.2.2).

3.31 Local Disable for Emergency Profile

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black
skinparam maxmessagesize 450
skinparam ParticipantPadding 100
skinparam sequenceArrowThickness 1

hide footbox

participant "Device" as DEV #FFFFFF
participant "eUICC" as ISDR #FFFFFF

DEV->>ISDR : (1) ESx.LocalDisableEmergencyProfile

Rnote over ISDR  #FFFFF
(2) Verify that the currently Enabled profile
     is the Emergency  Profile
Endrnote
ISDR-->>DEV : Error

group Profile switch
Rnote over ISDR  #FFFFF
(3) Disable Emergency Profile and
      enable previously Enabled Profile
Endrnote
ISDR-->>DEV : (4) Sucess
|||
ISDR->>DEV: (5) REFRESH, (UICC reset)
|||
Rnote over DEV, ISDR #FFFFFF
(6) Network attachment with the Enabled Profile
Endrnote
End
@enduml
```

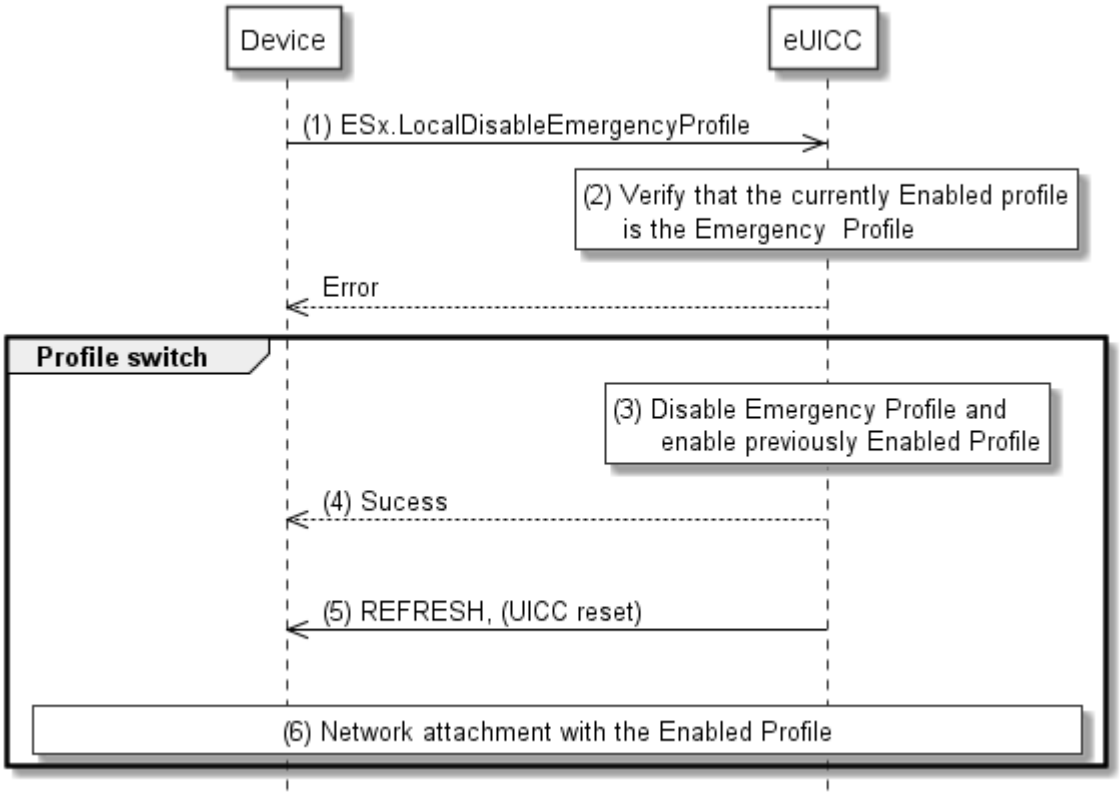


Figure 331: Local Disable of Emergency Profile

Start Conditions:

The start conditions are described in GSMA Remote Provisioning Architecture for the Embedded UICC [1].

Procedure:

(1) The Device SHALL call the **"ESx.LocalDisableEmergencyProfile"** function.

The eUICC SHALL verify that the currently Enabled Profile is the Emergency Profile (Emergency Profile attribute set). If the condition to be verified is not satisfied, the eUICC SHALL return a response indicating that the Emergency Profile is not Enabled, and the procedure SHALL end.

The eUICC SHALL NOT enforce POL1 of the Enabled Emergency Profile, and SHALL disable the Emergency Profile and enable the previously Enabled Profile.

NOTE: The previously Enabled Profile is the Profile that was Enabled, before the Emergency Profile was enabled by the "ESx.LocalEnableEmergencyProfile" command.

The eUICC SHALL return the successful execution status of the "**ESx.LocalDisableEmergencyProfile**" command to the Device.

The eUICC SHALL send a REFRESH proactive command in UICC reset mode to the Device. This will trigger the execution of a network attach procedure.

The eUICC and the Device SHALL perform a network attach procedure with the newly Enabled Profile.

Dependent on the configuration of the eUICC, the eUICC MAY send a Notification about the Profile change after Emergency Profile disabling to the SM-SR.

4 eUICC Interface Descriptions

This section contains the technical descriptions of those interfaces within the Remote Provisioning and Management system involving the eUICC directly, including the following:

- ES5, interface between the SM-SR and the eUICC.
- ES6, interface between the Operator and the eUICC
- ES8, interface between the SM-DP and the eUICC.
- ESx, interface between the Device and the eUICC.

The following table presents the normative list of all the functions that are defined in this section.

Request-response functions:

Interface	Function group	Functions	Function provider entity
ES5	Platform Management	CreateISDP	ISD-R

		EnableProfile	
		DisableProfile	
		DeleteProfile	
		eUICCCapabilityAudit	
		MasterDelete	
		SetFallbackAttribute	
		SetEmergencyProfileAttribute	
	eUICC Management	EstablishISDRKeySet	
		FinaliseISDRhandover	
		UpdateSMSRAddressingParameters	
ES6	Profile Management	UpdatePOL1byMNO	MNO-SD
		UpdateConnectivityParametersByMNO	
ES8	Profile Management	DownloadAndInstallation	ISD-P
		EstablishISDPKeySet	
		UpdateConnectivityParameters SCP03	
ESx	Local Management	LocalEnableEmergencyProfile	
		LocalDisableEmergencyProfile	
		LocalEnableTestProfile	
		LocalDisableTestProfile	

Table 5:: Request Response Functions

Notification handler functions:

Interface	Function group	Notification handler functions	Function provider Role
ES5	Platform Management	`HandleDefaultNotification` `HandleNotificationConfirmation`	SM-SR

Table 6: Notification Handler Functions

4.1 Functions Description

NOTE: 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 command.

4.1.1 ES5 (SM-SR–eUICC) Interface Description

4.1.1.1 ISD-P Creation

Function name: CreateISDP

Related Procedures: ISD-P creation

Function group: Platform Management

Function Provider entity: ISD-R

Description: This function creates an ISD-P on the eUICC.

Parameters:

- ISD-P-AID
- Cumulative Granted Non Volatile Memory for the ISD-P (optional)

Prerequisite:

- The SM-SR has assigned an ISD-P-AID.

Command Description:

INSTALL COMMAND

The command is an Install command as defined in GlobalPlatform Card Specification [6].

The following tables describe the installation command and the specific parameters within the data field:

Code	Value	Meaning
CLA	‘80’	See GlobalPlatform Card Specification section 11.1
INS	‘E6’	INSTALL
P1	‘0C’	See GlobalPlatform Card Specification [6] section 11.5.2.1
P2	‘00’	See GlobalPlatform Card Specification [6] section 11.5.2.2

Code	Value	Meaning
Lc	‘xx’	Data Field Length
Data	‘xxxx…’	See GlobalPlatform Card Specification [6] section 11.5.2.3
Le	‘00’	

Table 7: INSTALL Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	1	0	0	0	For make selectable
0	0	0	0	0	1	0	0	For Install

Table 8: INSTALL Reference Control Parameter P1

Reference Control Parameter P2 – ISD-P State Coding

P2 is set to ‘00’; according to GlobalPlatform Card Specification [6] section 11.5, this means no information provided.

Data Field

Name	Length	Value Description	MOC
Length of Executable Load File AID	’1’	‘05’ - ‘10’	M
Executable Load File AID	‘05’ – ‘10’	‘xxxx’	M
Length of Executable Module AID	‘1’	‘05’ - ‘10’	M
Executable Module AID	‘05’ – ‘10’	‘xxxx’	M
Length of Application AID	‘1’	‘05’ - ‘10’	M
Application AID (ISD-P-AID)	‘05’ – ‘10’	‘xxxx’	M
Length of Privileges	‘1’	‘01’ - ‘03’	M
Privileges	‘1’or ‘3’	See [6] section 11.1.2	M
Length of Install Parameters field	’2’-‘n’		M
Install Parameters field	‘0-n’	See [6] section 11.5.2.3.7	M
Length of Install Token	‘1’	00	M

Table 9: INSTALL Command Data Field

Privileges

Privileges granted to the ISD-P, as specified in Annex C, SHALL be at least:

- Security Domain
- Trusted Path
- Authorized Management

Install Parameters

Tag	Length	Value Description	MOC

'C9'	'1-n'	Application Specific Parameters: see GlobalPlatform Card Specification [6] section 11.5.3.2.			M
		Tag	**Length**	**Value Description**	**MOC**
		'81'	2	Secure Channel Protocol Identifier and Implementation Option "i"	M (n occurrences)
'EF'	'1-n'	System Specific Parameters			O
		Tag	**Length**	**Value Description**	**MOC**
		'83'	'2' or '4'	Cumulative Granted Non Volatile Memory	O

Table 10: INSTALL Parameters

Data *Returned*

None

***Response* Message**

Data Field Returned in the Response Message:

A single byte of '00' SHALL be returned indicating that no additional data is present, as defined in the GlobalPlatform Card Specification [6] section 11.5.3.1.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.5.3.2.

4.1.1.2 Profile Enabling

Function name: EnableProfile

Related Procedures: Profile Enabling

Function group: Platform Management

Function Provider entity: ISD-R

Description: This function is used to enable a Profile on the eUICC.

The function makes the target Profile enabled, and disables implicitly the currently Enabled Profile.

Parameters:

- ISD-P-AID

Prerequisites:

- SM-SR has checked that POL2 of both the currently Enabled Profile and the target Profile allow this action.
- The target Profile SHALL NOT be the Test Profile

Function Flow

Upon reception of the Profile Enabling command, the eUICC SHALL:

- Verify that the target Profile is in the disabled state
- Verify that POL1 of the currently Enabled Profile allows its disabling
- Verify that the target Profile is not the Test Profile
- If any of these verifications fail, terminate the command with an error status word
- If the current profile has been enabled by the activation of the Fall-Back Mechanism then
  - If the target Profile is not the previously Enabled profile and the POL1 of the previously enabled profile does not allow its own disabling, or contains the rule “Profile deletion is mandatory when its state is changed to disabled”, terminate the command with an error status word
- Disable the currently Enabled Profile and Enable the target Profile
- Send the REFRESH command in “UICC Reset” mode to the Device according to ETSI TS 102 223 [3]

NOTE: The eUICC SHALL send the command response (over SMS PoR or HTTP POST or CAT-TP SDU) before issuing the proactive command REFRESH. So it is possible but not required that the eUICC send the REFRESH command immediately. However the eUICC SHALL issue the REFRESH command within a time interval of 10 STATUS events after receiving the enable command.

- Send notification.

Command Description:

STORE DATA COMMAND

This command is a STORE DATA command, as described in GlobalPlatform Card Specification [6].

Code	Value	Meaning
CLA	‘80’	
INS	‘E2’	STORE DATA
P1	‘88’	Reference Control Parameter P1 0
P2	‘00’	Block Number (Not used for Enable command)
Lc	‘XX’	Length of data field
Data	‘XX’	Application Data and MAC (if present)
Le	Not present	

Table 11: STORE DATA COMMAND Message

Parameter P1 is coded according to the following table:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	X	X	X	RFU

Table 12: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A03'	Var	Enable Profile			M
		Tag	**Length**	**Value Description**	**MOC**
		'4F'	5-16	ISD-P-AID	M

Table 13: Enable Attribute Data Field

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL NOT be present.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.11.3.2.

Specific Processing State returned in response Message:

’69 85’: Profile is not in the Disabled state, or Profile is the Test Profile.

’69 E1’: POL1 of the currently Enabled Profile or of the previously enabled profile prevents this action.

4.1.1.3 Profile Disabling

Function name: DisableProfile

Related Procedures: Profile Disabling

Function group: Platform Management

Function Provider entity: ISD-R

Description: This function is used to disable a Profile on the eUICC.

This function makes the target Profile Disabled, and implicitly enables the Profile which has the Fall-Back Attribute set.

Parameters:

- ISD-P-AID of the currently Enabled Profile

Prerequisites:

- SM-SR has checked that POL2 allows this action
- The target Profile SHALL NOT be the Test Profile

Function flow

Upon reception of the Profile Disabling command, the eUICC SHALL:

- Verify that the target Profile is in Enabled state
- Verify that POL1 of the currently Enabled Profile allows its disabling
- Verify that the target Profile is not the Test Profile
- Verify that the target Profile is not the Profile with Fall-Back Attribute set
- If any of these verifications fail, terminate the command with an error status word.
- Disable the target Profile and enable the Profile with the Fall-Back Attribute set
- Send the REFRESH command in “UICC Reset” mode to the Device according to ETSI TS 102 223 [3].

Note: The same note about deferred REFRESH as for enable command applies as well to disable: The eUICC SHALL issue the REFRESH command within a time interval of 10 STATUS events after receiving the disable command.

Command Description:

STORE DATA COMMAND

This command is a STORE DATA command, as described in GlobalPlatform Card Specification [6].

Code	Value	Meaning
CLA	‘80’	
INS	‘E2’	STORE DATA
P1	'88'	Reference control parameter P1
P2	‘00’	Block Number (Not used for Enable command)
Lc	‘xx’	Length of data field
Data	‘xx’	Application Data and MAC (if present)
Le	Not present	

Table 14: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	X	X	X	RFU

Table 15: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A04'	Var	Disable Profile			M
		Tag	**Length**	**Value Description**	**MOC**
		'4F'	5-16	ISD-P-AID	M

Table 16: Disable Attribute Data Field

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL NOT be present.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.11.3.2.

Specific Processing State returned in response Message:

’69 85’: Profile is not in the Enabled state or Profile has the Fall-Back Attribute set or Profile is the Test Profile.

’69 E1’: POL1 of the Profile prevents disabling.

4.1.1.4 Profile Deletion

Function name: DeleteProfile

Related Procedures: Profile and ISD-P deletion, Profile and ISD-P deletion via SM-DP

Function group: Platform Management

Function Provider entity: ISD-R

Description: This function is used to delete a Profile from the eUICC.

This function deletes the ISD-P and its associated Profile.

Parameters:

- ISD-P-AID

Prerequisites:

- SM-SR SHALL check that POL2 allows this action
- The target Profile SHALL NOT be the Profile with the Fall-Back Attribute set
- The target Profile SHALL NOT be the Test Profile

Function flow

Upon reception of the DELETE command, the eUICC SHALL:

- If the Profile is in Disabled state:
  - Verify that POL1 of the target Profile allows its deletion. This includes, if the target Profile has been Disabled by the activation of the Fall-Back Mechanism described in section 3.16, verify that POL1 of the target Profile allows Disabling.
- Verify that the target Profile is not the Profile with Fall-Back Attribute set
- Verify that the target Profile is not the Test Profile
- Verify that the target Profile is not in the Enabled state
- If any of these verifications fail, terminate the command with an error status word
- Delete the ISD-P with its Profile.

NOTE: An incomplete Profile (i.e. the ISD-P is still in state SELECTABLE or PERSONALIZED) can always be deleted.

Command Description:

DELETE COMMAND

This function is realised through the GlobalPlatform DELETE command as defined in GlobalPlatform Card Specification Amendment C [9].

Command Message

The DELETE command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' - '8F', 'C0' - 'CF' or 'E0' - 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E4'	DELETE
P1	'00'	Reference control parameter P1
P2	'40'	Reference control parameter P2
Lc	'xx'	Length of data field
Data	'xxxx…'	TLV coded objects (and MAC if present)
Le	'00'	

Table 17: DELETE Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	Last (or only) command
-	X	X	X	X	X	X	X	RFU

Table 18: DELETE Reference Control Parameter P1

Reference Control Parameter P2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	1	–	–	–	–	–	–	Delete a root security domain and all associated Applications
–	–	X	X	X	X	X	X	RFU

Table 19: DELETE Command Reference Control Parameter P2

Data Field Sent in the Command Message

The data field of the DELETE command message SHALL contain the TLV coded name(s) of the object to be deleted.

Tag	Length	Value Description	MOC
'4F'	5-16	ISD-P-AID	M

Table 20: DELETE [card content] Command Data Field

Response Message

Data Field Returned in the Response Message:

A single byte of '00' SHALL be returned indicating that no additional data is present.

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.2.3.2.

Specific Processing State returned in response Message:

’69 85’: Profile is in Enabled State or Profile has the Fall-Back Attribute or Profile is the Test Profile.

’69 E1’: POL1 of the Profile prevents deletion (including the case where the Profile has been Disabled by the activation of the Fall-Back Mechanism, and its POL1 prevents disabling).

4.1.1.5 eUICC Capability Audit

Function name: eUICCCapabilityAudit

Related Procedures: -

NOTE: This function is not present in any procedure, however, it MAY be used and requested at any point of time by the Profile owner or SM-SR.

Function group: Platform Management

Function Provider entity: ISD-R

Description: This function is used to query the status of the eUICC.

Parameters:

It may be used to ensure the data within the SM-SR's EIS database is up to date. This function uses two commands which SHALL be implemented as an extension of the GlobalPlatform functions GET DATA and GET STATUS.

GET DATA

This function can return:

- Number of installed ISD-P and available not allocated memory
- ECASD Certificate

GET STATUS

This function can return:

- Each ISD-P-AID
- State of the ISD-Ps / Profiles

Prerequisites:

- None

Commands Description:

GET DATA

The GET DATA command is coded according to the following table:

Code	Value	Meaning
CLA	'80'	See GlobalPlatform Card Specification section 11.1.4.1
INS	'CA'	GET DATA
P1	'xx'	See below
P2	'xx'	See below
Lc	'xx'	Not present if no command data, otherwise length of data field
Data	'xxxx...'	Not present, or command data
Le	'00'	

Table 21: GET DATA Command Message

Parameter P1 and P2

The P1 and P2 parameters define the tag of the data object to be read.

Tag 'FF 21': Extended Card Resources Information available for Card Content Management, as defined in ETSI TS 102 226 [5].

Tag ‘BF 30’: Forwarded CASD Data mechanism as defined in GlobalPlatform Card Specification Amendment C [9].

This mechanism allows to retrieves ECASD data through the ISD-R.

Data field

If the P1 and P2 parameters are set to ‘BF 30’, the data field SHALL include one (and only one) of the following requests:

- ECASD recognition data: ‘5C 01 66’
- ECASD Certificate Store (containing ECASD Public Key Certificates): ‘5C 02 7F 21’

Response Message

If certificate data is requested, the certificate SHALL be returned TLV-coded as follows:

Name	Length	Value Description	MOC
Forwarded CASD Data tag	2	‘BF 30’	C
Length of the response	1, 2 or 3	'00' - '7F', or '81 80' - '81 FF' or '82 01 00' - '82 FF FF'	C
Certificate store tag	2	‘7F 21‘	M
Length of the certificate	1, 2 or 3	'00' - '7F', or '81 80' - '81 FF' or '82 01 00' - '82 FF FF'	M
Certificate data	n	‘xxxx…’	M

Table 22: GET DATA Command Data Field

Certificate Data

The following table describes the certificate data which will be returned by the eUICC Capability Audit command.

Tag	Length	Value Description			MOC
'7F21'	Var.	Certificate			M
		Tag	**Length**	**Value Description**	**MOC**
		'93'	1-16	Certificate Serial Number	M
		'42'	1-16	CA Identifier (value part of the DER-TLV encoding of the EUM OID e.g. bytes= 2B06010401… for OID=1.3.6.1.4.1….).	M
		'5F20'	16	Subject Identifier (EID	M
		'95'	2	Key Usage ‘0080’: Key Agreement	M
		'5F25'	4	Effective Date (YYYYMMDD, BCD format)	M
		'5F24'	4	Expiration Date (YYYYMMDD, BCD format)	M
		‘45’	1-16	ECASD Image Number (ISDN)	M

<table>
<tr><td></td><td></td><td>'73'</td><td>Var.</td><td>Discretionary Data:

<table><tr><th>Tag</th><th>Length</th><th>Value Description</th></tr><tr><td>'C0'</td><td>var</td><td>eUICC Supplier Identifier</td></tr><tr><td>'C1'</td><td>var</td><td>eUICC Product Line Identifier</td></tr><tr><td>'C2'</td><td>var</td><td>eUICC Extended GSMA SAS Accreditation Serial Number</td></tr><tr><td>‘C9’</td><td>20</td><td>Authority key identifier (value of the Subject Key Identifier extension of the EUM certificate)</td></tr></table>Other TLVs MAY be present</td><td>M</td></tr>
<tr><td></td><td></td><td>'7F49'</td><td>Var.</td><td>Public Key</td><td>M</td></tr>
<tr><td></td><td></td><td>'5F37'</td><td>Var.</td><td>Signature (to be computed as described in GlobalPlatform Card Specification Amendment E [11] and the signature SHALL include all the field starting from tag '93' to tag '7F49')</td><td>M</td></tr>
</table>

Table 23: eUICC Certificate Data Fields

Public Key Data Object

The public key data object contains an elliptic curves (EC) public key and the corresponding domain parameters.

<table>
<tr><th>Tag</th><th>Length</th><th colspan="3">Value Description</th><th>MOC</th></tr>
<tr><td>'7F49'</td><td>Var.</td><td colspan="3">Public Key Data Object</td><td>M</td></tr>
<tr><td></td><td></td><th>Tag</th><th>Length</th><th>Value Description</th><th>MOC</th></tr>
<tr><td></td><td></td><td>'B0'</td><td>Var</td><td>Public key – Q</td><td>M</td></tr>
<tr><td></td><td></td><td>'F0'</td><td>'01'</td><td>Key Parameter Reference
‘00’: NIST P-256
‘03’: brainpoolP256r1
‘40’: FRP256V1 [51]</td><td>M</td></tr>
</table>

Table 24: Public Key Data Object Data Field

An ECASD SHALL have at least one set of elliptic curve parameters preloaded (see GlobalPlatform Card Specification Amendment E [11]) as defined in the table above.

GET STATUS

The GET STATUS command is coded according to the following table:

Code	Value	Meaning
CLA	‘80’	See GlobalPlatform Card Specification [6] section 11.1.4.1
INS	‘F2’	GET STATUS

Code	Value	Meaning
P1	'40'	See GlobalPlatform Card Specification [6] section 11.4.2.1.
P2	'xx'	See GlobalPlatform Card Specification [6] section 11.4.2..2.
Lc	'xx'	Length of the data field
Data	'4F xx …'	See GlobalPlatform Card Specification [6] section 11.4.2.3.
Le	'00'	

Table 25: GET STATUS Command Message

Parameter P1

The following value will be used for P1:

'40' – Applications and Supplementary Security Domains only

Parameter P2

The parameter P2 controls the number of consecutive GET STATUS commands.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	X	X	X	X	-	-	RFU
-	-	-	-	-	-	1	-	Response Data Structure according to table 11-36 of GlobalPlatform Card Specification [6].
-	-	-	-	-	-	-	0	Get first or all occurrence(s)
-	-	-	-	-	-	-	1	Get next occurrence(s)

Table 26: GET STATUS Command Reference Control Parameter P2

Data field sent in the Command Message

The GET STATUS command message data field SHALL contain at least one TLV coded search qualifier: the AID (tag '4F'). It SHALL be possible to search for all the occurrences that match the selection criteria according to the reference control parameter P1 using a search criteria of '4F 00'.

The search is limited to the ISD-P instances.

The following other search criteria SHALL be supported: Life Cycle State (tag '9F70') and ISD-P Attributes (tag '53').

The tag list (tag '5C') indicates to the UICC how to construct the response data for each eUICC entity matching the search criteria.

The data field is structured as follows:

Tag	Length	Value Description	MOC
'4F'	0-16	Application AID	M
'xx' or 'xxxx'	0-n	Other search criteria	O
…	…	…	…
'5C'	1-n	Tag list	M

Table 27: GET STATUS Command Data Field

Response Message

Data Field Returned in the Response Message:

The tag list (tag '5C') identifies the extended information for ISD-P. The coding of the response message is defined as followed:

Tag	Length	Name			MOC
'E3'	Variable	GlobalPlatform Registry related data			M
		Tag	**Length**	**Name**	**MOC**
		'4F'	5-16	AID	M
		'9F70'	1	Life Cycle State	C
		'53'	1	ISD-P Properties (see Table 29)	C
		'8F'	2 or 4	Cumulative Granted Non-Volatile Memory as defined in GlobalPlatform Specification v2.2 amendment C [9]	C
		'91'	2 or 4	Cumulative Remaining Non-Volatile Memory as defined in GlobalPlatform Specification v2.2 amendment C [9]	C

Table 28: GET STATUS Command Data Field Return

If an ISD-P that matches the search criteria was installed without Cumulative Granted Memory option, the related tags '8F' and '91' SHALL be absent in the response, even if they were requested in the tag list of the command.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	X	X	X	-	-	-	RFU
-	-	-	-	-	X	X	0	Fall-Back Attribute not set
-	-	-	-	-	0	0	1	Fall-Back Attribute set
-	-	-	-	-	X	0	X	Emergency Profile Attribute not set
-	-	-	-	-	0	1	0	Emergency Profile Attribute set
-	-	-	-	-	0	X	X	Test Profile Flag not set
-	-	-	-	-	1	0	0	Test Profile Flag set

Table 29: ISD-P Properties

ISD-P State Coding

The life cycle of the ISD-P is coded as define in section 2.2.1.3.

Processing State returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.3.3.2.

4.1.1.6 Master Delete

Function name: MasterDelete

Related Procedures: Master Delete Procedure

Function group: Platform Management

Function Provider entity: ISD-R

Description: This function deletes a target Profile on the target eUICC regardless of POL1 rules. This function SHALL use the ISD-P token verification key(AES key with key version number '70' and key identifier '01') in order to authenticate the source of the command.

Parameter:

- ISD-P-AID
- Delete Token, calculated as defined in GlobalPlatform Card Specification Amendment D [10] , provided by the SM-DP

Prerequisites:

- The target Profile SHALL NOT be the Profile which has the Fall-Back Attribute set.
- The target Profile SHALL be in the Disabled state.

Function flow

Upon reception of the Master Delete command, the eUICC SHALL:

- Verify that the target Profile is in the Disabled state
- Verify that the target Profile is not the Profile with Fall-Back Attribute set
- Verify the Token (actually performed by the ISD-P). This includes verifying the signature of the Token, and verifying that the values of tags 42, 45, and 5F20 in the Token match the corresponding values in the ISD-P.
- If any of these verifications fail, terminate the command with an error status word.
- Delete the ISD-P with its Profile, regardless of POL1.

As token protection is only used by this command, this token SHALL be processed by the ISD-P even though the ISD-P does not have the token verification privilege. No receipt SHALL be generated by the command.

The eUICC SHALL support setting the value of tags 42, 45, and 5F20 by a STORE DATA command defined in GlobalPlatform Card Specification [6]. If the value of tag 5F20 is not set by the SM-DP, the default value SHALL be the value of the RID of ISD-P defined in section 2.2.3.

NOTE1: This deviates from the typical handling of tokens by SDs.

NOTE 2: The SM-DP MAY set the values of tags 42, 45 and 5F20 during profile download.

Command Description:

This function is realised through the GlobalPlatform DELETE command as defined in GlobalPlatform Card Specification Amendment C [9].

Command Message

DELETE COMMAND

The DELETE command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' – '8F', 'C0' – 'CF' or 'E0' – 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E4'	DELETE
P1	'00'	Reference control parameter P1
P2	'40'	Reference control parameter P2
Lc	'xx'	Length of data field
Data	'xxxx…'	TLV coded objects (and MAC if present)
Le	'00'	

Table 30: DELETE Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	Last (or only) command
-	X	X	X	X	X	X	X	RFU

Table 31: DELETE Reference Control Parameter P1

Reference Control Parameter P2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	1	–	–	–	–	–	–	Delete a root security domain and all associated Applications
–	–	X	X	X	X	X	X	RFU

Table 32: DELETE Command Reference Control Parameter P2

The Delete [card content] Data Field SHALL contain the following parameters:

Tag	Length	Value Description			MOC
'4F'	5-16	ISD-P-AID to be deleted			M
'B6'	Var.	Control Reference Template for Digital Signature			M
		Tag	**Length**	**Value Description**	**MOC**
		'42'	1-n	Identification Number of the ISD-P	M
		'45'	1-n	Image Number of the ISD-P	M
		'5F20'	1-n	Application Provider identifier	M
		'93'	1-n	Token identifier number	M
'9E'	1-n	Delete Token			M

Table 33: DELETE [card content] Command Data Field

Response Message

Data Field Returned in the Response Message:

A single byte of ‘00’ SHALL be returned indicating that no additional data is present.

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.2.3.2.

Specific Processing State returned in response Message:

’69 85’: Profile is not in the Disabled state or Profile has the Fall-Back Attribute set.

4.1.1.7 Set Fall-Back Attribute

Function name: SetFallbackAttribute

Related Procedures: -

Function group: Platform Management

Function Provider entity: ISD-R

Description: This function sets the Fall-Back Attribute for one Profile on the target eUICC.

Parameters:

- ISD-P-AID

Prerequisites:

- The Profile to be assigned the Fall-Back Attribute must have Provisioning capability.

Function flow

Upon reception of the STORE DATA command, the eUICC SHALL:

- Set the Fall-Back Attribute for the target Profile
- Remove the Fall-Back Attribute from the Profile that has the attribute currently assigned

Setting of the Fall-Back Attribute is done via ISD-R.

If the currently Enabled profile is the Profile with the Fall-Back Attribute set, and has been Enabled by the activation of the Fall-Back Mechanism, and the previously Enabled Profile has either of the POL1 rules “Disable not allowed” or “Profile deletion is mandatory when its state is changed to Disabled” set, then the eUICC SHALL prevent the execution of the function “Set Fall-Back Attribute”.

Command Description:

STORE DATA Command

This function is realised through the GlobalPlatform STORE DATA command as defined in GlobalPlatform Card Specification [6].

Command Message

The STORE DATA command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' – '8F', 'C0' – 'CF' or 'E0' – 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E2'	STORE DATA
P1	'88'	Reference control parameter P1
P2	'00'	Block number
Lc	'xx'	Length of data field
Data	'xxxxx…'	Application data and MAC (if present)
Le		Not present

Table 34: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	X	X	X	RFU

Table 35: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A05'	Var	Set Fall-Back Attribute			M
		Tag	Length	Value Description	MOC
		'4F'	5-16	ISD-P-AID	M

Table 36: Set Fall-Back Attribute Data Field

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL NOT be present.

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.11.3.2, with the following addition:

'69 E1': POL1 of the Profile Disabled by the activation of the Fall-Back Mechanism prevents this action.

4.1.1.8 ISD-R Key Set Establishment

Function name: EstablishISDRKeySet

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider entity: ISD-R

Description: This function is used to perform mutual authentication between the new SM-SR and the eUICC and to establish a shared secret key set between the new SM-SR and the ISD-R.

This function is based on Scenario 3 as defined in “GlobalPlatform Card Specification Amendment E [11]. Scenario 3 is modified by adding the additional step of authentication of the new SM-SR to the eUICC.

Adding this step to Scenario 3 requires an additional STORE DATA command to precede the command defined for Scenario 3. This new command provides the eUICC with the certificate of the new SM-SR and retrieves a random challenge from the eUICC. This random challenge then has to be signed by the new SM-SR and sent to the eUICC in the second command to prove to the eUICC that the new SM-SR is in possession of the private key related to the certificate presented. The sequence is pictured in Figure 23 of section 3.8.

Parameters:

- Ephemeral public key of the new SM-SR
- Certificate for the new SM-SR

Prerequisites:

- The ECASD certificate was provided to and verified by the new SM-SR
- The new SM-SR has generated an ephemeral key pair
- The new SM-SR has a signature from the CI.

Command Description:

This function is realised through GlobalPlatform STORE DATA commands as defined in GlobalPlatform Card Specification [6].

First STORE DATA command

Command Message

The STORE DATA command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	‘80’ – ‘8F’, ‘C0’ – ‘CF’ or ‘E0’ – ‘EF’	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	‘E2’	STORE DATA
P1	‘09’	Reference control parameter P1
P2	‘00’	Block number
Lc	‘xx’	Length of data field
Data	‘xxxxx…’	Application data and MAC (if present)
Le	‘00’	

Table 37: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	More blocks
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-			1	Case 4 command as defined in GlobalPlatform Amendment A [54]
-	-	-	-	-	X	X	-	RFU

Table 38: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description					MOC
'3A01'	Var	Certificate of off-card entity					M
		Tag	Length	Value Description			MOC
		'7F21'	Var.	Certificate			M
				Tag	Length	Value Description	MOC
				'93'	1-16	Certificate Serial Number	M
				'42'	1-16	CA Identifier	M
				'5F20'	1-16	Subject Identifier	M
				'95'	1	Key Usage, Signature Verification	M
				'5F25'	4	Effective Date (YYYYMMDD, BCD format)	O
				'5F24'	4	Expiration Date (YYYYMMDD, BCD format)	M
				'73'	3-127	Discretionary Data Tag / Length / Value Description 'C8' / 1 / '02', denoting an SM-SR certificate 'C9' / 20 / Authority key identifier (value of the Subject Key Identifier extension of the Root certificate) other TLVs MAY be present	M
				'7F49'	Var.	Public Key – details see tables below	M
				'5F37'	Var.	Signature	M

Table 39: Data Fields for Send SM-SR Certificate for ISD-R Key Establishment

The following TLV-encoded data are signed off-card with SK.CI.ECDSA to generate the content of tag '5F37' (signature), as described in GlobalPlatform Card Specification Amendment E [11]:

Tag	Length	Value Description	MOC
'93'	1-16	Certificate Serial Number	M
'42'	1-16	CA Identifier	M
'5F20'	1-16	Subject Identifier	M
'95'	1	Key Usage, Signature Verification	M

‘5F25’	4	Effective Date (YYYYMMDD, BCD format) – if present	C
‘5F24’	4	Expiration Date (YYYYMMDD, BCD format)	M
‘73’	3-127	Discretionary Data	M
‘7F49’	Var.	Public Key	M

Table 40: Data Signed to Generate the SM-SR Certificate

Key format is defined in section 4.1.1.5.

Response Message

Data Field Returned in the Response Message:

The STORE DATA response SHALL contain the following data:

Tag	Length	Data Element
'85'	Variable	Random Challenge

Table 41: Response Data for Send SM-SR Certificate

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.11.3.2.

Second STORE DATA command

Command Message

The STORE DATA command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' - '8F', 'C0' - 'CF' or 'E0' - 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E2'	STORE DATA
P1	'89'	Reference control parameter P1
P2	'01'	Block number
Lc	'xx'	Length of data field
Data	'xxxxx…'	Application data and MAC (if present)
Le	‘00’	

Table 42: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	-	-	1	Case 4 command as defined in GlobalPlatform Amendment A [54]
-	-	-	-	-	X	X	-	RFU

Table 43: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description					MOC
'3A02'	Var	Key Establishment					M
		Tag	**Length**	**Value Description**			**MOC**
		'A6'	Var	CRT tag (KAT)			
				Tag	**Length**	**Value Description**	**MOC**
				'90'	2	Scenario identifier '03' (see GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1) Scenario Parameters '0X' (See Table 45)	M
				'95'	'01'	Key Usage Qualifier '5C' (1 secure channel base key) or '10' (3 secure channel keys) (see GlobalPlatform Card Specification [6] Table 11-17)	M
				'96'	'01'	Key Access according to GlobalPlatform Card Specification [6] Table 11-18	O
				'80'	'01'	Key Type according to GlobalPlatform Card Specification [6] Table 11-16	M
				'81'	'01'	Key Length (in bytes)	M
				'82'	'01'	Key Identifier = '00' - '7F'	M
				'83'	'01'	Key Version Number = '01' - '7F'	M
				'91'	'00', '02', '03', '05' or '08'	Initial value of sequence counter	M
				'45'	1-n	Security Domain Image Number (SDIN)	O
				'84'	1-n	HostID (SHALL only be present if scenario parameter b3 is set)	C
'7F49'	Var	ePK.SR.ECKA					M
'5F37'	Var.	Signature					M

Table 44: Data Field for Key Establishment

b8	b7	b6	b5	b4	b3	b2	b1	Description
–	–	–	–	–	–	–	**1**	Do not delete existing keys (as defined in GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1) In the context of the ISD-R keyset establishment process, this option SHALL always be used by the SM-SR (see NOTE 1).
–	–	–	–	–	–	X	–	Include DR in key derivation process

b8	b7	b6	b5	b4	b3	b2	b1	Description
								(as defined in GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1)
–	–	–	–	–	X	–	–	Include Host and Card ID in key derivation process (as defined in GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1)
–	–	–	–	**1**	–	–	–	Certificate Verification precedes Key Establishment
X	X	X	X	–	–	–	–	RFU

Table 45: Scenario Parameters

NOTE 1: Deletion of other keysets, belonging to the former SM-SR, can be realized by the new SM-SR using the dedicated command “FinaliseISDRhandover” defined in section 4.1.1.9, only after it has received confirmation of the proper completion of ISD-R keyset establishment.

In case the scenario parameter specifies usage of HostID+CardID (bit b3=1), then the SM-SR and the eUICC SHALL use the SIN-LV and SDIN-LV of ISD-R, in lieu of the IIN-LV and CIN-LV of the card; this deviates from GP Amendment E [11].

The SM-SR knows the SIN and SDIN of ISD-R as per the EIS.

The following TLV-encoded data are signed off-card with SK.SR. ECDSA to generate the content of DGI '5F37' (signature), as described in GlobalPlatform Card Specification Amendment E [11]:

DGI	Length	Value Description					MOC
'3A02'	Var	Key set Establishment					M
		Tag	**Length**	**Value Description**			**MOC**
		'A6'	Var	CRT tag (KAT)			M
				Tag	**Length**	**Value Description**	**MOC**
				'90'	2	Scenario identifier ‘03’ (see GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1) Scenario Parameters ‘0X’ (See Table 45)	M
				'95'	'01'	Key Usage Qualifier '5C' (1 secure channel base key) or '10' (3 secure channel keys) (see GlobalPlatform Card Specification [6] Table 11-17)	M

DGI	Length	Value Description					MOC
				'96'	'01'	Key Access according to GlobalPlatform Card Specification [6] Table 11-18– if present	C
				'80'	'01'	Key Type according to GlobalPlatform Card Specification [6] Table 11-16	M
				'81'	'01'	Key Length (in bytes)	M
				'82'	'01'	Key Identifier = '00' - '7F'	M
				'83'	'01'	Key Version Number = '01' - '7F'	M
				'91'	'00', '02', '03', '05' or '08'	Initial value of sequence counter	M
				'45'	1-n	Security Domain Image Number (SDIN) – if present	C
				'84'	1-n	HostID (SHALL only be present if scenario parameter b3 is set)	C
'7F49'	Var	ePK.SR.ECKA					M
'0085'	Var	Random Challenge					M

Table 46: Data Signed to Generate the Signature

Response Message

Data Field Returned in the Response Message:

The STORE DATA response SHALL contain the following data:

Tag	Length	Data Element	MOC
'85'	Variable	DR	C
'86'	Variable	receipt	M

Table 47: Response Data for Scenario #3

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6]

4.1.1.9 Finalisation of the ISD-R Handover

Function name: FinaliseISDRhandover

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider entity: ISD-R

Description: This function deletes all keys in the ISD-R except for the key ranges indicated by the command parameter(s). It is intended as a simple clean-up mechanism for the new SM-SR after takeover to get rid of all keys of the previous SM-SR in the ISD-R.

Parameters:

- Key Ranges of keys not to be deleted.

Prerequisites:

- None.

Command Description:

DELETE COMMAND

This function is realised through a GlobalPlatform DELETE command as defined in GlobalPlatform Card Specification [6] with proprietary parameters. This command is sent to the ISD-R.

The DELETE command SHALL have the following parameters:

Code	Value	Meaning
CLA	'80'	See GlobalPlatform Card Specification [6] section 11.1.4.1
INS	'E4'	DELETE
P1	'00'	See GlobalPlatform Card Specification [6] section 11.2.2.1
P2	'00'	See GlobalPlatform Card Specification [6] section 11.2.2.2
Lc	'xx'	Length of data field
Data	'xxxx..'	TLV coded objects: Delete [card content] Data Field (See below)
Le	'00'	

Table 48: DELETE Command Message

The Delete [card content] Data Field SHALL contain one or two instances of following TLV:

Tag	Length	Value Description	MOC
'F2'	3	Range of keys NOT to be deleted. The 3 bytes are coded as follows: byte 1: Key Version Number of the key range byte 2: Key Identifier of first key of the key range byte 3: Key Identifier of last key of the key range	M

Table 49: Delete [card content] Command Data Field

NOTE: Two TLVs allow for one SCP80 and one SCP81 key set to "survive" key clean-up.

Example:

'F2 03 06 01 03 F2 03 43 01 02' will delete all keys except those with Key Version Number – Key identifier: '06' – '01', '06' – '02', '06' – '03', '43' – '01' and '43' – '02'.

Function flow

Upon reception of the DELETE command, the eUICC SHALL:

- Check that all keys of the key set(s) used for setting up the current secure channel are among the keys not to be deleted. For SCP81, this also includes the key set used

for the push SM. If that check fails, the command is terminated without deleting any key.

- Delete all keys except those in the key ranges indicated in the command parameters.

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL contain a single byte of '00'.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.2.3.2.

Specific Processing State returned in response Message:

'69 85': Key(s) of key set used for the current secure channel is/are among the keys to be deleted.

4.1.1.10 SM-SR Addressing Parameters Update

Function name: UpdateSMSRAddressingParameters

Related Procedures: SM-SR Change, Profile Download and Installation

Function group: eUICC Management

Function Provider entity: ISD-R

Description:

This function MAY be used by the new SM-SR to update SM-SR addressing parameters on the eUICC after an SM-SR Change procedure.

This function MAY be used by the SM-SR during Profile Download and Installation procedure to add a specific TP-DA for a newly downloaded Profile.

This function MAY be used by the SM-SR outside of the Profile Download and Installation or SM-SR Change procedure in case some parameters have changed.

This function has the following parameter:

- ISD-R AID
- SM-SR addressing Parameters

NOTE: The SM-SR addressing parameters for HTTPS can be updated by the function defined in GlobalPlatform Card Specification Amendment B [8], leveraging in particular the tag A5 to update only the relevant sub-TLVs, so they are not described here.

Prerequisites

- None

Function flow

Upon reception of the SM-SR addressing Parameters update command, the eUICC SHALL:

Update the SM-SR addressing Parameters of the ISD-R

Commands

This command is a STORE DATA command, as described in GlobalPlatform Card Specification [6] section 11.11.2.

Code	Value	Meaning
CLA	'80'	
INS	'E2'	STORE DATA
P1	'88'	Reference Control Parameter P1 0
P2	'00'	Block Number (Not used for Enable
Lc	'XX'	Length of data field
Data	'XX'	Application Data and MAC (if present)
Le	Not present	

Table 50: STORE DATA Command Message

Parameter P1 is coded according to the following table:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	X	X	X	RFU

Table 51: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A07'	Var	SM-SR Addressing Parameters			M
		Tag	**Length**	**Value Description**	**MOC**
		'A3'	n	SMS parameters	C
		'A4'	n	BIP parameters for CAT_TP	C
		'A5'	n	DNS parameters	C

Table 52: SMSR Addressing Parameters Update

The SM-SR MAY use each of the Tag 'A3', 'A4' and 'A5'to create or update the complete set of addressing parameters for the corresponding protocol as defined in the tables below.

The SM-SR MAY use Tag ‘A5’ with a length of zero to erase the DNS parameters.

SMS parameters value Description coding

Tag	Length	Value Description			MOC
’81’	2-12	SM-SR Platform Destination Address*			M
‘A2’	var	Profile-specific SM-SR Platform destination Addresses			O
		Tag	**Length**		
		'81'	3	ISD-P identifier: digits 15 to 20 of PIX of ISD-P	M
		'82'	2-12	Profile-specific SM-SR Platform Destination Address*	M
This structure can contain as many TLVs with tag ‘A2’ as there are ISD-Ps. The SM-SR is responsible to overwrite this list as it sees fit when a new ISD-P is created or after an SM-SR change. When an ISD-P is deleted, the eUICC SHALL remove the corresponding 'A2' TLV.					

Table 53: SMS Addressing Parameters Coding

*SM-SR Platform Destination Address is coded as specified for the TP-Destination-Address in 3GPP TS 23.040 [39].

BIP open channel parameters for CAT_TP link

Description
UICC/terminal interface transport level*
Data Destination Address comprehension TLV **

Table 54: BIP Open Channel Parameters for CAT_TP Link

*As defined in ETSI TS 102 226 [5] in the section “Data for CAT_TP link establishment” and “Data for BIP channel opening”.

**As defined in ETSI TS 102 223 [3].

The CR bit of the tags SHALL be set to zero.

DNS parameters

Tag	Length	Value Description			MOC
’81’	1-n	**SM-SR FQDN** Full Qualified Domain Name of the SM-SR that will be used in the DNS query. This parameter is coded in ASCII			M
‘A2’	0-n	**DNS servers List** List of couple IP/ports allowing to reach DNS servers			M
		Tag	**Length**		
		‘3E' or ‘BE’	1-n	IP address coded as an “Other Address” as specified by ETSI TS 102 223 [3]	M
		'82'	2	Port number (integer)	M
A3	0-n	**Proprietary parameters** Additional parameters that MAY be supported by the eUICC implementation			C
This structure can contain more than one TLVs with tag ‘A2’ to provide more than one IP/port couples. If the SM-SR uses Tag ‘A5’ with a length of zero then neither of the fields above are required to be present.					

Table 55: DNS Parameters

The values of the profile-specific connectivity parameters, used by the eUICC to open the BIP channel to communicate with the DNS Resolver Server, are those defined in the HTTPS Connectivity Parameters of the currently Enabled ISD-P defined in Table 95.

If the SM-SR does not support a DNS Resolver Server, then it SHALL set the IP address in the HTTPS Connectivity Parameters of the ISD-R as defined in GlobalPlatform Card Specification Amendment B [8].

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL NOT be present.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.11.2.

4.1.1.11 Handle Default Notification

Function name: HandleDefaultNotification

Related Procedures: Profile Enabling, Profile Enabling via SM-DP, Profile Disabling, Fall-Back Activation Procedure

Function group: eUICC Management

Function Provider entity: ISD-R

Description: This function provides a default notification from the eUICC to the SM-SR.

Parameters:

- EID
- ISD-P AID
- Mobile Equipment Identification (for example MEID, IMEI)
- Notification Sequence number
- Notification type

Prerequisites:

The eUICC has received a notification of network attachment.

> Note: There is no single method implemented by all devices to notify the eUICC of network attachment. The eUICC MAY rely on various heuristics to determine that network attachment is effective. As a worst-case safeguard, the eUICC SHALL attempt to send profile change notifications within a time interval of 10 STATUS events after card reset.

Notification Message

The eUICC notification is composed of a single BER-TLV tag including several COMPREHENSION-TLV data objects; the COMPREHENSION-TLV format is defined in ETSI TS 102 223 [3].

Description	Length (bytes)	Value	MOC
eUICC notification tag	1	'E1'. To avoid conflicts with the values defined in ETSI TS 101 220 [2], a tag from the proprietary class is used.	M
Length (A+B+C+D+E+F)	1 or 2	BER-TLV coding length	M
EID	A	See below	M
Notification type	B	See below	M
Notification sequence number	C	See below	M
ISD-P- AID	D	See ETSI TS 102 223 [3], clause 8.60	M
IMEI	E	See ETSI TS 102 223 [3], clause 8.20	C
MEID	F	See ETSI TS 102 223 [3], clause 8.81	C

Table 56: Data Format for Notification

IMEI and MEID are optional. In case the eUICC encounters any issue while getting the Mobile Equipment Identification of the Device, no value is provided. If both IMEI and MEID are retrieved, only one could be sent to limit overall message length.

COMPREHENSION-TLV for EID

Byte(s)	Description	Length
1	EID tag, '4C'.	1
2	Length (X) of the EID (SHALL NOT exceed 16 bytes)	1
3 to X+2	EID value, as defined in section 2.2.2.	X

Table 57: COMPREHENSION-TLV for EID

COMPREHENSION-TLV for Notification type

Byte(s)	Description	Length
1	Notification type tag, '4D'.	1
2	Length= '01'	1
3	Notification type	1

Table 58: COMPREHENSION-TLV for Notification type

Notification type:

Coding:

- '01': eUICC declaration – First network attachment
- '02': Profile change succeeded
- '03': Profile change failed and Roll-back
- '04': Void
- '05': Profile change after activation of the Fall-Back Mechanism
- '06': Profile change after Emergency Profile disabling
- '07': Profile change after Test Profile disabling
- '08' to 'FF': RFU

NOTE: In case the Notification type is '05', the SM-SR can inspect the ISD-P AID present in the notification message to determine whether it indicates the ISD-P AID of the Profile with the Fall-Back Attribute (denoting that this profile has been enabled after the previously enabled profile has lost connectivity) or another ISD-P AID (denoting that the previously enabled profile has been enabled again after the network connectivity has been restored).

COMPREHENSION-TLV for Notification sequence number

Byte(s)	Description	Length
1	Notification sequence number tag, '4E'.	1
2	Length='02'	1
3 to 4	Notification sequence number value	2

Table 59: COMPREHENSION-TLV for Notification Sequence Number

The notification sequence number identifies the notification message, and allows the SM-SR to distinguish a new notification from a retry. In case of a retry, the eUICC SHALL use the same notification sequence number. When a Notification Confirmation has been successfully received by the SM-SR, the eUICC SHALL increment the sequence number for the next notification.

NOTE: Depending on the eUICC implementation, the notification MAY also contain additional TLVs using EUM-specific tags.

An SM-SR is not required to record or process such specific tags, and can simply ignore them

In any case, the size of the complete notification SHALL fit into one SMS-MO if the notification is sent by SMS, and SHALL NOT exceed the size of 240 bytes if sent by HTTP or CAT-TP.

Secured data structure for eUICC notification over SCP80

The secured data containing the eUICC notification is the COMPREHENSION-TLV structure specified above, with no added layer of Expanded format.
This deviates from the requirement described in section 2.4.3.3.

Default Notification Protocol Priority

A protocol priority order for default notification MAY be defined for every Profile during profile installation or download, and updated using the functions defined in 4.1.2.2 and 4.1.3.4. This protocol priority order specifies which protocols to use, and in which order, among SMS, HTTPS and CAT_TP.

If not defined for a Profile, the default priority order is set as follow:

Priority	Protocol
1	SMS
2	HTTPS
3	CAT_TP

Table 60: Default Notification Protocol Priority

4.1.1.12 Notification Confirmation

Function name: HandleNotificationConfirmation

Related Procedures: Handle Default Notification

Function group: eUICC Management

Function Provider entity: ISD-R

Description: This function confirms the notification and triggers potential follow-up activities required by POL1.

Parameters:

- Notification Sequence number

Prerequisites:

- The SM-SR has received a notification from the eUICC.

Function flow

Upon reception of the STORE DATA command, the eUICC SHALL:

- Disable the retry mechanism for the notification
- Perform the follow-up activities required by POL1 upon the activity that triggered the original notification
- Return the result of any such activity in the response data

Command Description:

STORE DATA Command

This function is realised through the GlobalPlatform STORE DATA command as defined in GlobalPlatform Card Specification [6].

Command Message

The STORE DATA command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' – '8F', 'C0' – 'CF' or 'E0' – 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E2'	STORE DATA
P1	'89'	Reference control parameter P1
P2	'00'	Block number
Lc	'xx'	Length of data field
Data	'xxxxx…'	Application data and MAC (if present)
Le	'00'	

Table 61: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	-	-	1	Case 4 command
-	-	-	-	-	X	X	-	RFU

Table 62: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A08'	Var	Notification Confirmation			M
		Tag	**Length**	**Value Description**	**MOC**
		'4E'	2	Notification Sequence number	M

Table 63: Notification Confirmation Data Field

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL contain the data structure below.

- Not be present, if no follow-up activities had to be performed, or
- Contain the data structure below if follow-up activities were performed.

Tag	Length	Value Description			MOC
'80'	Var	List of Deleted ISD-Ps			M
		Tag	Length	Value Description	MOC
		'4F'	16	AID of ISD-P	M

Table 64: Notification Confirmation Response Data Field

NOTE: In the current version, the response will carry only one AID. However, the structure is defined in a generic way so that results of other follow-up activities can be added when required.

NOTE: If no follow-up activity has been performed at all, the data field SHALL contain tag 80 followed by a length of zero, and no value.

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.11.3.2.

4.1.1.13 Set Emergency Profile Attribute

Function name: SetEmergencyProfileAttribute

Related Procedures: -

Function group: Platform Management

Function Provider entity: ISD-R

Description: This optional function sets the Emergency Profile Attribute for one Profile on the target eUICC.

Parameters:

- ISD-P-AID

Prerequisites:

- The target profile SHALL NOT be enabled.
- The target Profile SHALL NOT have the Fall-Back Attribute set.

Function flow

Upon reception of the STORE DATA command, the eUICC SHALL:

- Verify that the target Profile has not the Fall-Back Attribute set.
- Set the Emergency Profile Attribute for the target Profile
- Remove the Emergency Profile Attribute from the Profile that has the attribute currently set.

Command Description:

STORE DATA Command

This function is realised through the GlobalPlatform STORE DATA command as defined in GlobalPlatform Card Specification [6].

Command Message

The STORE DATA command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' – '8F', 'C0' – 'CF' or 'E0' – 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E2'	STORE DATA
P1	'88'	Reference control parameter P1
P2	'00'	Block number
Lc	'xx'	Length of data field
Data	'xxxxx…'	Application data and MAC (if present)
Le		Not present

Table 41113-A: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	X	X	X	RFU

Table 41113-B: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A09'	Var	Set Emergency Profile Attribute			M
		Tag	Length	Value Description	MOC
		'4F'	5-16	ISD-P-AID	M

Table 41113-C: Set Emergency Profile Attribute Data Field

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL NOT be present.

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.11.3.2.

4.1.2 ES6 (Operator-eUICC) Interface Description

4.1.2.1 Policy Rules Update by Operator

Function name: UpdatePOL1byMNO

Related Procedures: Pol1 Update by Operator

Function group: Profile Management

Function Provider entity: MNO-SD

Description: This function is used to update POL1 on the eUICC.

This function has the following parameter:

- POL1

Prerequisites

- The Profile is enabled

Function flow

Upon reception of the POL1 update command, the eUICC SHALL:

- Update POL1 of the ISD-P containing the targeted MNO-SD.

Commands

INSTALL [for personalization] command

This function consists of an INSTALL [for personalization] command followed by a STORE DATA command, as described in GlobalPlatform Card Specification [6].

According to GlobalPlatform Card Specification [6], INSTALL [for personalization] command can only be used on applications Associated with a Security Domain. As an exception from this rule, the eUICC SHALL allow the MNO-SD to receive this command sequence with data destined to the ISD-P.

INSTALL [for personalization] command:

Code	Value	Meaning
CLA	'80'	See GlobalPlatform Card Specification section 11.1
INS	'E6'	INSTALL
P1	'20'	See GlobalPlatform Card Specification [6] section 11.5.2.1
P2	'00'	See GlobalPlatform Card Specification [6] section 11.5.2.2
Lc	'xx'	Data Field Length
Data	'xxxx…'	See GlobalPlatform Card Specification [6] section 11.5.2.3
Le	'00'	

Table 65: INSTALL [for Personalization] Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	1	0	0	0	0	0	For personalization

Table 66: INSTALL [for Personalization] Reference Control Parameter P1

Reference Control Parameter P2 – ISD-P State Coding

P2 is set to '00': according to GlobalPlatform Card Specification [6] section 11.5, this means no information is provided.

Data Field

Name	Length	Value	MOC
Length of data	'1'	'00'	M
Length of data	'1'	'00'	M
Length of Application AID	'1'	'05' – '10'	M
Application AID (Reserved value for Profile's ISD-P)	'05 – 10'	'xxxx'	M
Length of data	'1'	'00'	M
Length of data	'1'	'00'	M
Length of data	'1'	'00'	M

Table 67: INSTALL Command Data Field

The reserved value for Profile's ISD-P indicates that the Security Domain targeted by the INSTALL [for personalization] command is the ISD-P of the Profile containing the MNO-SD.

NOTE: This mechanism avoids the Operator having to know and keep track of the ISD-P AID assigned by the SM-SR.

Response Message

Data Field Returned in the Response Message:

A single byte of '00' SHALL be returned indicating that no additional data is present, as defined in the GlobalPlatform Card Specification [6] section 11.5.3.1.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.5.3.2.

Specific Processing State returned in response Message:

None

STORE DATA command:

This command is a STORE DATA command, as described in GlobalPlatform Card Specification [6].

Code	Value	Meaning
CLA	'80'	
INS	'E2'	STORE DATA
P1	'88'	Reference Control Parameter P1 0
P2	'00'	Block Number (Not used for Enable
Lc	'XX'	Length of data field
Data	'XX'	Application Data and MAC (if present)
Le	Not present	

Table 68: STORE DATA Command Message

Parameter P1 is coded according to the following table:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	X	X	X	RFU

Table 69: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A06'	Var	POL1 Policy Rules			M
		Tag	Length	Value Description	MOC
		'81'	'01'	New POL1	M

Table 70: POL1 Update Data Field

POL1 coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	0	0	0	No POL1 rule active
-	-	-	-	-	0	-	1	Disabling of this Profile not allowed
-	-	-	-	-	0	1	-	Deletion of this Profile not allowed
-	-	-	-	-	1	0	0	Profile deletion is mandatory when its state is changed to disabled
-	-	-	-	-	X	X	X	Other combinations are forbidden
X	X	X	X	X	-	-	-	RFU

Table 71: POL1 Coding

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL NOT be present.
Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.11.3.2

4.1.2.2 Connectivity Parameters Update by Operator

Function name: UpdateConnectivityParametersByMNO

Related Procedures: Connectivity Parameters Update by Operator

Function group: Profile Management

Function Provider entity: MNO-SD

Description: This function is used to update Connectivity Parameters on the eUICC.

This function has the following parameter:

- Connectivity Parameters

Prerequisites

- The Profile is enabled

Function flow

Upon reception of the Connectivity Parameters update command, the eUICC SHALL:

- Update the Connectivity Parameters of the ISD-P containing the targeted MNO-SD.

Commands

This function consists of an INSTALL [for personalization] command followed by a STORE DATA command, as described in GlobalPlatform Card Specification [6].

According to GlobalPlatform Card Specification [6], INSTALL [for personalization] command can only be used on applications Associated with a Security Domain. As an exception from this rule, the eUICC SHALL allow the MNO-SD to receive this command sequence with data destined to the ISD-P.

INSTALL [for personalization] command:

As defined in section 4.1.2.1.

STORE DATA command:

As defined in section 4.1.3.4.

4.1.3 ES8 (SM-DP-eUICC) Interface Description

4.1.3.1 ISD-P Key Set Establishment

Function name: EstablishISDPKeySet

Related Procedures: Key Establishment

Function group: Profile Management

Function Provider entity: ISD-P

Description: This function is used to perform mutual authentication between the SM-DP and the eUICC and to establish a shared secret key set between the SM-DP and the ISD-P.

This function is based on Scenario 3 as defined in GlobalPlatform Card Specification Amendment E [11]. Scenario 3 is modified by adding the additional step of authentication of the SM-DP to the eUICC.

Adding this step to Scenario 3 requires an additional STORE DATA command to precede the command defined for Scenario 3. This new command provides the eUICC with the certificate of the SM-DP and retrieves a random challenge from the eUICC. This random challenge then has to be signed by the SM-DP and sent to the eUICC in the second command to prove to the eUICC that the SM-DP is in possession of the private key related to the certificate presented. The sequence is pictured in Figure 12 of section 3.1.2.

NOTE: A complementary scenario based on RSA is FFS.

NOTE: Although the Function Provider entity is denoted as being the ISD-P, the APDUs that transport this function are executed by the ISD-R. The ISD-R will forward the appropriate content to the ISD-P

Parameters:

- ISD-P AID

- Ephemeral public key of the SM-DP
- Certificate for the SM-DP

Prerequisites:

- The ECASD certificate was provided to and verified by the SM-DP
- SM-DP has generated an ephemeral key pair
- SM-DP has a signature from the CI
- ISD-P was created

Command Description:

This function is realized through GlobalPlatform INSTALL [for personalization] and STORE DATA commands as defined in GlobalPlatform Card Specification [6].

INSTALL [for personalization] command

Command Message

Code	Value	Meaning
CLA	'80'	See GlobalPlatform Card Specification section 11.1
INS	'E6'	INSTALL
P1	'20'	See GlobalPlatform Card Specification [8] section 11.5.2.1
P2	'00'	See GlobalPlatform Card Specification [8] section 11.5.2.2
Lc	'xx'	Data Field Length
Data	'xxxx…'	See GlobalPlatform Card Specification [8] section 11.5.2.3.6
Le	'00'	

Table 72: INSTALL [for Personalization] Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	1	0	0	0	0	0	For personalization

Table 73: INSTALL [for personalization] Reference Control Parameter P1

Reference Control Parameter P2 – ISD-P State Coding

P2 is set to '00': according to GlobalPlatform Card Specification [8] section 11.5, this means no information is provided.

Data Field

Name	Length	Value	MOC
Length of data	'1'	'00'	M
Length of data	'1'	'00'	M
Length of Application AID	'1'	'05' – '10'	M
Application AID of ISD-P	'05 – 10'	'xxxx'	M
Length of data	'1'	'00'	M

Name	Length	Value	MOC
Length of data	'1'	'00'	M
Length of data	'1'	'00'	M

Table 74: INSTALL Command Data Field

Response Message

Data Field Returned in the Response Message:

A single byte of '00' SHALL be returned indicating that no additional data is present as defined in the GlobalPlatform [6] section 11.5.3.1.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [8] section 11.5.3.2.

Specific Processing State returned in response Message:

None

First STORE DATA command

Command Message

The STORE DATA command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' – '8F', 'C0' – 'CF' or 'E0' – 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E2'	STORE DATA
P1	'09'	Reference control parameter P1
P2	'00'	Block number
Lc	'xx'	Length of data field
Data	'xxxxx…'	Application data and MAC (if present)
Le	'00'	

Table 75: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	More blocks
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	-	-	1	Case 4 command as defined in GlobalPlatform Amendment A [54]
-	-	-	-	-	X	X	-	RFU

Table 76: STORE DATA Reference Control Parameter P

Data Field Sent in the Command Message

DGI	Length	Value Description	MOC

‘3A01’	Var	Certificate of off-card entity					M
		Tag	**Length**	**Value Description**			**MOC**
		‘7F21’	Var.	Certificate			M
				Tag	**Length**	**Value Description**	**MOC**
				‘93’	1-16	Certificate Serial Number	M
				‘42’	1-16	CA Identifier	M
				‘5F20’	1-16	Subject Identifier	M
				‘95’	1	Key Usage, Signature Verification	M
				‘5F25’	4	Effective Date (YYYYMMDD, BCD format)	O
				‘5F24’	4	Expiration Date (YYYYMMDD, BCD format)	M
				‘73’	3-127	Discretionary Data Tag / Length / Value Description 'C8' / 1 / ‘01’, denoting an SM-DP certificate ‘C9’ / 20 / Authority key identifier (value of the Subject Key Identifier extension of the Root certificate) other TLVs MAY be present	M
				‘7F49’	Var.	Public Key – details see tables below	M
				‘5F37’	Var.	Signature	M

Table 77: Data Fields for Send SM-DP Certificate for ISD-P Key Establishment

The following TLV-encoded data are signed off-card with SK.CI. ECDSA to generate the content of tag ‘5F37’ (signature), as described in GlobalPlatform Card Specification Amendment E [11]:

Tag	Length	Value Description	MOC
‘93’	1-16	Certificate Serial Number	M
‘42’	1-16	CA Identifier	M
‘5F20’	1-16	Subject Identifier	M
‘95’	1	Key Usage, Signature Verification	M
‘5F25’	4	Effective Date (YYYYMMDD, BCD format) – if present	C
‘5F24’	4	Expiration Date (YYYYMMDD, BCD format)	M
‘73’	3-127	Discretionary Data	M
‘7F49’	Var.	Public Key	M

Table 78: Data Signed to Generate the SM-DP Certificate

Key format is defined in section 4.1.1.5.

Response Message

Data Field Returned in the Response Message:

The STORE DATA response SHALL contain the following data:

Tag	Length	Data Element
'85'	Variable	Random Challenge

Table 79: Response Data for Send SM-DP Certificate

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.11.3.2.[6]

Second STORE DATA command

Command Message

The STORE DATA command message SHALL be coded according to the following table:

Code	Value	Meaning
CLA	'80' - '8F', 'C0' - 'CF' or 'E0' - 'EF'	See section 11.1.4 of GlobalPlatform Card Specification [6]
INS	'E2'	STORE DATA
P1	'89'	Reference control parameter P1
P2	'01'	Block number
Lc	'xx'	Length of data field
Data	'xxxxx…'	Application data and MAC (if present)
Le	'00'	

Table 80: STORE DATA Command Message

Reference Control Parameter P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	-	-	1	Case 4 command as defined in GlobalPlatform Amendment A [54]
-	-	-	-	-	X	X	-	RFU

Table 81: STORE DATA Reference Control Parameter

Data Field Sent in the Command Message

DGI	Length	Value Description					MOC
'3A02'	Var	Key set Establish					M
		Tag	Length	Value Description			MOC
		'A6'	Var	CRT tag (KAT)			
				Tag	Length	Value Description	MOC

DGI	Length	Value Description					MOC
				'90'	2	Scenario identifier '03' (see GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1) Scenario Parameters '0X' (See Table 83)	M
				'95'	'01'	Key Usage Qualifier '5C' (1 secure channel base key) or '10' (3 secure channel keys) (see GlobalPlatform Card Specification [6] Table 11-17)	M
				'96'	'01'	Key Access according to GlobalPlatform Card Specification [[6] Table 11-18	O
				'80'	'01'	Key Type according to GlobalPlatform Card Specification [6] Table 11-16	M
				'81'	'01'	Key Length (in bytes)	M
				'82'	'01'	Key Identifier = '00' - '7F'	M
				'83'	'01'	Key Version Number = '01' - '7F'	M
				'91'	'00', '02', '03', '05' or '08'	Initial value of sequence counter	M
				'45'	1-n	Security Domain Image Number (SDIN)	O
				'84'	1-n	HostID (SHALL only be present if scenario parameter b3 is set)	C
'7F49'	Var	ePK.DP.ECKA					M
'5F37'	Var.	Signature					M

Table 82: Send SM-DP Certificate Data Field

The following TLV-encoded data are signed off-card with SK.DP. ECDSA to generate the content of DGI '5F37' (signature), as described in GlobalPlatform Card Specification Amendment E [11]:

b8	b7	b6	b5	b4	b3	b2	b1	Description
0	**0**	**0**	**0**	**–**	**X**	**X**	**X**	As defined in GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1
-	-	-	-	**1**	**–**	**–**	**–**	Certificate Verification precedes Key Establishment

Table 83: Scenario Parameters

In case the scenario parameter specifies usage of HostID+CardID (bit b3=1), then the SM-DP and the eUICC SHALL use the SIN-LV and SDIN-LV of ISD-R, in lieu of the IIN-LV and CIN-LV of the card; this deviates from GP Amendment E [11], and ISD-P has no SIN/SDIN yet.

The SM-DP can know the SIN and SDIN of ISD-R by inspecting the EIS retrieved on ES3.

DGI	Length	Value Description					MOC
'3A02'	Var	Key set Establishment					M
		Tag	**Length**	**Value Description**			**MOC**
		'A6'	Var	CRT tag (KAT)			M
				Tag	**Length**	**Value Description**	**MOC**
				'90'	2	Scenario identifier '03' (see GlobalPlatform Card Specification Amendment E: Security Upgrade for Card Content Management [11] section 4.8.1) Scenario Parameters '0X' (See Table 83)	M
				'95'	'01'	Key Usage Qualifier '5C' (1 secure channel base key) or '10' (3 secure channel keys) (see GlobalPlatform Card Specification [6] Table 11-17)	M
				'96'	'01'	Key Access according to GlobalPlatform Card Specification [6] Table 11-18 – if present	C
				'80'	'01'	Key Type according to GlobalPlatform Card Specification [6] Table 11-16	M
				'81'	'01'	Key Length (in bytes)	M
				'82'	'01'	Key Identifier = '00' - '7F'	M
				'83'	'01'	Key Version Number = '01' - '7F'	M
				'91'	'00', '02', '03', '05' or '08'	Initial value of sequence counter	M
				'45'	1-n	Security Domain Image Number (SDIN) – if present	C
				'84'	1-n	HostID (SHALL only be present if scenario parameter b3 is set)	C
'7F49'	Var	ePK.DP.ECKA					M
'0085'	Var	Random Challenge					M

Table 84: Data Signed to Generate the Signature

Response Message

Data Field Returned in the Response Message:

The STORE DATA response SHALL contain the following data:

Tag	Length	Value Description	MOC
'85'	Variable	DR	C
'86'	Variable	Receipt	M

Table 85: Response Data for Scenario #3

Processing State Returned in the Response Message:

As defined in GlobalPlatform Card Specification [6] section 11.11.3.2.

4.1.3.2 Command coding for SCP03

All ES8 functions in subsequent sections require securing the commands by SCP03.

NOTE: The profile package itself is protected by SCP03t as defined in the next section.

Opening an SCP03 secure channel requires the following two commands:
INITIALIZE UPDATE

Code	Value	Description
CLA	See to GlobalPlatform Card Specification Amendment D [10]	Section 7.1.1
INS	See to GlobalPlatform Card Specification Amendment D [10]	INITIALIZE UPDATE
P1	'XX'	indicates the version of the target ISD-P key set used
P2	'XX'	indicates the key identifier of the target ISD-P
Lc	'08'	Length of the host challenge
Data	'XX…XX'	For Host Challenge see GlobalPlatform Card Specification Amendment D [10] for computation of the host challenge
Le	'00'	

Table 86: Initialize Update Command

EXTERNAL AUTHENTICATE

Code	Value	Description
CLA	See GlobalPlatform Card Specification Amendment D [10]	Section 7.1.2.
INS	See GlobalPlatform Card Specification Amendment D [10]	EXTERNAL AUTHENTICATE
P1	'33'	indicates the security level and SHALL be set to request C-DECRYPTION, R-DECRIPTION, R-MAC and C-MAC (see to GlobalPlatform Card Specification Amendment D [10])
P2	'00'	
Lc	'10'	Length of the host cryptogram and MAC
Data	'XX…XX'	Host cryptogram and MAC (see to GlobalPlatform Card Specification Amendment D [10] for computation of host cryptogram and MAC)
Le		Not Present

Table 87: External Authenticate Command

These two commands SHALL be following by any ES8 command as defined in subsequent sections depending on the procedure to be performed.

Those ES8 commands and their responses are modified by encrypting the data part and adding a MAC as defined in GlobalPlatform Card Specification Amendment D [10].

4.1.3.3 Download and Installation of a Profile

Function name: DownloadAndInstallation

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider entity: ISD-P

Description: This function is used to load a Profile into an ISD-P on the eUICC. The ISD-P must be already created and also already personalized. The Profile created by the SM-DP must be compatible with the targeted eUICC.

NOTE: The ISD-P identification is provided within the ES5 transport protocol.

The Profile SHALL be protected by SCP03t. The Profile SHALL include in particular:

- The setting of POL1, if defined by Operator
- The setting of connectivity parameters (see section 4.1.3.4)
- The setting of ISD-P state from ‘CREATED’ to ‘DISABLED’ when installation is finished.

Parameters:

- Profile

Prerequisites:

- ISD-P must be created
- ISD-P must be PERSONALIZED (as defined in GlobalPlatform Card Specification[6])
- Connection is secured via SCP03t

Check Figure 13 for further details.

Description of the SCP03t security protocol:

This section defines a secure channel protocol based on GlobalPlatform's SCP03 usable for TLV structures, named SCP03t hereafter.

Tag values are defined so that they can be used without conflict within the expanded remote management format which is used to transport data inside SCP80 or SCP81 of ES5.

As no SWs are used, errors are indicated by a special response tag with tag number +'80' (resulting in a 2 byte tag).

The data transported in the command TLVs specified below SHALL consist of the Profile Package specified in [53]; the response TLVs SHALL transport Profile Element (PE) responses as provided by the Profile Package processing specified in SIMalliance: eUICC Profile Package - Interoperable Format Technical Specification [53].

NOTE The SM-DP MAY support a former version v2.x of the SIMalliance: eUICC Profile Package - Interoperable Format Technical Specification, to download a profile onto an eUICC complying with a former version of this specification.

The SM-DP can inspect the EIS of the target eUICC to determine which versions of SIMalliance eUICC Profile Package [53] are supported by the target eUICC.

The Profile Package consists of a sequence of PE TLVs. However, SCP03t does not take that PE structure into account, but treats the whole Profile Package as one block of transparent data. That block of data is split into segments of a maximum size of 1024 bytes (including the tag and length field). The eUICC SHALL support profile command data segments of at least up to this size.

The options allowed in SCP03 are limited as follows in SCP03t:

- Response security is always the same as command security (if no error).
- BEGIN/END R-MAC SESSION is not supported.
- Only one option is defined: MAC + encryption.

The following sections describe the changes required to move from SCP03 to SCP03t. Everything else is inherited from SCP03.

As the security mechanisms are exactly the same as SCP03, the SCP03 key sets are used for SCP03t.

Secure channel initiation uses 2 TLVs equivalent to the INITIALIZE UPDATE and the EXTERNAL AUTHENTICATE APDUs.

Thereafter, the command and response TLVs are protected in the same way as SCP03 APDUs, using either:

- the SCP03t sessions keys resulting from the secure channel initiation
- or random keys which replaces session keys.

Each command TLV triggers one response TLV. A response MAY be empty or carry response data from the application layer.

In case the eUICC indicates a fatal error in a response TLV, it MAY stop sending subsequent response TLVs.

Secure Channel Initiation: INITIALIZE UPDATE command TLV

The following data SHALL be encapsulated in a TLV with tag '84':

Name	Length	Presence
Key version number	1 byte	Mandatory
Key identifier	1 byte	Mandatory (and value must be '00', consistently with SCP03)
Host challenge	8 bytes	Mandatory

Table 88: Initialize Update Command TLV

The data field of the response TLV SHALL contain the concatenation without delimiters of the following data elements, encapsulated in a TLV with tag '84'.

Name	Length	Presence
Key diversification data	10 bytes	Mandatory
Key information	3 bytes	Mandatory
Card challenge	8 bytes	Mandatory
Card cryptogram	8 bytes	Mandatory
Sequence Counter	3 bytes	Mandatory

Table 89: Response TLV Data Elements

In case of an error, tag '9F44' is used (see NOTE 1 below). The following values are defined:

- '01': error in length or structure of command data
- '03': referenced data not found

NOTE 1: an eUICC MAY also detect the error in length or structure of command data at the transport layer (expanded remote command format), and return a bad format TLV as defined in ETSI TS 102 226 [5] instead of the SCP03t-specific error tag.

Secure Channel Initiation: EXTERNAL AUTHENTICATE command TLV

The following data SHALL be encapsulated in a TLV with tag '85':

Name	Length	Presence
Security level	1 byte	Mandatory
Host cryptogram	8 bytes	Mandatory
MAC	8 bytes	Mandatory

Table 90: External Authenticate Command TLV

The security level SHALL be set to '33': "C DECRYPTION, R ENCRYPTION, C MAC, and R MAC".

The MAC SHALL be computed based on the values present in the TLV, as follows:

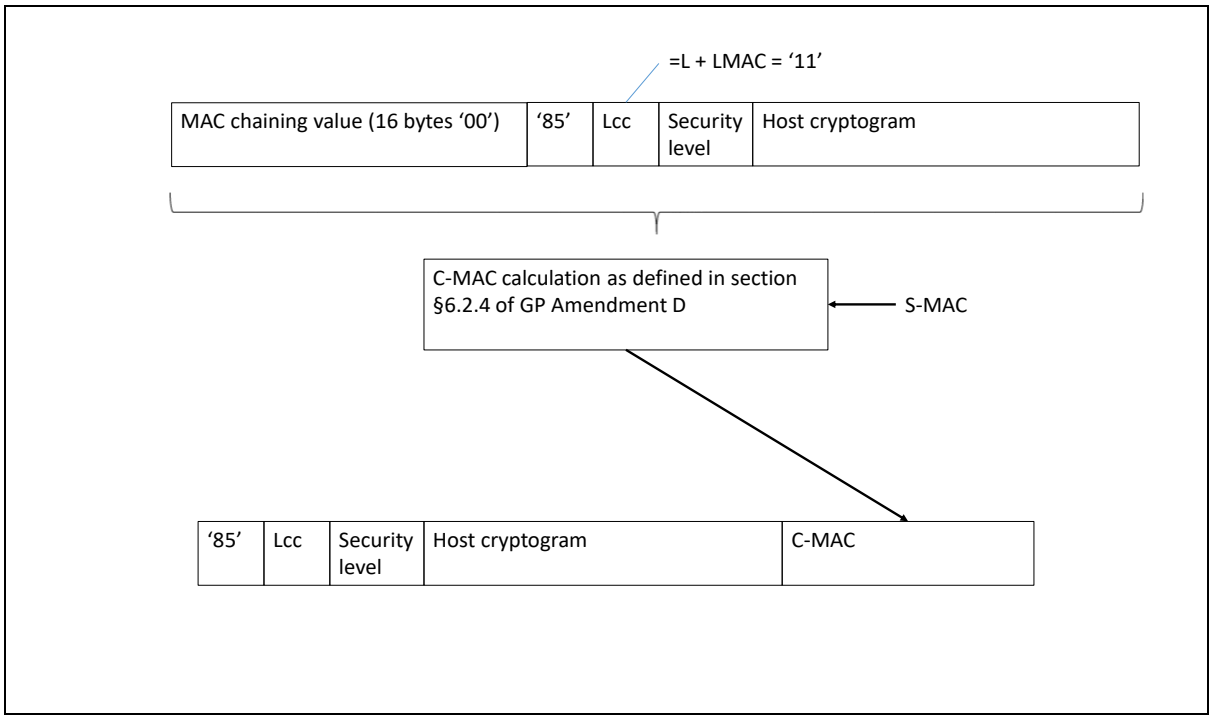


Figure 45: C-MAC Computation for External Authenticate Command TLV

If the message is accepted, a Response TLV with tag '85' and length zero SHALL be returned.

This TLV does not return an R-MAC.

In case of an error, tag '9F45' is used (see NOTE 1 above). The following values are defined:

- '01': error in length or structure of command data
- '02': security error

Command TLV C-MAC and C-DECRYPTION Generation and Verification

For encapsulating encrypted profile command data in a SCP03t TLV, tag '86' is used.

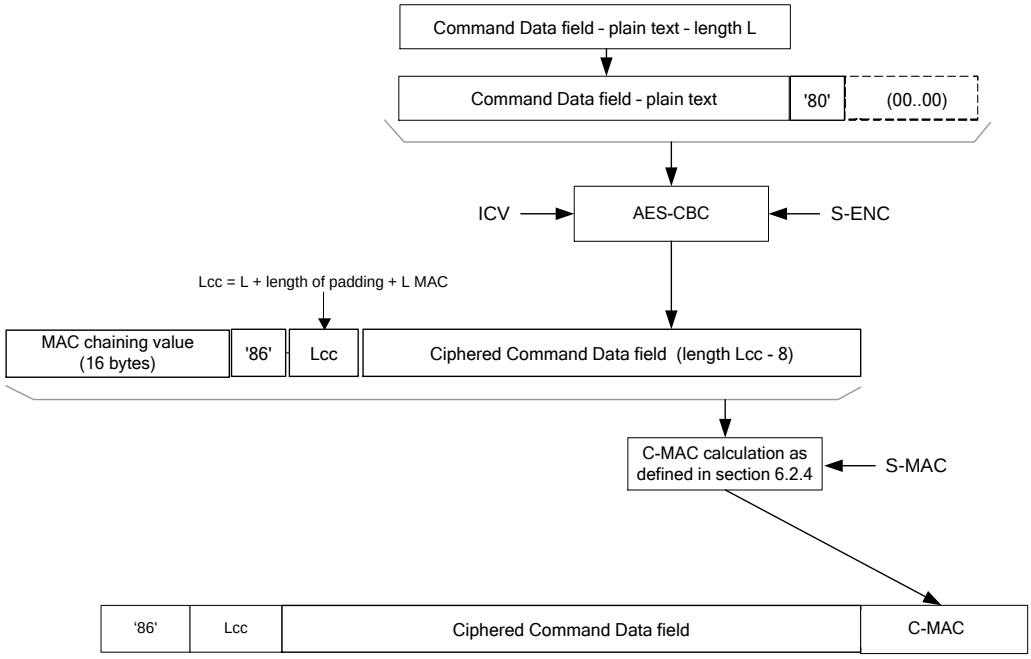


Figure 46: **TLV Command Data Field Encryption**

Response R-MAC and R-ENCRYPTION Generation and Verification

For encapsulating encrypted profile response data in a SCP03t TLV, tag '86' is used.

If there is no response data field, the length is ‘00’, and no R-MAC SHALL be generated, so the response TLV SHALL be ’86 00’.In case of an error, tag '9F46' is used (see NOTE 1 above), and no R-MAC nor R-ENCRYPTION SHALL be generated. The response data field contains only one byte, the following values are defined:

- '01': error in length or structure of command data
- '02': security error

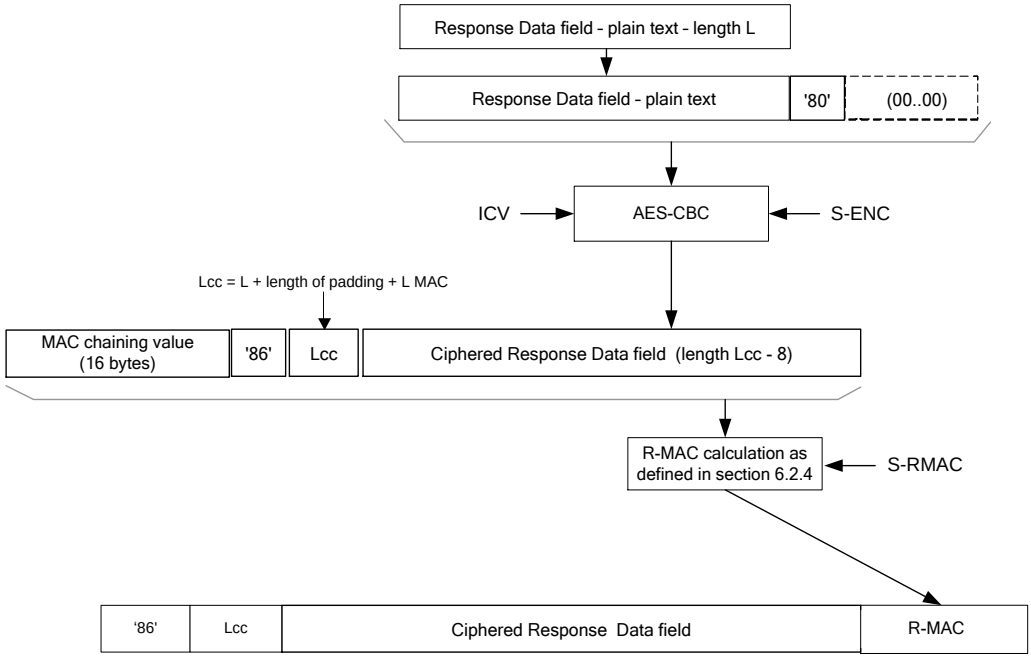


Figure 47: TLV Response Data Field Encryption

Profile protection:

Profile protection SHALL performed using either:

- Session keys (S-ENC, S-MAC, S-RMAC) resulting from the key agreement with eUICC (INITIALIZE UPDATE and EXTERNAL AUTHENTICATE).
- Or random keys per Profile (denoted PPK-ENC, PPK-MAC, PPK-RMAC in this document), generated by the SM-DP.

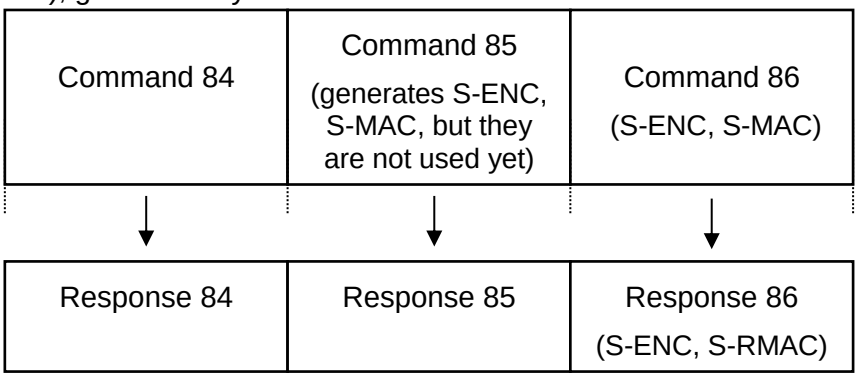


Figure 4133-A: Key usage for the protection of the SCP03t command and responses when using initial session keys

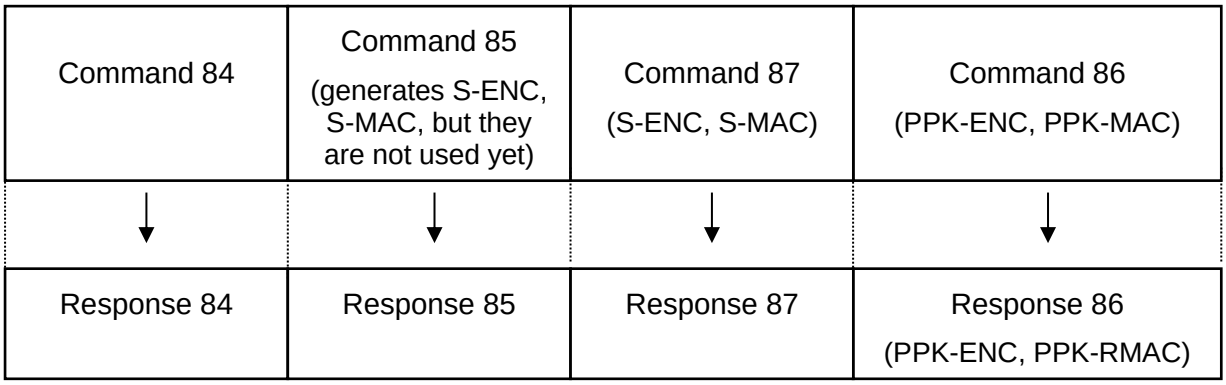


Figure 4133-B: Key usage for the protection of the SCP03t command and responses when using random keys

If random key mode is selected by the SM-DP, the initial MAC chaining value to be used for the first segment of the profile protection is provided together with the random keys and the encryption counter for ICV calculation is reset to its initial state (i.e. the value on 16 bytes is '00…01'). Otherwise the MAC chaining method SHALL be applied (i.e. the MAC chaining value of the previous command TLV SHALL be used).

PPK-ENC, PPK-MAC and PPK-RMAC SHALL have the same length as S-ENC, S-MAC, S-RMAC.

It is the SM-DP choice whether to use this random keyset (PPK-ENC, PPK-MAC and PPK-RMAC). This mode allows performing Profile Protection in advance without having any eUICC knowledge. It may help to provide a better SM-DP scalability. The eUICC SHALL be able to support both modes.

Session keys and, if used, the random keys SHALL only be used in the Profile download process. They SHALL be deleted on the eUICC at the latest at the end of the process.

In case of failure during the first attempt to download a Profile, the PPK-RMAC SHALL NOT be reused again. The SM-DP SHALL regenerate a new PPK-RMAC for every retry.

Replace session key command TLV

This command is used, during the download of a Protected Profile, to replace the SCP03t session keys (S-ENC, S-MAC and S-RMAC) by a new set of session keys (typically the PPK-ENC, PPK-MAC and PPK-RMAC) protecting the command and response TLVs. Note that all keys (S-ENC, S-MAC and S-RMAC) have to be replaced. This command doesn't allow to replace only a part of the session keys. The response SHALL be encrypted by PPK-ENC and MAC-ed by PPK-RMAC, where PPK-RMAC SHALL be different for each download attempt of the same Profile.

The following data SHALL be encapsulated in a BER-TLV with tag '87':

Tag	Length	Value description	MOC
80	16	Initial MAC chaining value	M
81	16 - 32	PPK-ENC	M
82	16 - 32	PPK-MAC	M
83	16 - 32	PPK-RMAC	M

Table 4133-C: Replace Session Key Command TLV

When using random keys for profile protection, the Replace session key command SHALL be sent directly before the SCP03t command TLVs containing the protected profile package (tag 86).

When using session keys for profile protection, the Replace session key command SHALL NOT be present.

On reception of this command the eUICC SHALL:

- Verify that the new keys are of same length as the old keys. If not the eUICC SHALL return an error ('01'), and the loading of the Profile SHALL be aborted.
- Replace the current session keys with the new set of keys.

Once the command is successfully executed, the eUICC SHALL use this new set of keys for decryption and MAC verification of subsequent SCP03t blocks of data, and encryption and MACing of responses. The key type of the new set of keys is the same as the session keys they replace.

If the command message is accepted, a Response TLV with tag '87' and length zero SHALL be returned. This TLV does not return an R-MAC.

In case of an error, tag '9F47' is used (see NOTE 1 above). The following values are defined:

- '01': error in length or structure of command data
- '02': security error

4.1.3.4 Connectivity Parameters Update using SCP03

Function name: UpdateConnectivityParameters SCP03

Related Procedures: Connectivity Parameters Update using SCP03

Function group: eUICC Management

Function Provider entity: ISD-P

Description: This function is used to update Connectivity Parameters on the eUICC.

This function has the following parameter:

- ISD-P AID
- Connectivity Parameters

Prerequisites

- None

Function flow

Upon reception of the Connectivity Parameters update command, the eUICC SHALL:

- Update the Connectivity Parameters of the targeted ISD-P

Commands

STORE DATA Command

This command is a STORE DATA command, as described in GlobalPlatform Card Specification [6] section 11.11.3.2.

Code	Value	Meaning
CLA	'80'	
INS	'E2'	STORE DATA
P1	'88'	Reference Control Parameter P1 0
P2	'00'	Block Number (Not used for Enable
Lc	'XX'	Length of data field
Data	'XX'	Application Data and MAC (if present)
Le	Not present	

Table 91: STORE DATA Command Message

Parameter P1 is coded according to the following table:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Last block
-	0	0	-	-	-	-	-	No general encryption information or non-encrypted data
-	-	-	0	1	-	-	-	DGI format of the command data field
-	-	-	-	-	X	X	X	RFU

Table 92: STORE DATA Reference Control Parameter P1

Data Field Sent in the Command Message

DGI	Length	Value Description			MOC
'3A07'	Var	Connectivity Parameters			M
		Tag	Length	Value Description	MOC

DGI	Length	Value Description			MOC
		'A0'	n	Connectivity parameters for SMS protocol	C
		'A1'	n	Connectivity parameters for HTTP protocol	C
		'A2'	n	Connectivity parameters for CAT_TP protocol	C

Table 93: Connectivity Parameters Data Field

The order of protocol connectivity parameters TLVs in the DGI define the protocol priority order to send notifications defined in section 4.1.1.11. If several TLVs are provided for the same protocol, the eUICC SHALL use the first TLV for this protocol, and ignore the extra TLVs for the same protocol.

NOTE 1: Void

NOTE 2: Multiple occurrences of each Connectivity Parameters TLV are possible, if they are sent by an off-card entity following a former version of this document.

SMS parameters coding

Tag	Length	Value Description	MOC
06*	Variable	SMSC Address*	M
81	1	PID**	O
82	1	DCS**	O

Table 94: Coding of Connectivity Parameters for SMS Protocol

* COMPREHENSION-TLV as defined in ETSI TS 102 223 [3], with the CR bit of the tags set to zero.

** Coding on one byte as specified in 3GPP TS 23.040 [39]

If no PID TLV is present, the eUICC SHALL use a default value of PID=00.

If no DCS TLV is present, the eUICC SHALL use a default value of DCS=04.

HTTP and CAT_TP parameters coding

Description
Bearer description*
Network Access Name (NAN) *
User Login*
User Password*

Table 95: Coding of Connectivity Parameters for HTTP and CAT_TP Protocols

* Comprehension TLVs as defined in ETSI TS 102 223 [3]. The CR bit of the tags SHALL be set to zero.

Response Message

Data Field Returned in the Response Message:

The data field of the response message SHALL NOT be present.

Processing State returned in the Response Message:

See GlobalPlatform Card Specification [6] section 11.11.3.2.

4.1.4 ESx (Device - eUICC) Interface Description

The eUICC MAY support the Local Enable and Disable command for the Emergency Profile.

The eUICC MAY support the Local Enable and Disable command for the Test Profile.

4.1.4.1 Local Enable for Emergency Profile

Function name: LocalEnableEmergencyProfile

Function group: Local Management

Function Provider entity: eUICC

Description: This function is used by the Device to locally enable the Emergency Profile. The eUICC SHALL NOT send notifications to the SM-SR. The Emergency Profile SHOULD remain enabled even after a restart of the Device. It is up to the Device to disable the Emergency Profile.

Prerequisites:

- A Profile with the Emergency Profile Attribute set exists on the eUICC.
- The Profile with the Emergency Profile Attribute set is not already enabled.

Command Description:

The Local Enable and Local Disable of a Profile with the Emergency Profile Attribute set is realised by using the ENVELOPE command with a dedicated Tag.

Data Field of ENVELOPE

Tag	Length	Value Description	MOC
‘E4’	1	00: Local Enable of Emergency Profile 01: Local Disable of Emergency Profile 02: Local Enable of Test Profile 03: Local Disable of Test Profile 04-FF: RFU	M

Table 4141: Data Field for Envelope containing Local Enable and Local Disable

Data Field Returned in the Response Message:

The structure of the response data is defined below:

