ETSI TS 103 383 V13.1.0 (2016-02)

Smart Cards;
Embedded UICC;
Requirements Specification
(Release 13)

Reference
RTS/SCP-ReUICCvd10

Keywords
embedded, Smart Card

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

- 0 early working draft;
- 1 presented to TC SCP for information;
- 2 presented to TC SCP for approval;
- 3 or greater indicates TC SCP approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Work on Machine-to-Machine (M2M) applications has given rise to the possibility of having a UICC that is embedded in a communication device in such a way that the UICC is not easily accessible or replaceable. The ability to change network subscriptions on such devices becomes problematic, thus necessitating new methods for securely and remotely provisioning access credentials on these Embedded UICCs (eUICC) and managing subscription changes from one MNO to another.

In its current state, the present document is to be considered as a "work in progress". It contains a restricted set of requirements related to the provisioning of profiles in an eUICC as well as general requirements on the architecture of the eUICC. As a consequence, some of the elements required to specify a complete technical solution are missing, among which are requirements for:

- management of profiles;
- management of credentials;
- the policy control function;

which will be defined in further versions of the present document.

1 Scope

The present document defines the use cases and requirements for an embedded UICC.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[2] ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

[3] Void.

[4] ETSI TS 102 241: "Smart Cards; UICC Application Programming Interface (UICC API) for Java Card (TM)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Recommendation ITU-T E.212: "The international identification plan for public networks and subscriptions".

[i.2] ETSI TR 102 216: "Smart cards; Vocabulary for Smart Card Platform specifications".

[i.3] ETSI TS 123 682: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements to facilitate communications with packet data networks and applications (3GPP TS 23.682)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 102 216 [i.2] and the following apply:

Attribute (of a Profile): indication that a Profile delivers some specific functions; the knowledge of attributes offered by Profiles could be used by any authorized entity accessing the eUICC (terminal, server, etc.) to determine a particular behaviour

Embedded UICC: UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the terminal, and enables the secure changing of subscriptions

Enabled Profile: Profile, the files and/or applications (e.g. NAA) of which are selectable over the UICC-Terminal interface

eUICC Management Credentials: credentials used to verify the authorization for the establishment of Profile Management Credentials and Profile Provisioning Credentials

eUICC Supplier: supplier of the eUICC modules and resident software (such as firmware and operating system)

Local Profile Management Credentials: data required to exist within an eUICC so that a secured communication can be set up between a terminal and the eUICC in order for the user to perform Local Profile Management Operations on the Profiles on the eUICC

Local Profile Management Operation: local Profile enabling or local Profile disabling

NOTE: The local Profile deletion is FFS.

Mobile Network Operator: entity providing communication services to its customers through mobile networks

Network Access Application: application residing on an eUICC that provides authorization to access a network

EXAMPLE: A USIM application.

NOTE: Copied from ETSI TR 102 216 [i.2], to be deleted when the current document is finalized.

Network Access Credentials: data required to authenticate to an ITU E.212 [i.1] Network

NOTE: Network Access Credentials may include data such as Ki/K, and IMSI stored within a NAA.

Operational Attribute: indication that a Profile, containing network access applications and associated network access credentials, is associated to an Operational Subscription

Operational Subscription: subscription that enables a device to access an ITU E.212 [i.1] network for the purpose of accessing telecommunication and related services

Policy: principles reflected in a set of rules that govern the behaviour of an eUICC and/or entities involved in the remote management of the eUICC

Policy Control Function: function that defines, updates or removes Policy Rules to implement a Policy

Policy Enforcement Function: function that executes Policy Rules to implement a Policy

Policy Rule: defines the actions required to implement a Policy and the conditions under which they are executed

eUICC Policy Control Credentials: credentials used for authorization and authentication for the establishment and update of the Policy Rules defined on the eUICC outside Profiles

NOTE: This definition might be refined according to the decision about the need to have Policy Rules defined inside and/or outside Profiles.

Profile: combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC

Profile Access Credentials: data required to exist within a Profile so that secured communication can be set up between an external entity and the eUICC in order to manage that Profile's structure and its data (e.g. operator OTA keys)

Profile Container: logical container for a Profile on an eUICC providing security services, enabling separation of Profiles and providing secure communication

Profile Container Initialization: process of preparing a Profile Container so that it is ready for Profile Loading and Installation

Profile Loading: transfer of a Profile from a Profile Provisioning Credentials holder into the eUICC so that it is ready for installation

Profile Transport: transfer of a cryptographically protected Profile from a Profile Management Credential holder to the eUICC

Profile Installation: process of allocating resources and registering parameters for a Profile to bring it to a state where it can be enabled

Profile Provisioning Credentials: data required to exist within an eUICC so that a Profile downloaded from an external entity can be decrypted and installed on the eUICC

Profile Management Credentials: data required to exist within an eUICC so that a secured communication can be set up between an external entity and the eUICC in order to manage the Profiles on the eUICC

Profile Management Operations: consists of Profile Transport, Profile deletion, Profile enabling, and Profile disabling