```
-- ASN1START

ResultCode ::= [0] INTEGER{
```

```
   success (0),
   errorProfileRef (8), -- Emergency/Test Profile does not exists
   errorAlreadyEnabled (9), -- Emergency/Test Profile is already enabled
   errorAlreadyDisabled (10), -- Emergency/Test Profile is already disabled
   errorForbidden (12), -- Transition is forbidden for the Test Profile
   undefinedError (127)
}

-- ASN1STOP
```

The following table defines the error codes that are permitted for each command:

Command	Response				
	(0)	(8)	(9)	(10)	(12)
LocalEnableEmergencyProfile	X	X	X		
LocalDisableEmergencyProfile	X			X	
LocalEnableTestProfile	X	X	X		X
LocalDisableTestProfile	X			X	

Table 4141: Error codes allowed for each Local command

NOTE In order to support a legacy implementation for the Device, the eUICC MAY support implementation specific commands to trigger the Local Enable and the Local Disable of the Emergency Profile.

4.1.4.2 Local Disable for Emergency Profile

Function name: LocalDisableEmergencyProfile

Function group: Local Management

Function Provider entity: eUICC

Description: This function is used by the Device to locally disable the Emergency Profile and enable the previously enabled Profile. In case the Local Disable fails, the Fall-Back Mechanism SHALL be activated. The Fall-Back Mechanism SHALL consider that its previously enabled Profile is the Profile that was enabled before the Local Enable of the Emergency Profile. After disabling the Emergency Profile the eUICC MAY send a notification to the SM-SR (see 4.1.1.11)

Prerequisites:

- A Profile with the Emergency Profile Attribute set exists on the eUICC
- The Profile with the Emergency Profile Attribute set is enabled

Command and Response Description:

See 4.1.4.1

4.1.4.3 Local Enable for Test Profile

Function name: LocalEnableTestProfile

Function group: Local Management

Function Provider entity: eUICC

Description: This function is used by the Device to locally enable the Test Profile. The eUICC SHALL NOT send notifications to the SM-SR. The Test Profile SHOULD remain enabled even after a restart of the Device. It is up to the Device to disable the Test Profile.

Prerequisites:

- A Test Profile exists on the eUICC.
- The Test Profile is not already enabled.
- The Emergency Profile is not currently enabled.

Command and Response Description:

See 4.1.4.1

4.1.4.4 Local Disable for Test Profile

Function name: LocalDisableTestProfile

Function group: Local Management

Function Provider entity: eUICC

Description: This function is used by the Device to locally disable the Test Profile and enable the previously enabled Profile. In case the Local Disable fails, the Fall-Back Mechanism SHALL be activated. The Fall-Back Mechanism SHALL consider that its previously enabled Profile is the Profile that was enabled before the Local Enable of the Test Profile. After disabling the Test Profile the eUICC MAY send a notification to the SM-SR (see 4.1.1.11).**Prerequisites:**

- A Test Profile exists on the eUICC
- The Test Profile is enabled

Command and Response Description:

See 4.1.4.1

5 Off-Card Interface Descriptions

This section provides the description of the interfaces and functions within the Remote Provisioning and Management system outside the eUICC, including the following:

- ES1, interface between the two entities fulfilling the Role EUM and the Role SM-SR.

- ES2, interface between the two entities fulfilling the Role Operator and the Role SM-DP.
- ES3, interface between the two entities fulfilling the Role SM-DP and the Role SM-SR.
- ES4, interface between the two entities fulfilling the Role Operator and the Role SM-SR, also used between the two entities fulfilling the Role M2M SP and the Role SM-SR.
- ES4A, interface between the two entities fulfilling the Role Operator and the Role SM-SR, for the specific purpose of configuring M2M SP authorisations and Operator notifications
- ES7, interface between the two entities fulfilling the Role SM-SR and the Role SM-SR.

The functions in this section are grouped into function groups. Each function group is provided by a unique Role and corresponds to an autonomous and consistent functionality.

When a function group is implemented by a Role, all the functions associated to this function group SHALL be implemented by that Role. In other words, function groups cannot be partially implemented; if a special function is requested, then all the functions of the corresponding function group SHALL be implemented.

The following table presents the normative list of all the functions that are defined in this section.

Request-response functions:

Interface	Function group	Functions	Function provider Role
ES1	eUICC Management	RegisterEIS UpdateEISAdditionalPropertiesRequest	SM-SR
ES2	Profile Management	GetEIS AuditEIS DownloadProfile SetFallBackAttribute SetEmergencyProfileAttribute UpdatePolicyRules UpdateSubscriptionAddress GetONC SetONC GetPLMA SetPLMA	SM-DP
	Platform Management	EnableProfile DisableProfile DeleteProfile	SM-DP

ES3	Profile Management	GetEIS AuditEIS CreateISDP SendData ProfileDownloadCompleted SetFallBackAttribute SetEmergencyProfileAttribute UpdatePolicyRules UpdateSubscriptionAddress UpdateConnectivityParameters GetONC SetONC GetPLMA SetPLMA	SM-SR
	Platform Management	EnableProfile DisableProfile DeleteISDP	SM-SR
ES4	Profile Management	GetEIS SetFallBackAttribute SetEmergencyProfileAttribute UpdatePolicyRules UpdateSubscriptionAddress AuditEIS GetPLMA	SM-SR
	Platform Management	EnableProfile DisableProfile DeleteProfile	SM-SR
	eUICC Management	PrepareSMSRChange SMSRchange	SM-SR
ES4A	Profile Management	GetONC SetONC GetPLMA SetPLMA	SM-SR
ES7	eUICC Management	CreateAdditionalKeySet HandoverEUICC AuthenticateSMSR	SM-SR

Table 96: Request-Response Functions

Notification handler functions:

Interface	Function group	Notification handler functions	Function handler/recipient

ES2	Platform Management	HandleProfileDisabledNotification HandleProfileEnabledNotification HandleProfileDeletedNotification	Operator
	Profile Management	HandleEmergencyProfileAttributeSetNotification HandleEmergencyProfileAttributeUnsetNotification HandleProfileDownloadedNotification HandlePLMAChangedNotification HandlePolicyRulesUpdatedNotification HandleProfileFallBackAttributeSetNotification HandleProfileFallBackAttributeUnsetNotification	Operator
	eUICC Management	HandleSMSRChangeNotification	Operator
ES3	Platform Management	HandleProfileDisabledNotification HandleProfileEnabledNotification HandleProfileDeletedNotification	SM-DP
	Profile Management	HandleEmergencyProfileAttributeSetNotification HandleEmergencyProfileAttributeUnsetNotificationHandleProfileDownloadedNotification HandlePLMAChangedNotification HandlePolicyRulesUpdatedNotification HandleProfileFallBackAttributeSetNotification HandleProfileFallBackAttributeUnsetNotification	SM-DP (see NOTE)
	eUICC Management	HandleSMSRChangeNotification	SM-DP
ES4	Platform Management	HandleProfileDisabledNotification HandleProfileEnabledNotification HandleProfileDeletedNotification	Operator or M2M SP (see NOTE below)
	Profile Management	HandleEmergencyProfileAttributeSetNotification HandleEmergencyProfileAttributeUnsetNotification HandleProfileDownloadedNotification HandlePLMAChangedNotification HandlePolicyRulesUpdatedNotification HandleProfileFallBackAttributeSetNotification HandleProfileFallBackAttributeUnsetNotification	M2M SP (see NOTE below)
	eUICC Management	HandleSMSRChangeNotification	Operator

Table 97: Notification Handler Functions

NOTE: the sending of notification to the M2M SP is conditional to authorisation of the M2M SP by the Operator owner of the Profile

5.1 Function Commonalities

Each functions represents an entry points that is provided by a Role (function provider), and that can be called by other Roles (function requester).

5.1.1 Common Data Types

The functions provided in this section deal with management of eUICC and Profile, so that the common data defined in this section need to be used in most of the functions.

5.1.1.1 Simple Types

Type name	Description	Type definition
Hexadecimal String	String of even length composed of characters between '0' to '9' and 'A' to 'F' or 'a' to 'f'.	
AID	The AID (Application IDentifier) of an Executable Load File, an Executable Module, a security domain, or an Application.	Hexadecimal string representation of 5 to 16 bytes.
DATETIME	Any date and time used within any interface of this specification	String format as specified by W3C: YYYY-MM-DDThh:mm:ssTZD Where: YYYY = four-digit year MM = two-digit month (01=Jan, etc.) DD = two-digit day of month (01-31) hh = two digits of hour (00 -23) mm = two digits of minute (00 - 59) ss = two digits of second (00 - 59) TZD = time zone designator (Z, +hh:mm or -hh:mm) Ex: 2001-12-17T09:30:47Z
EID	The EID type is for representing an eUICC-ID. An eUICC-ID is primarily used in the "Embedded UICC Remote Provisioning and Management System" to identify an eUICC. See section 2.2.2 for EID description.	Hexadecimal string
ICCID	The ICCID type is for representing an ICCID (Integrated Circuit Card IDentifier). The ICCID is primarily used to identify a Profile. ICCID is defined according to ITU-T recommendation E.118 [21] , with the derivation that up to 20 digits are allowed.	String representation of up to 20 decimal digits, non-swapped. Ex: 8947010008, 8947010000123456784. 89470100001234567846
KCV	The KCV stands for "Key Check Value". It provides the material for receiving entity to ensure that it uses the same key value as the sending entity. See Annex F for detail of KCV computation.	Hexadecimal string
MSISDN	The Mobile Station ISDN (Integrated Services Digital Network) Number	String representation of up to 15 decimal digits, as defined in [22]
IMSI	The IMSI (International Mobile Subscriber Identity) used to identify the Subscriber of a Mobile Subscription.	String representation of up to 15 decimal digits including MCC (3 digits) and MNC (2 or 3 digits), as defined in ITU E.212 [12]
OID	An Object IDentifier	String representation of an OID, i.e. of integers separated with dots (for example: '1.2', '3.4.5')
TAR	The TAR (Toolkit Application Reference) of a security domain or an Application.	String - Hexadecimal string representation of exactly 3 bytes
VERSION	The Version type is for indicating a version of any entity used within this specification. A version is defined by its major, minor and revision number	String representation of three integers separated with dots (for example: '1.15.3').

Table 98: Simple Types

5.1.1.2 Complex Types

5.1.1.2.1 SUBSCRIPTION ADDRESS

The **SUBSCRIPTION-ADDRESS** type is defined by:

Data name	Description	Type	No.	MOC
msisdn	The MSISDN of the Subscription associated to this Profile.	MSISDN	1	C
imsi	The IMSI of the Subscription associated to this Profile.	IMSI	1	C

Table 99: Subscription Address

Either the MSISDN, the IMSI, or both, SHALL be present.

NOTE: Additional address types could be added depending of the deployment mode (for example: SIP-URI).

5.1.1.2.2 POL2-RULE

The POL2-RULE type is defined by the following data structure:

Data name	Description	Type	No.	MOC
subject	Identifies the subject on which the rule has to be applied. In the current version of this release, the possible subject is restricted to “PROFILE”.	Enumeration{PROFILE}	1	M
action	Identifies the action/function on which the rule has to be applied.	Enumeration{ENABLE, DISABLE, DELETE}	1	M
qualification	Indicates the final result of the rule that has to be applied.	Enumeration{ Not allowed, Auto-delete}	1	M

Table 100: POL2 Rule

The Policy Rules defined in GSMA ‘Remote Provisioning Architecture for Embedded UICC’ [1] are translated as follows:

1. “Disabling of this Profile not allowed”
Subject=”PROFILE”, action=”DISABLE”, qualification=”Not allowed”

2. “Deletion of this Profile not allowed”
Subject=”PROFILE”, action=”DELETE”, qualification=”Not allowed”

3. “Profile deletion is mandatory when it is disabled”
Subject=”PROFILE”, action=”DISABLE”, qualification=”Auto-delete”

Any other combination SHALL be treated as **not valid** regarding this specification release.

5.1.1.2.3 POL2

The POL2 type is defined by the following data structure:

Data name	Description	Type	No.	MOC
Rules	List of Policy Rules defined for a given Profile.	POL2-RULE	1..N	O

Table 101: POL2 Type

An empty POL2 SHALL be represented as a POL2 data structure having no rules inside

5.1.1.2.4 PROFILE INFO

The **PROFILE INFO** type is defined by:

Data name	Description	Type	No.
iccid	Identification of the Profile.	ICCID	1
isd-p-aid	The ISD-P-AID of the ISD-P containing the Profile. This is the AID that has been allocated at ISD-P creation time by the SM-SR. The TAR of the ISD-P is included in the ISD-P-AID. See section 2.2.1.3.	AID	1
mno-id	Identification of the Operator owner of the Profile. Once this information is associated to the Profile, it remains unchanged during the Profile's life-time.	OID	1
fallbackAttribute	Boolean value to indicate the Profile having the Fall-Back Attribute set.	Boolean	1
subscriptionAddress	The address of the Subscription associated to this Profile.	SUBSCRIPTION-ADDRESS	1
state	The current state of the ISD-P containing the Profile as per defined in GSMA Remote Provisioning Architecture for Embedded UICC [1]. The 'Deleted' state is not defined as a possible state; a 'Deleted' ISD-P will simply not appear in the list of eUICC Profiles.	Enumeration{ Created, Enabled, Disabled}	1
smdp-id	Identification of the SM-DP that has initially downloaded and installed the Profile, or through which the Operator owning the profile MAY perform platform management. This value can be empty in case the Profile has been loaded during issuance of the eUICC, else the value is mandatory. Once this information is associated to the Profile, it remains unchanged during the Profile's life-time.	OID	1
ProfileType	Indicates an Operator specific type of Profile generated by the SM-DP or personalised on the eUICC at point of manufacturing (for example 3G_16K)	String	1
allocatedMemory	Indicates the amount of cumulative non volatile Memory granted to the ISD-P to contain the Profile. Note that the allocated memory is different from the real required memory space for Profile installation; most of the time the allocated memory will be greater than the strict required memory space value. This information is provided in case of using the cumulative granted memory mechanism. The value is expressed in bytes. For compatibility with earlier versions of this specification, a value of 0 SHALL denote that no cumulative granted memory was specified during the installation of the ISD-P containing the Profile.	Integer	1

freeMemory	Indicates the amount of memory free within Profile allocated space. This information is provided in case of using the cumulative granted memory mechanism. The value is expressed in bytes.	Integer	1
pol2	Contains the POL2 rules defined for this Profile.	POL2	1

Table 102: Profile Info

NOTE: the presence of each data element is specified in Annex E, according to the function in which the PROFILE INFO is transmitted.

5.1.1.2.5 KEY-COMPONENT

The **KEY-COMPONENT** type is defined by:

Data name	Description	Type	No.	MOC
type	Definition of the key type coding. This defines the algorithm associated with the key, coded on 1 byte. Meaning of the byte value follows GlobalPlatform Card Specifications [6], section 11.1.8. i.e. '88' AES (16, 24, or 32 long keys)	Hexadecimal string representation of exactly 1 byte	1	M
value	The value as a binary data. This data SHALL be encrypted with a transport key agreed between the provider and the requester.	Hexadecimal string	1	M

Table 103: Key Component

5.1.1.2.6 KEY

The **KEY** type is defined by:

Data name	Description	Type	No.	MOC
index	The Key index as an integer value between 0 and 127 (as defined in GlobalPlatform Card Specifications)	integer	1	M
kcv	The Key Check Value of the key	KCV	1	M
KeyComponents	A simple key is defined using only one Key Component, but it is also possible to define keys with multiple key components (like RSA keys)	KEY-COMPONENT	1..N	M

Table 104: Key Type

NOTE: A key may be:

- a symmetric key. In this case the key will be composed of a single key component. The key value being the same in SM-SR and eUICC SD.
- an asymmetric key. In this case, the key will be most probably be composed of multiple key components. The key value in SM-SR being the counter part of the key value in the eUICC (i.e.: the public key at the SM-SR and the private key in the eUICC or vice-versa)

5.1.1.2.7 CERTIFICATE

The **CERTIFICATE** type is defined by:

Data name	Description	Type	No.	MOC
index	Indicates the index of the private key, being the private counterpart of the certificate. Index is an integer value between 0 and 127 (as defined in GlobalPlatform Card Specifications)	Integer	1	M
ca-id	Identifier of the CA that has issued (and signed) the certificate. This SHALL match the CA Identifier included in the certificate itself.	OID	1	M
value	Value of the certificate. The certificate SHALL be coded according to GlobalPlatform Card Specification UICC Configuration [7], section 9.2.1	Hexadecimal string	1	M

Table 105: Certificate Type

5.1.1.2.8 KEYSET

The **KEY SET** type is defined by:

Data name	Description	Type	No.	MOC
version	The version of the key set (as an integer value). The version value of a key set SHALL be unique within SD definition. Possible values are from 1 to 127. Example: '48' stands for a SCP03 version '30'	Integer	1	M
type	Generally key set usage (SCP03...) can be fully deduced from the key set version. If version information should not be used, this element SHALL be present to indicate the real usage of this key set.	Enumeration{ SCP03, SCP80, SCP81, TokenGeneration, ReceiptVerification, CA}	1	O
cntr	The counter value linked to the key set. This element is optional: value '0' as to be considered if missing.	Integer	1	O
keys	List of keys contained in the key set	KEY	1..128	C(1)
certificates	A certificate (as defined in GlobalPlatform context) as a counter part of a secret key loaded in a key set.	CERTIFICATE	1..128	C(1)

Table 106: KeySet Type

NOTE: A key set provisioned at SM-SR level may be composed of a set of keys or certificates.

A key set SHALL include at least one key or certificate. But for a given index, it MAY exist only one key or one certificate.

5.1.1.2.9 SECURITY-DOMAIN

The **SECURITY-DOMAIN** type is defined by:

Data name	Description	Type	No.	MOC
aid	The AID of the security domain	AID	1	M

tars	The list of TARs allocated to security domain, as an SD MAY have several TARs. If this list is empty, the implicit TAR is defined by the byte 13, 14, 15 of the AID.	TAR	1..N	O
sin	The security domain Provider Identification Number as defined in GlobalPlatform Card Specification [6]. The owner of the security domain endorsing the Role defined in the 'role' data	Hexadecimal string	1	M
sdin	The security domain Identification Number as defined in GlobalPlatform Card Specification [6]	Hexadecimal string	1	M
role	Identification of the Role of the security domain.	numeration{ISD-R, ECASD}	1	M
keysets	The list of key sets defined within the security domain	KEYSET	1..127	M

Table 107: Security Domain Type

5.1.1.2.10 EUICC-CAPABILITIES

The **EUICC-CAPABILITIES** type allows listing the capabilities supported by the eUICC.

The **EUICC-CAPABILITIES** type is defined by:

Data name	Description	Type	No.	MOC
CAT_TP-Support	If CAT_TP according to ETSI TS 102 127 [25] is supported by the eUICC.	Boolean	1	M
CAT_TP-Version	SHALL contain the highest supported release number of ETSI TS 102 127 (defining CAT_TP) that is implemented by the eUICC. Conditional to the support of the CAT_TP. In case of support, the supported version SHALL be at least the minimum version mandated by the present specification.	Version	1	C
HTTP-Support	If RAM over HTTP according to GlobalPlatform Card Specification Amendment B [8] is supported by the eUICC.	Boolean	1	M
HTTP-Version	SHALL contain the highest supported release number of GlobalPlatform Amendment B (defining RAM over HTTP) that is implemented by the eUICC. Conditional to the support of the HTTP. In case of support, the supported version SHALL be at least the minimum version mandated by the present specification.	Version	1	C
secure-packet-version	SHALL contain the highest supported release number of ETSI TS 102 225 (defining secure packet) that is implemented by the eUICC. The support of this feature as defined in ETSI TS 102 225 is not optional. The supported version SHALL be at least the minimum version mandated by the present specification.	Version	1	M

Remote-provisioning-version	SHALL contain the highest supported release number of this specification SGP.02 that is implemented by the eUICC. The support of this feature is obviously not optional. As a consequence, the eUICC SHALL be compliant will all relevant specifications referenced in this specification. Note 1: If the document version has less than three digits, one or more extra ".0" SHALL be appended to obtain a value that conforms to the type "Version" defined in Table 98. For example a value of "3.1.0" denotes that the eUICC is compliant with version 3.1 of SGP.02 Note 2: For backwards-compatibility reasons, if an EIS contains a value "1.1.0" for this field, the off-card entity SHALL assume that the eUICC is compliant with version 3.0 of SGP.02 or earlier.	Version	1	M

Table 108: eUICC Capabilities Type

Additional eUICC capabilities MAY be indicated in the EIS's AdditionalProperties (see section A.3.5). This specification defines the combinations of key:values provided in Table 109.

Each new version of this specification may introduce additional key:values. An EUM may also provide additional key:values.

Servers compliant with former versions may not interpret all these values; however, the previous versions mandate the SM-SR to carry the information e.g. in GetEIS or in ES7.HandoverEUICC, whether or not it can interpret it.

Key	Value	MOC
"gsma.ESIM.DNSResolverClientSupport"	"true" or "false" (an absent key/value pair having the default meaning of "false")	O
"gsma.ESIM.OSUpdateSupported"	"true" or "false" (an absent key/value pair having the default meaning of "false")	O
"gsma.ESIM.updatedPlatformVersion"	An EUM specific string identifying the version of the OS after the update	C
"gsma.ESIM.JavaCardVersionSupported"	If the eUICC supports Java Card™ [66], the value SHALL be a string formatted as type VERSION, indicating the version of Java Card™ supported. If the eUICC does not support Java Card™ [66], the value SHALL be the string "none". Note 1: this field was introduced in v4.1; however, it may also be present if the eUICC is compliant with an earlier version. Note 2: See section 2.2.7 for the requirement on the minimal version.	M
"gsma.ESIM.ProfilePackageVersions"	This field indicates the list of major versions including the associated highest minor version number of the SIMalliance eUICC Profile Package: Interoperable Format Technical Specification [53] supported by the eUICC. The list shall be provided in a single string, where each version is a string formatted as type VERSION, and the different versions, if more than one, are separated by a semi-colon. Note: this field was introduced in v4.1.	M

“gsma.ESIM.UICCCapability”	This field indicates the UICC Capabilities supported by this eUICC. The SM-DP MAY use those fields to select or tailor the proper Profile Package to install on this eUICC. The value of this field SHALL be the hexadecimal representation of the value part of the DER encoded `UICCCapability` data object defined in figure 511210-A (i.e., without tag and length fields). Note: this field was introduced in v4.1.	M
“gsma.ESIM.TreProperties”	This field indicates the TRE properties of this eUICC. The SM-DP MAY use those fields to select or tailor the proper Profile Package to install on this eUICC. The value of this field SHALL be the hexadecimal representation of the value part of the DER encoded `TreProperties` data object defined in figure 511210-B (i.e., without tag and length fields). This field SHALL be present if the eUICC is compliant with version 4.2 or later. This field SHALL contain one of the following settings: • isDiscrete • isIntegrated • isIntegrated, usesRemoteMemory Note: this field was introduced in v4.2.	M
“gsma.ESIM.TreProductReference”	This field SHALL be present if the eUICC is an Integrated eUICC. This information is provided by the EUM at registration time, and remains unchanged during the eUICC’s lifetime. It SHALL contain an unique reference of the Integrated TRE product that the eUICC is based upon. The value of this field SHALL be a string coded as defined in GlobalPlatform DLOA specification [69] section 7.1.1. Note: this field was introduced in v4.2.	C
“gsma.ESIM.FieldTest”	“true” or “false” This field SHALL be present with the value “true” if the eUICC is a Field-Test eUICC. (an absent key/value pair having the default meaning of “false”)	C

Table 109: AdditionalProperties denoting additional eUICC capabilities

The UICC Capabilities to be indicated in the EIS in this version of the specification are defined as follows:

```
-- ASN1START
-- Definition of UICCCapability
UICCCapability ::= BIT STRING {
/* Sequence is derived from ServicesList[] defined in SIMalliance PEDefinitions*/
   contactlessSupport(0),  -- Contactless (SWP, HCI and associated APIs)
   usimSupport(1),         -- USIM as defined by 3GPP
   isimSupport(2),         -- ISIM as defined by 3GPP
   csimSupport(3),         -- CSIM as defined by 3GPP2

   akaMilenage(4),         -- Milenage as AKA algorithm
   akaCave(5),             -- CAVE as authentication algorithm
   akaTuak128(6),          -- TUAK as AKA algorithm with 128 bit key length
   akaTuak256(7),          -- TUAK as AKA algorithm with 256 bit key length
   rfu1(8),                -- reserved for further algorithms
   rfu2(9),                -- reserved for further algorithms

   gbaAuthenUsim(10),      -- GBA authentication in the context of USIM
   gbaAuthenISim(11),      -- GBA authentication in the context of ISIM
   mbmsAuthenUsim(12),     -- MBMS authentication in the context of USIM
   eapClient(13),          -- EAP client

   javacard(14),           -- Javacard support
   multos(15),             -- Multos support

   multipleUsimSupport(16), -- Multiple USIM applications are supported within the
same Profile
   multipleIsimSupport(17),  -- Multiple ISIM applications are supported within the
same Profile
   multipleCsimSupport(18),   -- Multiple CSIM applications are supported within
the same Profile
   berTlvFileSupport(19),  -- BER TLV files
   dfLinkSupport(20),      -- Linked Directory Files
   catTp(21),              -- Support of CAT TP
   getIdentity(22),        -- Support of the GET IDENTITY command as defined in
ETSI TS 102 221 [6]
   profile-a-x25519(23),   -- Support of ECIES Profile A as defined in 3GPP TS
33.501 [67]
   profile-b-p256(24),     -- Support of ECIES Profile B as defined in 3GPP TS
33.501 [67]
   suciCalculatorApi(25)   -- Support of the associated API for SUCI derivation as
defined in 3GPP 31.130 [68]

}
-- ASN1STOP
```

Figure 511210-A: Definition of UICCCapability

Future versions of this specification may add more bits to `UICCCapability`. The SM-SR SHALL transparently handle additional bits. The SM-DP SHALL ignore unknown additional bits.

The TRE properties to be indicated in the EIS in this version of the specification are defined as follows:

```
-- ASN1START
TreProperties ::= BIT STRING {
     isDiscrete(0),
     isIntegrated(1),
     usesRemoteMemory(2) -- refers to the usage of remote memory protected by
                  the Remote Memory Protection Function described in SGP.01 [1]
   }
-- ASN1STOP
```

Figure 511210-B: Definition of TRE properties

5.1.1.2.11 AUDIT TRAIL RECORD

The **AUDIT-TRAIL RECORD** type contains the description of a Platform or a Profile Management operation performed by SM-SR or a notification received by SM-SR from the given eUICC.

The **AUDIT-TRAIL-RECORD** type is defined by:

Data name	Description	Type	No.	MOC
EID	The EID type is for representing an eUICC-ID. An eUICC-ID is primarily used in the "Embedded UICC Remote Provisioning and Subscription Management System" to identify an eUICC. See section 2.2.2 for EID description.	EID	1	M
SMSRid	SMSRid defined SM-SR storing given eUICC	OID	1	M
operationDate	Date and time of logged operation	DATETIME	1	M
operationType	Notification Type as defined in section 4.1.1.11 or Command Type as defined below.	Hexadecimal String	1	M
requesterId	Identification of the entity that has requested the operation to be performed on the eUICC	OID	1	C
status	For command type Function Execution Status as defined in section 5.1.5 is stored	ExecutionStatus	1	C
ISD-P-AID	The ISD-P-AID of the ISD-P containing the Profile. Not present in case the operation type does not concern a specific ISD-P AID (example: EstablishISDRkeyset)	AID	1	C
ICCID	The ICCID of the Profile. Not present in case the operation type does not concern a specific ISD-P AID (example: EstablishISDRkeyset)	String	1	C
IMEI	See ETSI TS 102 223 [3], clause 8.20	Hexadecimal String	1	C
MEID	See ETSI TS 102 223 [3], clause 8.81	Hexadecimal String	1	C

Table 110: Audit Trail Record Type

NOTE: Requester Id OID is empty in case of notification.

5.1.1.2.12 Command Type

Command type coding:

- '0100': CreateISDP
- '0200': EnableProfile
- '0300': DisableProfile
- '0400': DeleteProfile
- '0500': eUICCCapabilityAudit
- '0600': MasterDelete
- '0700': SetFallbackAttribute
- '0800': EstablishISDRkeyset

- ‘0900’:FinaliseISDRhandover
- ‘0A00’: SetEmergencyProfileAttribute
- ‘0B00’ to ‘FF00’ RFU

NOTE: 1st byte is reserved for Notification Type as defined in section 4.1.1.11

5.1.1.2.13 EIS

The **EIS** type is for representing eUICC Information Set.

Data name	Description	Type	No.
eid	Identification of the eUICC. See section 5.1.1.1 for type description. This information is initially provided by the EUM at registration time, and remains unchanged during all the eUICC’s lifetime.	EID	1
eum-id	Identification of the eUICC Manufacturer (i.e. Card Vendor) that has manufactured the eUICC. This information is initially provided by the EUM at registration time, and remains unchanged during all the eUICC’s lifetime. The ‘eum-id’ indication, jointly with the ‘platformType’ and ‘version, may especially be useful for the SM-DP to perform the Profile generation and packaging.	OID	1
productionDate	The date/time where the eUICC has been manufactured by the card vendor. This information is initially provided by the EUM at registration time, and remains unchanged during all the eUICC’s lifetime.	DATETIME	1
platformType	Indication of the eUICC platform/OS type. This information is initially provided by the EUM at registration time, and remains unchanged during all the eUICC’s lifetime. The content of this field is not enforced by this specification; the EUM can use any convenient string value.	String	1
platformVersion	Indication of the version of the eUICC platform/OS type. This information is initially provided by the EUM at registration time, and remains unchanged during all the eUICC’s lifetime.	VERSION	1
remainingMemory	Indicates the current total available memory (whatever the underlying technology, flash or eeprom) for Profile download and installation. This value MAY be either:- • a value cached by the SM-SR based on the initial total memory and memory required by all Profiles currently loaded on the eUICC. • a value retrieved from the eUICC The value is expressed in Bytes. This information is initially provided by the EUM at registration time, but may change according to the eUICC usage.	Integer	1

Availablememoryforprofiles	Indicates the free memory (whatever the underlying technology, flash, eeprom) without any Profile, available for Profile(s) loading and installation. This value is initially provided by the EUM at the registration time. It is calculated when the ISD-R and the ECASD are created, instantiated and personalized. This value is informative. The SM-SR cannot know how this value evolves during the card life cycle when a patch or a filter is applied or when the ECASD or the ISD-R configuration is modified. The SM-SR SHALL return the value that it received initially via ES1.registerEIS or via ES7.HandoverEUICC.	Integer	1
lastAuditDate	Some information part of the EIS can be refreshed by requesting directly the information to the eUICC to have the list of information that can be retrieved. This indicates the last date where such operation has been performed, and so indicating the freshness of the information stored at SM-SR level. This information is optional. If not present, it means that no audit has been performed on the eUICC.	DATE	1
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC's lifetime.	OID	1
isd-p-loadfile-aid	AID of the Executable Load File to be used for instantiation of an ISD-P. This information is initially provided by the EUM at registration time, and remains unchanged during all the eUICC's lifetime.	AID	1
isd-p-module-aid	AID of the Executable Module to be used for instantiation of an ISD-P. This information is initially provided by the EUM at registration time, and remains unchanged during all the eUICC's lifetime.	AID	1
profiles	List of Profiles currently installed on the eUICC. This information is initially provided by the EUM at registration time, and may change during the eUICC's lifetime.	PROFILE INFO	1..N
ISD-R	Contains the information related to the ISD-R	SECURITY-DOMAIN	1
ECASD	Contains the information related to the ECASD Although the type of this data is SECURITY-DOMAIN, some restrictions apply in order to ensure the consistency of the signature when this structure is stored or reconstructed: • The data SHALL contain one single Tar element, with the TAR value for the ECASD specified in Annex H. • If there is more than one Keyset or Certificate per ECASD, they SHALL be ordered according to: o The Keyset 'version' if there is more than one Keyset o The Certificate 'index' if there is more than one Certificate per Keyset	SECURITY-DOMAIN	1
eUICC-Capabilities	Contains the capabilities supported by the eUICC. This information is initially provided by the EUM at registration time.	EUICC-CAPABILITIES	1
audit trail	History of all the platform and Profile Management operations or eUICC notifications related to the eUICC	AUDIT-TRAIL-RECORD	0..N

signatureAlgorithm	Indicates the signature algorithm used by the EUM to sign the relevant part of the EIS. See Annex E to have details of the data that SHALL be included in the signature.
	
	The algorithm naming follows RFC 4051 [24]
		Enumeration{
		rsa-sha256, rsa-sha384,
		rsa-sha512,
		ecdsa-sha256,
		ecdsa-sha384,
		ecdsa-sha512
		}
			1

Signature	Signature value of the EUM. See Annex E to have details of the data included in the computation of the signature	Byte[]	1
AdditionalProperty	Optional additional information. See table 111-B	See Annex A.3.5	0..N

Table 111: EIS Type

NOTE: NOTE: the presence of each data element is specified in Annex E, according to the function in which the EIS is transmitted.

NOTE: The ISD-P(s) are not represented in the EIS as a pure SECURITY-DOMAIN data type; ISD-P information is directly included in the Profile representation without distinction as the SM-SR doesn't have access to ISD-P credentials.

NOTE: All values defined as Integer SHALL be encoded in decimal.

For extensibility purpose, additional information MAY be carried in the EIS. These information SHALL be specified as AdditionalProperties as specified in sectionA.3.5. This specification defines the following combinations of key:values, but other combinations MAY be supported by EUMs:

Key	Value
"gsma.ESIM.ES1.transportKey"	A string agreed between requester and provider, allowing to identify the transport key used to cipher key components
"gsma.ESIM.ES1.SCP80.KeySize"	Length of keys in SCP80 keysets of ISD-R"
"gsma.ESIM.ES1.SCP81.KeySize"	Length of keys in SCP81 keysets of ISD-R"
"gsma.ESIM.EmergencyProfile.AID"	ISD-P-AID of the Profile with the Emergency Profile Attribute Set, if any. If this value is empty or missing, no Profile on this eUICC has the Emergency Profile Attribute set.
"gsma.ESIM.TestProfile.AID"	ISD-P-AID of the Test Profile, if any. If this value is empty or missing, no Test Profile is present on this eUICC.

Table 111-2: Common Additional Properties

5.1.1.2.14 PLMA

The **PLMA** type is defined by:

Data name	Description	Type	No.	MOC
mno-id	Identification of the Operator owner of the Profiles concerned by this PLMA. See section 5.1.1.1 for type description.	OID	1	M
profileType	Identification of the Profile Type of the Profiles concerned by this PLMA.	String	1	M

	This is an arbitrary String that is meaningful only in the context of a given Operator (mno-id). An empty profileType string means all Profile owned by the Operator identified by mno-id, and having an empty Profile Type or no Profile Type in the EIS.			
m2m-sp-id	Identification of the M2M SP that will issue requests to the SM-SR to perform authorised operations, or that will receive authorised notifications. See section 5.1.1.1 for type description. See sections 5.7.1.1 and 5.7.1.2 for the specification of how the SM-SR can identify the requester when it receives ES4 and ES3 requests	OID	1	M
authorisedOperations	A list of operation names that identify either requests that the M2M SP will be authorised to send to the SM-SR, or notifications that the M2M SP is authorised to receive from the SM-SR, related to the profiles matching the other criteria in this request. Any operation not in this list is not or no longer authorised for Profiles matching the other criteria in this PLMA: in this case the M2M SP is not authorised to execute the request, or to receive the notification, identified by the operation name. An empty list means no operation is allowed, and can be used to remove all authorisations, for Profiles matching the other criteria in this PLMA See below the possible values of this String	String	0…N	M

Table 511214-A: PLMA Type

Each String in the authorisedOperations list SHALL be a distinct operation name among table 511214-B below.

Operation name	Meaning of the corresponding authorisation
GetEIS	The M2M SP is authorised to view any Profile that matches the other criteria in the PLMA in the EIS it could get via ES3 or ES4
AuditEIS	The M2M SP is authorised to audit via ES3 or ES4 any Profile that matches the other criteria in the PLMA
EnableProfile	The M2M SP is authorised to request EnableProfile via ES3 or ES4 on any Profile that matches the other criteria in the PLMA
DisableProfile	The M2M SP is authorised to request DisableProfile via ES3 or ES4 on any Profile that matches the other criteria in the PLMA
DeleteProfile	The M2M SP is authorised to request deletion via ES3 or ES4 on any Profile that matches the other criteria in the PLMA
setEmergencyProfileAttribute	The M2M SP is authorised to request setting the Emergency Profile Attribute via ES3 or ES4 on any Profile that matches the other criteria in the PLMA
unsetEmergency ProfileAttribute	The Operator or M2M SP is authorised to unset the Emergency Profile Attribute on any Profile that matches the other criteria in the PLMA, as the result of requesting to set it on another Profile
SetFallBackAttribute	The M2M SP is authorised to request setting the Fall-Back Attribute via ES3 or ES4 on any Profile that match the other criteria in the PLMA
UnsetFallBackAttribute	The Operator or M2M SP is authorised to unset the Fall-Back Attribute on any Profile that match the other criteria in the PLMA, as the result of requesting to set it on another Profile
UpdateSubscriptionAddress	The M2M SP is authorised to request UpdateSubscriptionAddress via ES3 or ES4 on any Profile that match the other criteria in the PLMA
HandleProfileEnabledNotification	The M2M SP is authorised to receive notification via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has been Enabled
HandleProfileDisabledNotification	The M2M SP is authorised to receive notification via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has been Disabled

HandleProfileDeletedNotification	The M2M SP is authorised to receive notification via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has been deleted
HandleProfileDownloadedNotification	The M2M SP is authorised to receive notification via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has been downloaded
HandleProfilePolicyRulesUpdatedNotification	The M2M SP is authorised to receive notification via ES3 or ES4 that the POL2 has been updated on any Profile that matches the other criteria in the PLMA
HandleEmergencyProfileAttributeSetNotification	The M2M SP is authorised to receive notifications via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has had its Emergency Profile Attribute set.
HandleEmergencyProfileAttributeUnsetNotification	The M2M SP is authorised to receive notifications via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has had its Emergency Profile Attribute unset.
HandleProfileFallBackAttributeSetNotification	The M2M SP is authorised to receive notifications via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has had its Fall-Back Attribute set.
HandleProfileFallBackAttributeUnsetNotification	The M2M SP is authorised to receive notifications via ES3 or ES4 that any Profile that matches the other criteria in the PLMA has had its Fall-Back Attribute unset.

Table 511214-B: List of Operation Eligible to PLMA

NOTE: There is no explicit operation UnsetEmergencyProfileAttribute and UnsetFallBackAttribute; the Emergency Profile Attribute or Fall-Back Attribute are only unset as the result of setting it on another Profile.

5.1.1.2.15 ONC

The **ONC** type is defined by:

Data name	Description	Type	No.	MOC
mno-id	Identification of the Operator owner of the Profiles concerned by this ONC. See section 5.1.1.1 for type description.	OID	1	M
profileType	Identification of the Profile Type of the Profiles concerned by this ONC. This is an arbitrary String that is meaningful only in the context of a given Operator (mno-id). An empty profileType string means all Profiles for this mno-id which have no Profile Type set in the EIS.	String	1	M
discardedNotifications	A list of notifications names that identify which notifications SHALL NOT be sent from the SM-SR to the Profile owning Operator, related to the Profiles associated with the Profile Type, provided in this request. Any notification names in this list is not or no longer requested by the Operator owning the Profile, related to the Profiles associated with the Profile Type, provided in this request. An empty list means that all notifications are requested by the Operator owning the Profile, related to the Profiles associated with the Profile Type, provided in this request. It can be used to remove all previously configured ONC for this Profile Type. See table 511215-B below for the format of this String. If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the Operator SHALL receive all notifications for status changes for its own Profiles, associated with this Profile Type, see also section 3.21 for details.	String	0…N	M

Table 511215-A: ONC Type

Each String in the discardedNotification list SHALL be a distinct notification name among table 511215-B below.

Notification name	Meaning of the corresponding configuration
HandleProfileDisabledNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when a Profile, associated with the Profile Type in the ONC, was disabled.
HandleProfileEnabledNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when a Profile, associated with the Profile Type in the ONC, was enabled.
HandleProfileDeletedNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when a Profile, associated with the Profile Type in the ONC, was deleted.
HandleSMSRChangeNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when the SM-SR, managing an eUICC, has changed and the eUICC is hosting a Profile which is associated with the Profile Type in the ONC.
HandleEmergencyProfileAttributeSetNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when the Emergency Profile Attribute was set on a Profile, associated with the Profile Type in the ONC.
HandleEmergencyProfileAttributeUnsetNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when the Emergency Profile Attribute was unset on a Profile, associated with the Profile Type in the ONC
HandleProfileFallBackAttributeSetNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when the Fall-Back Attribute was set on a Profile, associated with the Profile Type in the ONC.
HandleProfileFallBackAttributeUnsetNotification	The Operator owning the Profile receives no notifications via ES3 or ES4 when the Fall-Back Attribute was unset on a Profile, associated with the Profile Type in the ONC

Table 511215-B: List of Notifications Requested by ONC

5.1.2 Request-Response Function

A request-response function functionally corresponds to the case where a requestor Role sends a request message to a replier Role which receives and processes the request, ultimately returning a message in response. A function may take input data and may provide output data. A function may also deliver no output data.

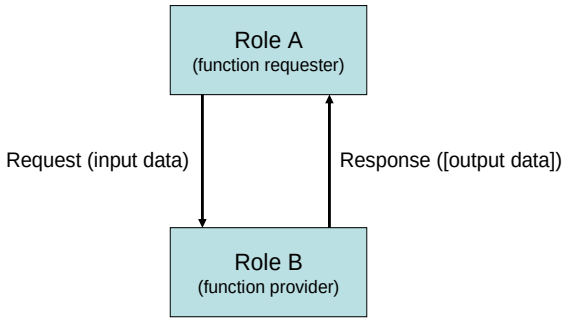


Figure 48: **Functions as a Request-Response Data Exchange**

At function definition level nothing is said about if the function is synchronous or asynchronous.

5.1.2.1 Validity Period

When a function is called, the function provider takes the responsibility to execute all the individual execution steps that are required to complete the function. Such processing may require some time to complete, but the function caller might want this processing duration to not exceed a specific amount of time called the "function validity period", as detailed in the following use cases:

- The function processing might no longer be valuable if it ends after the validity period. For example, a function is only valuable if it is executed within a minute. If more than a minute has elapsed, then it is no longer required to continue the function execution.
- Processing might not want to wait for an external event that might not occur before a very long time or an event that might even never occur at all. For example, it is possible when performing an OTA dialog that the Device is unreachable (switched off, lost…), or that an acknowledgement message coming from the Device is lost on the network (for example the loss of a PoR coming from an eUICC). If so, it might not be acceptable to wait several days or weeks for the Device to be switched on again, or even to wait forever for an acknowledgement message that will never come.
- It is desirable that the function provider system is not overloaded with requests that will be pending for a long period. The function caller would like to be notified as soon as possible that the function cannot be processed within a specific amount of time, and may then implement a calling side retry Policy.

By providing a validity period, the function caller indicates a specific amount of time to the function provider to process the function. The function caller has to ensure that the provided validity period is long enough so that the function provider is able to properly perform the requested function.

As a consequence, during this validity period, the function caller SHALL NOT issue the same request again as it might generate duplicate execution steps within the function provider system.

After the end of the validity period, the function provider SHALL no longer continue with new execution steps. It is only mandated to tell the function caller that the function processing has expired. It is then the caller responsibility to either:

- Request the same function again,
- Or simply abandon the overall process into which the function was called.

Input data name	Description	Type	No.	MOC
Function Requester Identifier	Identification of the function requester.	String	1	M
Function Call Identifier	Identification of the function call. This identifier enables to manage function call retry policies. When requesting for the execution of a function, the function caller SHALL provide a unique Function Call Identifier. Uniqueness is to be ensured in its own perimeter. In case the function caller wants to retry the same function, then it SHALL perform the same function call, providing the same Function Call Identifier.	String	1	C

	On function provider side, when receiving this retry attempt, if a call to a function if performed with an Function Call Identifier of a function already in process in its system, then the function provider SHALL refuse the new call If the function provider does not want to implement any retry Policy, then it might ignore this field. The Function Call identifier is only mandatory for request-response functions. It SHALL NOT be present for notification functions.			
Validity Period	This field defines the length of the period (provided as a **number of seconds**) during which the request is valid. The period starts at the time the function call was received by the function provider and ends a number of seconds later. During this period of time, the function provider has the responsibility to execute the function. When a validity period is provided in the function call, the function provider, on reception of the function call, SHALL either: • **Accept** the function call: in that case the function provider accepts the provided validity period or • **Reject** the function call: if the function provider immediately considers that the validity period is invalid (for example too long or too short) or cannot fulfil the requirements (i.e. cannot start the sequence of operations so that all of the operations are completed within the validity period), it SHALL NOT process the function and SHALL immediately return a Function Execution Status output parameter with a Status field set to 'Failed' and a Subject code and Reason code of the Status Code Data field set to 'Validity Period not accepted'. The function provider SHALL also indicate to the function caller an acceptable amount of time into which the request could be fulfilled, by setting the Acceptable Validity Period field in the output header. The Validity Period is only present (but optional) for request-response functions. If not specified, the function caller doesn't require any specific validity period. Nevertheless the function provider is free to apply any internal rule to restrict the validity period (it could be the case to ensure that a function request will never stay stacked in the system). In that case the function provider SHALL indicate to the function caller the applied validity period value in the Acceptable Validity Period field in the output header. The Validity Period SHALL NOT be present for notification functions.	Integer	1	O

Table 112: Validity Period and Functions Identifier

5.1.2.2 Exceptions

During the processing of a function, an unexpected behaviour may happen. This event, called an exception in this specification, may cause the function to be ended before the functional work to be completed (the exception is then considered as an error), or may let the functional work continue, but under specific conditions (the exception is then called a warning).

This is the function provider's responsibility to give information on any exception encountered during the processing of a function; however the behaviour of the function caller when receiving this exception may depend on its own context (for example stop its current processing, or perform a retry attempt, or try a workaround processing, etc.)

5.1.3 Notification Handler function

In some cases, functions are considered as notifications as they functionally correspond to events sent from one Role to another. If so, the Role that generates the notification is called the notification source or the notifier, and the Role that receives the notification is called the notification destination or the notification recipient or notification handler.

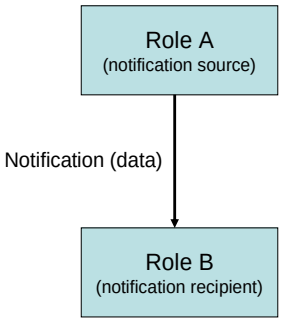


Figure 49: **Notification as One Way Events**

By definition, no validity period is applied for a notification, and no data can be returned back by the notification recipient to the notification source.

Similarly, no exception is expected in the context of a notification.

5.1.4 Functions Input Header

All functions (request-response and notification handler) SHALL include the following header as part of the input data:

Input data name	Description	Type	No.	MOC
Function Requester Identifier	Identification of the function requester.	String	1	M
Function Call Identifier	Identification of the function call. This identifier enables to manage function call retry policies. When requesting for the execution of a function, the function caller SHALL provide a unique Function Call Identifier. Uniqueness is to be ensured in its own perimeter. In case the function caller wants to retry the same function, then it SHALL perform the same function call, providing the same Function Call Identifier. On function provider side, when receiving this retry attempt, if a call to a function if performed with an Function Call Identifier of a function already in process in its system, then the function provider SHALL refuse the new call If the function provider does not want to implement any retry Policy, then it might ignore this field. The Function Call identifier is only mandatory for request-response functions. It SHALL NOT be present for notification functions.	String	1	C

Validity Period	This field defines the length of the period (provided as a **number of seconds**) during which the request is valid. The period starts at the time the function call was received by the function provider and ends a number of seconds later. During this period of time, the function provider has the responsibility to execute the function. The function provider, on reception of the function call, MAY: • **Accept** the function call: in that case the function provider accepts the provided validity period • **Reject** the function call: if the function provider immediately considers that the validity period is invalid (for example too long or too short) or cannot fulfil the requirements (i.e. cannot start the sequence of operations so that all of the operations are completed within the validity period), it SHALL NOT process the function and SHALL immediately return a Function Execution Status output parameter with a Status field set to 'Failed' and a Subject code and Reason code of the Status Code Data field set to 'Validity Period not accepted'. The function provider SHALL also indicate to the function caller an acceptable amount of time into which the request could be fulfilled, by setting the Acceptable Validity Period field in the output header. The Validity Period is only present (but optional) for request-response functions. If not specified, the function caller doesn't require any specific validity period. Nevertheless the function provider is free to apply any internal rule to restrict the validity period (it could be the case to ensure that a function request will never stay stacked in the system). In that case the function provider SHALL indicate to the function caller the applied validity period value in the Acceptable Validity Period field in the output header. The Validity Period SHALL NOT be present for notification functions.	Integer	1	O

Table 113: Functions Input Headers

Additionally to this common header, each function may define its own set of additional input data.

5.1.5 Functions Output Header

All functions (request-response) SHALL include the following header as part of the output data. Notifications don't have any output data.

Output data name	Description	Type	No.	MOC
`Processing Start`	The start time and date of the real processing of the function by the function provider (and not the time and date of reception of the request).	DATETIME	1	O
`Processing End`	The function processing end time and date.	DATETIME	1	O
`Acceptable Validity Period`	In case the validity period provided as input parameter is not acceptable, then the function provider SHALL return an acceptable value to the function caller (see section 5.1.4) as a **number of seconds**. In case the function call has been rejected because of a non acceptable validity period the function caller might then call again the same function with a validity period that is more convenient (but that MAY however differ from the exact value of the Acceptable Validity Period field sent in response to the previous function call).	Integer	1	C

`Function Execution Status`	Indicates whether the processing has been completed correctly or not. If required, provides information to give details on the processing result (status code, status code reason, status message…). The Execution Status type is described below.	ExecutionStatus	1	M

Table 114: Functions Output Headers

Where an Execution Status is:

Data name	Description	Type	No.	MOC
Status	It indicates whether the processing has been completed correctly or not. Value 'Executed-Success' means that the function has been processed correctly. Application output data MAY optionally be part of the function response. Value 'Executed-WithWarning' means that the function has been processed correctly, but that warnings have been generated during this execution. Application output data MAY optionally be part of the function response in order to provide details on the warnings. Value 'Failed' means that the function execution has encountered errors during its processing. The Status Code Data output structure SHALL give the reason of error in the processing (values depend on the function and MAY be implementation dependant). Value 'Expired' means that the validity period of the request has expired before the completion of the function processing. The Status Code Data output structure MAY give the reason of expiration of the function.	Enumeration {Executed-Success, Executed-WithWarning, Failed, Expired}	1	M
Status code data	It provides the reason of the Status. Present only if the Status is 'Execute-WithWarning', 'Failed', or 'Expired'. The Status Code Data type is described below.	Status code data	1	O

Table 115: Execution Status

Where a Status code data is:

Data name	Description	Type	No.	MOC
Subject code	Represents the system element concerned by the exception. A normative list of subjects is given in section 5.1.6.1	OID	1	M
Reason code	Represents the reason of the exception. A normative list of reasons is given in section 5.1.6.2	OID	1	M
Subject identifier	The identifier of the subject or any identification data of the subject that caused the exception (for example ICCID of the Profile when the Subject is a "Profile"). The possible values of the Subject Identifier depend on the function.	String	1	O
Message	It provides a textual and human readable explanation of the exception. The Message value is implementation dependant	String	1	O

Table 116: Status Code

5.1.6 Status Code

Status codes are used in a function call to indicate that an exception occurred during the processing of the function.

The “status code” is part of the Function output header (as defined in section 5.5.5). In this specification, the status codes are representing any exception from a simple warning to an error.

- When an error is raised (function output header status is ‘Failed’), it means that the expected functional behaviour has not been completed.
- When a warning is raised (function output header status is ‘Executed-WithWarning’’), it means that the expected functional behaviour has been completed, but under specific conditions that SHOULD be pointed out by the function provider.

Both Subject code and Reason code fields of the Status code data of the function output header are represented by an OID (Object IDentifier). These identifiers refer to a list of pre-defined elements and reasons (see below for details).

5.1.6.1 Subject Code

The Subject code represents, from the function provider perspective, the entity on which the exception occurred. The subject code can either be its own system (for example: an internal error), a part of the system (for example: eUICC, Profile …) or even the function caller itself (for example: Identification issue).

GlobalPlatform System, Messaging Specification for Management of Mobile-NFC Services [23] already defines some subject codes that are organised as a tree representation. This specification proposes to reuse the category “1. Generic” as defined in [23].

The subjects codes linked with the “Remote Provisioning Architecture for Embedded UICC”, are regrouped under a dedicated category, which has the identifier value “8. eUICC Remote Provisioning” to avoid any conflict with the categories already defined in [23].

The possible values for the Subject code used in the context of this specification are defined as follow:

1. Generic
    - 1.1. Function Requester
    - 1.2. Function Provider
        - 1.2.1. Validity Period
    - 1.3. Protocol
        - 1.3.1. Protocol Format
        - 1.3.2. Protocol Version
    - 1.4. External Resource
    - 1.5 Extension Resource
    - 1.6 Function
8. eUICC Remote Provisioning

8.1 eUICC

8.1.1 EID

8.2 Profile

8.2.1 Profile ICCID

8.2.2 POL1

8.2.3 POL2

8.2.4 Void

8.2.5 Profile Type

8.2.6 Subscription Address

8.2.7 PLMA

8.2.8 ONC

8.3 ISD-P

8.3.1 ISD-P-AID

8.4 ISD-R

8.5 ECASD

8.5.1 Certification Request

8.5.2 Embedded UICC Certificate Authority

8.6 EIS

8.7 SM-SR

8.7.1 SM-SR certificate

8.8 SM-DP

8.9 M2M SP

8.10 Operator

5.1.6.2 Reason Code

The Reason code represents, from the function provider perspective, the reason why the exception occurred.

As for Subject Code, GlobalPlatform System, Messaging Specification for Management of Mobile-NFC Services [23] already defines some reason codes that are organised as a tree representation. This specification proposes to reuse the following categories coming from [23]:

1. Access error
2. Format error
3. Conditions of use not satisfied
4. Processing error
5. Transport error
6. Security error

The possible values for the Reason code are defined as follow:

1. Access Error
    1.1. Unknown (Identification or Authentication)
    1.2. Not Allowed (Authorisation)
2. Format Error
    2.1. Invalid
    2.2. Mandatory Element Missing
    2.3. Conditional Element Missing
3. Conditions of Use Not Satisfied
    3.1. Unsupported
    3.2. Maximum Size Exceeded
    3.3. Already in Use (Uniqueness)
    3.4. Invalid Destination
    3.5. Invalid Transition
    3.6. Related Objects Exists
    3.7. Unavailable
    3.8. Refused
    3.9 Unknown
4. Processing Error
    4.1. Function Already in Progress
    4.2. Execution Error
    4.3. Stopped on Warning
    4.4. Busy
    4.5. Operation Already Processed
    4.6. Not Present / Missing
    4.7. Generation Not Possible
    4.8. Insufficient Memory
    4.9. Unassigned
5. Transport Error
    5.1. Inaccessible
    5.2. Timeout
    5.3. Time to Live Expired
    5.4 Delivered With No Response
    5.5 Connection Lost
6. Security Error
    6.1. Verification Failed

6.2. Decipher Failed

6.3. Certificate Expired

5.1.6.3 Status Code Example

Identification issue example:

State: The function requester tries to access a function, but its credentials are not known to the function provider

Function processing: The function provider raises an internal exception, as the function requester couldn't be identified

Returned Status Code:

- Subject code: **1.1** – Function requester
- Reason code: **1.1** – Unknown

Platform Management issue:

State: The function requester tries to create a new ISD-P, but with an ICCID already in used for another Profile

Function processing: The function provider raises an internal exception, as there is a conflicting AID.

Returned Status Code:

- Subject code: **8.2.1** – Profile ICCID
- Reason code: **3.3** – Already in use

5.1.6.4 Common Function Status Code

The following table provides the normative list of status codes that may be raised by any function defined in this specification. These statuses SHALL be implemented.

In addition each function MAY raise additional specific status codes. In that case, it is defined explicitly in the function description.

As an implementer's choice, it is also possible that a function MAY return additional status codes not described in this specification. The function caller SHALL be ready to handle such situation.

Common status code when 'Function execution status' is 'failed'

Subject code	Subject	Reason code	Reason	Description
1.1	Function requester	1.1	Unknown (Identification or Authentication)	The function caller is unknown to the function provider.
1.1	Function requester	1.2	Not allowed (authorisation)	The function caller is not allowed to use this function.
1.2	Function provider	4.2	Execution error	Internal processing error (this status code SHALL be returned only when no more accurate status code can be returned)

1.2	Function provider	4.4	Busy	Busy: not possible to process the function for the moment
1.2.1	Validity period	3.8	Refused	The requested validity period is not accepted by the function provider.
1.6	Function	2.1	Invalid	An input parameter of the function is invalid (wrong format, not acceptable value…). The contextual message conveyed with the status code data SHALL indicate the name of the concerned parameter.
1.6	Function	2.2	Mandatory Element Missing	A mandatory input parameter of the function is missing. The contextual message conveyed with the status code data SHALL indicate the name of the concerned parameter.
1.6	Function	2.3	Conditional Element Missing	A conditional input parameter of the function is missing. The contextual message conveyed with the status code data SHALL indicate the name of the concerned parameter.

Table 117: Function Execution Status 'Failed' Codes

Common status code when 'Function execution status' is 'Expired'

Subject code	Subject	Reason Code	Reason	Description
1.6	Function	5.3	Time to live expired	The function execution request has expired (end of validity period has been reached). This may be because the server had no time to execute the function or because the function was requesting a remote communication with the eUICC which was not present on the network during all the validity period.

Table 118: Function Execution Status 'Expired' Codes

5.2 ES1 (EUM – SM-SR) Interface Description

5.2.1 Register EIS

Function name: RegisterEIS

Related Procedures: eUICC registration at SM-SR: register a new EIS

Function group: eUICC Management

Function Provider: SM-SR

Description:

This function allows an eUICC Manufacturer (EUM) to register an eUICC represented by its eUICC Information Set (EIS) within an identified SM-SR information database.

The EIS contains the complete set of data that is applicable for the SM-SR to manage the lifecycle of this eUICC. This data set is split in two different parts:

- A fixed signed part containing the identification of the eUICC
- A variable part containing the keys for the Platform Management plus the list of the different Profile loaded with the identified eUICC

The ISD-R key components SHALL be ciphered using methods agreed in section 2.8.

The metadata describing the ciphering MAY be transported as AdditionalProperties in the EIS, or MAY be agreed out of band.

This function may return:

- A ‘Function execution status’ with ‘Executed-Success’ indicating that the registration function has been successfully executed on the SM-SR as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
EIS	This is the eUICC Information Set of the eUICC. See section 5.1.1.2 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1-N	M

Table 119: Register EIS Additional Input Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.6	Related Object Exists	Indicates that the EIS identified by this EID, is already register within the EIS database of the SM-SR
8.6	EIS	6.1	Verification failed	During the verification of the EIS signature, an error occurred.
8.6	EIS	2.1	Invalid	During the consistency review of the EIS data, an error was found (for example free memory is bigger than full memory)

Table 120: Register EIS Specific Status Codes

5.2.2 Update EIS AdditionalProperties

Function name: UpdateEISAdditionalProperties

Related Procedures: -

Function group: eUICC Management

Function Provider: SM-SR

Description:

This function allows an eUICC Manufacturer (EUM) to update the AdditionalProperties field within the EIS in an identified SM-SR information database. The only field that is updated is “gsma.ESIM.updatedPlatformVersion”, the others remain unchanged.

The AdditionalProperties field is defined in Table 109.

This function may return:

- A ‘Function execution status’ with ‘Executed-Success’ indicating that the update function has been successfully executed on the SM-SR as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
AdditionalProperties	This is the EIS field as described in section 5.1.1.2.10.	AdditionalProperties	1	M

Table 522-A: Update AdditionalProperties Additional Input Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	1.1	Unknown	Indicates that the EID is unknown to the function provider
1.6	Function	2.1	Invalid	Indicates that it is not allowed to update an additional property in the input data

Table 522-B: Update AdditionalProperties Specific Status Codes

5.3 ES2 (Operator – SM-DP) Interface Description

5.3.1 Getting eUICC Information

Function name: GetEIS

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider: SM-DP

Description: This function allows the Operator to retrieve up to date the EIS information. The SM-DP SHALL forward the function request to the SM-SR “**ES3.GetEIS**” as defined in section 5.4.1.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC to be audited. See section 5.1.1.1 for type description.	EID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management.	OID	1	M

	This information may change during the eUICC's lifetime.			

Table 121: Get EIS Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
eis	The relevant eUICC Information Set of the eUICC See section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	M

Table 122: Get EIS Additional Output Data

Specific status codes

In addition to those returned by **ES3.GetEIS**, this function may return:

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be solved by the SM-DP

Table 123: Get EIS Specific Status Codes

5.3.2 Download a Profile

Function name: DownloadProfile

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider: SM-DP

Description: This function allows the Operator to request that the SM-DP downloads a Profile, identified by its ICCID, via the SM-SR identified by the Operator on the target eUICC, the eUICC being identified by its EID.

Function flow

Upon reception of the function request, the SM-DP SHALL perform the following minimum set of verifications:

- The SM-DP SHALL verify it is responsible for downloading and installation of the Profile

The SM-DP MAY provide additional verifications.

In case one of these conditions is not satisfied, the SM-DP SHALL refuse the function request and return a 'Function execution status' indicating 'Failed' with the relevant status code (see table below).

The SM-DP SHALL perform/execute the function according to the Profile Download and Installation procedure described in section 3.1.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the function has been successfully executed by the function provider as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4 indicating that the Profile has not been downloaded before the expiration of the specified Validity Period.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below, indicating that the Profile has not been downloaded.
- A ‘Function execution status’ indicating ‘Executed_WithWarning’ indicating that the Profile has been downloaded successfully, but the optional Enable has failed or expired. In this case, the Status Code and if available, the eUICCResponseData are the ones reported by ES3.EnableProfile.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the target eUICC. See section 5.1.1.1 for type description.	EID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC's lifetime.	OID	1	M
profileType	Identification of the Profile type to download and install in the eUICC.	String	1	C
iccid	Identification of the Profile to download and install. See section 5.1.1.1 for type description.	ICCID	1	C
enableProfile	Indicates if the Profile SHALL be enabled after downloading and installation.	BOOLEAN	1	M

Table 124: Download Profile Additional Input Data

NOTE: Operator can either provide ICCID or the Profile type. In case the Profile type is provided, the SM-DP is free to select one of the Profiles that matches the Profile type.

Additional output data:

Output data name	Description	Type	No.	MOC
iccid	Indicates the Profile ICCID that has been downloaded and installed	ICCID	1	C
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES5 depending of the requested function.	Hex binary	1	O

Table 125: Download Profile Additional Output Data

Specific status codes

In addition to the Status Codes returned by ES3.EnableProfile, this function can return:

Subject Code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the SM-SR.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile, identified by this iccid is unknown to the SM-DP.
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.
8.2.5	Profile Type	3.9	Unknown	Indicates that the Profile type identified by this profileType is unknown to the SM-DP.
8.2.5	Profile Type	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the ProfileType.
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the SM-SR

Table 126: Download Profile Specific Status Codes

5.3.3 Updating the Policy Rules of a Profile

Function name: UpdatePolicyRules

Related Procedures: -

Function group: Profile Management

Function Provider: SM-DP

Description: This function allows the Operator to update POL2 of a Profile, identified by its ICCID, and installed on an eUICC identified by its EID.

The SM-DP SHALL forward this function request to the identified SM-SR by calling the **ES3.UpdatePolicyRules** function as defined in section 5.4.6.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile See section 5.1.1.1 for type description.	ICCID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC's lifetime.	OID	1	M
pol2	List of POL2 rules associated with the identified Profile. See section 5.1.1.2 for type description.	POL2	1	M

Table 127: Update Policy Rules Additional Input Data

Additional output data:

None

Specific status codes

In addition to those returned by **ES3.UpdatePolicyRules**, this function may return:

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be solved by the SM-DP

Table 128: Update Policy Specific Status Codes

5.3.4 Updating eUICC Information

Function name: UpdateSubscriptionAddress

Related Procedures: Profile Download and Installation, Profile Enabling, Profile Enabling via SM-DP

Function group: Profile Management

Function Provider: SM-DP

Description: This function enables the caller to update the Subscription Address for a Profile in the eUICC Information Set (EIS) of a particular eUICC identified by the EID and ICCID. The Subscription Address is the identifier, such as MSISDN and/or IMSI, through which the eUICC is accessible from the SM-SR via the mobile network when the Profile is in Enabled state. The function replaces the content of the Subscription Address. For consistency within the system, it is the responsibility of the caller to ensure that all data is provided. The SM-DP SHALL forward the function request to the SM-SR "**ES3.UpdateSubscriptionAddress**" as defined in section 5.4.7.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC to be updated. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the target Profile. See section 5.1.1.1 for type description.	ICCID	1	M
newSubscriptionAddress	The new Subscription Address	Subscription Address	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC's lifetime.	OID	1	M

Table 129: Update Subscription Address Additional Input Data

This function has no additional output data.

Specific status codes

In addition to those returned by **ES3.UpdateSubscriptionAddress**, this function may return:

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the SM-DP

Table 130: Update Subscription Address Specific Status Codes

5.3.5 Profile Enabling

Function name: EnableProfile

Related Procedures: Profile Enabling via SM-DP

Function group: Platform Management

Function Provider: SM-DP

Description:

This function allows the Operator owner of the Profile to request a SM-DP to enable a Profile in a specified eUICC, eUICC being identified by its EID.

The SM-DP receiving this request SHALL process it according to the "Profile Enabling via SM-DP" procedure described in the section 3.3 of this specification.

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the Profile has been enabled on the eUICC.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4

A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC's lifetime.	OID	1	M
iccid	Identification of the Profile to enable. See section 5.1.1.1 for type description.	ICCID	1	M

Table 131: Enable Profile Additional Input Data

Additional output data:

- None

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the SM-SR.
8.2	Profile	5.1	Inaccessible	Indicates that the profile change procedure couldn't complete after enabling the target profile, and the profile change was rolled-back on the eUICC,
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the SM-SR.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the SM-SR but installed on another eUICC than the one identified by the function caller.
8.2.1	Profile ICCID	3.5	Invalid Transition	Indicates that the Profile was already Enabled
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.
8.2.2	POL1	3.8	Refused	The POL1 of the impacted Profiles doesn't allow this operation.
8.2.3	POL2	3.8	Refused	The POL2 of the impacted Profiles doesn't allow this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the enabling command on the eUICC.
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the function provider.

Table 132: Enable Profile Specific Status Codes

5.3.6 Profile Disabling

Function name: DisableProfile

Related Procedures: Profile Disabling via SM-DP

Function group: Platform Management

Function Provider: SM-DP

Description: This function allows the Operator owner of the Profile to request an SM-DP to disable the Profile in a specified eUICC; eUICC being identified by its EID.

The SM-DP receiving this request SHALL process it according to Profile Disabling via SM-DP procedure described in section 3.5 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed-Success’ indicating that the Profile has been disabled on the eUICC.
- A ‘Function execution status’ with ‘Executed-WithWarning’, with a status code as defined in section 5.4.9, indicating that the Profile has been disabled on the eUICC, and deleted after application of a POL1 or POL2 rule.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.4.9 or a specific status code as defined in the table here after

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC’s lifetime.	OID	1	M
iccid	Identification of the Profile to disable. See section 5.1.1.1 for type description.	ICCID	1	M

Table 133: Disable Profile Additional Input Data

Additional output data:

None

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be solved by the SM-SR

Table 134: Disable Profile Specific Status Codes

5.3.7 Delete a Profile

Function name: DeleteProfile

Related Procedures: Profile and ISD-P Deletion

Function group: Platform Management

Function Provider: SM-DP

Description: This function allows the Operator to request deletion of the target ISD-P with the Profile to the SM-DP; eUICC being identified by its EID. The SM-DP SHALL forward the function request to the SM-SR "**ES3.DeleteISDP**" as defined in section 5.4.10.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to disable. See section 5.1.1.1 for type description.	ICCID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC's lifetime.	OID	1	M

Table 135: Delete Profile Additional Input Data

Additional output data:

None

Specific status codes

In addition to those returned by **ES3.DeleteISDP**, this function may return:

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the SM-DP

Table 136: Delete Profile Specific Status Codes

5.3.8 Notify a Profile is Disabled

Function name: HandleProfileDisabledNotification

Related Procedures: Profile Download and Installation, Profile Enabling via SM-DP, Profile Enabling, Fall-Back Activation Procedure, Profile Enabling via M2MSP, Profile Disabling via M2MSP

Function group: Platform Management

Notification handler/recipient: Operator

Description:

This function SHALL be called to notify that the Profile identified by its ICCID has been disabled on the eUICC identified by its EID. It is assumed that the ICCID is enough for the SM-DP to retrieve the Operator to notify.

This notification also conveys the date and time specifying when the operation has done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been disabled. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 137: Handle Profile Disabled Notification Additional Input Data

5.3.9 Notify a Profile Enabling

Function name: HandleProfileEnabledNotification

Related Procedures: Profile Disabling and Profile Disabling via SM-DP, Profile Download and Installation, Fall-Back Activation Procedure, Profile Enabling via M2MSP, Profile Disabling via M2MSP

Function group: Platform Management

Notification handler/recipient: Operator

Description:

This function SHALL be called to notify that the Profile identified by its ICCID has been enabled on the eUICC identified by its EID. It is assumed that the ICCID is sufficient for the SM-DP to retrieve the Operator to notify.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been enabled. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 138: Handle Profile Enabled Notification Additional Input Data

5.3.10 Notify a SM-SR Change

Function name: HandleSMSRChangeNotification

Related Procedures: SM-SR Change

Function group: eUICC Management

Notification handler/recipient: Operator

Description: This function SHALL be called for notifying each Operator owning a Profile hosted in the eUICC, identified by its EID, that the SM-SR has changed. The notification is sent by the new SM-SR to the SM-DP, which route this notification to the Operator.

What is performed by the Operator receiving this notification is out of scope of this specification.

Note that this notification also conveys the date and time specifying when the operation has been done.

Note that this notification is not related to a particular Profile. It is up to the notification recipient to determine if any Profile that is deployed on this eUICC needs subsequent action.

Additional input data:

Input data name	Description	Type	No.	MOC
eis	The relevant part of the eUICC Information Set linked with the Operator owning the Profile hosted in the eUICC. See section 5.1.1.2.13 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 139: Handle SM-SR Change Notification Additional Input Data

No output data is expected in response to this notification.

5.3.11 Notify a Profile Deletion

Function name: HandleProfileDeletedNotification

Related Procedures: Profile Enabling, Profile Enabling via SM-DP, Profile Enabling via M2M SP, Profile DIsabling via M2M SP, Profile and ISD-P Deletion via M2M SP

Function group: Platform Management

Notification handler/recipient: Operator

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been deleted on the eUICC identified by its EID.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been deleted. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 140: Handle Profile Deleted Notification Additional Input Data

5.3.12 Auditing eUICC Information

Function name: AuditEIS

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function provider: SM-DP

Description: This function allows the Operator to retrieve the up to date information for the Operator's Profiles. The SM-DP SHALL forward the request to the SM-SR.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC.to be audited See section 5.1.1.1 for type description.	EID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC's lifetime.	OID	1	M
iccid-list	List of "iccid" identifying Profiles to be audited	ICCID	1..N	C

Table 5312-A: AuditEIS Additional Input Data

If no list of ICCIDs is provided, it is implied that all the EIS data for the Profiles owned by the requesting Operator is required.

Additional output data:

Output data name	Description	Type	No.	MOC
Eis	For the relevant eUICC Information Set see section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included as defined in Annex E. Only the data for the requested Profiles are returned within the EIS. The Profiles that do not belong to the requestor are not included in the response. See section 5.4.2 for considerations on data filtering by the SM-SR.	EIS	1	C

Table 5312-B: AuditEIS Additional Output Data

Specific status codes

In addition to the status codes returned by ES3.AuditEIS, this function may return the following status codes:

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the SM-DP

Table 5312-C: AuditEIS Additional Specific Status Codes

5.3.13 Setting Authorisations of M2M -SP to Access Profiles

Function name: SetPLMA

Related Procedures: Set Profile Lifecycle Management Authorisations via SM-DP

Function group: Profile Management

Function Provider: SM-DP

Description:

This function allows the Operator owning Profiles to grant PLMAs to an M2M SP to perform certain operations, or receive certain notifications, related to Profiles, identified by a Profile Type.

The SM-DP receiving this request SHALL forward it to the SM-SR indicated by the Operator, according to procedure “Set Profile Lifecycle Management Authorisations via SM-DP” described in section 3.3.2 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the authorisations have been configured in the SM-SR.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in the table below, indicating that the authorisations have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
plma	The specification of the PLMA, and the criteria on which this PLMA applies. See section 5.1.1.2.14 for type description.	PLMA	1	M
smsr-id	Identification of the SM-SR on which to apply the PLMA.	OID	1	M

Table 5313-A: Set PLMA Additional Input Data

Additional output data:

- None

Specific status codes

In addition to the Status codes returned by ES3.SetPLMA, this function can return the following status codes

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the function provider.

Table 5313-B: Set PLMA Specific Status Codes

5.3.14 Retrieving Authorisations of M2M SP to Access Profiles

Function name: GetPLMA

Related Procedures: Retrieve Profile Lifecycle Management Authorisations by Operator

Function group: Profile Management

Function Provider: SM-DP

Description:

This function allows the Operator owner of Profiles to retrieve a list of PLMAs applicable to a certain Profile, or a certain Profile Type, or for a certain M2M SP.

The same function can also be used by the Operator playing the role of an M2M SP, to retrieve the list of PLMAs granted to this Operator, and applicable to a certain Profile, or a certain Profile Type, owned by another Operator.

The SM-DP receiving this request SHALL forward it to the SM-SR indicated by the Operator, according to procedure “Retrieve Profile Lifecycle Management Authorisations via SM-DP” described in section 3.3.4 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’, and additional output data providing the PLMAs.
- A ‘Function execution status’ with ‘Executed-WIthWarning’, to indicate that the result was truncated, plus additional output data providing part of the list of applicable PLMAs.
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
profileType	Identification of the Profile type for which PLMAs are searched	String	1	C
m2m-sp-id	Identification of the M2M SP for which PLMAs are searched	OID	1	C
iccid	Identification of one specific Profile for which PLMAs are searched	ICCID	1	C
mno-id	Identification of the Operator owning the Profiles to be matched (this input datum SHALL be present only in case the search criterion is a Profile Type). See section 5.1.1.1 for type description.	OID	1	C
smsr-id	Identification of the SM-SR from which to retrieve the PLMAs. This information may change during the eUICC's lifetime.	OID	1	M

Table 5314-A: GetPLMA Additional Input Data

One and only one of the input data profileType, m2m-sp-id and iccid SHALL be present.

Additional output data:

Output data name	Description	Type	No.	MOC
plma	The list of PLMAs that match the search criterion See section 5.1.1.2.14 for type description.	PLMA	N	M

Table 5314-B: GetPLMA Additional Output Data

Specific status codes

In addition to the Status codes returned by ES3.GetPLMA, this function can return the following Status Codes

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the function provider.

Table 5313-C: GetPLMA Specific Status Codes

5.3.15 Notify a Profile Download

Function name: HandleProfileDownloadNotification

Related Procedures: Profile Download

Function group: Profile Management

Notification handler/recipient: Operator (in the role of an M2M SP)

Description: This function SHALL be called to notify an Operator (acting as an M2M SP from the point of view of another Operator) that the Profile identified by its ICCID has been downloaded on the eUICC identified by its EID.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been downloaded. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5315: Handle Profile Downloaded Notification Additional Input Data

5.3.16 Notify the Change of Policy Rules of a Profile

Function name: HandlePolicyRulesUpdatedNotification

Related Procedures: POL2 Update, POL2 Update Via SM-DP

Function group: Profile Management

Notification handler/recipient: Operator (in the role of an M2M SP)

Description: This function SHALL be called to notify an Operator (acting as an M2M SP from the point of view of another Operator) that the Policy Rules have been updated on the Profile identified by its ICCID on the eUICC identified by its EID.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile whose POL2 has been updated. See section 5.1.1.1 for type description.	ICCID	1	M
Pol2	Value of the POL2 after being updated by the Operator owning the Profile See section 5.1.1.1 for type description.	POL2	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5316: Handle Policy Rules Updated Notification Additional Input Data

5.3.17 Notify a PLMA Setting

Function name: HandleSetPLMANotification

Related Procedures: Set Profile Lifecycle Management Authorisation, Set Profile Lifecycle Management Authorisation via SM-DP

Function group: Platform Management

Notification handler/recipient: Operator (acting in the role of an M2M SP)

Description: This function SHALL be called to notify an Operator (acting as an M2M SP from the point of view of another Operator) that a PLMA concerning this M2M SP has been set or updated.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
plma	The specification of the PLMA that now applies on a Profile Type. Information about the Profile Type are contained in the PLMA structure.	PLMA	1	M

	See section 5.1.1.2.14 for type description.			
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5317: Handle PLMA Setting Notification Additional Input Data

5.3.18 Setting Operator Configuration to Receive Notifications

Function name: SetONC

Related Procedures: Set Operator Notifications Configuration via SM-DP

Function group: Profile Management

Function Provider: SM-DP

Description:

This function allows the Operator to configure for which of its own Profiles, associated with a Profile Type, it wants to receive which kind of status change notifications; whatever the origin of the status change is.

The SM-DP receiving this request SHALL forward it to the SM-SR indicated by the Operator, according to procedure “Set Operator Notifications Configuration via SM-DP” described in section 3.21.2 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the notifications configuration has been configured in the SM-SR.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in table 5318-C, indicating that the authorisations have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
onc	The specification of the ONC, and the criterion on which this ONC applies. See section 5.1.1.2.15 for type description.	ONC	1	M
smsr-id	Identification of the SM-SR on which to apply the ONC.	OID	1	M

Table 5318-A: SetONC Additional Input Data

Additional output data:

- None

Specific status codes

In addition to the Status codes returned by ES3.SetONC, this function can return the following Status Codes

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the function provider.

Table 5318-C: SetONC Specific Status Codes

5.3.19 Retrieving Operator Notification Configuration

Function name: GetONC

Related Procedures: Retrieve Operator Notifications Configuration via SM-DP

Function group: Profile Management

Function Provider: SM-DP

Description:

This function allows the Operator to retrieve a list of status change notifications it does not want to receive for its own Profiles, associated with a Profile Type.

The SM-DP receiving this request SHALL forward it to the SM-SR indicated by the Operator, according to procedure “Retrieve Operator Notifications Configuration via SM-DP” described in section 3.21.4 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’, and additional output data providing the configured ONC.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in table 5319-C, indicating that the authorisations have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator, and additional output data providing the configured ONC.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
profileType	Identification of the Profile Type for which the ONC is searched	String	1	C
iccid	Identification of one specific Profile for which the ONC is searched	ICCID	1	C
smsr-id	Identification of the SM-SR from which to retrieve this ONC. This information may change during the eUICC's lifetime.	OID	1	M

Table 5319-A: GetONC Additional Input Data

One and only one of the input data profileType or iccid SHALL be present.

Additional output data:

Output data name	Description	Type	No.	MOC
onc	The ONC including the list of unwanted notifications that match the search criterion See section 5.1.1.2.15 for type description. NOTE: If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the output data of this function will list no notification names, as all notifications will be sent for Profiles assigned with this Profile Type. See also section 3.21.4 and table 511215-A for details.	ONC	N	M

Table 5319-B: GetONC Additional Output Data

Specific status codes

In addition to the list of status codes returned by ES3.GetONC, this function may return the following list of status codes:

Subject code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or cannot be resolved by the function provider.

Table 5319-C: GetONC Specific Status Codes

5.3.20 Setting the Emergency Profile Attribute

Function name: SetEmergencyProfileAttribute

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via M2M SP

Function group: Platform Management

Function Provider: SM-DP

Description:

This function allows the Operator owner of the Profile to request an SM-DP to set the Emergency Profile Attribute on a Profile in a specified eUICC, eUICC being identified by its EID.

The SM-DP receiving this request SHALL process it according to the “Emergency Profile Attribute Management” procedure described in the section 3.25 of this specification (option b: via SM-DP).

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Emergency Profile Attribute has been set on the targeted Profile.

- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC’s lifetime.	OID	1	M
iccid	Identification of the Profile on which to set the Emergency Profile Attribute. See section 5.1.1.1 for type description.	ICCID	1	M

Table 5320-A: Set Emergency Profile Attribute Additional Input Data

Additional output data:

- None

Specific status codes

In addition to the status codes returned by ES3.setEmergencyProfileAttribute, this function may return the following status codes:

Subject Code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the function provider.

Table 5320-C: Set Emergency Profile Attribute Specific Status Codes

5.3.21 Notifying the Emergency Profile Attribute Setting

Function name: HandleEmergencyProfileAttributeSetNotification

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator

Description: This function SHALL be called to notify that the Emergency Profile Attribute has been set on the Profile identified by its ICCID on the eUICC identified by its EID.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has the Emergency Profile Attribute set. See section 5.1.1.1 for type description.	ICCID	1	C
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5321: Handle Emergency Profile Attribute Set Notification Additional Input Data

5.3.22 Notifying the Emergency Profile Attribute Unsetting

Function name: HandleEmergencyProfileAttributeUnsetNotification

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator

Description:

This function SHALL be called to notify that the Emergency Profile Attribute has been unset on the Profile identified by its ICCID, on the eUICC identified by its EID.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
Iccid	Identification of the Profile that has the Emergency Profile Attribute unset.	ICCID	1	M

	See section 5.1.1.1 for type description.			
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5322: Handle Profile Emergency Profile Attribute Unset

5.3.23 Setting the Fall-Back Attribute

Function name: SetFallBackAttribute

Related Procedures: Fall-Back Attribute Management

Function group: Platform Management

Function Provider: SM-DP

Description:

This function allows the Operator owner of the Profile to request an SM-DP to set the Fall-Back Attribute on a Profile in a specified eUICC, eUICC being identified by its EID.

The SM-DP receiving this request SHALL process it according to the “Fall-Back Attribute Management” procedure described in sections 3.28 and 3.29 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Fall-Back Attribute has been set on the targeted Profile.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
smsr-id	Identification of the SM-SR currently in charge of eUICC management. This information may change during the eUICC’s lifetime.	OID	1	M
iccid	Identification of the Profile on which to set the Fall-Back Attribute. See section 5.1.1.1 for type description.	ICCID	1	M

Table 5323-A: Set Fall-Back Attribute Additional Input Data

Additional output data:

- None

Specific status codes

In addition to the status codes returned by ES3.SetFallBackAttribute, this function may return the following status codes:

Subject Code	Subject	Reason code	Reason	Description
8.7	SM-SR	3.9	Unknown	Indicates that the SM-SR, identified by this smsr-id, is unknown to or whose address cannot be resolved by the function provider.

Table 5323-C: Enable Profile Specific Status Codes

5.3.24 Notifying the Fall-Back Attribute is Set

Function name: HandleProfileFallBackAttributeSetNotification

Related Procedures: Fall-Back Attribute Management, Fall-Back Attribute Management via SM-DP, Fall-Back Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator

Description:

This function SHALL be called to notify that the Fall-Back Attribute has been set on the Profile identified by its ICCID, on the eUICC identified by its EID.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile on which the Fall-Back Attribute has been set. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5324: Handle Profile Fall-Back Attribute Set additional input data

5.3.25 Notifying the Fall-Back Attribute is Unset

Function name: HandleProfileFallBackAttributeUnsetNotification

Related Procedures: Fall-Back Attribute Management, Fall-Back Attribute Management via SM-DP, Fall-Back Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator

Description:

This function SHALL be called to notify that the Fall-Back Attribute has been unset on the Profile identified by its ICCID, on the eUICC identified by its EID.

This notification also conveys the date and time specifying when the operation has been done.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
Iccid	Identification of the Profile on which the Fall-Back Attribute has been unset. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5325: Handle Profile Fall-Back Attribute Unset Additional Input Data

5.4 ES3 (SM-DP – SM-SR) Interface Description

This section describes operations and notifications on the interfaces between the SM-DP and the SM-SR. The SM-DP usually acts on behaf of an Operator. When that is the case, the SM-DP SHALL indicate, in each request sent to the SM-SR, the mno-id identifying the requesting Operator. The way the mno-id is provided by the SM-DP is specified in Annex B.

Similarly, the SM-SR SHALL indicate, in each notification sent to the SM-DP, the mno-id identifying the targeted Operator.

NOTE: The execution of several ES3 functions by the SM-SR is conditioned by the verification that the Operator requesting to perform an operation on a Profile via its SM-DP, or the Operator to be notified via its SM-DP:

- is the owner of the targeted Profile

or

- is authorised for this operation or notification by the owner of the targeted Profile.

The specification of this verification by the SM-SR is described in sections 5.7.1.2 and 5.7.1.3, based on the identities supplied as described above.

5.4.1 Getting eUICC Information

Function name: GetEIS

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the SM-DP, requesting on behalf of an Operator, retrieving the eUICC Information Set (EIS) of a particular eUICC from the SM-SR information database based on the EID.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the download function has been successfully executed on the SM-SR as requested by the function caller.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M

Table 141: Get EIS Additional Input Data

The SM-SR SHALL filter the list of Profiles returned in the EIS, considering the authorisation granted by the Profile owners; for each Profile, this includes:

- If the SM-DP indicates that it is requesting this operation on behalf of the owner of the Profile, the SM-SR SHALL include this Profile in the returned EIS.
- If the SM-DP indicates that it is requesting this operation on behalf of an Operator that is not the owner of the targeted Profile, the SM-SR SHALL include the Profile in the returned EIS only if the Operator owning the Profile has granted a PLMA allowing the operation “GetEIS” to the Operator requesting the operation.

Additional output data:

Output data name	Description	Type	No.	MOC
eis	The relevant eUICC Information Set of the eUICC. See section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	C

Table 142: Get EIS Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	1.1	Unknown	Indicates that the EID is unknown to the function provider
8.6	EIS	1.2	Not Allowed (Authorisation)	Function requester is not allowed to manage this EIS, identified by this EID.

Table 143: Get EIS Specific Status Codes

5.4.2 Auditing eUICC Information

Function name: AuditEIS

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function provider: SM-SR

Description: This function allows the SM-DP, requesting on behalf of an Operator, to retrieve up to date EIS information. The SM-SR SHALL use the relevant functions of the ES5 interface to retrieve the information from the eUICC. At the end of the successful execution of this function, the SM-SR SHALL update its EIS database upon the basis of this information.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

If the SM-DP provides a list of ICCID of Profiles to audit, the SM-SR SHALL verify for each profile that the Operator, on behalf of which the SM-DP requests this operation,

- is either the owner of the targeted Profile
  or
- is authorised by the Operator owning the targeted Profile(s)

to perform the operation “AuditEIS” on a Profile that matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria).

This SHALL also be applied if the list of ICCIDs identifies

- Profiles that are owned by this Operator
  and / or

- Profiles that are owned by other Operators.

The SM-SR MAY provide additional verifications.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the function has been successfully executed on the SM-SR as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC to be audited. See section 5.1.1.1 for type description.	EID	1	M
iccid-list	List of “iccid” identifying Profiles to be audited	ICCID	1..N	C

Table 144: Audit EIS Additional Input Data

If no list of ICCIDs is provided, it is implied that all authorised Profiles in the EIS are requested.

The SM-SR SHALL filter the list of Profiles returned in the EIS, considering the authorisation granted by the Profile owners; for each Profile, this includes:

- If the SM-DP indicates that it is requesting this operation on behalf of the owner of the Profile, the SM-SR SHALL include this Profile in the returned EIS.
- If the SM-DP indicates that it is requesting this operation on behalf of an Operator that is not the owner of the targeted Profile, the SM-SR SHALL include the Profile in the returned EIS only if the Operator owning the Profile has granted a PLMA allowing the operation “AuditEIS” to the Operator requesting the operation.

Additional output data:

Output data name	Description	Type	No.	MOC
eis	The relevant eUICC Information Set of the eUICC See section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	C

Table 145: Audit EIS Additional Output Data

Specific status codes

Subject Code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider

8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by one of the ICCIDs in the list is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2	Profile	1.2	Not Allowed (Authorisation)	One or more Profiles identified by ICCIDs in the list do not belong to function requester
8.6	EIS	1.2	Not Allowed (Authorisation)	Function requester is not allowed to manage this EIS, identified by this EID.
1.6	Function	5.4	Delivered With No Response	The function execution request has been delivered to remote entity but no response is received.

Table 146: Audit EIS Specific Status Codes

5.4.3 Create a New ISD-P in an eUICC

Function name: CreateISDP

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the SM-DP to request the creation of an ISD-P to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

Function flow

Upon reception of the function request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC
- The Profile identified by its ICCID is not already present within its EIS database (meaning allocated to another ISD-P)
- The requested amount of memory can be satisfied

SM-SR MAY provide additional verifications.

In case one of these conditions is not satisfied, the SM-SR SHALL refuse the function request and return a ‘Function execution status’ indicating ‘Failed’ with the relevant status code (see table below).

The SM-SR receiving this request SHALL process it according to the “Profile Download and Installation” procedure described in the section 3.1 of this specification.

When the SM-SR ends successfully this function it SHALL update the eUICC EIS by adding a new Profile entry in the EIS with following values:

- The iccid value received as parameter
- The isd-p-aid value as allocated by the SM-SR
- The mno-id value received as parameter
- The state value as ‘Created’
- The smdp-id retrieved from the authentication context of the caller

- The Cumulative Granted Non Volatile Memory value received as parameter

NOTE: The initial Subscription Address and the initial POL2 can be set after the Profile is completely downloaded using the "**ES3.ProfileDownloadCompleted**" function.

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the ISD-P has been successfully created on the eUICC as requested by the function caller.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
Iccid	Identification of the Profile to download and install. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	The identification of the Operator owning the Profile	OID	1	M
RequiredMemory	Indicates the Cumulative Granted Non Volatile Memoryallocated to the ISD-P to contain the Profile. The value is expected in Bytes.	Integer	1	M
moreToDo	Indicates to the function provider that the function caller has something else to do with the targeted eUICC right after this function execution. This indication MAY be used by the function provider to decide if it has to keep the remote communication channel with the eUICC open (this may be relevant or not, depending on the remote communication channel. This is the case for instance for Remote Administration over HTTPS as defined in section 2.4.4. The only purpose is to optimise resource management and save execution time of the overall procedure. It is up to the function provider to support this feature or not. This input data is optional; if missing the function provider SHALL consider that the function caller has nothing else to do.	Boolean	1	O

Table 147: Create ISD-P Additional Input Data

If the "RequiredMemory" parameter of this ES3.CreateISDP function call is equal to '0', the "Cumulative Granted Non Volatile Memory" parameter SHALL NOT be used in the INSTALL command of the ES5.CreateISDP function.

Additional output data:

Output data name	Description	Type	No.	MOC
isd-p-aid	The AID, allocated by the SM-SR, of the ISD-P containing the Profile. The Tar value is included in the AID. See Annex H "Coding of the PIX for 'Embedded UICC Remote Provisioning and Management' (Normative)".	AID	1	C (see note)

euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES8 depending of the requested function.	Hexadecimal string	1	O

Table 148: Create ISD-P Additional Output Data

NOTE In case of error or expiration of the function execution, the output data isd-p-aid SHOULD be absent.

This output data isd-p-aid was mandatory in version 3.2 and earlier of this specification. For backward-compatibility with such versions, the SM-SR MAY send this output data anyway, and the SM-DP SHOULD be ready to receive this data, even in case of error and expiration. In such a case, the value of this data is irrelevant, so the SM-SR SHOULD return a value that is clearly not a valid AID (ex: '0000000000') and the SM-DP SHOULD ignore the data, whatever the value is.

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider
8.2.1	Profile ICCID	3.3	Already in use	Indicates that the ICCID is already allocated to another Profile managed by the function provider.
8.4	ISD-R	4.2	Execution error	Error during execution of the creation command on the eUICC. In that case, the output data "euiccResponseData contains the exact response coming from the eUICC.
8.1	eUICC	4.8	Insufficient memory	The eUICC has not enough free memory to execute the creation of the new ISD-P with this required amount of memory.

Table 149: Create ISD-P Specific Status Codes

5.4.4 Download a New Profile

Function name: SendData

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the SM-DP to send securely commands defined in ES8 interface (i.e.: Profile download or establish a key set) to an ISD-P or the ISD-R through the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

Function flow

Upon reception of the function request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC.
- The targeted ISD-P (designated in the sd-aid or in the commands) is created on the eUICC and is managed by the calling SM-DP.
- If the SM-DP requests to send the commands to the ISD-R: the commands are allowed to be executed by ISD-R, including ISD-P key establishment as described in section 4.1.3.1.

NOTE1: this verification implies the parsing and analysing of the commands.

NOTE2: this verification allows to prevent the SM-DP to perform arbitrary operations in the ISD-R

The SM-SR MAY provide additional verifications.

In case one of these conditions is not satisfied, the SM-SR SHALL refuse the function request and return a ‘Function execution status’ indicating ‘Failed’ with the relevant status code (see table below).

This function allows sending commands defined in the ES8 interface in several steps. This may be necessary in case of the data is too big compared to eUICC capabilities. It is up to the function caller to determine if it has to handle this situation based on the eUICC capabilities described in EIS.

The SM-SR is free to select the most relevant OTA protocol to communicate up to the eUICC. As a consequence, the data format provided by the function caller SHALL NOT depend of the selected OTA protocol capabilities (for example SM-DP can consider there is no limit on data length). The data provided by the SM-DP SHALL be a list of C-APDU as defined in ETSI TS 102 226 [5] section 5.2.1, or TLV commands as defined in this document, section 4.1.3.3. The SM-SR has the responsibility to build the final Command script, depending on eUICC capabilities and selected protocol:

- by adding the Command scripting template for definite or indefinite length,
- and, if necessary, by segmenting the provided command script into several pieces
- and, if necessary, by adding the relevant Script Chaining TLVs.

Annex K provides a description of heuristics that MAY be used to implement Script Chaining.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the function has been successfully executed by the function provider as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
sd-aid	Identification of the SD which SHALL process the commands contained in the data argument. sd-aid could identify either the ISD-P or the ISD-R.	AID	1	M
data	The data to send into the targeted ISD-P and eUICC. The data SHALL contain a list a C-APDU as defined in ETSI TS 102 226 [5], section 5.2.1 or TLV commands as defined in this document, section 4.1.3.3. The C-APDU can contain any of the commands defined in ES8 interface. The commands SHALL be secured according to section 2.5.	Hexadecimal string	1	M
moreToDo	See section 5.4.3 for description of this input data	Boolean	1	O

Table 150: Send Data Additional Input Data

Due to an ambiguity in former version of the specifications, an SM-DP following a former version of this document may send all commands of a Profile download procedure (including ISD-P key establishment commands) pointing the ISD-P as the targeted security domain (argument sd-aid). For backward-compatibility, the SM-SR SHOULD detect such cases, and support them by appropriately sending the commands to the ISD-R or the ISD-P.

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the Random Challenge (RC) in case of the key establishment procedure or the detailed error returned by the eUICC in case of one command execution failed on eUICC. The response data is defined in ES8 depending of the requested function.	Hexadecimal string	1	C

Table 151: Send Data Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider
8.3.1	ISD-P-AID	3.9	Unknown	Indicates that the ISD-P identified by this SD-AID is unknown to the function provider.
8.3	ISD-P	4.2	Execution error	Error during execution of one command, when error occurs at ISD-P level.
8.3.1	ISD-P-AID	1.2	Not allowed (Authorisation)	Indicates that the function caller is not allowed to execute commands in the targeted ISD-P.
8.4	ISD-R	1.2	Not allowed (Authorisation)	Indicates that the function caller is not allowed to execute the requested commands in the ISD-R.

Table 152: Send Data Specific Status Codes

5.4.5 Indicating the Profile Download is Completed

Function name: ProfileDownloadCompleted

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the SM-DP to indicate to the SM-SR that the Profile download (identified by its ICCID) has been completed on the eUICC; eUICC being identified by its EID.

This function allows optionally to set a first Subscription Address, typically the MSISDN, and saves it in the EIS, and optionally a first POL2 associated to the newly download Profile. In case no POL2 is provided at that time, it means that the Profile won't be protected by any POL2 at SM-SR side. But the POL2 MAY be set or updated at any time later using the "UpdatePolicyRules" function defined in section 5.4.6.

The Subscription Address is the identifier, such as MSISDN and/or IMSI, through which the eUICC is accessible from the SM-SR via the mobile network when the Profile is in Enabled state. The Subscription Address MAY be set or updated at any time later using the "**UpdateSubscriptionAddress**" function defined in section 5.4.7.

On reception of this function request the SM-SR SHALL immediately update the EIS to set the identified Profile:

- (Optional) the provided ProfileType as defined in section 5.1.1.2.4
- (Conditional) the new Subscription Address. If the Profile is to be enabled after it is loaded then the Subscription Address becomes mandatory.
- (Optional) the provided POL2

At the end of this function call, the Profile state is "Disabled". The SM-DP may call the function "**ES3.EnableProfile**" (see section 5.4.8) to enable the Profile if required by the Operator.

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the function has been correctly executed.
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC.	EID	1	M

	See section 5.1.1.1 for type description.			
iccid	Identification of the Profile See section 5.1.1.1 for type description.	ICCID	1	M
ProfileType	Indicates, through an SM-DP reference, the type of Profile generated by the SM-DP (for example 3G_16K)	String	1	O
subscriptionAddress	The Subscription Address related to the identified Profile	SUBSCRIPTION-ADDRESS	1	O
pol2	The POL2 to associate with the identified Profile.	POL2	1	O

Table 153: Profile Download Completed Additional Input Data

Additional output data:

No additional data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.3	POL2	2.1	Invalid	Indicates that the POL2 is invalid

Table 154: Profile Download Completed Specific Status Codes

5.4.6 Updating the Policy Rules of a Profile

Function name: UpdatePolicyRules

Related Procedures: -

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the SM-DP authorised by the Operator to update POL2 of a Profile, identified by its ICCID, and installed on an eUICC identified by its EID.

The function can update a Profile in “Disabled” or “Enabled” state and SHALL return an error for any other Profile state.

The function completely replaces the definition of existing POL2. It means that it is the responsibility of the caller to provide the complete definition of POL2.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the update Policy Rules function has been successfully executed by the SM-SR as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
  A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile See section 5.1.1.1 for type description.	ICCID	1	M
pol2	List of POL2 rules associated with the identified Profile. See section 5.1.1.1 for type description.	POL2	1	M

Table 155: Update Policy Rules Additional Input Data

Table 156: Void

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.3	POL2	2.1	Invalid	Indicates that the POL2 is invalid.

Table 157: Update Policy Rules Specific Status Codes

5.4.7 Updating eUICC Information

Function name: UpdateSubscriptionAddress

Related Procedures: Profile Download and Installation, Profile Enabling, Profile Enabling via SM-DP

Function group: Profile Management

Function Provider: SM-SR

Description: This function enables the caller to update the Subscription Address for a Profile in the eUICC Information Set (EIS) of a particular eUICC identified by the EID and ICCID. The Subscription Address is the identifier, such as MSISDN and/or IMSI, through which the eUICC is accessible from the SM-SR via the mobile network when the Profile is in Enabled state.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

The SM-SR SHALL verify that the request is:

- Either sent on behalf of an Operator owning the targeted Profile
  or
- Sent on behalf of an Operator that is not the owner of the targeted Profile, but the Operator owning the targeted Profile has granted a PLMA allowing the operation "UpdateSubscriptionAddress" to the Operator requesting the operation.

The SM-SR MAY provide additional verifications.

The function replaces the content of the Subscription Address. For consistency within the system, it is the responsibility of the caller to ensure that all data is provided. This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the UpdateSubscriptionAddress function has been successfully executed by the SM-SR as requested by the function caller.
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the target Profile. See section 5.1.1.1 for type description.	ICCID	1	M
newSubscriptionAddress	The new Subscription Address	Subscription Address	1	M

Table 158: Update Subscription Address Additional Input Data

Additional output data:

This function has no additional output data:

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	1.1	Unknown	Indicates that the EIS identified by this EID, is unknown to the function provider
8.2.1	ICCID	1.1	Unknown	Indicates that the Profile identified by the ICCID, is unknown to the function provider
8.2.6	Subscription Address	1.2	Not Allowed (Authorisation)	Function requester is not allowed to manage the Subscription Address.

Table 159: Update Subscription Address Specific Status Codes

5.4.8 Profile Enabling

Function name: EnableProfile

Related Procedures: Profile Enabling via SM-DP

Function group: Platform Management

Function Provider: SM-SR

Description: This function allows the SM-DP to request a Profile Enabling to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

The SM-SR SHALL verify that the request is

- Either sent on behalf of an Operator owning the targeted Profile
  or
- Sent on behalf of an Operator that is not the owner of the targeted Profile, but the Operator owning the targeted Profile has granted a PLMA allowing the operation “EnableProfile” to the Operator requesting the operation.

The SM-SR MAY provide additional verifications.

The SM-SR receiving this request SHALL process it according to “Profile Enabling via SM-DP” procedure described in the section 3.3 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Profile has been enabled on the eUICC.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to enable. See section 5.1.1.1 for type description.	ICCID	1	M

Table 160: Enable Profile Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES8 depending of the requested function.	Hexadecimal String	1	O

Table 161: Enable Profile Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2	Profile	5.1	Inaccessible	Indicates that the Profile change procedure couldn't complete after enabling the target Profile, and the Profile change was rolled-back on the eUICC,
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.1	Profile ICCID	3.5	Invalid Transition	Indicates that the Profile was already Enabled
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.
8.2.2	POL1	3.8	Refused	The POL1 of the impacted Profiles doesn't allow this operation.
8.2.3	POL2	3.8	Refused	The POL2 of the impacted Profiles doesn't allow this operation.
8.2.7	PLMA	3.8	Refused	No PLMA allows the SM-DP, or the Operator on behalf of which the SM-DP sent the request, to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the enabling command on the eUICC. In that case, the output data "euiccResponseData" contains the exact response coming from the eUICC.

Table 162: Enable Profile Specific Status Codes

5.4.9 Profile Disabling

Function name: DisableProfile

Related Procedures: Profile Disabling via SM-DP

Function group: Platform Management

Function Provider: SM-SR

Description: This function allows the SM-DP authorised by the Operator to request a Profile Disabling to the SM-SR in charge of the management of the targeted eUICC, eUICC being identified by its EID.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

The SM-SR receiving this request SHALL process it according to Profile Disabling procedure described in section 3.5 of this specification.

The SM-SR SHALL verify that the request is:

- Either sent on behalf of an Operator owning the targeted Profile
  or
- Sent on behalf of an Operator that is not the owner of the targeted Profile, but the Operator owning the targeted Profile has granted a PLMA allowing the operation "DisableProfile" to the Operator requesting the operation.

The SM-SR MAY provide additional verifications.

This function may return:

- A 'Function execution status' with 'Executed-Success' indicating that the Profile has been disabled on the eUICC.
- A 'Function execution status' with 'Executed-WithWarning', with a status code as defined below, indicating that the Profile has been disabled on the eUICC, and deleted after application of a POL1 or POL2 rule.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to disable. See section 5.1.1.1 for type description.	ICCID	1	M

Table 163: Disable Profile Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case of the function execution failed at the eUICC.	Hexadecimal String	1	O

Table 164: Disable Profile Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1	eUICC	3.8	Refused	Indicates that the target Profile can't be disabled. (for example the Profile is the only Profile in the eUICC)
8.2	Profile	5.1	Inaccessible	Indicates that the Profile change procedure couldn't complete after enabling the Profile with the Fall-Back Attribute set, and the Profile change was rolled-back on the eUICC,
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the SM-SR.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to SM-SR.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the SM-SR but installed on another eUICC than the one identified by the function caller.
8.2.1	Profile ICCID	3.5	Invalid Transition	Indicates that the Profile was already Disabled
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.
8.2.2	POL1	3.6	Related Object Exists	The POL1 of the target Profile has triggered its deletion after disabling it This status code SHALL only be sent along Status ="Executed-WithWarning"
8.2.2	POL1	3.8	Refused	The POL1 of the target Profile doesn't allow this operation.
8.2.3	POL2	3.6	Related Object Exists	The POL2 of the target Profile has triggered its deletion after disabling it This status code SHALL only be sent along Status ="Executed-WithWarning"
8.2.3	POL2	3.8	Refused	The POL2 of the target Profile doesn't allow this operation.
8.2.7	PLMA	3.8	Refused	No PLMA allows the SM-DP, or the Operator on behalf of which the SM-DP sent the request, to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the disabling command on the eUICC. In that case, the output data "euiccResponseData contains the exact response coming from the eUICC.

Table 165: Disable Profile Specific Status Codes

5.4.10 Delete an ISD-P

Function name: DeleteISDP

Related Procedures: Profile and ISD-P Deletion via SM-DP

Function group: Platform Management

Function Provider: SM-SR

Description: This function allows the SM-DP to request deletion of the target ISD-P with the Profile to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID. The target Profile can only be a Profile that can be managed by the SM-DP authorised by the Operator.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

On reception of the function request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC
- The ISD-P identified by its AID exists on the targeted eUICC
- The SM-DP is authorised to delete the target Profile by the Operator owning the target Profile.
- The POL2 of the target Profile allows the deletion
- The target Profile is not the Profile having the Fall-Back Attribute set

The SM-SR SHALL verify that the request is:

- Either sent on behalf of an Operator owning the targeted Profile
  or
- Sent on behalf of an Operator that is not the owner of the targeted Profile, but the Operator owning the targeted Profile has granted a PLMA allowing the operation “DeleteProfile” to the Operator requesting the operation.

The SM-SR MAY provide additional verifications.

In case one of these conditions is not satisfied, the SM-SR SHALL refuse the function request and return a ‘Function execution status’ indicating ‘Failed’ with the relevant status code (see table below).

The SM-SR receiving this request SHALL process it according to “Profile and ISD-P deletion via SM-DP” procedure described in section 3.7 of this specification.

In case the target Profile is “Enabled”, the SM-SR SHALL automatically disable it before executing the deletion. This function is described in section 4.1.1.3 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Profile has been deleted on the eUICC.
- A 'Function execution status' with 'Executed- WithWarning' indicating that the Profile has been deleted on the eUICC, with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to delete.	ICCID	1	M

	See section 5.1.1.1 for type description.			

Table 166: Delete ISD-P Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES8 depending of the requested function.	Byte[]	1	O

Table 167: Delete ISD-P Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.
8.2.1	Profile ICCID	3.8	Refused	Indicates that the Profile cannot be deleted because it is the last Profile of the eUICC or the Fall-Back Profile.
8.2.2	POL1	3.8	Refused	The POL1 of the Profile doesn't allow this operation.
8.2.3	POL2	3.8	Refused	The POL2 of the Profile doesn't allow this operation.
8.2.7	PLMA	3.8	Refused	No PLMA allows the SM-DP, or the Operator on behalf of which the SM-DP sent the request, to execute this operation.
8.3	ISD-P	4.6	Not Present / Missing	The target ISD-P was not found on this eUICC (in this case the Function Execution Status SHALL be 'Executed- WithWarning'
8.4	ISD-R	4.2	Execution error	Error during execution of the deletion (or disabling) command on the eUICC. In that case, the output data "euiccResponseData contains the exact response coming from the eUICC.

Table 168: Delete ISD-P Specific Status Codes

NOTE: in case Profile Disabling is performed automatically before deletion, this function MAY raises any status code coming from the execution of the Profile disabling function defined in section5.4.9.

5.4.11 Update Connectivity Parameters

Function name: UpdateConnectivityParameters

Related Procedures: -

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the Operator, or the SM-DP authorised by the Operator to update the Connectivity Parameters store in the ISD-P, identified by its ICCID, and installed on an eUICC identified by its EID.

The function can update a Profile in “Disabled” or “Enabled” state and SHALL return an error for any other Profile state.

The function updates the definition of existing Connectivity Parameters.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the update of the Connectivity Parameters function has been successfully executed by the SM-SR as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile See section 5.1.1.1 for type description.	ICCID	1	M
connectivityParameters	A command string secured with SCP03 as described in section 4.1.3.2, and including ES8 command “Connectivity Parameters Update” specified in section 4.1.3.4, containing the connectivityParameters to associate with the identified Profile.	Hexadecimal String	1	M

Table 169: Update Connectivity Parameters Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case of update of the Connectivity Parameters in the ISD-P on the targeted eUICC.	Hexadecimal String	1	O

Table 170: Update Connectivity Parameters Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.

8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.3	ISD-P	4.2	Execution error	Error during execution of Connectivity Parameters update. In that case, the output data “euiccResponseData” contains the exact response coming from the eUICC.

Table 171: Update Connectivity Parameters Specific Status Codes

5.4.12 Notify a Profile is Disabled

Function name: HandleProfileDisabledNotification

Related Procedures: Profile Download and Installation, Profile Enabling, Profile Enabling via SM-DP, Fall-Back Activation Procedure, Profile Enabling via M2MSP

Function group: Platform Management

Notification handler/recipient: SM-DP

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been disabled on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all SM-DP servers that match one or the other of the following conditions:

- The SM-DP can relay the notification to the Operator that owns the Profile, and the Operator has not opted to not receive such notifications (see section 3.21).
- The SM-DP can relay the notification to another Operator, and the Operator owner of the Profile has granted the other Operator with a PLMA authorising this Operation “HandleProfileDisabledNotification”.

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has done.

In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
Iccid	Identification of the Profile that has been disabled. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	Identification of the Operator owner of the Profile that has been disabled.	OID	1	M

	See section 5.1.1.1 for type description.			
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 172: Handle Profile Disabled Notification Additional Input Data

5.4.13 Notify a Profile Enabling

Function name: HandleProfileEnabledNotification

Related Procedures: Profile Disabling, Profile Disabling via SM-DP, Profile Enabling via M2M SP, Profile Disabling via M2M SP, Fall-Back Activation Procedure

Function group: Platform Management

Notification handler/recipient: SM-DP

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been enabled on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all SM-DP servers that match one or the other of the following conditions:

- The SM-DP can relay the notification to the Operator that owns the Profile, and the Operator has not opted to not receive such notifications (see section 3.21)
- The SM-DP can relay the notification to another Operator, and the Operator owner of the Profile has granted the other Operator with a PLMA authorising this Operation “HandleProfileEnabledNotification”.

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

What is performed by the Operator receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been disabled. See section 5.1.1.1 for type description.	ICCID	1	M

mno-id	Identification of the Operator owner of the Profile that has been enabled. See section 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 173: Handle Profile Enabled Notification Additional Input Data

5.4.14 Notify an SM-SR Change

Function name: HandleSMSRChangeNotification

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider: SM-DP

Description: This function SHALL be called for notifying each SM-DP authorised by the Operator owning a Profile hosted in the eUICC, identified by its EID, that the SM-SR has changed. The notification is sent by the new SM-SR to the SM-DP, which SHALL route this notification to the Operator.

This notification also conveys the date and time specifying when the operation has been done.

This notification is not related to a particular Profile. It is up to the notification recipient to perform any action related to each Profile that is deployed on this eUICC

Additional input data:

Input data name	Description	Type	No.	MOC
eis	The relevant part of the eUICC Information Set linked with the Operator owning the Profile hosted in the eUICC. See section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	M
mno-id	Identification of the Operator concerned by the SM-SR change. See 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 174: Handle SM-SR Change Notification Additional Input Data

Additional output data:

No output data is expected in response to this notification.

5.4.15 Notify a Profile Deletion

Function name: HandleProfileDeletedNotification

Related Procedures: Profile Enabling, Profile Enabling via SM-DP, Profile Enabling via M2M SP, Profile Disabling via M2M SP, profile and ISD-P Deletion via M2M SP

Function group: Platform Management

Notification handler/recipient: SM-DP

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been deleted on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all SM-DP servers that match one or the other of the following conditions:

- The SM-DP can relay the notification to the Operator that owns the Profile, and the Operator has not opted to not receive such notifications (see section 3.21)
- The SM-DP can relay the notification to another Operator, and the Operator owner of the Profile has granted the other Operator with a PLMA authorising this Operation “HandleProfileDeletedNotification”.

ICCID may be not enough to identify right address of recipient; SM-SR should map it internally to SM-DP notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case of multiply handlers are served, SM-SR SHOULD ensure ‘completionTimestamp’ to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been deleted. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	Identification of the Operator owner of the Profile that has been deleted. See section 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 175: Handle Profile Deleted Notification Additional Input Data

5.4.16 Setting Authorisations of M2M -SP to Access Profiles

Function name: SetPLMA

Related Procedures: Set Profile Lifecycle Management Authorisation via SM-DP

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator owning Profiles to grant a PLMA to an M2M SP to perform certain operations, or receive certain notifications, related to a set of Profiles, identified by a Profile Type.

The SM-SR receiving this request SHALL verify that the mno-id in the PLMA matches the mno-id of the Operator on behalf of which the SM-DP declares to send this request.

If the request is acceptable, the SM-SR SHALL record the PLMA. The new PLMA overwrites the previous PLMA that might have been granted with the same identifiers.

From this point on, any request from the M2M SP on a Profile matching these identifiers, or any notification to the M2M SP related to a Profile matching these identifiers, SHALL be allowed or not based on the new PLMA, as described in sections 5.7.1.1, 5.7.1.2, and 5.7.1.3.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the authorisations have been configured in the SM-SR.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in the table here after, indicating that the authorisations have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
plma	The specification of the PLMA, and the criteria on which this PLMA applies. See section 5.1.1.2.14 for type description.	PLMA	1	M

Table 5416-A: SetPLMA Additional Input Data

Additional output data:

- None

Specific status codes

Subject code	Subject	Reason code	Reason	Description

8.2.5	Profile Type	4.9	Unassigned	Indicates that the Profile Type in the PLMA doesn't match the Profile Type of any Profile owned by the Operator identified by its mno-id. The SM-SR MAY support this Status Code. If it does support it, the SM-SR SHALL record the PLMA anyway, and the Execution Status SHALL be Executed-WithWarning
8.2.7	PLMA	3.6	Related Objects Exists	Indicates that the new PLMA has overwritten a former PLMA on the same identifiers. In this case the Execution Status SHALL be Executed-WithWarning
8.2	Profile	1.2	Not Allowed (Authorisation)	Indicates that the requesting SM-DP is not allowed to configure PLMAs for the specified Operator
8.9	M2M SP	1.1	Unknown	Indicates that the M2M SP to grant authorisations to is unknown to or not connected to this SM-SR
8.10	Operator	1.1	Unknown	Indicates that the Operator, addressed by the mno-id in the PLMA is unknown.

Table 5416-B: SetPLMA Specific Status Codes

5.4.17 Retrieving Authorisations of M2M SP to Access Profiles

Function name: GetPLMA

Related Procedures: Retrieve Profile Lifecycle Management Authorisation by Operator

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the SM-DP to retrieve, on behalf of an Operator owning Profiles, a list of PLMAs applicable to a certain Profile, or a certain Profile Type, or for a certain M2M SP.

The same function can also be used on behalf of an Operator playing the role of an M2M SP, to retrieve the list of PLMAs granted to this Operator, and applicable to a certain Profile, or a certain Profile Type, owned by another Operator.

The SM-SR SHALL verify that the request is

- Either sent on behalf of an Operator owning the targeted Profile
  or
- Sent on behalf of an Operator that is not the owner of the targeted Profile, but the Operator owning the targeted Profile has granted a PLMA allowing at least one operation for the target Profile or Profile Type to the Operator requesting the operation.

If this verification fails, the SM-SR SHALL terminate the request and return a response with the 'Function execution status' indicating 'Failed', and no PLMA.

Otherwise, the SM-SR SHALL return the complete list of all PLMAs applicable to the specified search criterion; if the search criterion is on a specific Profile or Profile Type, this includes even PLMAs that are granted to an M2M SP that is not the Operator on behalf of which the SM-DP sent this request.

In case the list of PLMAs is very long, the SM-SR MAY truncate the result. The caller can then issue another call to getPLMA with more restrictive criteria.

NOTE The order of the PLMAs returned in the truncated list is implementation-dependent.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’, and additional output data providing the PLMAs.
- A ‘Function execution status’ with ‘Executed-WIthWarning’, to indicate that the result was truncated, plus additional output data providing part of the list of applicable PLMAs.
- A ‘Function execution status’ indicating ‘Failed’ if the requester was not allowed to request this information.

Additional input data:

Input data name	Description	Type	No.	MOC
profileType	Identification of the Profile type for which PLMAs are searched	String	1	C
m2m-sp-id	Identification of the M2M SP for which PLMAs are searched	OID	1	C
iccid	Identification of one specific Profile	ICCID	1	C
mno-id	Identification of the Operator owning the Profiles to be matched (this input datum SHALL be present only in case the search criterion is a Profile Type). See section 5.1.1.1 for type description.	OID	1	C

Table 5417-A: GetPLMA Additional Input Data

One and only one of the input data profileType, m2m-sp-id and iccid SHALL be present.

Additional output data:

Output data name	Description	Type	No.	MOC
plma	The list of PLMAs that match the search criteria See section 5.1.1.2.14 for type description.	PLMA	N	M

Table 5417-B: GetPLMA Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
1.1	Function requester	1.2	Not Allowed (Authorisation)	Indicates that the Operator on behalf of which the SM-DP called the function is not the owner of the specified Profile, or doesn't have a PLMA granted that applies to the targeted Profile or Profile type (including, if the targeted Profile or Profile type is unknown to this SM-SR)
8.2	Profile	1.2	Not Allowed (Authorisation)	Indicates that the requesting SM-DP is not allowed to configure PLMAs for the specified Operator
8.9	M2M SP	1.1	Unknown	Indicates that the M2M SP is unknown to or not connected to this SM-SR
8.10	Operator	1.1	Unknown	Indicates that the Operator, addressed by the mno-id in the PLMA is unknown.

Table 5417-C: GetPLMA Specific Status Codes

5.4.18 Notify a Profile Download

Function name: HandleProfileDownloadNotification

Related Procedures: Profile Download

Function group: Profile Management

Notification handler/recipient: SM-DP (when the corresponding Operator is in the role of an M2M SP)

Description: This function SHALL be called to notify an Operator (acting as an M2M SP from the point of view of another Operator) that the Profile identified by its ICCID has been downloaded on the eUICC identified by its EID.

The SM-SR SHALL inspect the PLMAs that apply to this Profile, and only send this notification to an SM-DP known to be serving an Operator that has been granted a PLMA by the Operator owner of the Profile for the authorised operation "HandleProfileDownloadedNotification".

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure 'completionTimestamp' to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been downloaded. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	Identification of the Operator owner of the Profile that has been downloaded. See section 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed.	DATETIME	1	M

	See section 5.1.1.1 for type description.			

Table 5418: Handle Profile Downloaded Notification Additional Input Data

5.4.19 Notify the Change of Policy Rules of a Profile

Function name: HandlePolicyRulesUpdatedNotification

Related Procedures: POL2 Update Via SM-DP

Function group: Platform Management

Notification handler/recipient: SM-DP DP (when the corresponding Operator is in the role of an M2M SP)

Description: This function SHALL be called to notify an Operator (acting as an M2M SP from the point of view of another Operator) that the Policy Rules have been updated on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL inspect the PLMAs that apply to this Profile, and only send this notification to an SM-DP known to be serving an Operator that has been granted a PLMA by the Operator owner of the Profile for the authorised operation “HandlePolicyRuleUpdatedNotification”.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure ‘completionTimestamp’ to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile whose POL2 has been updated. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	Identification of the Operator owner of the Profile whose POL2 has been updated. See section 5.1.1.1 for type description.	OID	1	M
Pol2	Value of the POL2 after being updated by the Operator owning the Profile See section 5.1.1.1 for type description.	POL2	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5419: Handle Policy Rules Updated Notification Additional Input Data

5.4.20 Notify a PLMA Setting

Function name: HandleSetPLMANotification

Related Procedures: Set Profile Lifecycle Management Authorisations, Set Profile Lifecycle Management Authorisation via SM-DP

Function group: Platform Management

Notification handler/recipient: SM-DP DP (when the corresponding Operator is in the role of an M2M SP)

Description: This function SHALL be called to notify an Operator (acting as an M2M SP) that a PLMA, granted by another Operator to it, has been set or updated.

This notification also conveys the date and time specifying when the operation has been done. In case of multiply handlers are served the SM-SR SHOULD ensure 'completionTimestamp' to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
plma	The specification of the PLMA that now applies on a subset of Profiles. Information about the subset are contained in the PLMA structure. See section 5.1.1.2.14 for type description.	PLMA	1	M
mno-id	Identification of the Operator owner of the Profile Type related to PLMA See section 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5420: Handle PLMA Setting Notification Additional Input Data

5.4.21 Setting Operator Configuration to Receive Notifications

Function name: SetONC

Related Procedures: Set Operator Notifications Configuration via SM-DP

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator to configure for which of its own Profiles, associated with a Profile Type, it wants to receive which kind of status change notifications; whatever the origin of the status change is.

The SM-SR receiving this request SHALL verify that the mno-id in the ONC matches the mno-id of the Operator on behalf of which the SM-DP declares to send this request.

If the request is acceptable, the SM-SR SHALL record the ONC. The new ONC overwrites the previous ONC that might have been granted with the same identifiers.

From this point on, any status change notification, irrespective of the cause and related to a Profile matching these identifiers, SHALL be sent or not based on the new ONC.

This function may return:

- A ‘Function execution status’ with ‘Executed-Success’ indicating that the notifications have been configured in the SM-SR.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in the table here after, indicating that the notifications have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

NOTE: If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the Operator will receive all notifications for status changes for its own Profiles, associated with this Profile Type, see also section 3.21 for details.

Additional input data:

Input data name	Description	Type	No.	MOC
onc	The specification of the ONC, and the criterion on which this ONC applies. See section 5.1.1.2.15 for type description.	ONC	1	M

Table 5421-A: SetONC Additional Input Data

Additional output data:

- None

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.2.5	Profile Type	4.9	Unassigned	Indicates that the Profile Type in the ONC doesn’t match the Profile Type of any Profile owned by the Operator identified by its mno-id. The SM-SR MAY support this Status Code. If it does support it, the SM-SR SHALL record the ONC anyway, and the Execution Status SHALL be Executed-WithWarning
8.2.8	ONC	3.6	Related Objects Exists	Indicates that the new ONC has overwritten a former ONC on the same identifiers. In this case the Execution Status SHALL be Executed-WithWarning
8.10	Operator	1.1	Unknown	Indicates that the Operator, addressed by the mno-id in the ONC, is unknown.
8.10	Operator	1.2	Not Allowed (Authorisation)	Indicates that the requesting SM-DP is not allowed to configure ONCs for the Operator, addressed by the mno-id in the ONC.

Table 5421-B: SetONC Specific Status Codes

5.4.22 Retrieving Operator Notification Configuration

Function name: GetONC

Related Procedures: Retrieve Operator Notifications Configuration via SM-DP

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator to retrieve a list of status change notifications it wants not to receive for its own Profiles, associated with a Profile Type.

The SM-SR receiving this request SHALL verify that the mno-id in the ONC matches the mno-id of the Operator on behalf of which the SM-DP declares to send this request.

If the request is acceptable, the SM-SR SHALL return the ONC including the list of notifications the Operator does not want to receive, applicable to the specified search criterion.

This function may return:

- A ‘Function execution status’ with ‘Executed-Success’, and additional output data providing the configured ONC.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in the table below, indicating that the notifications have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator, and additional output data providing the configured ONC.

- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
profileType	Identification of the Profile Type for which the ONC applies is searched	String	1	C
iccid	Identification of one specific Profile for which the ONC applies is searched	ICCID	1	C

Table 5422-A: GetONC Additional Input Data

One and only one of the input data profileType and iccid SHALL be present.

Additional output data:

Output data name	Description	Type	No.	MOC
onc	The ONC including the list of unwanted notifications that match the search criterion	ONC	N	M

	See section 5.1.1.2.15 for type description. NOTE: If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the output data of this function will list no notification names, as all notifications will be sent for Profiles assigned with this Profile Type. See also section 3.21.4 and table 511215-A for details.			

Table 5422-B: GetONC Additional Output Data

5.4.23 Setting the Emergency Profile Attribute

Function name: SetEmergencyProfileAttribute

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via the M2M SP

Function group: Platform Management

Function Provider: SM-SR

Description:

This function allows the SM-DP authorised by the Operator to request the setting of the Emergency Profile Attribute on the targeted Profile to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

The SM-SR SHALL verify that the request is

- Either sent on behalf of an Operator owning the targeted Profile
  or
- Sent on behalf of an Operator that is not the owner of the targeted Profile, but the Operator owning the targeted Profile has granted a PLMA allowing the operation “SetEmergencyProfileAttribute” to the Operator requesting the operation.

If one Profile currently has the Emergency Profile Attribute set, the SM-SR SHALL verify that the Operator owning the Profile with the Emergency Profile Attribute set has granted a PLMA authorising the operation “UnsetEmergencyProfileAttribute” to the Operator requesting the operation.

The SM-SR MAY provide additional verifications.

The SM-SR receiving this request SHALL process it according to “Emergency Profile Attribute Management” procedure described in the section 3.25 of this specification.

After setting the Emergency Profile Attribute, the SM-SR SHALL add or update the AdditionalProperty `'gsma.ESIM.EmergencyProfile.AID'` of the EIS. This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Emergency Profile Attribute has been set on the targeted Profile.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4

- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to get the Emergency Profile Attribute set. See section 5.1.1.1 for type description.	ICCID	1	M

Table 5423-A: Set Emergency Profile Attribute Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES5.SetEmergencyProfileAttribute.	Hexadecimal String	1	O

Table 5423-B: Set Emergency Profile Attribute Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.7	PLMA	3.8	Refused	No PLMA allows the SM-DP, or the Operator on behalf of which the SM-DP sent the request, to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the command on the eUICC. In that case, the output data “euiccResponseData” contains the exact response coming from the eUICC.

Table 5423-C: Set Emergency Profile Attribute Specific Status Codes

5.4.24 Notifying the Emergency Profile Attribute Setting

Function name: HandleEmergencyProfileAttributeSetNotification

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: SM-DP

Description: This function SHALL be called to notify that the Emergency Profile Attribute has been set on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all SM-DP servers that match one or the other of the following conditions:

- The SM-DP can relay the notification to the Operator that owns the Profile, and the Operator has opted to receive such notifications (see section 3.21)
- The SM-DP can relay the notification to another Operator, and the Operator owner of the Profile has granted the other Operator with a PLMA authorising this Operation “HandleEmergencyProfileAttributeSetNotification”.
- The SM-DP can relay the notification to any Operator having a Profile on this eUICC. In this case Identification of the Profile that has the Emergency Profile Attribute set and Identification of the Operator owner of the Profile that has the Emergency Profile Attribute set are optional.

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has the Emergency Profile Attribute set. See section 5.1.1.1 for type description.	ICCID	1	C
mno-id	Identification of the Operator owner of the Profile that has the Emergency Profile Attribute set. See section 5.1.1.1 for type description.	OID	1	C
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5424: Handle Emergency Profile Attribute Set Notification Additional Input Data

5.4.25 Notifying the Emergency Profile Attribute Unsetting

Function name: HandleEmergencyProfileAttributeUnsetNotification

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: SM-DP

Description: This function SHALL be called to notify that the Emergency Profile Attribute has been unset on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all SM-DP servers that match one or the other of the following conditions:

- The SM-DP can relay the notification to the Operator that owns the Profile, and the Operator has opted to receive such notifications (see section 3.21)
- The SM-DP can relay the notification to another Operator, and the Operator owner of the Profile has granted the other Operator with a PLMA authorising this Operation "HandleEmergencyProfileAttributeUnsetNotification".

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has the Emergency Profile Attribute unset. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	Identification of the Operator owner of the Profile that has the Emergency Profile Attribute unset. See section 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5425: Handle Emergency Profile Attribute Unset Notification Additional Input Data

5.4.26 Setting the Fall-Back Attribute

Function name: SetFallBackAttribute

Related Procedures: Fall-Back Attribute Management

Function group: Platform Management

Function Provider: SM-SR

Description:

This function allows the SM-DP authorised by the Operator to request the setting of the Fall-Back Attribute on the targeted Profile to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

The SM-DP SHALL indicate on behalf of which Operator it is requesting this operation.

The SM-SR SHALL verify that the request is

- Either sent on behalf of an Operator owning the targeted Profile
  or
- Sent on behalf of an Operator that is not the owner of the targeted Profile, but the Operator owning the targeted Profile has granted a PLMA allowing the operation "SetFallBackAttribute" to the Operator requesting the operation.

In both cases, the SM-SR SHALL verify that the Operator owning the Profile which currently has the Fall-Back Attribute set has granted, to the Operator requesting the operation, a PLMA authorising the operation "UnsetFallBackAttribute", applicable for the Profile that currently has the Fall-Back Attribute set.

The SM-SR MAY provide additional verifications.

The SM-SR receiving this request SHALL process it according to "Fall-Back Attribute Management via SM-DP" procedure described in the section 3.28 of this specification.

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the Fall-Back Attribute has been set on the targeted Profile.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile on which to set the Fall-Back Attribute. See section 5.1.1.1 for type description.	ICCID	1	M

Table 5426-A: Set Fall-Back Attribute Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES5.SetFallBackAttribute.	Hexadecimal String	1	O

Table 5426-B: Set Fall-Back Attribute Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.2	POL1	3.8	Refused	The POL1 of a Profile on the targeted eUICC doesn't allow this operation.
8.2.7	PLMA	3.8	Refused	No PLMA allows the SM-DP, or the Operator on behalf of which the SM-DP sent the request, to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the command on the eUICC. In that case, the output data "euiccResponseData" contains the exact response coming from the eUICC.

Table 5426-C: Set Fall-Back Attribute Specific Status Codes

NOTE: A POL1 may interfere with the Set Fall-Back Attribute operation in very specific circumstances described in section 4.1.1.7.

5.4.27 Notifying the Fall-Back Attribute is Set

Function name: HandleProfileFallBackAttributeSetNotification

Related Procedures: Fall-Back Attribute Management, Fall-Back Attribute Management via SM-DP, Fall-Back Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: SM-DP

Description:

This function SHALL be called to notify that the Fall-Back Attribute has been set on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all SM-DP servers that match one or the other of the following conditions:

- The SM-DP can relay the notification to the Operator that owns the Profile, and the Operator has opted to receive such notifications (see section 3.21)
- The SM-DP can relay the notification to another Operator, and the Operator owner of the Profile has granted the other Operator with a PLMA authorising this Operation "HandleProfileFallBackAttributeSetNotification".

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile on which the Fall-Back Attribute has been set. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	Identification of the Operator owner of the Profile that has had its Fall-Back Attribute set. See section 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5427: Handle Profile Fall-Back Attribute Set Notification Additional Input Data

5.4.28 Notifying the Fall-Back Attribute is Unset

Function name: HandleProfileFallBackAttributeUnsetNotification

Related Procedures: Fall-Back Attribute Management, Fall-Back Attribute Management via SM-DP, Fall-Back Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: SM-DP

Description: This function SHALL be called to notify that the Fall-Back Attribute has been unset on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all SM-DP servers that match one or the other of the following conditions:

- The SM-DP can relay the notification to the Operator that owns the Profile, and the Operator has opted to receive such notifications (see section 3.21)
- The SM-DP can relay the notification to another Operator, and the Operator owner of the Profile has granted the other Operator with a PLMA authorising this Operation “HandleProfileFallBackAttributeUnsetNotification”.

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile on which the Fall-Back Attribute has been unset. See section 5.1.1.1 for type description.	ICCID	1	M
mno-id	Identification of the Operator owner of the Profile on which the Fall-Back Attribute has been unset. See section 5.1.1.1 for type description.	OID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5427: Handle Profile Fall-Back Attribute Unset Notification Additional Input Data

5.5 ES4 (Operator - SM-SR, and M2M SP – SM-SR) Interface Description

NOTE: The execution of several ES4 functions by the SM-SR is conditioned by the verification that the Operator or M2M SP requesting to perform an operation on a Profile, or the Operator or M2M SP to be notified, is authorised for this operation or notification by the owner of the Profile. The specification of this verification by the SM-SR is described in sections 5.7.1.2 and 5.7.1.3.

5.5.1 Getting eUICC Information

Function name: GetEIS

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the Operator or the M2M SP to retrieve the eUICC Information Set (EIS) of a particular eUICC from the SM-SR information database based on the EID. The retrieved EIS contains only the data that is applicable for that particular Operator. The Operator utilises the retrieved EIS, for instance, to verify the eligibility of the eUICC (for example type, certificate and memory).

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the download function has been successfully executed on the SM-SR as requested by the function caller.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M

Table 176: Get EIS Additional Input Data

The SM-SR SHALL filter the list of Profiles returned in the EIS, considering the authorisation granted by the Profile owners; for each Profile, this includes:

- If the function caller is the owner of the Profile, the SM-SR SHALL include this Profile in the returned EIS.
- If the function caller is not the owner of the targeted Profile, the SM-SR SHALL include the Profile in the returned EIS only if the Operator owning the Profile has granted a PLMA allowing the operation “GetEIS” to the function caller.

Additional output data:

Output data name	Description	Type	No.	MOC
eis	The relevant eUICC Information Set of the eUICC See section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	C

Table 177: Get EIS Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	1.1	Unknown	Indicates that the EID, is unknown to the function provider
8.6	EIS	1.2	Not Allowed (Authorisation)	Function requester is not allowed to manage this EIS, identified by this EID.

Table 178: Get EIS Specific Status Code

5.5.2 Updating the Policy Rules of a Profile

Function name: UpdatePolicyRules

Related Procedures: -

Function group: Profile Management

Function Provider: SM-SR

Description: This function allows the Operator to update POL2 of a Profile, identified by its ICCID, and installed on an eUICC identified by its EID.

The general description of this function is detailed in section 5.4.6 of this specification.

5.5.3 Updating eUICC Information

Function name: UpdateSubscriptionAddress

Related Procedures: Profile Enabling

Function group: Profile Management

Function Provider: SM-SR

Description: This function enables the caller to update the Subscription Address for a Profile in the eUICC Information Set (EIS) of a particular eUICC identified by the EID and ICCID. The function replaces the content of the Subscription Address. For consistency within the system, it is the responsibility of the caller to ensure that all data is provided.

On reception of the function request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC.
- The Profile identified by its ICCID is loaded on the targeted eUICC.
- The target Profile is owned by the requesting Operator, or an Operator that had granted a PLMA that authorises the requesting M2M SP to perform the operation “UpdateSubscriptionAddress” on a Profile that matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria)

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the UpdateSubscriptionAddress function has been successfully executed by the SM-SR as requested by the function caller.

A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the target Profile. See section 5.1.1.1 for type description.	ICCID	1	M
newSubscriptionAddress	The new Subscription Address	Subscription Address	1	M

Table 179: Update Subscription Address Additional Input Data

Additional output data:

This function has no additional output data.

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	1.1	Unknown	Indicates that the EIS identified by this EID, is unknown to the function provider
8.2.1	ICCID	1.1	Unknown	Indicates that the Profile identified by the ICCID, is unknown to the function provider
8.2.6	Subscription Address	1.2	Not Allowed (Authorisation)	Function caller is not allowed to manage the Subscription Address.

Table 180: Update Subscription Address Status Codes

5.5.4 Auditing eUICC Information

Function name: AuditEIS

Related Procedures: Profile Download and Installation

Function group: Profile Management

Function provider: SM-SR

Description: This function allows the Operator to retrieve the up to date EIS information. The SM-SR SHALL use the relevant functions of the ES5 interface to retrieve the information from the eUICC. The SM-SR SHALL update its EIS database upon the basis of this information.

If the function caller provides a list of ICCID of Profiles to audit, the SM-SR SHALL verify for each Profile that the function caller

- is either the owner of the targeted Profile
  or
- is authorised by the Operator owning the targeted Profile(s)

to perform the operation “AuditEIS” on a Profile that matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria).

This SHALL also be applied if the list of ICCIDs identifies

- Profiles that are owned by this Operator
  and / or
- Profiles that are owned by other Operators.

The SM-SR MAY provide additional verifications.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the function has been successfully executed on the SM-SR as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC.to be audited See section 5.1.1.1 for type description.	EID	1	M
iccid-list	List of “iccid” identifying Profiles to be audited	ICCID	1..N	C

Table 181: AuditEIS Additional Input Data

If no list of ICCIDs is provided, it is implied that all authorised Profiles in the EIS are requested.

The SM-SR SHALL filter the list of Profiles returned in the EIS, considering the authorisation granted by the Profile owners; for each Profile, this includes:

- If the function caller is the owner of the Profile, the SM-SR SHALL include this Profile in the returned EIS.
- If the function caller is not the owner of the targeted Profile, the SM-SR SHALL include the Profile in the returned EIS only if the Operator owning the Profile has granted a PLMA allowing the operation “AuditEIS” to the function caller.

Additional output data:

Output data name	Description	Type	No.	MOC
Eis	For the relevant eUICC Information Set see section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.Only data for the requested Profiles is returned within EIS. The Profiles that do not belong to the requestor are not included in the response. This access control function is realised within the SM-SR, there is no need to limit the data on the eUICC side.	EIS	1	C

Table 182: AuditEIS Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
1.6	Function	5.4	Delivered With No Response	The function execution request has been delivered to the remote entity but no response is received.
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider
8.2	Profile	1.2	Not Allowed (Authorisation)	One or more Profiles identified by ICCIDs in the list do not belong to function requester
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by one of the ICCIDs in the list is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.7	PLMA	3.8	Refused	No PLMA allows the M2M SP to execute this operation.
8.6	EIS	1.2	Not Allowed (Authorisation)	Function requester is not allowed to manage this EIS, identified by this EID.

Table 183: AuditEIS Additional Specific Status Codes

5.5.5 Profile Enabling

Function name: EnableProfile

Related Procedures: Profile Enabling

Function group: Platform Management

Function Provider: SM-SR

Description: This function allows the Operator to request a Profile Enabling to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

On reception of the function request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC.
- The Profile identified by its ICCID is loaded on the targeted eUICC.
- The target Profile is owned by the requesting Operator or an Operator that had granted a PLMA that authorises the requesting M2M SP to perform the operation “EnableProfile” on a Profile that matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria).

- The target Profile is in Disabled state
- The POL2 of the target Profile and the POL2 of the currently Enabled Profile allow the enabling.

The SM-SR MAY provide additional verifications.

In case one of these conditions is not satisfied, the SM-SR SHALL refuse the function request and return a 'Function execution status' indicating 'Failed' with the relevant status code (see table below).

The SM-SR receiving this request SHALL process it according to "Profile Enabling" procedure described in the section 3.2 of this specification.

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the Profile has been enabled on the eUICC.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4
- A 'Function execution status' indicating 'Failed'
  with a status code indicating a Unknown eUICC
  with a status code indicating a Unknown ICCID
- With a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
Iccid	Identification of the Profile to enable. See section 5.1.1.1 for type description.	ICCID	1	M

Table 184: Enable Profile Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES5 depending of the requested function.	Hex binary	1	O

Table 185: Enable Profile Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.

8.2	Profile	5.1	Inaccessible	Indicates that the Profile change procedure couldn't complete after enabling the target Profile, and the Profile change was rolled-back on the eUICC,
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.1	Profile ICCID	3.5	Invalid Transition	Indicates that the Profile was already Enabled
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.
8.2.2	POL1	3.8	Refused	The POL1 of one the impacted Profiles don't allow this operation.
8.2.3	POL2	3.8	Refused	The POL2 of one the impacted Profiles don't allow this operation.
8.2.7	PLMA	3.8	Refused	No PLMA allows the M2M SP to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the enabling command on the eUICC. In that case, the output data "euiccResponseData contains the exact response coming from the eUICC.

Table 186: Enable Profile Specific Status Codes

5.5.6 Profile Disabling

Function name: DisableProfile

Related Procedures: Profile Disabling

Function group: Platform Management

Function Provider: SM-SR

Description: This function allows the Operator or the M2M SP to request a Profile Disabling to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

On reception of the function request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC.
- The Profile identified by its ICCID is loaded on the targeted eUICC.
- The target Profile is owned by the requesting Operator, or an Operator that had granted a PLMA that authorises the requesting M2M SP to perform the operation "DisableProfile" on a Profile that matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria)
- The target Profile is in Enabled state
- The POL2 of the target Profile allows the disabling.

This function may return:

- A 'Function execution status' with 'Executed-Success' indicating that the Profile has been disabled on the eUICC.

- A ‘Function execution status’ with ‘Executed-WithWarning’, with a status code as defined below, indicating that the Profile has been disabled on the eUICC, and deleted after application of a POL1 or POL2 rule.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to disable. See section 5.1.1.1 for type description.	ICCID	1	M

Table 187: Disable Profile Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES5 depending of the requested function.	Hex binary	1	O

Table 188: Disable Profile Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1	UICC	3.8	Refused	Indicates that the target Profile can’t be disabled. (for example the Profile is the only Profile in the eUICC)
8.2	Profile	5.1	Inaccessible	Indicates that the Profile change procedure couldn’t complete after enabling the Profile with the Fall-Back Attribute set, and the Profile change was rolled-back on the eUICC,
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.1	Profile ICCID	3.5	Invalid Transition	Indicates that the Profile was already Disabled
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.

Subject code	Subject	Reason code	Reason	Description
8.2.2	POL1	3.6	Related Object Exists	The POL1 of the target Profile has triggered its deletion after disabling it This status code SHALL only be sent along Status =”Executed-WithWarning”
8.2.2	POL1	3.8	Refused	The POL1 of the target Profile doesn’t allow this operation.
8.2.3	POL2	3.6	Related Object Exists	The POL2 of the target Profile has triggered its deletion after disabling it This status code SHALL only be sent along Status =”Executed-WithWarning”
8.2.3	POL2	3.8	Refused	The POL2 of the target Profile doesn’t allow this operation.
8.2.7	PLMA	3.8	Refused	No PLMA allows the M2M SP to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the disabling command on the eUICC. In that case, the output data “euiccResponseData” contains the exact response coming from the eUICC.

Table 189: Disable Profile Specific Status Codes

5.5.7 Delete a Profile

Function name: DeleteProfile

Related Procedures: Profile and ISD-P Deletion

Function group: Platform Management

Function Provider: SM-SR

Description: This function allows the Operator or the M2M SP to request deletion of the target ISD-P with the Profile to the SM-SR in charge of the management of the targeted eUICC; eUICC being identified by its EID.

On reception of the function request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC.
- The Profile identified by its ICCID is loaded on the targeted eUICC.
- The POL2 of the target Profile allows the deletion.
- The target Profile is not the Profile having the Fall-Back Attribute.
- The target Profile is owned by the requesting Operator, or an Operator that had granted a PLMA that authorises the requesting M2M SP to perform the operation “DeleteProfile” on a Profile that matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria).

The SM-SR MAY provide additional verifications.

In case one of these conditions is not satisfied, the SM-SR SHALL refuse the function request and return a ‘Function execution status’ indicating ‘Failed’ with the relevant status code (see table below).

The SM-SR receiving this request SHALL process it according to “ISD-P Deletion” procedure described in the section 3.6 of this specification.

In case the target Profile is “Enabled”, the SM-SR SHALL automatically disable it before executing the deletion. This function is described in section 4.1.1.3.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Profile has been deleted on the eUICC.
- A 'Function execution status' with 'Executed- WithWarning' indicating that the Profile has been deleted on the eUICC, with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to delete. See section 5.1.1.1 for type description.	ICCID	1	M

Table 190: Delete Profile Additional InputDdata

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC	Byte[]	1	O

Table 191: Delete Profile Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.

8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.1	Profile ICCID	1.2	Not Allowed (Authorisation)	Indicates that the function caller is not allowed to perform this function on the target Profile.
8.2.1	Profile ICCID	3.8	Refused	Indicates that the Profile cannot be deleted because it is the last Profile of the eUICC or the Fall-Back Profile.
8.2.2	POL1	3.8	Refused	The POL1 of the Profile doesn't allow this operation.
8.2.3	POL2	3.8	Refused	The POL2 of the Profile doesn't allow this operation.
8.2.7	PLMA	3.8	Refused	No PLMA allows the M2M SP to execute this operation.
8.3	ISD-P	4.6	Not Present / Missing	The target ISD-P was not found on this eUICC (in this case the Function Execution Status SHALL be 'Executed- WithWarning')
8.4	ISD-R	4.2	Execution error	Error during execution of the deletion (or disabling) command on the eUICC. In that case, the output data "euiccResponseData" contains the exact response coming from the eUICC.

Table 192: Delete Profile Specific Status Codes

NOTE: in case Profile disabling is performed automatically before deletion, this function MAY raise any status code coming from the execution of the Profile disabling function defined in section 5.5.6.

5.5.8 Prepare SM-SR Change

Function name: PrepareSMSRChange

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider: SM-SR

Description: This function allows the Initiator to request to a new SM-SR to prepare for a change for an eUICC identified by its EID.

The check is used to give the opportunity to the new SM-SR to ensure that any necessary business agreement is in place.

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the PrepareSMSRChange function has been successfully executed on the SM-SR as requested by the function caller.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC

eid	provide the EID of the eUICC See section 5.1.1.1 for type description.	EID	1	M
currentSMSRid	Identification of the current SM-SR. See section 5.1.1.1 for type description.	OID	1	M

Table 193: Prepare SM-SR Change Additional Input Data

Table 194: Void

Table 195: Void

Specific status codes

Subject Code	Subject	Reason code	Reason	Description
1.2	Function Provider	3	Condition Of Use Not satisfied	Indicates that function provider is not capable of managing the eUICC identified by this EID,
8.7	SM-SR	1.1	Unknown	The new SM-SR doesn't know or have access to the current SM-SR managing this eUICC
8.1.1	EID	3.3	Already in Use (Uniqueness)	Indicates that the eUICC identified by this EID is already managed by this SM-SR.

Table 196: Prepare SM-SR Change Specific Status Codes

5.5.9 SM-SR Change

Function name: SMSRChange

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider: SM-SR

Description: This function allows the initiator to request to the current SM-SR to change for a specific eUICC identified by its EID.

The SM-SR receiving this request SHALL process it according to the "SM-SR Change" procedure described in GSMA Remote Provisioning Architecture for Embedded UICC [1].

This function may return:

- A 'Function execution status' with 'Executed-Success' indicating that the function has been successfully executed by the function provider as requested by the function caller. In this case, the eUICC is unambiguously managed by the new SM-SR (SM-SR2).
- A 'Function execution status' with 'Executed-WithWarning' indicating either:
  - that the eUICC has been successfully transferred to the new SM-SR, but additional configuration has not completed and may need to be done again. In this case, the eUICC is unambiguously managed by the new SM-SR (SM-SR2), but

the new SM-SR SHALL perform such configuration operations automatically at a later point in time
    - or that the eUICC was already managed by the new SM-SR (SM-SR2). This happens when this is the second attempt to perform the SM-SR Change, after the first attempt expired whereas it was already successful from the point of view of the new SM-SR.
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 of a specific status code as defined in the Specific status code table below, to indicate that the procedure has failed or expired before the effective transfer of OTA management to the new SM-SR. In this case, the eUICC is still managed unambiguously by the current SM-SR (SM-SR1).
- A 'Function execution status' indicating 'Expired' with the status code as defined in section 5.1.6.4, indicating that the procedure has expired before confirming the proper transfer.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
targetSMSRid	Identification of the new SM-SR. See section 5.1.1.1 for type description.	OID	1	M

Table 197: SM-SR Change Additional Input Data

Specific status codes

In addition to the status codes returned by ES7.handoverEUICC, this function can return the following specific status codes:

Subject Code	Subject	Reason code	Reason	Description
1.6	Function	5.3	Time to live expired	The function execution request has expired (end of validity period has been reached). This may be because the server had no time to execute the function or because the function was requesting a remote communication with the eUICC which was not present on the network during all the validity period. If this status code is returned when 'Execution Status' is 'Failed', this means the current SM-SR (SM-SR1) is still managing the eUICC.
1.6	Function	4.5	Operation Already Processed	The function is the second attempt to transfer the same eUICC to the same new SM-SR after a previous attempt has expired, and the previous attempt had indeed succeeded from the point of view of the new SM-SR. In this case the Execution-Status SHALL be 'Executed-WithWarning'
8.1.1	EID	1.1	Unknown	Indicates that the EID , is unknown to the function provider
8.1	eUICC	1.2	Not Allowed (Authorisation)	Function requester is not allowed to manage the eUICC
8.1	eUICC	4.4	Busy	Other operations pending on the eUICC
8.4	ISD-R	4.2	Execution error	Error during the creation of a new key set at the ISD-R level

8.5.2	eUICC Certificate Authority Certification	6.3	Certificate Expired	ECASD Certificate Expired
8.7	SM-SR	3.9	Unknown	The targetSMSRid is unknown

Table 198: SM-SR Change Specific Status Codes

5.5.10 Notify a Profile is Disabled

Function name: HandleProfileDisabledNotification

Related Procedures: Profile Download and Installation, Profile Enabling, Fall-Back Activation Procedure, Profile Enabling via M2MSP, Profile Disabling via M2MSP, Profile Enabling via SM-DP

Function group: Platform Management

Notification handler/recipient: Operator or M2M SP

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been disabled on the eUICC identified by its EID, if and only if:

- The recipient of the notification is the Operator owning the Profile and has not set an ONC to discard those notifications,
  or
- The recipient of the notification is an M2M SP (including, another Operator that is not the owner of the Profile), and the Operator owner of the Profile has granted the M2M SP with a PLMA authorising the Operation “HandleProfileDisabledNotification”.

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has done.

In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

What is performed by the Operator or M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been disabled. See section 5.1.1.1 for type description.	ICCID	1	M

completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 199: Handle Profile Disabled Notification Additional Input Data

5.5.11 Notify a Profile is Enabled

Function name: HandleProfileEnabledNotification

Related Procedures: Profile Disabling, Profile Disabling via SM-DP, Fall-Back Activation Procedure, Profile Enabling via M2M SP, Profile Disabling via M2M SP

Function group: Platform Management

Notification handler/recipient: Operator or M2M SP

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been enabled on the eUICC identified by its EID, if and only if:

- The recipient of the notification is the Operator owning the Profile and has not set an ONC to discard those notifications
  Or
- The recipient of the notification is an M2M SP (including, another Operator that is not the owner of the Profile), and the Operator owner of the Profile has granted the M2M SP with a PLMA authorising the Operation “HandleProfileEnabledNotification”.

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

What is performed by the Operator or M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been disabled. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 200: Handle Profile Enabled Notification Additional Input Data

5.5.12 Notify a SM-SR Change

Function name: HandleSMSRChangeNotification

Related Procedures: SM-SR Change

Function group: eUICC Management

Notification handler/recipient: Operator

Description: This function SHALL be called for notifying each Operator owning a Profile hosted in the eUICC, identified by its EID, that the SM-SR has changed. The notification is sent by the new SM-SR.

This notification also conveys the date and time specifying when the operation has been done.

This notification is not related to a particular Profile. It is up to the notification recipient to perform any action related to each Profile that is deployed on this eUICC.

Additional input data:

Input data name	Description	Type	No.	MOC
eis	The relevant part of the eUICC Information Set linked with the Operator owning the Profile hosted in the eUICC. See section 5.1.1.2.13 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 201: Handle SM-SR Change Notification Additional Input Data

Additional output data:

No output data is expected in response to this notification.

5.5.13 Notify a Profile Deletion

Function name: HandleProfileDeletedNotification

Related Procedures: Profile enabling, Profile Enabling via SM-DP, Profile Enabling via M2M SP, Profile Disabling via M2M SP, Profile and ISD-P Deletion via M2M SP

Function group: Platform Management

Notification handler/recipient: Operator or M2M SP

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been deleted on the eUICC identified by its EID, if and only if:

- The recipient of the notification is the Operator owning the Profile and has not set an ONC to discard those notifications
  or
- The recipient of the notification is an M2M SP (including, another Operator that is not the owner of the Profile), and the Operator owner of the Profile has granted the M2M SP with a PLMA authorising the Operation “HandleProfileDeletedNotification”.

ICCID may be not enough to identify right address of recipient; SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure ‘completionTimestamp’ to be equal for every message.

What is performed by the Operator or M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been deleted. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 202: Handle Profile Deleted Notification Additional Input Data

5.5.14 Notify a Profile Download

Function name: HandleProfileDownloadedNotification

Related Procedures: Profile Download

Function group: Profile Management

Notification handler/recipient: M2M SP

Description: This function SHALL be called to notify that the Profile identified by its ICCID has been downloaded on the eUICC identified by its EID.

The SM-SR SHALL inspect the PLMAs that apply to this Profile, and only send this notification to recipients which have a PLMA that includes the authorisation to receive this notification.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure ‘completionTimestamp’ to be equal for every message.

What is performed by the M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has been downloaded. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5514: Handle Profile Downloaded Notification Additional Input Data

5.5.15 Notify the Change of Policy Rules of a Profile

Function name: HandlePolicyRulesUpdatedNotification

Related Procedures: POL2 Update, POL2 Update via SM-DP

Function group: Profile Management

Notification handler/recipient: M2M SP

Description: This function SHALL be called to notify an M2M SP that the Policy Rules have been updated on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL inspect the PLMAs that apply to this Profile, and only send this notification to an M2M SP that has been granted a PLMA by the Operator owner of the Profile for the authorised operation “HandlePolicyRuleUpdatedNotification”.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure ‘completionTimestamp’ to be equal for every message.

What is performed by the M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
Eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile whose POL2 has been updated. See section 5.1.1.1 for type description.	ICCID	1	M
Pol2	Value of the POL2 after being updated by the Operator owning the Profile See section 5.1.1.1 for type description.	POL2	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5515: Handle Policy Rules Updated Notification Additional Input Data

5.5.16 Notify a PLMA Setting

Function name: HandleSetPLMANotification

Related Procedures: Set Profile Lifecycle Management Authorisation, Set Profile Lifecycle Management Authorisation via SM-DP

Function group: Platform Management

Notification handler/recipient: M2M SP

Description: This function SHALL be called to notify an M2M SP that a PLMA concerning this M2M SP has been set or updated.

This notification also conveys the date and time specifying when the operation has been done. In case of multiple handlers are served the SM-SR SHOULD ensure 'completionTimestamp' to be equal for every message.

What is performed by the M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
plma	The specification of the PLMA that now applies on a Profile Type. Information about the Profile Type are contained in the PLMA structure See section 5.1.1.2.14 for type description	PLMA	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5516-A: Handle PLMA Changed Notification Additional Input Data

5.5.17 Retrieving Authorisations of M2M SP to Access Profiles

Function name: GetPLMA

Related Procedures: Retrieve Profile Lifecycle Management Authorisation by Operator, Retrieve Profile Lifecycle Management Authorisation by M2M SP

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator owner of Profiles to retrieve the list of PLMAs applicable to a certain Profile, or a certain Profile Type, or for a certain M2M SP.

The same function can also be used by the M2M SP to retrieve the list of PLMAs granted to this M2M SP, and applicable to a certain Profile, or a certain Profile Type.

The SM-SR receiving this request SHALL verify the requester is allowed to retrieve such information, and return the list of all PLMAs applicable to the specified search criterion:

- If the requester is the owner of the targeted Profiles, the authorisation is implied.
- If the requester is an M2M SP (including, another Operator that is not the owner of the targeted Profiles), the list of PLMAs is only returned if at least a PLMA exist for this M2M SP and for the targeted Profile or Profile Type

If this verification fails, the SM-SR SHALL terminate the request and return a response with the 'Function execution status' indicating 'Failed', and no PLMA.

Otherwise, the SM-SR SHALL return the complete list of all PLMAs applicable to the specified search criterion; if the search criterion is on a specific Profile or Profile Type, this includes even PLMAs that are granted to an M2M SP that is not the function requester.

In case the list of PLMAs is very long, the SM-SR MAY truncate the result. The caller can then issue another call to getPLMA with more restrictive criteria.

NOTE The order of the PLMAs returned in the truncated list is implementation-dependent.

This function may return:

- A 'Function execution status' with 'Executed- Success', and additional output data providing the PLMAs.
- A 'Function execution status' with 'Executed-WIthWarning', to indicate that the result was truncated, plus additional output data providing part of the list of applicable PLMAs.
- A 'Function execution status' indicating 'Failed' if the requester was not allowed to request this information.

Additional input data:

Input data name	Description	Type	No.	MOC
profileType	Identification of the Profile type for which PLMAs are searched	String	1	C
m2m-sp-id	Identification of the M2M SP for which PLMAs are searched	OID	1	C
iccid	Identification of one specific Profile	ICCID	1	C
mno-id	Identification of the Operator owning the Profiles to be matched (this input datum SHALL be present only in case the search criterion is a Profile Type). See section 5.1.1.1 for type description.	OID	1	C

Table 5517-A: GetPLMA Additional Input Data

One and only one of the input data profileType, m2m-sp-id and iccid SHALL be present.

Additional output data:

Output data name	Description	Type	No.	MOC
plma	The list of PLMAs that match the search criterion See section 5.1.1.2.14 for type description.	PLMA	N	M

Table 5517-B: RetrievePLMA Additional Output Data

Specific status codes:

Subject code	Subject	Reason code	Reason	Description
1.1	Function requester	1.2	Not Allowed (Authorisation)	Indicates that the Operator or M2M SP which called this function is not doesn't have a PLMA granted that applies to the targeted Profile or Profile type (including, if the targeted Profile or Profile type is unknown to this SM-SR)
8.9	M2M SP	1.1	Unknown	Indicates that the M2M SP specified in the search criterion is unknown to this SM-SR
8.10	Operator	1.1	Unknown	Indicates that the Operator, addressed by the mno-id in the PLMA, is unknown.

Table 5517-C: GetPLMA Specific Status Codes

5.5.18 Setting the Emergency Profile Attribute

Function name: SetEmergencyProfileAttribute

Related Procedures: Emergency Profile Attribute Management

Function group: Platform Management

Function Provider: SM-SR

Description:

This function allows an Operator or an M2M SP authorised by the Operator via PLMA to request the setting of the Emergency Profile Attribute on the targeted Profile to the SM-SR in charge of the management of the targeted eUICC, eUICC being identified by its EID.

The SM-SR SHALL verify that the request is

- Either sent by an Operator owning the targeted Profile
  or
- Sent by an M2M SP, but the Operator owning the targeted Profile has granted a PLMA allowing the operation "SetEmergencyProfileAttribute" to the M2M SP requesting the operation.

If one Profile currently has the Emergency Profile Attribute set, the SM-SR SHALL verify that the Operator owning the Profile with the Emergency Profile Attribute set has granted a PLMA authorising the operation "UnsetEmergencyProfileAttribute" to the Operator requesting the operation.

The SM-SR MAY provide additional verifications.

The SM-SR receiving this request SHALL process it according to "Emergency Profile Attribute Management" procedure described in sections 3.25 and 3.26 of this specification.

After setting the Emergency Profile Attribute, the SM-SR SHALL add or update the AdditionalProperty `'gsma.ESIM.EmergencyProfile.AID'` of the EIS.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Emergency Profile Attribute has been set on the targeted Profile.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile to get the Emergency Profile Attribute set. See section 5.1.1.1 for type description.	ICCID	1	M

Table 5518-A: Set Emergency Profile Attribute Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES5.SetEmergencyProfileAttribute.	Hexadecimal String	1	O

Table 5518-B: Set Emergency Profile Attribute Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.7	PLMA	3.8	Refused	No PLMA allows the M2M SP to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the command on the eUICC. In that case, the output data “euiccResponseData” contains the exact response coming from the eUICC.

Table 5518-C: Set Emergency Profile Attribute Specific Status Codes

5.5.19 Notifying the Emergency Profile Attribute setting

Function name: HandleEmergencyProfileAttributeSetNotification

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator or M2M SP

Description: This function SHALL be called to notify that the Emergency Profile Attribute has been set on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all Operator and M2M SP servers that match one or the other of the following conditions:

- The Operator that owns the Profile, and the Operator has not set an ONC to discard such notifications (see section 3.21)
- The M2M SP, where the Operator owner of the Profile has granted the M2M SP with a PLMA authorising this Operation “HandleEmergencyProfileAttributeSetNotification”.
- Any Operator having a Profile on this eUICC. In this case identification of the Profile that has the Emergency Profile Attribute set and Identification of the Operator owner of the Profile that has the Emergency Profile Attribute set are optional.

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

What is performed by the Operator or M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has the Emergency Profile Attribute set. See section 5.1.1.1 for type description.	ICCID	1	C
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5519: Handle Emergency Profile Attribute Set Notification Additional Input Data

5.5.20 Notifying the Emergency Profile Attribute Unsetting

Function name: HandleEmergencyProfileAttributeUnsetNotification

Related Procedures: Emergency Profile Attribute Management, Emergency Profile Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator or M2M SP

Description: This function SHALL be called to notify that the Emergency Profile Attribute has been unset on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to all Operator and M2M SP servers that match one or the other of the following conditions:

- The Operator that owns the Profile, and the Operator has opted to receive such notifications (see section 3.21)
- The M2M SP, and the Operator owner of the Profile has granted the M2M SP with a PLMA authorising this Operation "HandleEmergencyProfileAttributeUnsetNotification".

ICCID may be not enough to identify right address of recipient, SM-SR should map it internally to Operator notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served, the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

What is performed by the Operator or M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile that has the Emergency Profile Attribute unset. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5520: Handle Emergency Profile Attribute Unset Notification Additional Input Data

5.5.21 Setting the Fall-Back Attribute

Function name: SetFallBackAttribute

Related Procedures: Fall-Back Attribute Management

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator owner of the Profile or an M2M SP authorised by the Operator owner of the Profile, to request the SM-SR to set the Fall-Back Attribute on a Profile in a specified eUICC, eUICC being identified by its EID. On reception of this request, the SM-SR SHALL perform the following minimum set of verifications:

- The SM-SR is responsible for the management of the targeted eUICC.
- The Profile identified by its ICCID is loaded on the targeted eUICC.
- The target Profile is owned by the requesting Operator, or by an Operator that had granted a PLMA that authorises the requesting M2M SP to perform the operation “setFallbackAttribute” on a Profile that matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria)
- The Operator owning the Profile which currently has the Fall-Back Attribute set has granted a PLMA that authorises the requesting Operator or M2M SP to perform the operation “UnsetFallBackAttribute”, and that the Profile that currently has the Fall-Back Attribute set matches the criteria of the PLMA (see section 5.7.1.1 for the detail of the matching of the criteria).

The SM-SR MAY provide additional verifications.

The SM-SR receiving this request SHALL process it according to “Fall-Back Attribute Management” procedures described in section 3.27 and 3.29 of this specification.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the Fall-Back Attribute has been set on the targeted Profile.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile on which to set the Fall-Back Attribute. See section 5.1.1.1 for type description.	ICCID	1	M

Table 5521-A: Set Fall-Back Attribute Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
euiccResponseData	Contains the detailed error returned by the eUICC in case the function execution failed on eUICC. The response data is defined in ES5.SetFallBackAttribute.	Hexadecimal String	1	O

Table 5521-B: Set Fall-Back Attribute Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	3.9	Unknown	Indicates that the eUICC, identified by this EID, is unknown to the function provider.
8.2.1	Profile ICCID	3.9	Unknown	Indicates that the Profile identified by this ICCID is unknown to the function provider.
8.2.1	Profile ICCID	3.4	Invalid destination	Indicates that the Profile identified by this ICCID is known to the function provider but installed on another eUICC than the one identified by the function caller.
8.2.2	POL1	3.8	Refused	The POL1 of a Profile on the targeted eUICC doesn't allow this operation (see Note).
8.2.7	PLMA	3.8	Refused	No PLMA allows the function requester to execute this operation.
8.4	ISD-R	4.2	Execution error	Error during execution of the command on the eUICC. In that case, the output data "euiccResponseData" contains the exact response coming from the eUICC.

Table 5521-C: Set Fall-Back Attribute Specific Status Codes

NOTE A POL1 may interfere with the Set Fall-Back Attribute operation in very specific circumstances described in section 4.1.1.7

5.5.22 Notifying the Fall-Back Attribute is Set

Function name: HandleProfileFallBackAttributeSetNotification

Related Procedures: Fall-Back Attribute Management, Fall-Back Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator or M2M SP

Description:

This function SHALL be called to notify the Operator and the M2M SP that the Fall-Back Attribute has been set on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to:

- the Operator owning the Profile, if it has not set an ONC to not receive those notifications
- the M2M SP SP (including, another Operator that is not the owner of the Profile), if the Operator owner of the Profile has granted the M2M SP with a PLMA authorising the operation "HandleProfileFallBackAttributeSetNotification"

ICCID may be not enough to identify right address of recipient, the SM-SR should map it internally to Operator or M2M SP notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

What is performed by the Operator or M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile on which the Fall-Back Attribute has been set. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5522: Handle Profile Fall-Back Attribute Set Notification Additional Input Data

5.5.23 Notifying the Fall-Back Attribute is Unset

Function name: HandleProfileFallBackAttributeUnsetNotification

Related Procedures: Fall-Back Attribute Management, Fall-Back Attribute Management via SM-DP, Fall-Back Attribute Management via M2M SP

Function group: Profile Management

Notification handler/recipient: Operator or M2M SP

Description:

This function SHALL be called to notify that the Fall-Back Attribute has been unset on the Profile identified by its ICCID on the eUICC identified by its EID.

The SM-SR SHALL send this notification to:

- the Operator owning the Profile, if it has not set an ONC to not receive those notifications
- the M2M SP SP (including, another Operator that is not the owner of the Profile), if the Operator owner of the Profile has granted the M2M SP with a PLMA authorising the operation “HandleProfileFallBackAttributeUnsetNotification”

ICCID may be not enough to identify right address of recipient, the SM-SR should map it internally to Operator or M2M SP notification endpoint.

This notification also conveys the date and time specifying when the operation has been done. In case multiple handlers are served the SM-SR SHOULD ensure completionTimestamp to be equal for every message.

What is performed by the Operator or M2M SP receiving this notification is out of scope of this specification.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
iccid	Identification of the Profile on which the Fall-Back Attribute has been unset. See section 5.1.1.1 for type description.	ICCID	1	M
completionTimestamp	Indication of the date/time when the operation has been performed. See section 5.1.1.1 for type description.	DATETIME	1	M

Table 5523: Handle Profile Fall-Back Attribute Unset Notification Additional Input Data

5.6 ES7 (SM-SR – SM-SR) Interface Description

5.6.1 Create Additional Key Set

Function name: CreateAdditionalKeySet

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider: current SM-SR

Description: This function enables a new SM-SR to request for a new key set to be created in the ISD-R for the eUICC identified by the EID. The new key set belongs the new SM-SR and is unknown to the current SM-SR.

The current SM-SR SHALL map this function onto the second STORE DATA command in the **ES5.EstablishISDRKeySet** (see section 4.1.1.8), using the following rules:

- The order of TLVs SHALL follow the order denoted in Table 44
- The following parameters of this command as defined in Table 42 are not provided by the new SM-SR and it is the current SM-SR's responsibility to set these parameters as defined below.
  - Scenario identifier SHALL be set to '03'
  - Key Usage Qualifier SHALL be set to '10' (3 secure channel keys)
  - Key Access SHALL no be present, meaning a default value of '00' (The key may be used by the Security Domain and any associated Application)
  - Key Type SHALL be set to '88' (AES)
  - Key Length SHALL be set to '10' (16 bytes)
  - Key Identifier SHALL be set to '01'
- The length of `Initial value of sequence counter` SHALL be 0, meaning the sequence counter SHALL have its default value

- The SDIN (tag 45 in Table 44) SHALL be included if and only if the bit b3 of the byte of Parameter for Scenario #3 is set to 1. In this case, the value of this field SHALL be the value of the SDIN of the ISD-R
- The value of other parameters are provided by the new SM-SR.

NOTE This command includes a signature that is computed by the new SM-SR. Structural differences, for example in the order of TLVs, would invalidate the signature as the eUICC would not be able to verify it. The rules above ensure that both SM-SR follow the same structure, and the same values, even for parameters not explicitly supplied by the new SM-SR.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the function has been successfully executed by the function provider as requested by the function caller.
- A ‘Function execution status’ with ‘Expired’ with a status code as defined in section 5.1.6.4
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See 5.1.1.1 for type description.	EID	1	M
keyVersionNumber	The Key Version Number of the to-be-created keyset.	Integer	1	M
initialSequenceCounter	The initial value of the Sequence Counter of the keyset	Integer	1	O (see note 1)
eccKeyLength	The length of the Elliptic Curve Cryptography keys.	Enumeration {ECC-256, ECC-354, ECC-512, ECC-521 }	1	M
scenarioParameter	Scenario parameter as defined in Table 45	Hexadecimal String representation of 1 Byte	1	M
hostId	Host ID as defined in Table 4-17 of the Amendment E of GlobalPlatform 2.2 Card Specification [11]	Hexadecimal String	1	C (see note 2)
ephemeralPublicKey	The ephemeral public key calculated by new SM-SR	Byte[]	1	M
signature	The signature associated to the authenticate SM-SR function. The signature is computed off-card by the new SM-SR SK.SR. ECDSA. See section 4.1.1.8	Hexadecimal String	1	M

Table 203: Create Additional Key Set Additional Input Data

NOTE 1: the input argument initialSequenceCounter is kept for backwards-compatibility of the API, but the rules stated above imply that the current SM-SR SHALL ignore the value provided by the new SM-SR.

NOTE 2: According to Table 44, hostId SHALL only be present in the Second STORE DATA APDU of ISD-R key establishment when the bit b3, of the byte of Parameter for Scenario #3, is set to 1.

Additional output data:

Output data name	Description	Type	No.	MOC
derivationRandom	A random number generated in the SE for additional entropy in the key derivation process	Hexadecimal String	1	C
Receipt	A Message Authentication Code (MAC)	Hexadecimal String	1	M

Table 204: Create Additional Key Set Additional Output Data

NOTE: To avoid subliminal channel attacks, in case the execution Status is Failed or Expired, the SM-SR SHOULD return empty hexadecimal strings for derivation random and Receipt.

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	1.1	Unknown	Indicates that the EID, is unknown to the function provider
8.4	ISD-R	4.2	Execution error	Error during the creation of the key set at the ISD-R level. In that case, the output data “euiccResponseData contains the exact response coming from the eUICC.

Table 205: Create Additional Key Set Specific Status Codes

5.6.2 Handover eUICC Information

Function name: HandoverEUICC

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider: SM-SR

Description: This function enables to request for the handover management of an eUICC represented by its eUICC Information Set (EIS).

The EIS contains the complete set of data including information about Profiles, audit trail, which is applicable for the SM-SR to manage the lifecycle of this eUICC

The function provider SHALL execute the function accordingly to the procedure detailed in section 3.8. The handover is only committed at the end of the successfully procedure

execution. In particular, if one of the operations fails or expires before having verified the receipt, the function provider SHALL return an error (Function execution status indicating 'Failed')

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the Handover eUICC function has been successfully executed on the SM-SR as requested by the function caller.
- A 'Function execution status' with 'Executed-WithWarning' with a status code defined in the table below, indicating either:
  - that the eUICC has been successfully transferred to the new SM-SR, but additional configuration has not completed and may need to be done again. The new SM-SR SHALL perform such operations automatically at a later point in time.
  - or that the eUICC is already managed by the receiving SM-SR (SM-SR2). This may happen when this is the second attempt to perform the SM-SR Change, after the first attempt expired on the old SM-SR (SM-SR1), whereas it was already successful from the point of view of SM-SR2.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 of a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eis	The eUICC Information Set of the eUICC See section 5.1.1.1 for type description. The list of EIS data fields that SHALL be included is defined in Annex E.	EIS	1	M

Table 206: Handover EUICC Additional Input Data

Specific status codes

In addition to the status codes returned by ES7.AuthenticateSMSR and ES7.CreateAdditionalKeyset, this function may return one of the following specific status codes:

Subject code	Subject	Reason code	Reason	Description
1.2	Function Provider	3	Condition Of Use Not satisfied	Indicates that function provider is not capable of managing the eUICC identified by this EID.
1.4	External Resource	1.1	Unknown	One Operator owning a Profile on this eUICC is unknown to or not reachable from the new SM-SR

1.6	Function	4.5	Operation Already Processed	The function is the second attempt to transfer an eUICC to the same new SM-SR, after a previous attempt had already succeeded from the point of view of this SM-SR, whereas it had expired from the point of view of the old SM-SR. In this case the Execution-Status SHALL be 'Executed-WithWarning'.
8.1.1	EID	1.1	Unknown	Indicates that the preparation step hasn't been performed for the eUICC
8.4	ISD-R	4.2	Execution error	Error during the creation of the key set at the ISD-R level. In that case, the output data "euiccResponseData contains the exact response coming from the eUICC.
8.4	ISD-R	4.3	Stopped on Warning	Error during the configuration of ISD-R by SM-SR2, after creating SM-SR2 keyset. This Status Code SHALL only be used when the Function Execution Status' is "Executed_WithWarning"
8.5.2	eUICC Certificate Authority Certificate	6.3	Certificate Expired	ECASD Certificate expired
8.5.1	ECASD Certification Request	6.1	Verification Failed	The verification of the receipt by SM-SR2 failed. SM-SR2 sends the failure message to SM-SR1.

Table 207: Handover eUICC Specific Status Codes

5.6.3 Authenticate SM-SR

Function name: AuthenticateSMSR

Related Procedures: SM-SR Change

Function group: eUICC Management

Function Provider: SM-SR

Description: This function is used to authenticate the new SM-SR to the eUICC identified by the EID. The function will return the random challenge generated by the eUICC to be used to create the signature for the second step in the SM-SR key establishment procedure.

This function may return:

- A 'Function execution status' with 'Executed- Success' indicating that the AuthenticateSMSR function has been successfully executed by the SM-SR as requested by the function caller.
- A 'Function execution status' with 'Expired' with a status code as defined in section 5.1.6.4
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table below.

Additional input data:

Input data name	Description	Type	No.	MOC
eid	Identification of the targeted eUICC. See section 5.1.1.1 for type description.	EID	1	M
smsrCertificate	SM-SR Certificate. The format of this field is a byte array which content corresponds to the full content of tag '7F21' (including the two '7F21' bytes) defined in Table 39	Byte[]	1	M

Table 208: Authenticate SM-SR Additional Input Data

Additional output data:

Output data name	Description	Type	No.	MOC
randomChallenge	The random challenge	Byte[]	1	M

Table 209: Authenticate SM-SR Additional Output Data

NOTE: To avoid subliminal channel attacks, in case the execution Status is Failed or Expired, the SM-SR SHOULD return an empty hexadecimal strings as Random Challenge.

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.1.1	EID	1.1	Unknown	Indicates that the EID, is unknown to the function provider
8.4	ISD-R	4.2	Execution error	Error during the creation of the Random Challenge at the ISD-R level
8.7.1	SM-SR Certificate	6.3	Certificate Expired	SM-SR certificate expired
8.7.1	SM-SR Certificate	6.1	Verification failed	SM-SR certificate signature cannot be verified

Table 210: Authenticate SM-SR Specific Status Codes

Table 211: Void

5.7 ES4A (Operator – SM-SR) Interface Description

5.7.1 Setting M2M -SP Authorisations to Access Profiles

Function name: SetPLMA

Related Procedures: Set Profile Lifecycle Management Authorisations

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator owner of Profiles to grant a PLMA to an M2M SP to perform certain operations, or receive certain notifications, related to a certain subset of the Profiles owned by the Operator.

The SM-SR receiving this request SHALL verify that the mno-id in the PLMA matches the mno-id of the Operator who sends this request.

If the request is acceptable, the SM-SR SHALL record the PLMA.

The new PLMA overwrites the previous PLMA that might have been granted with the same identifiers.

From this point on, any request from the M2M SP on such a Profile, or any notification to the M2M SP related to such a Profile, SHALL be allowed or not based on the new PLMA, as described in sections 5.7.1.1 to 5.7.1.3.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’ indicating that the authorisations have been configured in the SM-SR.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in the table here after, indicating that the authorisations have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator.
- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
plma	The specification of the PLMA, and the criteria on which this PLMA applies. See section 5.1.1.2.14 for type description.	PLMA	1	M

Table 571-A: Set PLMA Additional Input Data

Additional output data:

- None

Specific status codes

Subject	Subject	Reason	Reason	Description

code		code		
8.9	M2M SP	1.1	Unknown	Indicates that the M2M SP to grant authorisations to is unknown to or not connected to this SM-SR
8.2.5	Profile Type	4.9	Unassigned	Indicates that the Profile Type in the PLMA doesn't match the Profile Type of any Profile owned by the Operator identified by its mno-id. The SM-SR MAY support this Status Code. If it does support it, the SM-SR SHALL record the PLMA anyway, and the Execution Status SHALL be Executed-WithWarning
8.2.7	PLMA	3.6	Related Objects Exists	Indicates that the new PLMA has overwritten a former PLMA on the same set of Profile/eUICC for the same M2M SP. In this case the Execution Status SHALL be Executed-WithWarning
8.10	Operator	1.1	Unknown	Indicates that the Operator, addressed by the mno-id in the PLMA, is unknown.

Table 571-B: SetPLMA Specific Status Codes

5.7.1.1 Matching of PLMAs Criteria When Receiving ES4 Requests

When an SM-SR receives a request on ES4 interface (where the client is an Operator or an M2M SP) to perform a Profile Lifecycle Management command targeting a certain Profile, it SHALL verify that the function requester is authorised to perform that operation on that Profile. The verification SHALL include:

- If the ES4 function requester is the Operator owner of the Profile, the authorisation is granted
- If the ES4 function requester is an M2M -SP (including, if the requester is an Operator that is not the owner of the targeted Profile), the SM-SR SHALL:
  - Check that the requested operation is eligible to PLMAs (e.g. updatePolicyRules is not eligible to such an authorisation)
  - Check that there exists a PLMA, that includes:
    - An m2m-sp-id that matches the identifier of the requesting M2M -SP.
    - An mno-id that matches the targeted Profile's mno-id
    - A profileType that matches the targeted Profile's ProfileType, or, if the targeted Profile's Profile Type is missing, an empty profileType
    - An authorisedOperation that matches the Profile Lifecycle Management command name, as listed in section 5.5.16.1.

NOTE Even passing these checks doesn't mean that the request will be accepted and executed, as the SM-SR also performs other checks (e.g. POL2).

NOTE The Profile Type of the targeted Profile can be found in the EIS of the eUICC where this Profile is installed

5.7.1.2 Matching of PLMAs Criteria When Receiving ES3 Requests

When an SM-SR receives a request on ES3 interface (where the client is an SM-DP acting on behalf of an Operator) to perform a Profile Lifecycle Management command targeting a certain Profile, it SHALL verify that the function requester is authorised to perform that operation on that Profile. The verification SHALL include:

- The SM-SR SHALL extract the identity of the Operator that initiated the request to the SM-DP (ES2 requester)

- If this ES2 requester is the Operator owning the target Profile, the authorisation is granted
- If this ES2 requester is an Operator that is not the owner of the targeted Profile, the SM-SR SHALL
  - Check that the requested operation is eligible to PLMAs (e.g. updatePolicyRules is not eligible to such an authorisation)
  - Check that there exists a PLMA, that includes:
    - An m2m-sp-id that matches the identifier of the ES2 requester.
    - An mno-id that matches the targeted Profile's mno-id
    - A profileType that matches the targeted Profile's profileType, or, if the targeted Profile's profileType is missing, an empty profileType
    - An authorisedOperation that matches the Profile Lifecycle Management command name, as listed in section 5.5.16.1

NOTE Even passing these checks doesn't mean that the request will be accepted and executed, as the SM-SR also performs other checks (e.g. POL2).

NOTE The Profile Type of the targeted Profile can be found in the EIS of the eUICC where this Profile is installed

5.7.1.3 Matching of PLMA Criteria Before Sending Notifications

Similarly, after executing an operation that affects a Profile, the SM-SR SHALL verify if a notification recipient is authorised to receive notifications indicating Profile state changes. The verification SHALL include:

- If the notification recipient is the Operator owner of the Profile, the authorisation is granted
- If the notification recipient is an M2M SP (including, if the notification recipient is an Operator that is not the owner of the targeted Profile), the SM-SR SHALL:
  - Check that the requested notification is eligible to PLMA
  - Check that there exists a PLMA, that includes:
    - An m2m-sp-id that matches the identifier of the M2M SP.
    - An mno-id that matches the targeted Profile's mno-id.
    - A profileType that matches the targeted Profile's profileType, or, if the targeted Profile's Profile Type is missing, an empty profileType.
    - An authorisedOperation that matches the notification name, as listed in section 5.5.16.1.

NOTE Even passing these checks doesn't mean that the notification will be sent, as the SM-SR also performs other checks (e.g. check that the Operator has not set an ONC to discard this notifications).

NOTE The Profile Type of the targeted Profile can be found in the EIS of the eUICC where this Profile is installed.

5.7.2 Retrieving M2M SP Authorisations to Access Profiles

Function name: GetPLMA

Related Procedures: Retrieve Profile Lifecycle Management Authorisation by Operator

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator owner of Profiles to retrieve the list of PLMA applicable to a certain Profile, or a certain Profile type, or for a certain M2M SP.

The SM-SR receiving this request SHALL verify that the requester is the owner of the targeted Profile(s), and return the list of all PLMAs applicable to the specified search criteria.

In case the list of PLMAs is very long, the SM-SR MAY truncate the result. The caller can then issue another call to getPLMA with more restrictive criteria.

NOTE The order of the PLMAs returned in the list is implementation-dependant.

This function may return:

- A ‘Function execution status’ with ‘Executed- Success’, and additional output data providing the PLMAs.
- A ‘Function execution status’ with ‘Executed-WIthWarning’, to indicate that the result was truncated, plus additional output data providing part of the list of applicable PLMAs.

Additional input data:

Input data name	Description	Type	No.	MOC
profileType	Identification of the Profile type for which PLMAs are searched	String	1	C
m2m-sp-id	Identification of the M2M SP for which PLMAs are searched	OID	1	C
iccid	Identification of one specific Profile	ICCID	1	C
mno-id	Identification of the Operator owning the Profiles to be matched (this input datum SHALL be present only in case the search criterion is a Profile Type). See section 5.1.1.1 for type description.	OID	1	C

Table 572-A: retrievePLMA Additional Input Data

One and only one of the input data profileType, m2m-sp-id and iccid SHALL be present.

Additional output data:

Output data name	Description	Type	No.	MOC
plma	The list of PLMA that match the search criterion See section 5.1.1.2.14 for type description.	PLMA	N	M

Table 572-B: retrievePLMA Additional Output Data

Specific status codes

Subject code	Subject	Reason code	Reason	Description
1.1	Function requester	1.2	Not Allowed (Authorisation)	Indicates that the Operator or M2M SP which called this function is not doesn't have a PLMA granted that applies to the targeted Profile or Profile type (including, if the targeted Profile or Profile type is unknown to this SM-SR)
8.9	M2M SP	1.1	Unknown	Indicates that the M2M SP specified in the search criterion is unknown to this SM-SR
8.10	Operator	1.1	Unknown	Indicates that the Operator, addressed by the mno-id in the PLMA is unknown.

Table 572-C: getPLMA Specific Status Codes

5.7.3 Setting Operator Configuration to Receive Notifications

Function name: SetONC

Related Procedures: Set Operator Notifications Configuration

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator to configure for which of its own Profiles, associated with a Profile Type, it wants to receive which kind of status change notifications; whatever the origin of the status change is.

The SM-SR receiving this request SHALL verify that the mno-id of the function caller matches with the one in the ONC.

If the request is acceptable, the SM-SR SHALL record the ONC. The new ONC overwrites the previous ONC that might have been granted with the same identifiers.

From this point on, any status change notification, irrespective of the cause and related to a Profile matching these identifiers, SHALL be sent or not based on the new ONC.

This function may return:

- A 'Function execution status' with 'Executed-Success' indicating that the notifications have been configured in the SM-SR.
- A 'Function execution status' with 'Executed-WithWarning' with a specific status code as defined in the table here after, indicating that the notifications have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator.
- A 'Function execution status' indicating 'Failed' with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

NOTE:
If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile

Type, then the Operator will receive all notifications for status changes for its own Profiles, associated with this Profile Type, see also section 3.21 for details.

Additional input data:

Input data name	Description	Type	No.	MOC
onc	The specification of the ONC, and the criterion on which this ONC applies. See section 5.1.1.2.15 for type description.	ONC	1	M

Table 573-A: SetONC Additional Input Data

Additional output data:

- None

Specific status codes

Subject code	Subject	Reason code	Reason	Description
8.2.5	Profile Type	4.9	Unassigned	Indicates that the Profile Type in the ONC doesn't match the Profile Type of any Profile owned by the Operator identified by its mno-id. The SM-SR MAY support this Status Code. If it does support it, the SM-SR SHALL record the ONC anyway, and the Execution Status SHALL be Executed-WithWarning
8.2.8	ONC	3.6	Related Objects Exists	Indicates that the new ONC has overwritten a former ONC on the same identifiers. In this case the Execution Status SHALL be Executed-WithWarning
8.10	Operator	1.1	Unknown	Indicates that the Operator, addressed by the mno-id in the ONC, is unknown.
8.10	Operator	1.2	Not Allowed (Authorisation)	Indicates that the requesting SM-DP is not allowed to configure ONCs for the Operator, addressed by the mno-id in the ONC.

Table 573-B: SetONC Specific Status Codes

5.7.4 Retrieving Operator Notification Configuration

Function name: GetONC

Related Procedures: Retrieve Operator Notifications Configuration

Function group: Profile Management

Function Provider: SM-SR

Description:

This function allows the Operator to retrieve a list of status change notifications it does not want to receive for its own Profiles, associated with a Profile Type.

The SM-SR receiving this request SHALL verify that the mno-id of the function caller matches with the one in the ONC.

If the request is acceptable, the SM-SR SHALLreturn the ONC including the list of requested notifications applicable to the specified search criterion.

This function may return:

- A ‘Function execution status’ with ‘Executed-Success’, and additional output data providing the configured ONC.
- A ‘Function execution status’ with ‘Executed-WithWarning’ with a specific status code as defined in the table below, indicating that the notifications have been configured in the SM-SR but that some side-effects of this configuration may require the attention of the Operator, and additional output data providing the configured ONC.

- A ‘Function execution status’ indicating ‘Failed’ with a status code as defined in section 5.1.6.4 or a specific status code as defined in the table here after.

Additional input data:

Input data name	Description	Type	No.	MOC
profileType	Identification of the Profile Type for which the ONC is searched	String	1	C
iccid	Identification of one specific Profile for which the ONC is searched	ICCID	1	C

Table 574-A: GetONC Additional Input Data

One and only one of the input data profileType and iccid SHALL be present.

Additional output data:

Output data name	Description	Type	No.	MOC
onc	The ONC including the list of discarded notifications that match the search criterion See section 5.1.1.2.15 for type description. NOTE: If no Operator Notification Configuration has yet been set in the SM-SR for a given Profile Type, then the output data of this function will list no notification names, as all notifications will be sent for Profiles assigned with this Profile Type. See also section 3.21.3 and table 511215-A for details.	ONC	N	M

Table 574-B: GetONC Additional Output Data

Annex A Mapping of Functions into Messages (Normative)

This Annex provides the mapping of the functions defined in section 5 into messages to be exchanged between the Roles.

Any technology can be used to transport those messages (mail, file, Web Services…) as soon as it is agreed between the sender and the receiver.

However, for interoperability purpose, Annex B of this specification specifies the particular binding to the Web Service technology, following the OASIS and W3C WS-* standard.

All along this Annex we can indifferently use either “function caller” or “sender entity” wording to designate the entity that has issued the function execution request. It is also the case regarding “function provider” and “receiver entity” to designate the entity that executes the function.

A.1 Namespaces and Schema References

In the context of this specification, a specific set of namespaces is used:

- rpsX: http://namespaces.gsma.org/esim-messaging/X

The “X” at the end of the URI indicates the major version (for example 3 or 4) of this specification.

Note: For backward-compatibility with former versions, version 4 of this specification uses constructs in namespace “/4” but also continues to use constructs defined in the “/3” namespace for operations and types that already existed in v3.

The XML schema defined in this specification refers to the following namespaces:

- xs: Extensible Markup Language (XML) 1.0, W3C Recommendation as defined in [47].
- ds: XML Signature Syntax and Processing (Second Edition), W3C Recommendation as defined in [48].

A.2 Message: <rps3:RPSMessage>

A message in the context of GSMA Embedded UICC Remote Provisioning and Management is composed of a mandatory header and a mandatory body. RPS message types are located in **euicc.root.xsd** file

XML Type	Description
rps3:RPSMessage	Root element of any GSMA Embedded SIM Remote Provisioning and Subscription Management message. Any RPS message is composed of a mandatory header and a mandatory body.

rps3:RPSHeader	Header of the message. Contains mainly information for the transport of the message.
rps3:RPSBody	Contains the core of the message. In the context of this specification, it SHALL be composed of one single element defined within one of the interfaces ES1, ES2, ES3, ES4 and ES7.

Table A2: RPS message types

NOTE: To avoid misleading interpretation of WSA messages, it is recommended to avoid the presence of the characters '#' and '?' in rps3 messages.

A.2.1 Void

A.2.2 Void

A.3 Common Types

A.3.1 Common Message Types

Common request types are located in **euicc.common.request.xsd** file.

XML Type	Description
rps3:BaseRequestType	The base type for a Request types. All requests extend this type.
rps3:BaseResponseType	The base type for a Response types. All responses extend this type.
rps3:BaseNotificationType	The base type for a Notification types. All notifications extend this type.

Table A31: Common Message Types

A.3.2 Void

A.3.3 Void

A.3.4 Simple Types Mapping

Common simple types are located in **euicc.common.types.xsd** file.

Type	XML Type	Description
AID	rps3:AIDType	The AID (Application IDentifier) type defined in section 5.1.1.1 SHALL be mapped to the <rps3:AIDType>. The type is defined as a hexadecimal string representation of 5 to 16 bytes.
Datetime	xs:dateTime	The Datetime type defined in section 5.1.1.1 SHALL be mapped to the simple built-in XML time <xs:datetime>.
EID	rps3:EIDType	The EID (eUICC IDentifier) type defined in section 5.1.1.1 SHALL be mapped to the <rps3:EIDType>. The type is defined as a hexadecimal string representation of 16 bytes.
ICCID	rps3:ICCIDType	The ICCID (Integrated Circuit Card IDentifier) type defined in section 5.1.1.1 SHALL be mapped to the <rps3:ICCIDType>. The type is defined as a string representation (up to 20 digits), non-swapped as per ITU E.118 representation. Example: 893301000000000011
MSISDN	rps3:MSISDNType	The MSIDN (Mobile Station ISDN Number) type defined in section 5.1.1.1 SHALL be mapped to the <rps3:MSISDNType>. The type is defined as a string representation of up to 15 decimal digits as defined in ITU E.164, including Country code, National Destination Code (optional) and Subscriber Number. Example: 380561234567
IMSI	rps3:IMSIType	The IMSI (International Mobile Subscriber Identity) type defined in section 5.1.1.1 SHALL be mapped to the <rps3:IMSIType>. The type is defined as a string representation of up to 15 decimal digits including MCC (3 digits) and MNC (2 or 3 digits), as defined in ITU E.212. Example: 242011234567890
OID	rps3:ObjectIdentifierType	The OID (Object Identifier) type defined in section 5.1.1.1 SHALL be mapped to the <rps3:ObjectIdentifierType>. The type is defined as a string representation of an OID, i.e. of

		integers separated with dots (for example: '1.2', '3.4.5').
TAR	rps3:TARType	The TAR (Toolkit Application reference) type defined in section 5.1.1.1 SHALL be mapped to the <rps3:TARType>. The type is defined as a hexadecimal string representation of exactly 3 bytes. Example: 363443.
Version	rps3:ThreeDigitVersion	The Version type defined in section 5.1.1.1 SHALL be mapped to the <rps3: ThreeDigitVersion>. The type is defined as a string representation of exactly 3 integers separated by a '.'. Example: 1.15.9

Table A34: Common Simple Types

A.3.4.1 Void

A.3.4.2 Void

A.3.4.3 Void

A.3.4.4 Void

A.3.4.5 Void

A.3.4.6 Void

A.3.4.7 Void

A.3.4.8 Void

A.3.4.9 Void

A.3.5 Complex Type Mapping

Common complex types already defined in version 3 of this specification are located in **euicc.common.types.xsd** file.

Type	XML Type	Description
EIS	rps3:EISType	The EIS type defined in section 5.1.1.2.13 SHALL be mapped to the <rps3: EISType>. This type contains the whole information defined for EIS, but depending on the function where it is used, it may be filled with only a partial content.

		All information requiring to be signed by the EUM at registration time is regrouped under the element <rps3:EumSignedInfo>. The signature is provided within the <ds:Signature> element (see section A.10 of this Annex).
Additional Properties	rps3:AdditionalProperties	The <rps3:AdditionalProperties> allows a neutral representation of any data based on a "Key:Value pair" representation. Such representation can be used without breaking the XML validation process.
Eum Signed Info	rps3:EumSignedInfo	The <rps3:EumSignedInfo> element contains all data included in the signature performed by the EUM. All other data of the EIS are not signed.
Profile Info	rps3:ProfileInfo	The <rps3:ProfileInfo> element contains the description of one Profile loaded on the eUICC (the <rps3:Eis> may contain several Profile <rps3:ProfileInfo>). The <rps3:ProfileInfo> maps the PROFILE INFO type defined in section 5.1.1.2.4.
Security Domain	rps3:SecurityDomainType	The <rps3:SecurityDomainType> provides description of a Security Domain and maps the SECURITY-DOMAIN type defined in section 5.1.1.2.9. It is used to contain the information of the ISD-R and ECASD.
Key Set	rps3:KeySet	The <rps3:Keyset> element contains the description of a key set and maps the KEYSET type defined in section 5.1.1.2.8.
Key Type	rps3:KeyType	The <rps3:KeyType> contains the description of a key and maps the KEY type defined in section 5.1.1.2.6.
Key Component	rps3:KeyComponent	The <rps3:KeyComponent> element contains the description of a key component and maps the KEY-COMPONENT type defined in section 5.1.1.2.5.
GP Certificate	rps3:GPCertificateType	The <rps3:GPCertificateType> contains the description of a key and maps the

		CERTIFICATE type. defined in section 5.1.1.2.7.
Audit Trail	rps3:AuditTrail	History of all the platform and Profile Management operations or eUICC notifications related to the eUICC. It contains list of Audit Trail Records.
Audit Trail Record	rps3:AuditTrailRecord	Single record contains eUICC audit information. Defined in section 5.1.1.2.11.
eUICC Capabilities	rps3:EuiccCapablities	The <rps3:EuiccCapabilities> element maps the EUICC-CAPABILITIES data type defined in section 5.1.1.2.10.
POL2	rps3:POL2Type	List of POL2 rules.
POL2 Rule	rps3:POL2RuleType	The <rps3:POL2Type> maps the POL2 data type defined in section 5.1.1.2.3.
Subscription Address	rps3:SubscriptionAddressType	The <rps3:SubscriptionAddressType> maps the SUBSCRIPTION-ADDRESS data type defined in section 5.1.1.2.1.

Table A35: Common Complex Types

Common complex types introduced in version 4 of this specification are located in **rps4.euicc.common.types.xsd** file.

Type	XML Type	Description
PLMA	rps4:PLMAtype	The PLMA type defined in section 5.1.1.2.14 SHALL be mapped to the <rps4:PLMAType>.
ONC	rps4:ONCtype	The ONC type defined in section 5.1.1.2.15 SHALL be mapped to the <rps4:ONCType>.

A.3.5.1 Void

A.3.5.2 Void

A.3.5.3 EUM Signature

Description moved to section A.10

A.3.5.4 Void

A.3.5.5 Void

A.3.5.6 Void

A.3.5.7 Void

A.3.5.8 Void

A.3.5.9 Void

A.4 The ES1 Interface Functions

The table below describe where definition of ES1 functions messages are located in **euicc.request.ES1.xsd** and **rps4.euicc.request.ES1.xsd**.

Interface.Function	XML Type
ES1.RegisterEIS	rps3:ES1-RegisterEISRequest
	rps3:ES1RegisterEISResponse
ES1.UpdateEISAdditionalProperties	rps4: ES1-UpdateEISAdditionalPropertiesRequest
	rps4: ES1-UpdateEISAdditionalPropertiesResponse

Table A4: ES1 Interface Functions

A.4.1 Void

A.5 The ES2 Interface Functions

The table below describe where definition of ES2 functions messages are located in **rps3.euicc.request.ES2.xsd** and **rps4.euicc.request.ES2.xsd**.

Interface.Function	XML Type
ES2.GetEIS	rps3:ES2-GetEISRequest
	rps3:ES2-GetEISResponse
ES2.DownloadProfile	rps3:ES2-DownloadProfileRequest

	rps3:ES2-DownloadProfileResponse
ES2.UpdatePolicyRules	rps3:ES2-UpdatePolicyRulesRequest
	rps3:ES2-UpdatePolicyRulesResponse
ES2.UpdateSubscriptionAddress	rps3:ES2-UpdateSubscriptionAddressRequest
	rps3:ES2-UpdateSubscriptionAddressResponse
ES2.EnableProfile	rps3:ES2-EnableProfileRequest
	rps3:ES2-EnableProfileResponse
ES2.DisableProfile	rps3:ES2-DisableProfileRequest
	rps3:ES2-DisableProfileResponse
ES2.DeleteProfile	rps3:ES2-DeleteProfileRequest
	rps3:ES2-DeleteProfileResponse
ES2.HandleProfileDisabledNotification	rps3:ES2-HandleProfileDisabledNotification
ES2.HandleProfileEnabledNotification	rps3:ES2-HandleProfileEnabledNotification
ES2.HandleSMSRChangeNotification	rps3:ES2-HandleSMSRChangeNotification
ES2.HandleProfileDeletedNotification	rps3:ES2-HandleProfileDeletedNotification
ES2.AuditEis	rps3:ES2-AuditEISRequest
	rps3:ES2-AuditEISResponse
ES2.GetONC	rps4:ES2-GetONCRequest
	rps4:ES2-GetONCResponse
ES2.SetONC	rps4:ES2-SetONCRequest
	rps4:ES2-SetONCResponse
ES2.GetPLMA	rps4:ES2-GetPLMARequest
	rps4:ES2-GetPLMAResponse
ES2.SetPLMA	rps4:ES2-SetPLMARequest
	rps4:ES2-SetPLMAResponse
ES2.HandleProfileDownloadedNotification	rps4:ES2-HandleProfileDownloadedNotification

ES2.HandlePLMAChangedNotification	rps4:ES2-HandlePLMAChangedNotification
ES2.HandlePolicyRulesUpdatedNotification	rps4:ES2-HandlePolicyRulesUpdatedNotification
ES2.SetFallBackAttribute	rps4:ES2-SetFallBackAttributeRequest
	rps4:ES2-SetFallBackAttributeResponse
ES2.SetEmergencyProfileAttribute	rps4:ES2-SetEmergencyProfileAttributeRequest
	rps4:ES2-SetEmergencyProfileAttributeResponse
ES2.HandleEmergencyProfileAttributeSetNotification	rps4:ES2-HandleEmergencyProfileAttributeSetNotification
ES2.HandleEmergencyProfileAttributeUnsetNotification	rps4:ES2-HandleEmergencyProfileAttributeUnsetNotification
ES2.HandleProfileFallBackAttributeSetNotification	rps4:ES2-HandleProfileFallBackAttributeSetNotification
ES2.HandleProfileFallBackAttributeUnsetNotification	rps4:ES2-HandleProfileFallBackAttributeUnsetNotification

Table A5: ES2 Interface Functions

A.5.1 To A.5.12Void

Descriptions moved to table and files referenced by section A.5

A.6 The ES3 Interface Functions

The table below describe where definition of ES3 functions messages are located in **rps3.euicc.request.ES3.xsd** and **rps4.euicc.request.ES3.xsd**.

Interface.Function	XML Type
ES3.GetEIS	rps3:ES3-GetEISRequest
	rps3:ES3-GetEISResponse
ES3.AuditEIS	rps3:ES3-AuditEISRequest
	rps3:ES3-AudtiEISResponse
ES3.CreateISDP	rps3:ES3-CreateISDPRequest
	rps3: ES3-CreateISDPResponse

ES3.SendData	rps3:ES3-SendDataRequest
	rps3:ES3-SendDataResponse
ES3.ProfileDownloadCompleted	rps3:ES3-ProfileDownloadCompletedRequest
	rps3:ES3-ProfileDownloadCompletedResponse
ES3.UpdatePolicyRules	rps3:ES3-UpdatePolicyRulesRequest
	rps3: ES3-UpdatePolicyRulesResponse
ES3.UpdateSubscriptionAddress	rps3:ES3-UpdateSubscriptionAddressRequest
	rps3:ES3-UpdateSubscriptionAddressResponse
ES3.EnableProfile	rps3:ES3-EnableProfileRequest
	rps3:ES3-EnableProfileResponse
ES3.DisableProfile	rps3:ES3-DisableProfileRequest
	rps3:ES3-DisableProfileResponse
ES3.DeleteISDP	rps3:ES3-DeleteISDPRequest
	rps3:ES3-DeleteISDPResponse
ES3.UpdateConnectivityParameters	rps3:ES3- UpdateConnectivityParametersRequest
	rps3:ES3- UpdateConnectivityParametersResponse
ES3.HandleProfileDisabledNotification	rps3:ES3-HandleProfileDisabledNotification
ES3.HandleProfileEnabledNotification	rps3:ES3-HandleProfileEnabledNotification
ES3.HandleSMSRChangeNotification	rps3: ES3-HandleSMSRChangeNotification
ES3.HandleProfileDeletedNotification	rps3: ES3-HandleProfileDeletedNotification
ES3.GetONC	rps4:ES3-GetONCRequest
	rps4:ES3-GetONCResponse
ES3.SetONC	rps4:ES3-SetONCRequest
	rps4:ES3-SetONCResponse
ES3.GetPLMA	rps4:ES3-GetPLMARequest
	rps4:ES3-GetPLMAResponse
ES3.SetPLMA	rps4:ES3-SetPLMARequest

	rps4:ES3-SetPLMAResponse
ES3.HandleProfileDownloadedNotification	rps4:ES3-HandleProfileDownloadedNotification
ES3.HandlePLMAChangedNotification	rps4:ES3-HandlePLMAChangedNotification
ES3.HandlePolicyRulesUpdatedNotification	rps4:ES3-HandlePolicyRulesUpdatedNotification
ES3.SetFallBackAttribute	rps4:ES3-SetFallBackAttributeRequest
	rps4:ES3-SetFallBackAttributeResponse
ES3.SetEmergencyProfileAttribute	rps4:ES3-SetEmergencyProfileAttributeRequest
	rps4:ES3-SetEmergencyProfileAttributeResponse
ES3.HandleEmergencyProfileAttributeSetNotification	rps4:ES3-HandleEmergencyProfileAttributeSetNotification
ES3.HandleEmergencyProfileAttributeUnsetNotification	rps4:ES3-HandleEmergencyProfileAttributeUnsetNotification
ES3.HandleProfileFallBackAttributeSetNotification	rps4:ES3-HandleProfileFallBackAttributeSetNotification
ES3.HandleProfileFallBackAttributeUnsetNotification	rps4:ES3-HandleProfileFallBackAttributeUnsetNotification

Table A6: ES3 Interface functions

A.6.1 to A.615 Void

Descriptions moved to table and files referenced by section A.6

A.7 The ES4 Interface Functions

The table below describe where definition of ES4 functions messages are located in **rps3.euicc.request.ES4.xsd** and **rps4.euicc.request.ES4.xsd**.

Interface.Function	XML Type
ES4.GetEIS	rps3:ES4-GetEISRequest
	rps3:ES4-GetEISResponse
ES4.UpdatePolicyRules	rps3:ES4-UpdatePolicyRulesRequest

	rps3:ES4-UpdatePolicyRulesResponse
ES4.UpdateSubscriptionAddress	rps3:ES4-UpdateSubscriptionAddressRequest
	rps3:ES4-UpdateSubscriptionAddressResponse
ES4.AuditEIS	rps3:ES4-AuditEISRequest
	rps3:ES4-AuditEISResponse
ES4.EnableProfile	rps3:ES4-EnableProfileRequest
	rps3:ES4-EnableProfileResponse
ES4.DisableProfile	rps3:ES4-DisableProfileRequest
	rps3:ES4-DisableProfileResponse
ES4.DeleteProfile	rps3:ES4-DeleteProfileRequest
	rps3:ES4-DeleteProfileResponse
ES4.PrepareSMSRChange	rps3:ES4-PrepareSMSRChangeRequest
	rps3:ES4-PrepareSMSRChangeResponse
ES4.SMSRChange	rps3:ES4-SMSRChangeRequest
	rps3:ES4-SMSRChangeResponse
ES4.HandleProfileDisabledNotification	rps3:ES4-HandleProfileDisabledNotification
ES4.HandleProfileEnabledNotification	rps3:ES4-HandleProfileEnabledNotification
ES4.HandleSMSRChangeNotification	rps3:ES4-HandleSMSRChangeNotification
ES4.HandleProfileDeletedNotification	rps3:ES4-HandleProfileDeletedNotification
ES4.GetPLMA	rps4:ES4-GetPLMARequest
	rps4:ES4-GetPLMAResponse
ES4.HandleProfileDownloadedNotification	rps4:ES4-HandleProfileDownloadedNotification
ES4.HandlePLMAChangedNotification	rps4:ES4-HandlePLMAChangedNotification
ES4.HandlePolicyRulesUpdatedNotification	rps4:ES4-HandlePolicyRulesUpdatedNotification

ES4.HandleEmergencyProfileAttributeSetNotification	rps4:ES4-HandleEmergencyProfileAttributeSetNotification
ES4.HandleEmergencyProfileAttributeUnsetNotification	rps4:ES4-HandleEmergencyProfileAttributeUnsetNotification
ES4.HandleProfileFallBackAttributeSetNotification	rps4:ES4-HandleProfileFallBackAttributeSetNotification
ES4.HandleProfileFallBackAttributeUnsetNotification	rps4:ES4-HandleProfileFallBackAttributeUnsetNotification

Table A7: ES4 Interface functions

A.7.1 to A.7.13Void

Descriptions moved to table and files referenced by section 394A.7

A.8 The ES4A Interface Functions

The table below describes where definition of ES4A functions messages are located in **rps4.euicc.request.ES4A.xsd**.

Interface Function	XML Type
ES4A.GetONC	rps4:ES4A-GetONCRequest
	rps4:ES4A-GetONCResponse
ES4A.SetONC	rps4:ES4A-SetONCRequest
	rps4:ES4A-SetONCResponse
ES4A.GetPLMA	rps4:ES4A-GetPLMARequest
	rps4:ES4A-GetPLMAResponse
ES4A.SetPLMA	rps4:ES4A-SetPLMARequest
	rps4:ES4A-SetPLMAResponse

Table A8: ES4A Interface Functions

A.9 The ES7 Interface Functions

The table below describes where the definition of ES7 functions messages are located in euicc.request.ES7.xsd.

Interface.Function	XML Type	XSD File

ES7.CreateAdditionalKeySet	rps3:ES7-CreateAdditionalKeySetRequest See Notes 1 and 2	euicc.request.ES7.xsd
	rps3:ES7-CreateAdditionalKeySetResponse	
ES7.HandoverEUICC	rps3:ES7-HandoverEUICCRequest	
	rps3:ES7-HandoverEUICCResponse	
ES7.AuthenticateSMSR	rps3:ES7-AuthenticateSMSRRequest	
	rps3:ES7-AuthenticateSMSRResponse	

NOTE1 **ES7.CreateAdditionalKeySet**: Due to backward compatibility reasons, the XML Schema defining this element does not allow to omit the initialSequenceCounter element, nor to give it an empty value. However, whichever value set in this element by the calling SM-SR will be ignored by the SM-SR receiving this command (see NOTE 1 of section 5.6.1). The calling SM-SR SHOULD set a value that is clearly not relevant as an initial sequence counter value (e.g. -1)

NOTE 2 **ES7.CreateAdditionalKeySet:** Due to backward compatibility reasons, the XML Schema defining this element does not allow to omit the hostId element. However, the value set in this element by the calling SM-SR is irrelevant if the scenarioParameter does not specify to use a hostId (see NOTE 2 of section 5.6.1). In this case, the calling SM-SR SHOULD set an empty value (empty string).

A.9.1 to A.8.3 Void

Descriptions moved to table and files referenced by section 394A.9

A.10 EUM Signature

The EUM signature over some information of the EIS is provided within the <rps3:EumSignature> element of type <ds:SignatureType> as defined in XML Signature Syntax and Processing (Second Edition) [26].

The <rps3:EumSignature> SHALL include:

- A <ds:SignedInfo> element specifying:
  - a <ds:CanonicalizationMethod> element;

This specification mandates the support of the following method 'http://www.w3.org/2001/10/xml-exc-c14n#'

- a <ds:SignatureMethod> element; this specification mandates usage of one of the following signature method to have a compliant level of security (RSA and EC key length following recommendation given in section 2.3.3)
  http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
  http://www.w3.org/2001/04/xmldsig-more#rsa-sha384
  http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
  http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
  http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384
  http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512
- a unique <ds:Reference> element
  - with no URI attribute as the signed info applies always only on the whole <rps3:EumSignedInfo> element (so no need to specify it in the instance document);
  - with a digesting method as one of:
    http://www.w3.org/2001/04/xmlenc#sha256
    http://www.w3.org/2001/04/xmldsig-more#sha384
    http://www.w3.org/2001/04/xmlenc#sha512
    - with a <ds:Transforms> transforms element containing one single <ds:Transform> element, to specify the canonicalization method for the reference
      - This specification mandates the support of the following method 'http://www.w3.org/2001/10/xml-exc-c14n#'

- A <ds:KeyInfo> containing a reference to the certificate used to generate the signature. This is achieved by including a <ds:X509Data> element containing either:
  - a <ds:X509SubjectName>, providing the subject value of a certificate that the receiving entity is supposed to have. In this case, it is the responsibility of the EUM to ensure that the Subject of its certificates are sufficiently distinctive to uniquely identify its certificates (for a given eum-id).
  - Or a <ds:X509Certificate>, containing the full certificate definition (including the public key)
- <ds:SignatureValue> element providing the signature value applied on whole <ds:SignedInfo> element, as specified by the W3C, after application of the specified canonicalization, transform and digesting methods as specified within the <ds:SignedInfo> element.

Example of <ds:Signature>:

```
<EumSignature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm=http://www.w3.org/2001/10/xml-exc-c14n#/>
    <ds:SignatureMethod Algorithm=http://www.w3.org/2001/04/xmldsig-more#rsa-sha256/>
    <ds:Reference>
```

```
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm=http://www.w3.org/2001/04/xmlenc#sha256/>
            <ds:DigestValue>dHLkPm5pcyBub3QgYSBzaWduYXR1cmGB</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>dHLkPm5pcyBub3QgYSBzaWduYXR1cmGB</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
            <ds:X509SubjectName>CN=gsma, O=GSMA, C=UK</ds:X509SubjectName>
        </ds:X509Data>
    </ds:KeyInfo>
</ds:Signature>
```

Annex B Binding to SOA Environment (Normative)

This section provides the binding of the messages defined in Annex A into a SOA infrastructure.

Web Services technology, following the OASIS and W3C WS-* standard, is the SOA environment recommended for the deployment of the off-card entities interfaces specified in this document. This technology provides interoperability and loose coupling between the interface provider and the interface consumer, also named respectively as "message receiver" and "message sender", “or “function provider” and “function requester”.

However this specification does not prevent from using another type of technology if it is suitable for a specific deployment. For sure, it implies that both message sender and message receiver uses the same technology and security around matches the level of expectation expressed in this document.

Nevertheless, in case Web Services is used, this section is normative and implementation SHALL comply with the requirements provided in this section.

B.1 General Recommendations

Systems are now highly multi-threaded. It is consequently possible for a function caller to perform massive parallel processing, and thus to call several Web Services in parallel. However, to avoid implementation and integration issues, this specification mandates that Function requester SHALL NOT perform parallel Web Services calls when they are targeting the same eUICC.

Web Services related to the same eUICC SHALL be serialised by the Function requester. For example to avoid key establishment to happen before ISD-P is created. Procedures described in section 3 SHALL be strictly followed regarding the sequence call.

If several Web Service calls are received by the Function provider for the same eUICC, then the Function provider could either:

- Return the following exception: 'Function for the same eUICC is already in process'.
- Or accept the new function execution request, and queue it to be executed after the already accepted function execution requests for this eUICC. This can only be applicable to asynchronous request (see B.2.3.3).

B.2 SOAP Binding

This section provides normative rules defining how to map the GSMA Embedded UICC Remote Provisioning messages (called RPS messages in the rest of section) defined in Annex A to a Web Services implementation, the rules being conditioned by Message Exchange Patterns (MEP), see B.2.3).

This specification mandates usage of SOAP v1.2 as the minimal version and specified in [40].

This section makes use of the following namespaces:

- wsa: the namespace for WS-Addressing message elements as defined in [41]
- wsmc: the namespace for WS-MakeConnection elements as defined in [43]

B.2.1 Message Binding

A RPS message consists of a body and a header (see A.2). This concept maps very well to the concept of SOAP messages that also contains a header and a body.

The binding of the messages defined in Annex A to SOAP SHALL follow the rules defined in this section.

- SOAP Header
  - The information contained in the RPSHeader of the message SHALL be transferred into the SOAP header. See also B.2.1.1
- SOAP Body
  - Only the element contained in the RPSBody structure SHALL be sent into the SOAP Body. It means that:
    The RPSMessage envelope SHALL NOT be sent.
    The full RPSHeader structure SHALL NOT be sent.
    The RPSBody envelope SHALL NOT be sent
  - The SOAP body SHALL contain the rps3:MessageVersion attribute filled with the value of the <rps3:RPSMessage>/<rps3:MessageVersion> attribute.
  - The SOAP body SHALL use pre-defined namespaces prefixes for XML nodes which are used as signature material. Namespace to prefix mapping:
    - `'http://namespaces.gsma.org/esim-messaging/3'` SHALL be mapped to `'rps3'`.
    - `'http://www.w3.org/2000/09/xmldsig#'` SHALL be mapped to `'ds'`.

NOTE: the location of namespace declaration in XML affects the signature computation. The canonicalization method specified in A.3.5.3 ensures the consistent location of the namespace declaration before computation or verification of the signature.

As a consequence one RPS message corresponds to one SOAP message, and it is impossible to send several RPS messages in a single SOAP message.

Note that all information of the RPS message is bound to the SOAP message, so no information is lost during the binding.

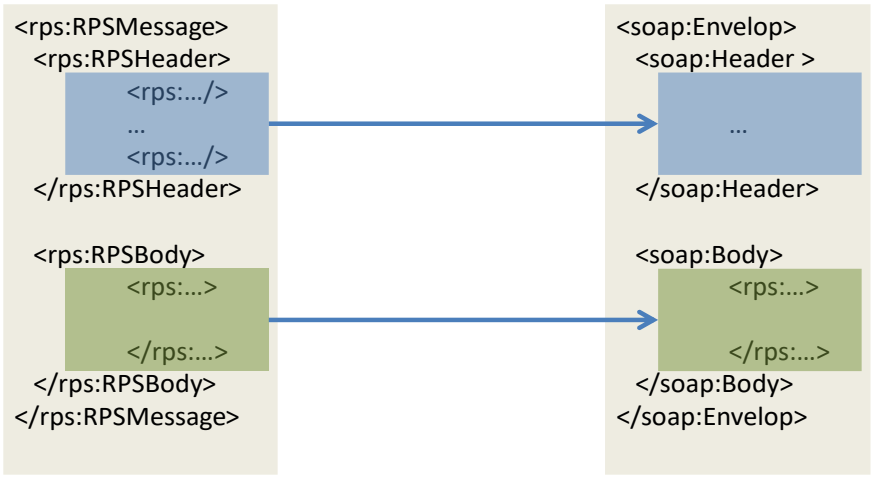


Figure 141: RPS Message Binding

NOTE: Characters '#' and '?' in rps3 message values should not be present.

B.2.1.1 RPS Header Binding to WS-Addressing Elements

This section describes the binding of RPS header into WS-Addressing properties. WS-Addressing properties are described in further detail in [41] and [42]. Only the elements that are used throughout this section are detailed here.

The presence of the characters '#' and '?' SHOULD be avoided in rps3 fields, in order to avoid ambiguity and interoperability problems. These problems could be caused by the presence of these characters in fields that will be encapsulated in a URI. However, if present, those characters SHOULD be escaped as described in RFC 3986 [74] section 2.1.

- `/wsa:From`

This element is defined in WS-Addressing core specifications [41] as:

This OPTIONAL element (of type `wsa:EndpointReferenceType`) provides the value for the [source endpoint] property.

In the context of this specification this element is MANDATORY except in the synchronous response and defines the function requester. It SHALL be filled with:

- The sender URI. This value is not mapped from any value of the RPS Header, but it should be representative of the sender entity.
- A mandatory query parameter "EntityId" containing the `<rps3:SenderEntity>/<rps3:EntityId>` value. Identifies the direct function caller.
- An optional query parameter "EntityName" containing the `<rps3:SenderEntity>/<rps3:EntityName>` value. Names the direct function caller.
- An optional query parameter "UserName" containing the `<rps3:SenderName>`

- A mandatory query parameter "MnoId" only for ES3 request messages containing the `<rps3:MnoId></rps3:MnoId>` value, to identify the Operator which sent the request to the SM-DP via ES2.

Example:

The following content:

```
<rps:SenderEntity>
      <rps:EntityId>1.3.6.1.4.1.11111</rps:EntityId>
      <rps:EntityName>ACompany</rps:EntityName>
</rps:SenderEntity>
<rps:SenderName>aSenderAccountId</rps:SenderName>
<rps3:MnoId>1.3.5.6.1</rps3:MnoId>
```

Would be mapped into:

```
<wsa:From>
      <wsa:Address>http://ACompany.com/RPS?EntityId=1.3.6.1.4.1.11111
?EntityName=ACompany?UserName=aSenderAccountId?MnoId=1.3.5.6.1</wsa:A
ddress>
</wsa:From>
```

- `/wsa:To`

This element is defined in WS-Addressing core specifications [41] as:

This REQUIRED element (of type `xs:anyURI`) provides the value for the [destination] property.

In the context of this specification this element is MANDATORY and defines the function provider. It SHALL be filled with:

- The URL of the web service endpoint to which the message is sent. This value is not mapped from any value of the RPS Header, but it should be representative of the receiving entity.
- An optional query parameter “EntityId” containing the `<rps3:ReceiverEntity>/<rps3:EntityId>` value
- A mandatory query parameter “MnoId” only for ES3 response and notification messages containing the `<rps3:MnoId></rps3:MnoId>` value, to identify the Operator to which the SM-DP SHALL send the response or notification via ES2. The parameter “MnoId” represents:
  - Either the Operator which is owner of the Profile
  - Or the Operator which is an M2M SP and has a PLMA set to receive this notification

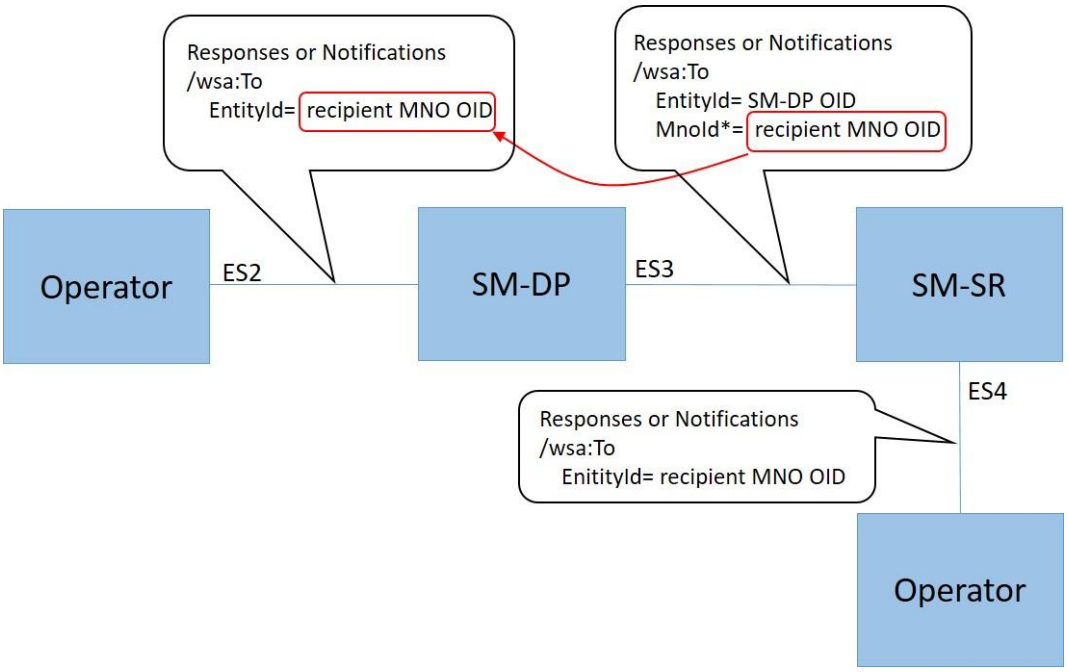


Figure B211-A: MnoId Parameter on ES3 Interface

By mapping the “MnoID”, provided on ES3 interface, into the “EntityId” on the ES2 interface, the SM-DP or any interconnected routing entity can identify the Operator to which the response or notification SHALL be sent.

Example:

The following content:

```
<rps3:ReceiverEntity>
   <rps3:EntityId>1.3.6.1.4.1.22222</rps3:EntityId>
</rps3:ReceiverEntity>
```

Would be mapped into:

```
<wsa:To>http://ACompany.com/SMDP/ES2Services?EntityId=1.3.6.1.4.1.22222<
/wsa:To>
```

- `/wsa:ReplyTo`

This element is defined in WS-Addressing core specifications [41] as:

This OPTIONAL element (of type `wsa:EndpointReferenceType`) provides the value for the [reply endpoint] property. If this element is NOT present, then the value of the [address] property of the [reply endpoint] EPR is "http://www.w3.org/2005/08/addressing/anonymous".

In the context of this specification this element is OPTIONAL. This element SHALL be present only when:

- MEP follows Asynchronous Request-Response with callback and
- When Message sender wants the response to be sent to a specific endpoint

If missing, the response SHALL be sent to (in the preferred order):

- a well-known endpoint mutually agreed between message sender and message receiver
- or to the message originating endpoint.

If present, the /wsa:ReplyTo SHALL be filled with:

- The value set in <rps3:ResponseEndpoint>
- An optional query parameter “EntityId” containing the <rps3:ReceiverEntity>/<rps3:EntityId> value

Example:

The following content:

```
<rps3:ResponseEndpoint>http://ACompany.com/SMDP/ES3Services</rps3:Res
ponseEndpoint>
<rps3:ReceiverEntity>
      <rps3:EntityId>1.3.6.1.4.1.33333</rps3:EntityId>
</rps3:ReceiverEntity>
```

Would be mapped into:

```
<wsa:ReplyTo>
      <wsa:Address>http://ACompany.com/SMDP/ES3Services?EntityId=1.3.
6.1.4.1.33333</wsa:Address>
</wsa:ReplyTo>
```

- `/wsa:MessageID`

This element is defined in WS-Addressing core specifications [41] as:

This OPTIONAL element (whose content is of type `xs:anyURI`) conveys the [message id] property.

In the context of this specification this element is MANDATORY whatever the MEP. This element SHALL be filled with:

- The value set in `<rps3:MessageId>`.

NOTE: Usage of a fragment in `<rps3:MessageId>` should be avoided.

- An optional query parameter “TransactionID” containing the `<rps3:TransactionId>` value. This query parameter SHALL be present only if `<rps3:TransactionId>` is present.
- An optional query parameter “ContextID” containing the `<rps3:ContextId>` value. If this optional query parameter is present, it SHALL be included in any new request generated by the function provider entity for another functional provider entity. This identifier MAY be used to provide end-to-end logging management between the different web services.
- A mandatory query parameter “MessageDate” containing the `<rps3:MessageDate>` value

- A mandatory query parameter "ProfileType" only for notifications messages containing the `<rps3:ProfileType></rps3:ProfileType>` value.

NOTE: This information allows the recipient to route the message based on "ProfileType".

Example:

The following content:

```
<rps3:MessageId>//MySenderDomain/123</rps3:MessageId>
<rps3:TransactionId>MyTansactionID1</rps3:TransactionId>
<rps3:ContextId>MyContextID1</rps3:ContextId>
<rps3:MessageDate>2013-04-18T09:45:00Z</rps3:MessageDate>
<rps3:ProfileType>3G_16K</rps3:ProfileType>
```

Would be mapped into:

```
<wsa:MessageID>//MySenderDomain/123?TransactionId=MyTansactionID1?ContextId
=MyContextID1?MessageDate=2013-04-18T09:45:00Z?ProfileType=3G_16K
</wsa:MessageID>
```

- `/wsa:Action`

This element is defined in WS-Addressing core specifications [41] as:

This REQUIRED element (whose content is of type `xs:anyURI`) conveys the value of the [action] property.

In the context of this specification this element is MANDATORY, and the format of this element SHALL be:

[target namespace] [delimiter][interface name] [delimiter][function group][delimiter][operation name][direction token]

Where:

- [target namespace]: ‘http://gsma.com’
- [interface name]: One of the following label ‘ES1’, ‘ES2’ ‘ES3’, ‘ES4’ ‘ES7’,
- [function group]:
  - For Synchronous Request-Response MEP, for Notification MEP, and for Asynchronous with Polling MEP, the [function group] value SHALL be filled with the name of the functions group (see Table 96 and Table 97). Possible values are:
    eUICCManagement
    ProfileManagement
    PlatformManagement
  - For Asynchronous with callback MEP, the [function group] value SHALL be filled with the name of the functions group appended with the "CallBack" string. Possible values are:
    ProfileManagementCallBack
    PlatformManagementCallBack
    eUICCManagementCallBack

- [Operation name]: the name of the function as contained in the /`rps3:RPSHeader/rps3:MessageType` element
- [direction token] = Follows OASIS WS-* specifications, i.e.:
  - For Synchronous Request-Response MEP: the [direction token] is already part of the [Operation Name] as the "Request" string for the request, and as the "Response" string for the response. So no additional qualifier SHALL be added.
  - For Notification (One-Way MEP): no direction Token (empty string) needs to be added after the [Operation name]
  - For Asynchronous with callback MEP or Asynchronous with Polling: as these MEP are indeed mapped to two one-way service calls, then there is no need to have a direction token, neither for the request, nor for the asynchronous response (empty strings). The ‘Resquest’ and ‘Response’ qualifier SHALL be removed from the [Operation name].
- [delimiter]: “/”

Examples:

- For the ES2 ‘GetEIS’ part of the ‘Profile Management’ function group, the relevant /wsa:Action SHALL be (assumed to be called as a Synchronous Request-Response MEP):
  - For the request:

```
<wsa:Action>http://gsma.com/ES2/ProfileManagement/ES2-GetEISRequest</wsa:Action>
```

  - For the response:

```
<wsa:Action>http://gsma.com/ES2/ProfileManagement/ES2-GetEISResponse</wsa:Action>
```

- For the ES3 ‘HandleProfileDisabledNotification’ part of the ‘Platform Management’ function group, the relevant /wsa:Action SHALL be for the request (no response expected):

```
<wsa:Action>http://gsma.com/ES3/PlatformManagement/ES3-HandleProfileDisabledNotification</wsa:Action>
```

- For the ES3 ‘EnableProfile’ part of the ‘Platform Management’ function group, the relevant /wsa:Action SHALL be (assumed to be called as a Asynchronous Request-Response with callback MEP):
  - For the request:

```
<wsa:Action>http://gsma.com/ES3/PlatformManagement/ES3-EnableProfile</wsa:Action>
```

  - For the response:

```
<wsa:Action>http://gsma.com/ES3/PlatformManagementCallBack/ES3-EnableProfile</wsa:Action>
```

- For the ES3 ‘EnableProfile’ part of the ‘Platform Management’ function group, the relevant /wsa:Action SHALL be (assumed to be called as a Asynchronous with Polling MEP):
  - For the request:

```
      <wsa:Action>http://gsma.com/ES3/PlatformManagement/ES3-
EnableProfile</wsa:Action>
```

- For the response:

```
      <wsa:Action>http://gsma.com/ES3/PlatformManagement/ES3-
EnableProfile</wsa:Action>
```

- `/wsa:FaultTo`

This element is defined in WS-Addressing core specifications [41] as:

This OPTIONAL element (of type wsa:EndpointReferenceType) provides the value for the [fault endpoint] property.

In the context of this specification this element SHALL NOT be used. Any fault SHALL be sent to (in the preferred order):

- The endpoint specified in the /wsa:ReplyTo, if present,
- Else, to a well know endpoint mutually agreed between message sender and message receiver
- Or to the message originating endpoint.

- /wsa:RelatesTo

This element is defined in WS-Addressing core specifications [41] as:

This OPTIONAL (repeating) element information item contributes one abstract [relationship] property value, in the form of an (IRI, IRI) pair. The content of this element (of type `xs:anyURI`) conveys the [message id] of the related message.

In the context of this specification this element is MANDATORY if the message is an asynchronous response. This element SHALL be filled with the value of the `<wsa:MessageID>` of the related request.

Example:

The following content in SOAP request:

```
<wsa:MessageID>//MySenderDomain/123?TransactionId=MyTansactionID1?Contex
tId=MyContextID1?MessageDate=2013-04-18T09:45:00Z</wsa:MessageID>
```

triggers the following determination of <rps3:relatesTo>:

```
<rps:RelatesTo>//MySenderDomain/123</rps:RelatesTo>
```

The `<wsa:RelatesTo>` in the SOAP response SHALL be equal to the `<wsa:MessageID>` of the request:

```
<wsa:RelatesTo>//MySenderDomain/123?TransactionId=MyTansactionID1?Contex
tId=MyContextID1?MessageDate=2013-04-18T09:45:00Z</wsa:RelatesTo>
```

NOTE: There is no direct mapping from `<rps3:RelatesTo>` to `<wsa:RelatesTo>`. The `<wsa:RelatesTo>` SHALL be equal to `<wsa:MessageId>` from the request, while `<rps3:RelatesTo>` is only a subset of `<wsa:RelatesTo>`.

A function requester receiving a SOAP response from a function provider compliant with a version v3.2 or earlier of the current specification, SHOULD be ready to handle a <wsa:RelatesTo> value that is not equal to the value of the <wsa:MessageID> of the SOAP request.
A function provider sending a SOAP response to a function requester compliant with a version v3.2 or earlier of the current specification, MAY return a <wsa:RelatesTo> value that is not equal to the value of the <wsa:MessageID> of the SOAP request.

NOTE: Versions v3.2 and earlier derived from WS-Addressing specification [41], and stated that the <wsa:RelatesTo> was equal to the <rps3:relatesTo>, and consequently, equal to the <rps3:messageId> of the corresponding request, but different from the <wsa:MessageID> of the corresponding request.

B.2.1.2 Use of WS-MakeConnection

WS-MakeConnection SHALL be used in asynchronous scenarios when the receiving party of a request cannot initiate a connection to the sending party (due to network security constraints for example). In this scenario, the sending party SHALL poll for a processed request using WS-MakeConnection [43]. This scenario is described in the Message Exchange Pattern: Asynchronous with Polling (Annex B-Section 2.3.3).

All the following elements are described in further detail in WS-MakeConnection [43], only the elements that are used throughout this document are detailed here.

To indicate to the Function provider that the Function requester is not addressable and will use Asynchronous with polling MEP (see B.2.3.3), the /wsa:ReplyTo header element SHALL indicate one of the two anonymous URL:

- The WS-Addressing anonymous URL ‘http://www.w3.org/2005/08/addressing/anonymous’. This SHALL allow the function requester to poll for the first response message available for the function requester
- The WS-MakeConnection anonymous URL ‘http://docs.oasis-open.org/ws-rx/wsmc/200702/anonymous?id=<value of <wsa:MessageId>’. This SHALL allow the Function requester to poll for the response for this specific message.

By using one of the two above anonymous /wsa:ReplyTo URL constructs, the Function provider knows that ‘Asynchronous with Polling’ mode is requested and SHALL answer with HTTP 202 (ACCEPT), see B.2.3.3.

To get a Function execution response, The Function provider SHALL send a new SOAP message with the /wsmc:MakeConnection element in the body; this new message establishes

a contextualised back-channel for the transmission of the message response according to matching criteria (defined below).

In the context of this specification, the SOAP message allowing getting a function execution response message SHALL contain:

In the Header:

- `/wsa:Action` element with the specific value 'http://docs.oasis-open.org/ws-rx/wsmc/200702/MakeConnection'

In the body:

- `/wmc:MakeConnection` element with a sub element /`wsmc:Address` containing one of the anonymous URI defined here above and identifying the initiating endpoint contained in the /wsa:ReplyTo element of the original function execution request. Function provider SHALL NOT return message response in the HTTP response unless they have been addressed to this URI.
  - If the Function provider has not any response ready for the Function requester it SHALL answer with an empty response and HTTP 202 (ACCEPT)
  - If the Function provider has a response ready it SHALL return the response and use HTTP response code 200 (OK)

B.2.1.3 RPS Body Binding and signature

At least the RPS Body elements which are used for signature computation or verification (for example rps3:EumSignedInfo and ds:SignedInfo) SHALL have whitespaces between XML nodes trimmed (i.e. remove leading and trailing whitespaces).

Example :

1) EUM Signature before trimming :

```
<EumSignature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
 <ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm=http://www.w3.org/2001/10/xml-exc-c14n#/>
  <ds:SignatureMethod Algorithm=http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256/>
  <ds:Reference>
   <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
   </ds:Transforms>
   <ds:DigestMethod Algorithm=http://www.w3.org/2001/04/xmlenc#sha256/>
   <ds:DigestValue>dHLkPm5pcyBub3QgYSBzaWduYXR1cmGB</ds:DigestValue>
  </ds:Reference>
 </ds:SignedInfo>
 <ds:SignatureValue>dHLkPm5pcyBub3QgYSBzaWduYXR1cmGB</ds:SignatureValue>
 <ds:KeyInfo>
  <ds:X509Data>
   <ds:X509SubjectName>CN=gsma, O=GSMA, C=UK</ds:X509SubjectName>
  </ds:X509Data>
 </ds:KeyInfo>
</ds:Signature>
```

2) EUM Signature after trimming (on one line):

```
<EumSignature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:C
anonicalizationMethod Algorithm=http://www.w3.org/2001/10/xml-exc-c14n#/><ds:Sig
natureMethod Algorithm=http://www.w3.org/2001/04/xmldsig-more#rsa-sha256/><ds:Re
ference><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-ex
c-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm=http://www.w3.org/2001/04/x
mlenc#sha256/><ds:DigestValue>dHLkPm5pcyBub3QgYSBzaWduYXR1cmGB</ds:DigestValue><
/ds:Reference></ds:SignedInfo><ds:SignatureValue>dHLkPm5pcyBub3QgYSBzaWduYXR1cmG
B</ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:X509SubjectName>CN=gsma, O=GSM
A, C=UK</ds:X509SubjectName></ds:X509Data></ds:KeyInfo></ds:Signature>
```

NOTE All examples in this specification are not trimmed, for better readability.

B.2.2 Security

To secure the messages being sent between Function requester and Function provider, one of the two following mechanisms SHALL be used:

- Relying on mutual authenticated transport level security (Transport Layer Security, TLS)
- Relying on transport level security (TLS) with only server side authentication and WS-Security standards

This specification mandates usage of TLS v 1.2 defined in RFC 5246 [15] to allow appropriate algorithm and key length as defined in section 2.4.1.

B.2.2.1 Secure Channel Set-Up

The process of setting up secure channel is out of scope of this document. This process includes the exchange of the following information:

- Function requester and Function provider OIDs SHALL be registered and respective values have been communicated to each party
- Function requester and Function provider URL SHALL have been communicated to each party
- Function requester and Function provider SHALL agree on the MEP for response handling of asynchronous function: Asynchronous Request-Response with callback or Asynchronous with polling.
- Function requester and Function provider SHALL agree on the type of security mechanism used and respective credential:
  - WS-Security
    If UsernameToken Profile is used, the Username and Password SHALL be setup at receiving entities.
    If X509 Certificate Token Profile is used, the receiving entity SHALL trust the sending entity issued certificate.
  - Transport Level Security
    Function requester and Function provider party trust must have been established on a X509 certificate chain basis.

- Function requester and Function provider SHALL agree on the WSDL, which SHALL consist in the WSDL specified in section B.4, with the addition of the <Policy> elements implied by the the WS-Security if any, and complying with the WS-Security elements specified in section B.2.2.2

NOTE: Receiving entity and sending entity could either be the Function requester of the Function provider.

B.2.2.2 Identification/Authentication/Authorisation

Authentication of the sending party of a SOAP message SHALL rely on either the Transport layer security (using TLS certificate of the sending party) or the WS-Security [44]. In this latter case the SOAP message SHALL include specific WS-Security elements containing a security token, UserNameToken or X509Token as agreed during secure channel set-up (see 2.3.1).

Message receiver SHALL be able to process Web Service Security tokens as specified in the OASIS specification [44], specifically:

- UsernameToken Profile 1.1. as defined in [45]. Example:

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="...">
      <S11:Header>
          …
             <wsse:Security>
                   <wsse:UsernameToken>
                         <wsse:Username>ACompany</wsse:Username>
                         <wsse:Password>MyPassword</wsse:Password>
                   </wsse:UsernameToken>
                   …
             </wsse:Security>
    ….
```

- X509 Certificate Token Profile 1.1. as defined in [46], with '#X509v3' token type. The X509 certificate of the sender SHALL be included as a BinarySecurityToken. In order to prove that the sender owns the corresponding private key, the SOAP message SHALL then include a <ds:Signature> with the following properties:
  - A <ds:SignedInfo> element in context of WS-Security X.509 certificate token profile specifying:
    - a canonicalization method,
      This specification mandates the support of the following method
      'http://www.w3.org/2001/10/xml-exc-c14n#'
    - a signature method; this specification mandates usage of one of the following signature method to have a compliant level of security (RSA and EC key length following recommendation given in section 2.3.3)
      http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
      http://www.w3.org/2001/04/xmldsig-more#rsa-sha384
      http://www.w3.org/2001/04/xmldsig-more#rsa-sha512

http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512

- at least one <ds:Reference> element pointing to the BinarySecurityToken (see note); and with a digesting method as one of:
  http://www.w3.org/2001/04/xmlenc#sha256
  http://www.w3.org/2001/04/xmldsig-more#sha384
  http://www.w3.org/2001/04/xmlenc#sha512
  - including a <ds:Transforms> element with a <ds:Transform> element to specify the canonicalization method for the reference.
    This specification mandates the support of the following method 'http://www.w3.org/2001/10/xml-exc-c14n#'

NOTE Including the X.509 token in the signature is recommended by Oasis' Web Services Security: SOAP Message Security 1.1 [44], to protects against certificate substitution attacks.

Example:

```
<S11:Envelope xmlns:S11="...">
      <S11:Header>
            …
            <wsse:Security xmlns:wsse="..." xmlns:wsu="..." >
                  <wsse:BinarySecurityToken ValueType="…#X509v3"
                        EncodingType="…#Base64Binary" wsu:Id="binarytoken">
                        MIIEZzCCA9CgAwIBAgIQEmtJZc0…
                  </wsse:BinarySecurityToken>
                                    <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:SignedInfo>
                              <ds:CanonicalizationMethod
Algorithm=http://www.w3.org/2001/10/xml-exc-c14n#/>
                              <ds:SignatureMethod
Algorithm=http://www.w3.org/2001/04/xmldsig-more#rsa-sha256/>
                              <ds:Reference URI="#binarytoken">
                                    <ds:Transforms>
                                          <ds:Transform Algorithm="http://w
ww.w3.org/2001/10/xml-exc-c14n#" />
                                    </ds:Transforms>
                                    <ds:DigestMethod
Algorithm=http://www.w3.org/2001/04/xmlenc#sha256/>
                                    <ds:DigestValue>dHLk..</ds:DigestValue>
                              </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>HFLP…</ds:SignatureValue>
```

```
                    <ds:KeyInfo>
                          <wsse:SecurityTokenReference>
                                <wsse:Reference URI="#binarytoken" />
                          </wsse:SecurityTokenReference>
                    </ds:KeyInfo>
              </ds:Signature>
        </wsse:Security>
        …
```

B.2.2.3 Integrity

The integrity of the message SHALL exclusively rely on the transport level security (TLS).

B.2.2.4 Confidentiality

The confidentiality of the message SHALL exclusively rely on the transport level security (TLS).

B.2.3 Message Exchange Pattern (MEPs) – HTTPS Binding

B.2.3.1 MEP: Synchronous Request-Response

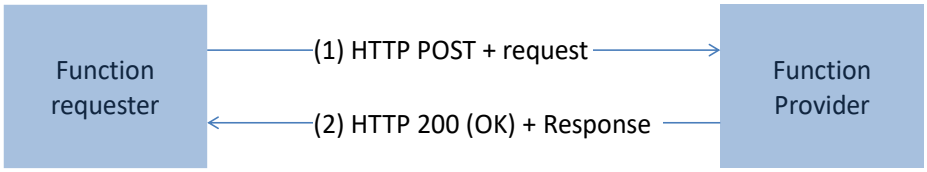


Figure 142: MEP: Synchronous Request-Response

(1) The SOAP header of the message sent in a HTTP POST from Function requester to Function provider SHALL contain:

`/wsa:From` (REQUIRED)

`/wsa:To` (REQUIRED)

`/wsa:MessageID` (REQUIRED)

`/wsa:Action` (REQUIRED)

(2) The response to the message is on the HTTP(s) return channel with code 200 (OK) and the SOAP header SHALL contain:

`/wsa:From` (OPTIONAL)

`/wsa:To` (REQUIRED)

`/wsa:MessageID` (REQUIRED)

`/wsa:Action` (REQUIRED)

B.2.3.2 MEP: Asynchronous Request-Response With Callback

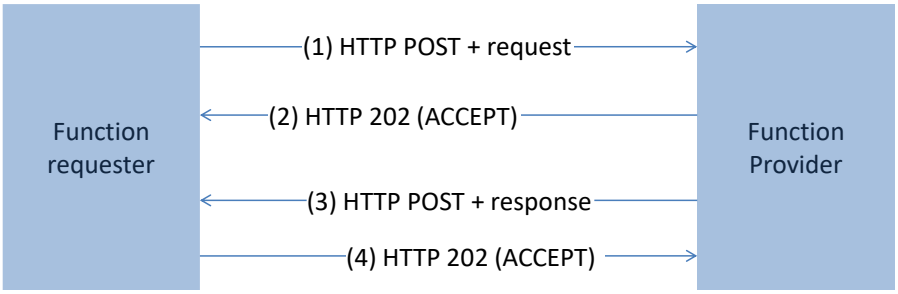


Figure 143: MEP: Asynchronous Request-Response With Callback

(1) The SOAP header of the message sent in a HTTP POST from Function requester to Function provider SHALL contain:

`/wsa:From` (REQUIRED)

`/wsa:To` (REQUIRED)

`/wsa:ReplyTo` (OPTIONAL)

`/wsa:MessageID` (REQUIRED)

`/wsa:Action` (REQUIRED)

(2) The Function requester SHALL be able to handle 202 (ACCEPT) HTTP response codes.

NOTE: In case the response is 200 (OK) steps (3) and (4) will be skipped if it is not a new session.

(3) The response to the message is sent in a HTTP POST from Function provider to Function requester, and the SOAP header SHALL contain:

`/wsa:From` (REQUIRED)

`/wsa:To` (REQUIRED)

`/wsa:MessageID` (REQUIRED)

`/wsa:Action` (REQUIRED)

`/wsa:RelatesTo` (Value of <wsa:MessageId> of the original message to which this is the response) (REQUIRED)

(4) Function requester SHALL reply with a HTTP 202 (ACCEPT).

B.2.3.3 MEP: Asynchronous With Polling

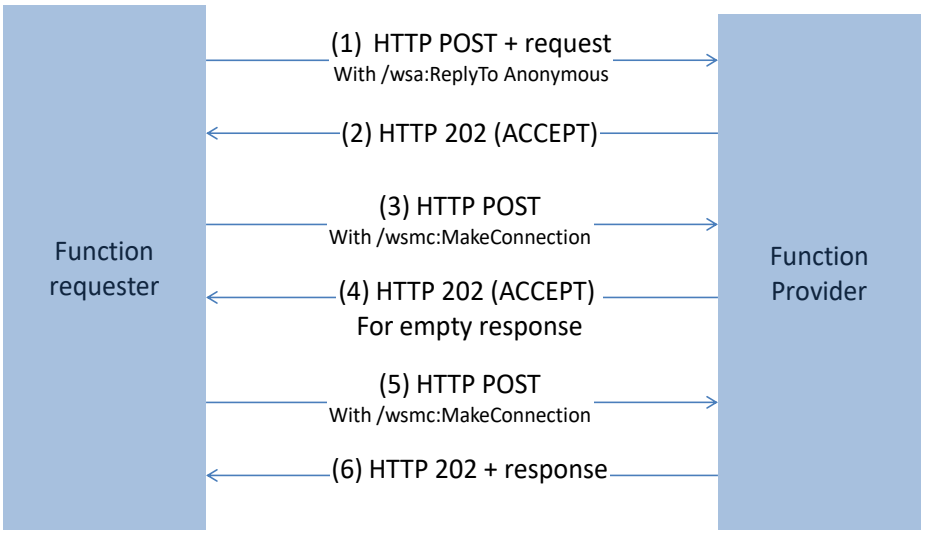


Figure 144: MEP: Asynchronous With Polling

(1) The SOAP header of the message sent in a HTTP POST from Function requester to Function provider SHALL contain:

`/wsa:From` (REQUIRED)

`/wsa:To` (REQUIRED)

`/wsa:ReplyTo` (REQUIRED) containing one of the two possible anonymous URL (see Annex B-Section 2.1.2)

`/wsa:MessageID` (REQUIRED)

`/wsa:Action` (REQUIRED)

(2) Function provider SHALL reply with a HTTP 202 (ACCEPT). (3 or 5) Function provider makes a WS-MakeConnection call as defined in Annex B-Section 2.1.2 with a header containing:

```
<wsa:Action>http://docs.oasis-open.org/ws-rx/wsmc/200702/MakeConnection<wsa:Action>
```

And a body containing:

```
<wsmc:MakeConnection ...>
    <wsmc:Address>AnonymousURL (same value as /wsa:ReplyTo above)</wsmc:Address>
</wsmc:MakeConnection>
```

(4 or 6) The response to the message is sent in a HTTP response from Function provider to Function requester, and the SOAP header SHALL contain:

`/wsa:From` (REQUIRED)

`/wsa:To` (REQUIRED)

`/wsa:MessageID` (REQUIRED)

`/wsa:Action` (REQUIRED)

`/wsa:RelatesTo` (Value of <wsa:MessageId> of the original message to which this is the response) (REQUIRED)

B.2.3.4 MEP: Notification (One-Way)

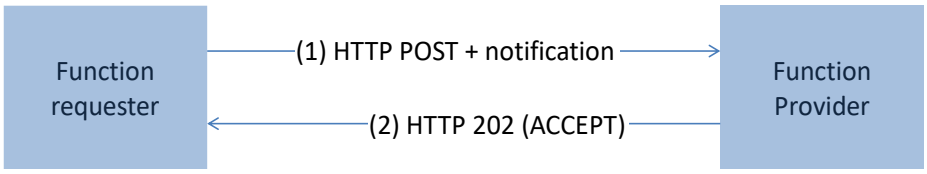


Figure 145: MEP: Synchronous Request-Response

(1) The SOAP header of the message sent in a HTTP POST from Function requester to Function provider SHALL contain:

`/wsa:From` (REQUIRED)

`/wsa:To` (REQUIRED)

`/wsa:MessageID` (REQUIRED)

`/wsa:Action` (REQUIRED)

(2) The response to the message is on the HTTP return channel with code 202 (ACCEPT) and with an empty body.

B.2.4 Binding Examples

B.2.4.1 Binding of a Message for ES4.EnableProfile Function Request

The xml hereunder illustrates an RPS message for requesting the execution of the **ES4.EnableProfile** function:

```
<?xml version="1.0" encoding="UTF-8"?>
<RPSMessage xmlns="http://namespaces.gsma.org/esim-messaging/1"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    MessageVersion="1.0.0">
```

```
    <RPSHeader>
        <SenderEntity>
            <EntityId>1.3.6.1.4.1.111111</EntityId><!-- Sample OID  -->
            <EntityName>ACompany</EntityName>
        </SenderEntity>
        <SenderName>aSenderAccountId</SenderName>
        <ReceiverEntity>
            <EntityId>1.3.6.1.4.1.222222</EntityId><!-- Sample OID -->
        </ReceiverEntity>

<ResponseEndpoint>http://ACompany.com/RPS/MyEndPoint</ResponseEndpoint>
        <TransactionId>MyTransID1</TransactionId>
        <MessageId>//MySenderDomain/123</MessageId>
        <MessageType>ES4-EnableProfileRequest</MessageType>
        <MessageDate>2013-04-18T09:30:47Z</MessageDate>
    </RPSHeader>
    <RPSBody>
        <ES4-EnableProfileRequest>
            <FunctionCallIdentifier>callId:1</FunctionCallIdentifier>
            <ValidityPeriod>3600</ValidityPeriod>
            <Eid>89001012012341234012345678901224</Eid>
            <ICCID>89330100000000000001</ICCID>
        </ES4-EnableProfileRequest>
    </RPSBody>
</RPSMessage>
```

In the case where:

- security is set with TLS, with mutual authentication based on certificate
- the MEP is : Asynchronous Request-Response with callback

This function execution request is bound to the following SOAP message:

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope               xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
    xmlns:rps3="http://namespaces.gsma.org/esim-messaging/3">
    <s:Header>
        <wsa:From>

<wsa:Address>http://ACompany.com/RPS?EntityId=1.3.6.1.4.1.111111?EntityName
=ACompany?UserName=aSenderAccountID</wsa:Address>
        </wsa:From>
```

```
<wsa:To>http://AnotherCompany.com?EntityId=1.3.6.1.4.1.222222</wsa:To>

<wsa:MessageID>//MySenderDomain/123?TransactionId=MyTransID1?MessageDate=20
13-04-18T09:30:47Z</wsa:MessageID>
        <wsa:Action>http://gsma.com/ES4/ProfileManagement/ES4-
EnableProfile</wsa:Action>
        <wsa:ReplyTo>
            <wsa:Address>http://ACompany.com/RPS/MyEndPoint</wsa:Address>
        </wsa:ReplyTo>
    </s:Header>
    <s:Body rps3:MessageVersion="1.0.0">
        <rps3:ES4-EnableProfileRequest>

<rps3:FunctionCallIdentifier>callID:1</rps3:FunctionCallIdentifier>
            <rps3:ValidityPeriod>3600</rps3:ValidityPeriod>
            <rps3:Eid>89001012012341234012345678901224</rps3:Eid>
            <rps3:ICCID>89330100000000000001</rps3:ICCID>
        </rps3:ES4-EnableProfileRequest>
    </s:Body>
</s:Envelope>
```

B.2.4.2 Binding of a Message for ES4.EnableProfile Function Response

The xml hereunder illustrates a possible message response for the **ES4.EnableProfile** function execution request illustrated in the example of the previous section 2.2.1:

```
<?xml version="1.0" encoding="UTF-8"?>
<RPSMessage xmlns="http://namespaces.gsma.org/esim-messaging/1"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    MessageVersion="1.0.0">

    <RPSHeader>
        <SenderEntity>
            <EntityId>1.3.6.1.4.1.222222</EntityId><!-- Sample OID  -->
        </SenderEntity>
        <SenderName>AnotherSenderAccountId</SenderName>
        <ReceiverEntity>
            <EntityId>1.3.6.1.4.1.111111</EntityId><!-- Sample OID -->
        </ReceiverEntity>
        <TransactionId>MyTransID1</TransactionId>
        <MessageId>//MyProviderDomain/99</MessageId>
```

```
        <MessageType>ES4-EnableProfileResponse</MessageType>
        <RelatesTo>//MySenderDomain/123</RelatesTo>
        <MessageDate>2013-04-18T09:45:00Z</MessageDate>
    </RPSHeader>
    <RPSBody>
        <ES4-EnableProfileResponse>
            <FunctionExecutionStatus>
                <Status>EXECUTED_SUCCESS</Status>
            </FunctionExecutionStatus>
        </ES4-EnableProfileResponse>
    </RPSBody>
</RPSMessage>
```

In the context described in the example of the previous section 2.2.1, the function execution response is bound to the following SOAP message:

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:rps3="http://namespaces.gsma.org/esim-messaging/1">
  <s:Header>
    <wsa:From>
<wsa:Address>http://AnotherCompany.com/RPS?EntityId=1.3.6.1.4.1.222222?User
Name=AnotherSenderAccountId</wsa:Address>
    </wsa:From>
    <wsa:To>http://AnotherCompany.com?EntityId=1.3.6.1.4.1.111111</wsa:To>
    <wsa:MessageID>
//MyProviderDomain/99?TransactionId=MyTransID1?MessageDate=2013-04-
18T09:45:00Z</wsa:MessageID>
    <wsa:Action>http://gsma.com/ES4/PlatformManagement/ES4-
EnableProfile</wsa:Action>
    <wsa:RelatesTo>
//MySenderDomain/123?TransactionId=MyTransID1?MessageDate=2013-04-
18T09:30:47Z //MySenderDomain/123
    </wsa:RelatesTo><!-- Matching request in section B.2.4.1 -->
  </s:Header>
  <s:Body rps3:MessageVersion="1.0.0">
    <rps3:ES4-EnableProfileResponse>
      <rps3:FunctionExecutionStatus>
        <rps3:Status>EXECUTED_SUCCESS</rps3:Status>
      </rps3:FunctionExecutionStatus>
    </rps3:ES4-EnableProfileResponse>
  </s:Body>
</s:Envelope>
```

B.2.5 URI – query structure

The URI specification [65] treats the query part as being unstructured. The following rules SHALL be applied for query in URI:

- The query is composed of a series of field key-value pairs.
- Within each pair, the field key and the value are separated by an equals sign, "=".
- The series of pairs is separated by a questionmark, "?".

Examples:

```
http://ACompany.com/RPS?EntityId=1.3.6.1.4.1.11111?EntityName=ACompany?User
Name=aSenderAccountId
```

where

```
EntityId=1.3.6.1.4.1.11111?EntityName=ACompany?UserName=aSenderAccountId
```

represents the whole query and `EntityName=ACompany` is one field name-value pair.

B.3 Function Binding

NOTE: In the tables below the Asynchronous Request-Response with Callback MEP can be replaced by an Asynchronous Request-Response with Polling MEP. In this case the /wsa:Action value has to be updated accordingly.

B.3.1 ES1

Function name	Binding Information	
RegisterEIS	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES1/eUICCManagement/ES1-RegisterEISRequest
	/wsa:Action Response	http://gsma.com/ES1/eUICCManagement/ES1-RegisterEISResponse
UpdateEISAdditionalProperties	**Binding Information**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES1/eUICCManagement/ES1-UpdateEISAdditionalPropertiesRequest
	/wsa:Action Response	http://gsma.com/ES1/eUICCManagement/ES1-UpdateEISAdditionalPropertiesResponse

Table 227: ES1 Function Binding

B.3.2 ES2

Function name	Binding Information	
GetEIS	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES2/DataPreparation/ES2-GetEISRequest
	/wsa:Action Response	http://gsma.com/ES2/DataPreparation/ES2-GetEISResponse
DownloadProfile	**MEP**	Asynchronous Request-Response with CallBack

	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-DownloadProfile
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagementCallback/ES2-DownloadProfile
UpdatePolicyRules	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-UpdatePolicyRulesRequest
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagement/ES2-UpdatePolicyRulesResponse
UpdateSubscriptionAddress	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-UpdateSubscriptionAddressRequest
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagement/ES2-UpdateSubscriptionAddressResponse
EnableProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES2/PlatformManagement/ES2-EnableProfile
	/wsa:Action Response	http://gsma.com/ES2/PlatformManagementCallback/ES2-EnableProfile
DisableProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES2/PlatformManagement/ES2-DisableProfile
	/wsa:Action Response	http://gsma.com/ES2/PlatformManagementCallback/ES2-DisableProfile
DeleteProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES2/PlatformManagement/ES2-DeleteProfile
	/wsa:Action Response	http://gsma.com/ES2/PlatformManagementCallback/ES2-DeleteProfile
HandleProfileDisabledNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/PlatformManagement/ES2-HandleProfileDisabledNotification
	/wsa:Action Response	(none)
HandleProfileEnabledNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/PlatformManagement/ES2-HandleProfileEnabledNotification
	/wsa:Action Response	(none)

HandleSMSRChangeNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/PlatformManagement/ES2-HandleSMSRChangeNotification
	/wsa:Action Response	(none)
HandleProfileDeletedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/PlatformManagement/ES2-HandleProfileDeletedNotification
	/wsa:Action Response	(none)
AuditEIS	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-AuditEIS
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagementCallBack/ES2-AuditEIS
SetFallBackAttribute	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-SetFallBackAttribute
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagementCallBack/ES2-SetFallBackAttribute
HandleProfileFallBackAttributeSetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-HandleProfileFallBackAttributeSetNotification
	/wsa:Action Response	(none)
HandleProfileFallBackAttributeUnsetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-HandleProfileFallBackAttributeUnsetNotification
	/wsa:Action Response	(none)
SetEmergencyProfileAttribute	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-SetEmergencyProfileAttribute
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagementCallBack/ES2-SetEmergencyProfileAttribute
HandleEmergencyProfileAttributeSetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-HandleEmergencyProfileAttributeSetNotification
	/wsa:Action Response	(none)
HandleEmergencyProfileAttributeUnsetNotification	**MEP**	Notification (One-Way)

	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-HandleEmergencyProfileAttributeunSetNotification
	/wsa:Action Response	(none)
GetONC	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-GetONCRequest
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagement/ES2-GetONCResponse
SetONC	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-SetONCRequest
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagement/ES2-SetONCResponse
GetPLMA	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-GetPLMARequest
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagement/ES2-GetPLMAResponse
SetPLMA	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-SetPLMARequest
	/wsa:Action Response	http://gsma.com/ES2/ProfileManagement/ES2-SetPLMAResponse
HandleProfileDownloadedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-HandleProfileDownloadedNotification
	/wsa:Action Response	(none)
HandlePLMAChangedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-HandlePLMAChangedNotification
	/wsa:Action Response	(none)
HandlePolicyRulesUpdatedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES2-HandlePolicyRulesUpdatedNotification
	/wsa:Action	(none)

	Response	

Table 228: ES2 Function Binding

B.3.3 ES3

Function name	Binding Information	
GetEIS	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-GetEISRequest
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-GetEISResponse
AuditEIS	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-AuditEIS
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagementCallBack/ES3-AuditEIS
CreateISDP	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-CreateISDP
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagemenCallBack/ES3-CreateISDP
SendData	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-SendData
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagementCallBack/ES3-SendData
ProfileDownloadCompleted	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-ProfileDownloadedCompletedRequest
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-ProfileDownloadedCompletedResponse
UpdatePolicyRules	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-UpdatePolicyRulesRequest
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-UpdatePolicyRulesResponse
UpdateSubscriptionAddress	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-UpdateSubscriptionAddressRequest

	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-UpdateSubscriptionAddressResponse
EnableProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-EnableProfile
	/wsa:Action Response	http://gsma.com/ES3/PlatformManagementCallBack/ES3-EnableProfile
DisableProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-DisableProfile
	/wsa:Action Response	http://gsma.com/ES3/PlatformManagementCallBack/ES3-DisableProfile
DeleteISDP	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-DeleteISDP
	/wsa:Action Response	http://gsma.com/ES3/PlatformManagementCallBack/ES3-DeleteISDP
UpdateConnectivityParameters	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-UpdateConnectivityParameters
	/wsa:Action Response	http://gsma.com/ES3/PlatformManagementCallBack/ES3-UpdateConnectivityParameters
HandleProfileDisabledNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-HandleProfileDisabledNotification
	/wsa:Action Response	(none)
HandleProfileEnabledNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-HandleProfileEnabledNotification
	/wsa:Action Response	(none)
HandleSMSRChangeNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-HandleSMSRChangeNotification
	/wsa:Action Response	(none)
HandleProfileDeletedNotification	**MEP**	Notification (One-Way)

	/wsa:Action Request	http://gsma.com/ES3/PlatformManagement/ES3-HandleProfileDeletedNotification
	/wsa:Action Response	(none)
SetFallBackAttribute	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-SetFallBackAttribute
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagementCallBack/ES3-SetFallBackAttribute
HandleProfileFallBackAttributeSetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-HandleProfileFallBackAttributeSetNotification
	/wsa:Action Response	(none)
HandleProfileFallBackAttributeUnsetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES2/ProfileManagement/ES3-HandleProfileFallBackAttributeUnsetNotification
	/wsa:Action Response	(none)
SetEmergencyProfileAttribute	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-SetEmergencyProfileAttribute
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagementCallBack/ES3-SetEmergencyProfileAttribute
HandleEmergencyProfileAttributeSetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-HandleEmergencyProfileAttributeSetNotification
	/wsa:Action Response	(none)
HandleEmergencyProfileAttributeUnsetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-HandleEmergencyProfileAttributeUnsetNotification
	/wsa:Action Response	(none)
GetONC	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-GetONCRequest
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-GetONCResponse
SetONC	**MEP**	Synchronous Request-Response

	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-SetONCRequest
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-SetONCResponse
GetPLMA	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-GetPLMARequest
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-GetPLMAResponse
SetPLMA	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES3-SetPLMARequest
	/wsa:Action Response	http://gsma.com/ES3/ProfileManagement/ES3-SetPLMAResponse
HandleProfileDownloadedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES2-HandleProfileDownloadedNotification
	/wsa:Action Response	(none)
HandlePLMAChangedNotification	**/wsa:Action Response**	(none)
	MEP	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES2-HandlePLMAChangedNotification
HandlePolicyRulesUpdatedNotification	**/wsa:Action Response**	(none)
	MEP	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES3/ProfileManagement/ES2-HandlePolicyRulesUpdatedNotification

Table 229: ES3 Function Binding

B.3.4 ES4

Function name	Binding Information	
GetEIS	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-GetEISRequest

	/wsa:Action Response	http://gsma.com/ES4/ProfileManagement/ES4-GetEISResponse
UpdatePolicyRules	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-UpdatePolicyRulesRequest
	/wsa:Action Response	http://gsma.com/ES4/ProfileManagement/ES4-UpdatePolicyRulesResponse
UpdateSubscriptionAddress	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-UpdateSubscriptionAddressRequest
	/wsa:Action Response	http://gsma.com/ES4/ProfileManagement/ES4-UpdateSubscriptionAddressResponse
AuditEIS	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-AuditEIS
	/wsa:Action Response	http://gsma.com/ES4/ProfileManagementCallBack/ES4-AuditEIS
EnableProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/PlatformManagement/ES4-EnableProfile
	/wsa:Action Response	http://gsma.com/ES4/PlatformManagementCallBack/ES4-EnableProfile
DisableProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/PlatformManagement/ES4-DisableProfile
	/wsa:Action Response	http://gsma.com/ES4/PlatformManagementCallBack/ES4-DisableProfile
DeleteProfile	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/PlatformManagement/ES4-DeleteProfile
	/wsa:Action Response	http://gsma.com/ES4/PlatformManagementCallBack/ES4-DeleteProfile
PrepareSMSRChange	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/eUICCManagement/ES4-PrepareSMSRChange
	/wsa:Action Response	http://gsma.com/ES4/eUICCManagementCallBack/ES4-PrepareSMSRChange

SMSRChange	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/eUICCManagement/ES4-SMSRChange
	/wsa:Action Response	http://gsma.com/ES4/eUICCManagementCallBack/ES4-SMSRChange
HandleProfileDisabledNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/PlatformManagement/ES4-HandleProfileDisabledNotification
	/wsa:Action Response	(none)
HandleProfileEnabledNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/PlatformManagement/ES4-HandleProfileEnabledNotification
	/wsa:Action Response	(none)
HandleSMSRChangeNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/eUICCManagement/ES4-HandleSMSRChangeNotification
	/wsa:Action Response	(none)
HandleProfileDeletedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/PlatformManagement/ES4-HandleProfileDeletedNotification
	/wsa:Action Response	(none)
SetFallBackAttribute	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-SetFallBackAttribute
	/wsa:Action Response	http://gsma.com/ES4/ProfileManagementCallBack/ES4-SetFallBackAttribute
HandleProfileFallBackAttributeSetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-HandleProfileFallBackAttributeSetNotification

	/wsa:Action Response	(none)
HandleProfileFallBackAttributeUnset Notification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-HandleProfileFallBackAttributeUnsetNotification
	/wsa:Action Response	(none)
SetEmergencyProfileAttribute	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-SetEmergencyProfileAttribute
	/wsa:Action Response	http://gsma.com/ES4/ProfileManagementCallBack/ES4-SetEmergencyProfileAttribute
HandleEmergencyProfileAttributeSet Notification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-HandleEmergencyProfileAttributeSetNotification
	/wsa:Action Response	(none)
HandleEmergencyProfileAttributeUnsetNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-HandleEmergencyProfileAttributeUnsetNotification
	/wsa:Action Response	(none)
GetPLMA	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES4-GetPLMARequest
	/wsa:Action Response	http://gsma.com/ES4/ProfileManagement/ES4-GetPLMAResponse

HandleProfileDownloadedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES2-HandleProfileDownloadedNotification
	/wsa:Action Response	(none)
HandlePLMAChangedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES2-HandlePLMAChangedNotification
	/wsa:Action Response	(none)
HandlePolicyRulesUpdatedNotification	**MEP**	Notification (One-Way)
	/wsa:Action Request	http://gsma.com/ES4/ProfileManagement/ES2-HandlePolicyRulesUpdatedNotification
	/wsa:Action Response	(none)

Table 230: ES4 Functions Binding

B.3.5 ES7

Function name	Binding Information	
CreateAdditionalKeySet	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES7/eUICCManagement/ES7-CreateAdditionalKeySet
	/wsa:Action Response	http://gsma.com/ES7/eUICCManagementCallBack/ES7-CreateAdditionalKeySet
HandoverEUICC	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES7/eUICCManagement/ES7-HandoverEUICC
	/wsa:Action Response	http://gsma.com/ES7/eUICCManagementCallBack/ES7-HandoverEUICC
AuthenticateSMSR	**MEP**	Asynchronous Request-Response with CallBack
	/wsa:Action Request	http://gsma.com/ES7/eUICCManagement/ES7-AuthenticateSMSR
	/wsa:Action Response	http://gsma.com/ES7/eUICCManagementCallBack/ES7-AuthenticateSMSR

Table 231: ES7 Function Binding

B.3.6 ES4A

Function name	Binding Information	
GetONC	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4A/ProfileManagement/ES4A-GetONCRequest
	/wsa:Action Response	http://gsma.com/ES4A/ProfileManagement/ES4A-GetONCResponse
SetONC	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4A/ProfileManagement/ES4A-SetONCRequest
	/wsa:Action Response	http://gsma.com/ES4A/ProfileManagement/ES4A-SetONCResponse
GetPLMA	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4A/ProfileManagement/ES4A-GetPLMARequest
	/wsa:Action Response	http://gsma.com/ES4A/ProfileManagement/ES4A-GetPLMAResponse
SetPLMA	**MEP**	Synchronous Request-Response
	/wsa:Action Request	http://gsma.com/ES4A/ProfileManagement/ES4A-SetPLMARequest
	/wsa:Action Response	http://gsma.com/ES4A/ProfileManagement/ES4A-SetPLMAResponse

Table B37: ES4A Functions Binding

B.4 Web Service Description Language (WSDL)

The **Web Services Description Language** (**WSDL**) is an XML-based interface definition language that is used for describing the functionality offered by a web service. It provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns.

WSDL files are provided within the SGP.02 v4.0 WSDL.ZIP package.

This package is composed of the following WSDL files:

- ES1_SMSR.wsdl
- ES2_MNO.wsdl
- ES2_SMDP.wsdl
- ES3_SMDP.wsdl
- ES3_SMSR.wsdl
- ES4_MNO.wsdl

- ES4_SMSR.wsdl
- ES4A_SMSR.wsdl
- ES7_SMSR_Provider.wsdl
- ES7_SMSR_Requester.wsdl

These WDSL files reference XML schemafiles (.xsd), which are also provided within the SGP.02 v4.0 WSDL.ZIP package.

These WSDL files define a version of Web Services API that does not leverage WS-Security. In case the Function requester and Function provider agree on using WS-Security, the WSDL files SHALL be modified by the addition of elements specifying the WS-Security options agreed as per section B.2.2.

Annex C Use of GlobalPlatform Privileges (Normative)

GlobalPlatform defines the following privileges:

Privilege Number	Privilege	Description
0	Security Domain	Application is a Security Domain.
1	DAP Verification	Application is capable of verifying a DAP; Security Domain privilege SHALL also be set.
2	Delegated Management	Application is capable of Delegated Card Content Management: Security Domain privilege SHALL also be set.
3	Card Lock	Application has the privilege to lock the card.
4	Card Terminate	Application has the privilege to terminate the card.
5	Card Reset	Application has the privilege to modify historical bytes on one or more card interfaces. This privilege was previously labelled "Default Selected".
6	CVM Management	Application has the privilege to manage a shared CVM of a CVM Application.
7	Mandated DAP Verification	Application is capable of and requires the verification of a DAP for all load operations: Security Domain privilege and DAP Verification privilege SHALL also be set.
8	Trusted Path	Application is a Trusted Path for inter-application communication.
9	Authorized Management	Application is capable of Card Content Management; Security Domain privilege SHALL also be set.
10	Token Verification	Application is capable of verifying a token for Delegated Card Content Management.
11	Global Delete	Application may delete any Card Content.
12	Global Lock	Application may lock or unlock any Application.
13	Global Registry	Application may access any entry in the GlobalPlatform Registry.

14	Final Application	The only Application accessible in card Life Cycle State CARD_LOCKED and TERMINATED.
15	Global Service	Application provides services to other Applications on the card.
16	Receipt Generation	Application is capable of generating a receipt for Delegated Card Content Management.
17	Ciphered Load File Data Block	The Security Domain requires that the Load File being associated to it is to be loaded ciphered.
18	Contactless Activation	Application is capable of activating and deactivating other Applications on the contactless interface.
19	Contactless Self-Activation	Application is capable of activating itself on the contactless interface without a prior request to the Application with the Contactless Activation privilege.

Table 232: GlobalPlatform Privileges

Privileges description in an eUICC:

The following rules apply for an eUICC with at least one Profile installed.

Security Domain Privilege:

GlobalPlatform Card Specification [6] states: “This privilege distinguishes a Security Domain from a 'normal' Application.”

DAP Verification Privilege:

GlobalPlatform Card Specification [6] states: “An application provider may require that their Application code to be loaded on the card SHALL be checked for integrity and authenticity. The DAP Verification privilege provides this service on behalf of an Application provider.”

Delegated Management:

GlobalPlatform Card Specification [6] states: “The privilege allows an Application Provider to manage Card Content with authorisation.” A “Security Domain having the Token Verification privilege controls such authorisation.”

Card Lock:

GlobalPlatform Card Specification [6] states: “This privilege allows an Application to set the card life cycle state to CARD_LOCKED.”

On the eUICC, the Card Lock privilege is not applicable and SHALL NOT be assigned to any security domain/Application. The equivalent mechanism of disabling a Profile SHALL be used.

Card Terminate:

GlobalPlatform Card Specification [6] states: “This privilege allows an Application to set the card life cycle state to TERMINATED.”

On the eUICC, the Card Terminate privilege is not applicable and SHALL NOT be assigned to any security domain/Application. The equivalent mechanism of deleting a Profile SHALL be used.

Card Reset:

GlobalPlatform Card Specification [6] states: “An Application installed or made selectable with the Card Reset privilege and no Implicit Selection parameter is registered in the GlobalPlatform Registry as the implicitly selectable Application on the Basic Logical Channel for all card I/O interfaces supported by the card if no other Application (other than the Issuer Security Domain) is already registered as implicitly selectable on the Basic Logical Channel of any card I/O interface”.

This privilege is relevant only when the Profile is enabled. Therefore, several Applications may have this privilege on the eUICC, but this privilege SHALL be unique within a Profile.

If the Application inside a Profile with the Card Reset privilege is deleted the privilege is reassigned to the corresponding MNO-SD.

CVM Management:

GlobalPlatform Card Specification [6] states: “The CVM Application, if present on a card, provides a mechanism for a Cardholder Verification Method (CVM), including velocity checking, that may be used by all Applications on the card”.

If an Application in a Profile has this privilege, it SHALL be relevant only when the Profile is enabled. In that case, several Applications in the Profile may have this privilege, but the corresponding CVM identifiers SHALL be unique within a Profile.

Mandated DAP Verification:

GlobalPlatform Card Specification [6] states: “A Controlling Authority may require that all Application code to be loaded onto the card SHALL be checked for integrity and authenticity. The Mandated DAP Verification privilege of the Controlling Authority's Security Domain detailed in this Specification provides this service on behalf of the Controlling Authority”.

If a Security Domain in a Profile has this privilege, it SHALL be relevant only when the Profile is enabled.

The DAP verification is mandated only when loading an Application inside the Profile.

Trusted Path:

GlobalPlatform Card Specification [6] states: "The 'Trusted Path' privilege qualifies an Application as a Receiving Entity. Each Application present on the card playing the Role of a

Receiving Entity SHALL: Enforce the Issuer's security rules for inter-application communication; Ensure that incoming messages are properly provided unaltered to the Trusted Framework; Ensure that any response messages are properly returned unaltered to the off-card entity".

Authorised Management:

GlobalPlatform Card Specification [6] states: "Having a Security Domain with this privilege allows a Security Domain provider to perform Card Content management without authorisation (i.e. a token) in the case where the off-card entity is authenticated as the owner (Security Domain Provider) of the Security Domain".

Token Verification:

GlobalPlatform Card Specification [6] states: "This privilege allows a Security Domain Provider, to authorize any Card Content management operation".

This privilege SHALL be set to MNO-SD, if the Delegated Management privilege is used in the Profile.

Global Delete:

GlobalPlatform Card Specification [6] states: "This privilege provides the capability to remove any Executable Load File or Application from the card even if the Executable Load File or Application does not belong to this Security Domain".

For MNO-SD and Applications inside a Profile, this privilege SHALL only allow deletion of Applications in the corresponding Profile.

Global Lock:

GlobalPlatform Card Specification [6] states: "This privilege provides the right to initiate the locking and unlocking of any Application on the card, independent of its Security Domain Association and hierarchy. It also provides the capability to restrict the Card Content Management functionality of OPEN".

For MNO-SD and Applications inside a Profile, this privilege SHALL only allow locking of Applications in the corresponding Profile.

Global Registry:

GlobalPlatform Card Specification [6] states: "The search is limited to the Executable Load Files, Applications and Security Domains that are directly or indirectly associated with the eUICC entity receiving the command. When the eUICC entity receiving the command has the Global Registry privilege, the search applies to all Executable Load Files, Applications and Security Domains registered in the GlobalPlatform Registry".

For ISD-P and Applications inside a Profile, this privilege SHALL only allow looking for Applications in the corresponding Profile.

Final Application:

GlobalPlatform Card Specification [6] states: “If a Security Domain has the Final Application privilege only the GET DATA command SHALL be processed, all other commands defined in this specification SHALL be disabled and SHALL return an error”.

On the eUICC, the Final Application privilege is not applicable and SHALL NOT be assigned to any security domain/Application.

Global Service:

GlobalPlatform Card Specification [6] states: “One or more Global Services Applications may be present on the card to provide services to other Applications on the card.

The MNO-SD or Applications inside a Profile with the Global Service privilege SHALL offer service only when the Profile is enabled. Therefore, it is possible to have several Applications registered on the same service in the same eUICC.

Receipt Generation:

GlobalPlatform Card Specification [6] states: “This privilege allows a Security Domain Provider, typically the Card Issuer, to provide a confirmation for the performed card content management. A Security Domain with Receipt Generation privilege requires the knowledge of keys and algorithms used for Receipts generation”.

This privilege SHALL be set to MNO-SD, if the Delegated Management privilege is used in the Profile.

Ciphered Load File Data Block:

GlobalPlatform Card Specification [6] states: “This privilege allows a Security Domain Provider to require that the Load File Data Block being associated to it SHALL be ciphered”.

Contactless Activation:

GlobalPlatform Card Specification [6] states: “The Contactless Activation privilege identifies the CRS Application. This Privilege allows:

- The Activation/Deactivation of Applications on the Contactless Interface
- The update of the Selection Priority
  - Manage the Volatile Priority
  - Reorder the GlobalPlatform Registry
- Notification by the OPEN when:

- An Application is INSTALLED, LOCKED, unlocked or deleted
- The availability state of an Application is changed between NON_ACTIVATABLE, ACTIVATED, or DEACTIVATED.
- One of the Application's contactless registry parameters is updated".

If an Application in a Profile has this privilege, it SHALL be relevant only when the Profile is enabled. In that case, several Applications may have this privilege on the card, but this privilege SHALL be unique within a Profile.

Contactless Self-Activation:

GlobalPlatform Card Specification [6] states: "The Contactless Self-Activation Privilege allows an Application to activate itself without a prior request to the CRS Application".

If an Application in a Profile has this privilege, it SHALL be relevant only when the Profile is enabled.

Privilege Number	Privilege	ISD-R	ISD-P	MNO-SD	Applications inside a Profile	ECASD
0	Security Domain	√	√	√		√
1	DAP Verification					
2	Delegated Management					
3	Card Lock					
4	Card Terminate					
5	Card Reset					
6	CVM Management			√ **		
7	Mandated DAP Verification					
8	Trusted Path	√	√	√		
9	Authorized Management		√ *	√		
10	Token Verification			√ ***		
11	Global Delete			√ **		
12	Global Lock			√ **		
13	Global Registry			√ **		
14	Final Application					
15	Global Service					√
16	Receipt Generation			√ ***		

17	Ciphered Load File Data Block				
18	Contactless Activation				
19	Contactless Self-Activation				

Table 233: GlobalPlatform Application Privileges

A tick (√) denotes the presence of the indicated privilege and its assignment to the Security Domain or Application.

A blank cell denotes that the assignment of the privilege is managed by the owner of the Application (according to GlobalPlatform Card Specification [6]) of the Security Domain.

A black cell denotes that the privilege cannot be assigned.

* Authorized Management privilege is only set when ISD-P is in CREATED state to allow Profile Download and Installation.

** These privileges are mandatory for cards compliant to GlobalPlatform Card Specification UICC Configuration [7].

*** These privileges are mandatory for cards compliant to GlobalPlatform Card Specification UICC Configuration [7], if the Delegated Management privilege is used in the Profile.

Annex D Data Definitions (Normative)

- Coding of the IMEI

The value of IMEI SHALL be directly copied from Terminal Response of the Provide Local Information command (see ETSI TS 102 223 [3] and ETSI TS 124 008[20]).

Annex E EIS Usage in Functions (Normative)

This table gives additional information on the EIS usage depending on the function:

- Column ‘EUM Signed’: ‘X’ indicates if the data is part of the signature computed by the EUM at the initial registration time.
- Other columns:
  - An ‘M’, ‘O’, ‘C’, indicates that the data is,respectively, Mandatory, Optional, Conditional, and that the entity processing the EIS SHALL be ready to receive the data
  - An empty cell indicates that the data SHALL NOT be provided

Data name	EUM Signed	ES1.RegisterEIS	ES2.GetEIS ES2.AuditEISES2.HandleSMSRChangeN	ES3.GetEIS ES3.AuditEIS ES3.HandleSMSRChangeNotification	ES4.GetEIS ES4.AuditEIS ES4.HandleSMSRChangeNotification	ES7.HandloverEUICC
eid	X	M	M	M	M	M
eum-id	X	M	M	M	M	M
productionDate	X	M	M	M	M	M
platformType	X	M	M	M	M	M
platformVersion	X	M	M	M	M	M
remainingMemory		M	M	M	M	M
Availablememoryforprofiles		M	M	M	M	M
lastAuditDate			C	C	C	C
smsr-id		M	M	M	M	M
isd-p-loadfile-aid	X	M	M	M	M	M
isd-p-module-aid	X	M	M	M	M	M
Profiles		M(1)	O(3)	O(3bis)	M(3)	M
Iccid		M	M	M	M	M
isd-p-aid		M	M	M	M	M
mno-id		M	M	M	M	M
fallbackAttribute		M	M	M	M	M
subscriptionAddress		M	M	M	M	M
State		M	M	M	M	M
smdp-id		O	C	C	C	C

Data name	EUM Signed	ES1.RegisterEIS	ES2.GetEIS ES2.AuditEISES2.HandleSMSRChangeN	ES3.GetEIS ES3.AuditEIS ES3.HandleSMSRChangeNotification	ES4.GetEIS ES4.AuditEIS ES4.HandleSMSRChangeNotification	ES7.HandoverEUICC
ProfileType		O	O	O	O	O
allocatedMemory		M	M	M	M	M
freeMemory		C	C	C	C	C
pol2		M	M	M	M	M
ISD-R		M(2)	C(4)(7)	M(4)	C(4)(7)	M(4bis)
ECASD	X	M(2)	M(2)	M	M	M(4)
eUICC-Capabilities	X	M	M	M	M	M
audit trail						M
signatureAlgorithm	X	M	M	M	M	M
signature		M(5)	M(5)	M(5)	M(5)	M(5)
AdditionalProperty		O	C(6)	C(6)	C(6)	C(6)

Table 234: EIS Usage

NOTE 1: The initial EIS comes with the information of the Profile(s) loaded and installed by the EUM during the manufacturing.

NOTE 2: The initial EIS comes with the definition of the two Security Domains ISD-R and ECASD.

NOTE 3: The EIS SHALL only contain the information of the Profiles owned by the requesting Operator

NOTE 3bis: The EIS SHALL only contain the information of the Profiles owned by an Operator that has authorised the requesting SM-DP to see its Profiles.

NOTE 4: The EIS SHALL contain all Security Domains definition with Key Sets that only contain mandatory values on ISD-R..

NOTE 4bis: The EIS SHALL contain all Security Domain definition of the ISD-R, including the description of the keysets used by the current SM-SR, without the key values; the KVN/Key identifiers SHALL be provided in the EIS, but the key values SHALL be provided as empty hexadecimal strings. This allows the SM-SR2 to know which keys are already present, and which KVN/Key identifiers are available to add new keys.

NOTE 5: The EIS is signed using the private key of the EUM (see Figure 8).

NOTE 6: The EIS SHALL contain:

- Any AdditionalProperty defined in ES1.RegisterEIS and whose name does not start with “gsma.ESIM.ES1”.
- Any AdditionalProperty added or updated by the SM-SR during the life of the eUICC.

NOTE 7: *Deprecated element,* it SHOULD be used only for backward compatibility to GSMA 3.1 specification. *Deprecated element* means that it will be removed in next specification release, so service caller or service provider SHOULD NOT rely on it.

Annex F Key Check Values (Normative)

All key check values that have to be computed in the context of this specification SHALL follow the recommendation of GlobalPlatform Card Specification [6] section B5 and GlobalPlatform Card Specification Amendment B [8] section 3.8. Extract:

“For a DES key, the key check value is computed by encrypting 8 bytes, each with value '00', with the key to be checked and retaining the 3 highest-order bytes of the encrypted result.”

“For a AES key, the key check value is computed by encrypting 16 bytes, each with value '01', with the key to be checked and retaining the 3 highest-order bytes of the encrypted result.”

“A key check value SHALL be computed as the three most significant bytes of the SHA-1 digest of the PSK TLS Key”.

Annex G Device Requirements (Normative)

Functional Device Requirements	Requirement

No.	

DEV1	For connectivity the Device SHALL support:
	• At least one of the network access technologies defined by 3GPP in the non-exhaustive following list:
	  ○ GERAN,
	  ○ UTRAN
	  ○ E-UTRAN.
	• UDP over IP [32] (subject to the right support of access network technology)
	• TCP over IP [33] (subject to the right support of access network technology)

DEV2	For Network connection control the Device SHALL support: • RPLMN details (LAC/TAC, NMR). • QoS (failures, duration, power, location). • SMS management. • New network selection after SIM/USIM update.
DEV3	For reporting to a server the Device SHALL support: • SMS-PP MO as defined in [3] and SMS-PP MO as defined [39] or [29] BIP as defined in DEV4 The Device SHOULD support: • USSD

DEV4	For Profile and Platform Management the Device SHALL support:
	• SMS-PP MT as defined in [3], and SMS-PP MT as defined [39] or [29]
	• BIP (subject to the support of the right network access technology) as defined in [3] including support of commands:
	  ○ OPEN CHANNEL (UDP and TCP over IP)
	  ○ CLOSE CHANNEL
	  ○ RECEIVE DATA
	  ○ SEND DATA
	  ○ GET CHANNEL STATUS
	  ○ ENVELOPE (EVENT DOWNLOAD - Data available)
	  ○ ENVELOPE (EVENT DOWNLOAD – Channel status)

DEV5	The Device SHALL contain a unique IMEI (International Mobile Equipment Identity) value compliant with the format defined in ETSI TS 123 003 [31]. The value of IMEI SHALL be directly copied from TERMINAL RESPONSE of the Provide Local Information command (see ETSI TS 102 223 [3] and ETSI TS 124 008[20]).
DEV6	• The Device SHALL support, as a minimum, the following set of commands (in addition to BIP commands) as defined in ETSI TS 102 223 [3] and 3GPP TS 31.111 [27]. Basic SAT commands (TERMINAL PROFILE, FETCH, TERMINAL RESPONSE) • PROVIDE LOCAL INFORMATION (location information, IMEI, NMR, date and time, access technology, at least)

	• SEND SHORT MESSAGE • POLL INTERVAL, POLLING OFF, TIMER MANAGEMENT [at least one timer], ENVELOPE (TIMER EXPIRATION) • SET UP EVENT LIST and ENVELOPE (EVENT DOWNLOAD – location status, call connected, call disconnected, Access Technology Changed, Network Rejection) • ENVELOPE (SMS-PP DOWNLOAD) • REFRESH Command (At least mode 4 - "UICC reset")
DEV7	The Device SHALL comply with the GSMA-EICTA document "Security Principles Related to Handset Theft" [30]
DEV8	The Device MAY retrieve the EID defined in section 2.2.2 of this specification from the eUICC and SHALL support the following commands as described in [35]: • AT+CCHO (Open Logical Channel) • AT+CCHC (Close Logical Channel) • AT+CGLA (Generic UICC Logical Channel Access)
DEV9	The Device SHALL support from the [35] the following commands for all generic purposes: • AT+CRSM (Restricted SIM access)

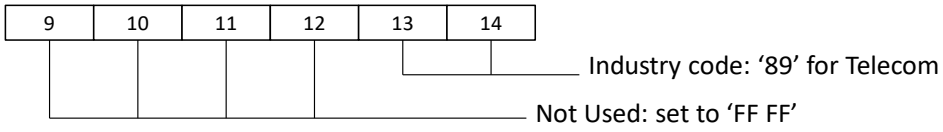
Annex H Coding of the PIX for 'Embedded UICC Remote Provisioning and Management' (Normative)

The following coding of the PIX, following ETSI TS 101 220 [2], applies for ISD-R, ISD-P and ECASD:

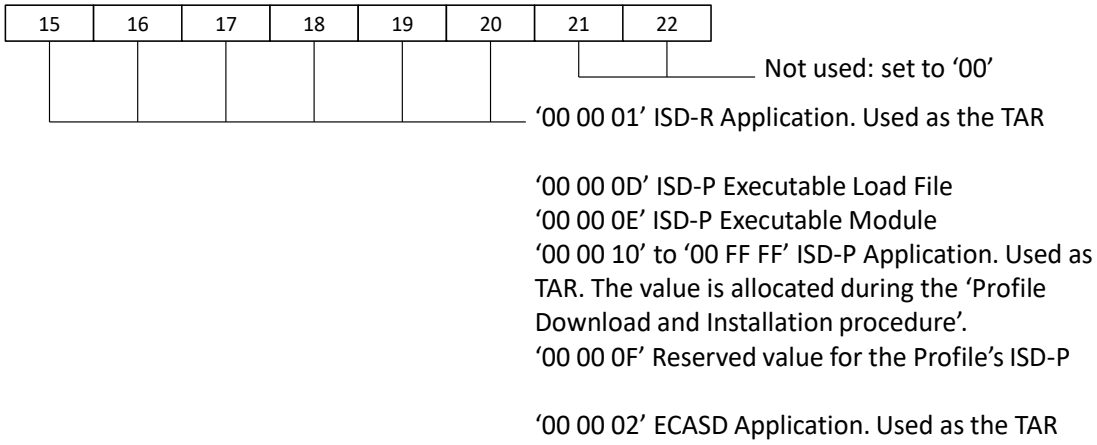
- **Digits 1 to 4** - Application code for 'Embedded UICC Remote Provisioning and Subscription Management'
  - Coding: Fixed value '10 10'

- **Digits 5 to 8** - Not used
  - Coding: Fixed value 'FF FF'

- **Digits 9 to 14** - Application provider code



- **Digits 15 to 22** - Application Provider field 8 hexadecimal digits



Annex I List of Identifiers (Normative)

OIDs

The following identifiers for remote provisioning are created under a dedicated OID tree under ISO branch:

- ASN.1 notation: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)}
- dot notation: 1.3.6.1.4.1
- IOD-IRI notation: /ISO/Identified-Organization/6/1/4/1

The private enterprise numbers may be found under the Internet Assigned Numbers Authority: http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

EUM Identifier

Identifier	Uniqueness	Registration Entity
EUM OID	within the ecosystem	ISO 1.3.6.1.4.1
SIN	within the ecosystem	ISO, according to ISO 7812-2 [19]

eUICC Identifier

Identifier	Uniqueness	Registration Entity
EID	within the ecosystem	GSMA ESIM Technical Specification
ECASD AID	within the eUICC	GSMA ESIM Technical Specification
ISD-R AID	within the eUICC	GSMA ESIM Technical Specification
ISD-P AID	within the eUICC	SM-SR within a range Defined in GSMA ESIM Technical Specification
ICCID	Global	ITU
ISD-R TAR	within the eUICC	GSMA ESIM Technical Specification

MNO-SD AID	Within the Profile	ETSI TS 101 220 (ISD AID)
MNO-SD TAR	Within the Profile	ETSI TS 101 220 (ISD TAR)

SM-SR Identifier

Identifier	Uniqueness	Registration Entity
SMSR OID (called SRID in [1])	within the ecosystem	ISO 1.3.6.1.4.1

SM-DP Identifier

Identifier	Uniqueness	Registration Entity
SMDP OID (called DPID in [1])	within the ecosystem	ISO 1.3.6.1.4.1

Operator Identifier

Identifier	Uniqueness	Registration Entity
Operator OID	within the ecosystem	ISO 1.3.6.1.4.1
MCC+MNC (IMSI)	Global	ITU-T for MCC and National Regulators for MNC

Annex J Verification of EID (Informative)

Verification of an EID is performed as follows:

- Using the 32 digits as a decimal integer, compute the remainder of that number on division by 97.
- If the remainder of the division is 1, the verification is successful; else the EID is invalid.

NOTE: Examples of valid EIDs are:

- 8900 1012 0123 4123 4012 3456 7890 1224
- 8900 1567 01020304 0506 0708 0910 1152
- 8904 4011 1122 3344 1122 3344 1122 3321

Annex K : Script Chaining implementation (Informative)

Management of Script Chaining TLVs by the SM-SR MAY be performed as described in this annex. The value and semantics of the Script Chaining TLVs are defined in ETSI TS 102 226 [5].

There are three cases where the Script Chaining implementation may be needed:

- To chain the various sub commands scripts that result from segmenting a single command script sent in a single ES3.sendData call, if this command script is too big to fit into one transport APDU.
- To chain the two parts of the Key Establishment with Scenario#3-Mutual Authentication described in section 3.1.2.
- To chain two or more parts of the Download and Installation of the Profile as described in section 3.1.3 that have been sent in two or more ES3.sendData calls.

The last two cases can be determined by the SM-SR, by inspecting the command script passed as argument of the ES3.sendData call, and recognise if:

- it end with the “First STORE DATA command” C-APDU belonging to the EstablishISDPKeySet function.
- it starts with a SCP.03t TLV structure Initialize Update Command, External Authenticate Command or Command Data Field Encryption) belonging to the DownloadAndInstallation function.

In all cases, if argument `moreToDo` of the ES3.sendData call is `false`, there is no point to open a new chaining session (Script Chaining TLV with Script Chaining value of “`first script –xxx`”), and if one such session is already open, it can be marked to terminate after this last script (by adding a Script Chaining TLV with Script Chaining value of “`subsequent script - last script`”).

Annex L Examples of PLMA Setting (Informative)

This annex presents a fictitious scenario where an Operator1 identified by its mno-id=6.7.8.9 successively calls one of the SetPLMA operations, and illustrates how this affects the authorisations for the specified M2M SP identified by an OID=1.2.3.4.

The table reads with time ascending from top to bottom.

Time	mno-id	m2m-sp-id	profile Type	authorised Operations	Consequences
t0	-	-	-	-	No PLMA set: M2M SP is not authorised for any operation or any notifications on Profiles of Operator1.
t1	6.7.8.9	1.2.3.4	ABC	Enable, HandleProfileDownloadedNotification	1.2.3.4 is authorised to enable Profiles of type ABC of Operator1 and is authorised to receive notifications when a Profile of type ABC of Operator1 is downloaded
t2	6.7.8.9	1.2.3.4	ABC	Enable, Disable	1.2.3.4 is authorised to enable and disable Profiles of type ABC of Operator1 but is not authorised any more to receive notifications when a Profile of type ABC of Operator1 is downloaded
t3	6.7.8.9	1.2.3.4	Empty and Missing are treated as the same	Enable	1.2.3.4 is authorised to enable Profiles of Operator1 without a Profile Type in EIS. 1.2.3.4 is still authorised to enable and disable Profiles of type ABC of Operator1
t4	6.7.8.9	1.2.3.4	Empty and Missing are treated as the same		1.2.3.4 is not authorised for any operation on Profiles of Operator1 without a Profile type in EIS 1.2.3.4 is still authorised to enable and disable Profiles of type ABC of Operator1
t5	6.7.8.9	1.2.3.4	ABC	Enable	1.2.3.4 is authorised to enable profiles of type ABC of Operator1
t6	6.7.8.9	1.2.3.4	ABC		1.2.3.4 is not authorised for any operation for Profile type ABC of Operator1

Annex M Examples of ONC Setting (Informative)

This annex presents a fictitious scenario where an Operator1 identified by its mno-id=6.7.8.9 successively calls one of the SetONC operations, and illustrates how this affects the notifications for the Operator.

The table reads with time ascending from top to bottom.

Time	mno-id	profile Type	discarded Notifications	Consequences
t0	-	-	-	No ONC set: Operator1 receives all notifications for all owned Profiles.
t1	6.7.8.9	ABC	HandleProfileEnabledNotification	Operator1 receives “no“ Enable notifications for owned Profiles of type ABC. Operator1 receives for owned Profiles with a Profile type in EIS (apart from ABC) “all” notifications. Operator1 receives for owned Profiles without a Profile type in EIS “all” notifications.
t2	6.7.8.9	ABC	HandleProfileEnabledNotification, HandleProfileDisabledNotification	Operator1 receives “no“ Enable and “no” Disable notifications for owned Profiles of type ABC. Operator1 receives for owned Profiles with a Profile type in EIS (apart from ABC) “all” notifications. Operator1 receives for owned Profiles without a Profile type in EIS “all” notifications.
t3	6.7.8.9	Empty and Missing are treated as the same	HandleProfileEnabledNotification	Operator1 receives “no“ Enable and “no” Disable notifications for owned Profiles of type ABC. Operator1 receives for owned Profiles with a Profile type in EIS (apart from ABC) “all” notifications. Operator1 receives “no“ Enable notifications for owned Profiles without a Profile type in EIS.
t4	6.7.8.9	Empty and Missing are treated as the same	Empty and Missing are treated as the same	Operator1 receives “no“ Enable and “no” Disable notifications for owned Profiles of type ABC. Operator1 receives for owned Profiles with a Profile type in EIS (apart from ABC) “all” notifications. Operator1 receives for owned Profiles without a Profile type in EIS “all” notifications.

Table O1: Example of Applying ONC

Annex N Document Management (Informative)

N.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	19/12/2013	1st Release of Document, submitted to PSMC#119 for approval	GSMA Embedded SIM Leadership Team and PSMC	Ian Smith, GSMA
V2.0	16/09/2014	2nd Release of Document	GSMA Embedded SIM Leadership Team and PSMC	Alexis Michel, Oberthur Technologies
V3.0	29/05/2015	3nd Release of Document	GSMA Embedded SIM Leadership Team and PSMC	Alexis Michel, Oberthur Technologies
V3.1	12/05/16	Minor Release of Documents	GSMA Embedded SIM Leadership Team and PSMC	Alexis Michel, Oberthur Technologies
V3.2	20/06/17	Minor Release of Document	GSMA Embedded SIM Leadership Team and PSMC	Jérôme Duprez, Gemalto
V4.0	25/02/19	Major release of Document	GSMA Embedded SIM Leadership Team and TG	Yolanda Sanz / GSMA

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V4.1	03 Apr 2020	Minor release of document	ISAG	Jérôme Duprez, Thales
V4.2	07 April 2020	Draft 1: CR4101R04 SGP.02 Integrated eUICC CR4103R04 SGP.02 Integrated eUICC REQ ID01 Draft 2: CR4102R03 Clarification on Notification Procedure CR4104R01 SGP.02 Hardware Characteristics of the eUICC CR4105R00 Clarify the fields in the Additional Properties Table.	ISAG	Jérôme Duprez, Thales
V4.2.1	26 November 2021	Draft 1: CR4201R03 Clarify last step for roll back decision Draft 2: CR4202R00 Changes resulting from introduction of SGP.29 CR4203R00 Fix in initial value of Seq counter CR4204R01 URI Handling escaping special characters CR4205r02 Editorials and Clarifications on notifications	ISAG	Jérôme Duprez, Thales
V4.3	25 January 2023	Draft 0: branched from v4.2.1, but was somehow corrupted Draft 1: started over from v4.2.1 official Document Draft 2: CR4301R01 SGP.02 Field-Test eUICC Draft 3: CR4302R01 SGP.02 Clarify keyset encryption on ES1 CR4303R01 SGP.02 Clarify CVM Management privileges CR4304R00 SGP.02 Clarify EIS indicator for Emergency Profile Draft 4:	ISAG	Jérôme Duprez, Thales

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
		CR4305R02 SGP.02 Clarify Mandated DAP privilege		

N.2 Other Information

Type	Description
Document Owner	eSIMG
Editor / Company	Jérôme Duprez, Thales

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.