Provisioning: container creation and initialization, loading, and installation of a Profile into an eUICC

Provisioning Attribute: indication that a Profile, containing network access applications and associated network access credentials, is associated with the Provisioning Subscription

Provisioning Subscription: subscription, with its associated Profile, that enables a device to access a mobile network for the purpose of management of operational Profiles on the eUICC

Subscriber: entity that has a subscription with a telecommunications service provider

Subscription: commercial relationship for the supply of services between the Subscriber and Telecommunications Service Provider

Subscription Manager: combination of the functions of the SM-SR and the SM-DP

Subscription Manager - Data Preparation: role that prepares Profiles to be securely provisioned on the eUICC e.g. encryption of Profile

NOTE 1: Also known as Profile Provisioning Credentials holder.

NOTE 2: "securely" is felt to relate to requirements captured in an appropriate section of the present document. The term "securely" may be removed from this definition once those requirements are specified.

Subscription Manager - Secure Routing: role that securely performs functions which directly manage the Profiles on the eUICC

NOTE: "securely" is felt to relate to requirements captured in an appropriate section of the present document. The term "securely" may be removed from this definition once those requirements are specified.

Telecommunications Service Provider: MNO, or party trusted by the MNO acting on behalf of the MNO, which provides services to the subscriber

3.1a Definitions for further study

Definitions are required for the following terms:

- **Initialized State.**

NOTE: This definition is required. Best proposal so far: "refers to the state the eUICC is in when a Profile with the Operational Attribute is either not active or not present, and the eUICC is only accessible for the purpose of management of operational Profiles".

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ATR	Answer To Reset
CA	Certificate Authority
CAT	Card Application Toolkit
CS	Circuit Switched
CSIM	CDMA Subscriber Identity Module
EID	eUICC Identifier
eUICC	embedded UICC
FFS	For Further Study
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISIM	IM Services Identity Module
LPMC	Local Profile Management Credentials
M2M	Machine to Machine (communication)
MF	Master File
MNO	Mobile Network Operator
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MTC	Machine-Type Communication
NAA	Network Access Application
NAC	Network Access Credentials
NAS	Non Access Stratum
OEM	Original Equipment Manufacturer
OTA	Over-The-Air
PCF	Policy Control Function
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMC	Profile Management Credentials
PPC	Profile Provisioning Credentials
PS	Packet Switched
PUK	PIN Unblocking Key
RAM	Remote Application Management
RFM	Remote File Management
SD	Security Domain
SIM	Subscriber Identity Module
SM	Subscription Manager
SM-DP	Subscription Manager - Data Preparation
SMS	Short Message Service
SM-SR	Subscription Manager - Secure Routing
SP	Service Provider
TBD	To Be Defined
USIM	Universal Subscriber Identity Module

4 Abstract (informative)

The present document enables remote management of an embedded UICC (eUICC) for purposes of changing an MNO subscription without requiring a physical removal and replacement of the UICC in the end Device.

The present document develops use cases and requirements for the "enhanced, remote management" of a UICC, which is embedded in a communication device, i.e. where the UICC is not intended to be removed. This type of embedded UICC (eUICC) is compatible with Machine-to-Machine (M2M) applications. The eUICC may be embedded at the manufacturing site in advance, depending on the country and network operator, and is compatible for use in a variety of end-user equipment. In these scenarios there may be a requirement to remotely change a subscription easily, similar to what is currently achieved by physically changing the UICC.

The purpose for defining these requirements is to provide ease of use and deployment benefits for end users/consumers and thereby stimulate the M2M sector. A further intent is to enable the creation of common standards and processes for remote management of profiles on an eUICC, such that interoperability is ensured.

It is noted that new business models and usage scenarios, primarily driven by M2M, struggle when supported by the traditional UICC/SIM card. For example:

- By installing a physical UICC, the user is connected to a specific network, as the card only provides access to one network. Should the user wish to (or need to) use another network, then they or the M2M Service Provider has to fit another card in the user's device.
- Changing a UICC may be problematic since that M2M equipment may be remotely located and/or hermetically sealed. It should be noted that where the UICC is not intended to be sealed and inaccessible, the portability of traditional form factor UICC cards is perceived to be a user benefit.
- Non-standard provisioning and re-provisioning methods are being defined and used. These present security implications and a risk of fragmentation within the industry.

New remote provisioning/re-provisioning mechanisms are required to support the new business models and usage scenarios.

5 Background (informative)

5.1 Overview of the use cases

A range of use cases is identified in this clause to derive requirements for the development of a trusted framework for the management of an embedded UICC (eUICC). This is not intended to be an exhaustive list of use cases and applications, but a set of examples to ensure requirements will be flexible enough to securely support current and future use cases.

Use cases are provided as a means to understand and add context to the overall requirements.

5.2 Use Case 1 - Provisioning of multiple eUICCs for M2M

5.2.1 Overview

A Machine-to-Machine Service Provider (M2M SP) sets-up subscriptions for a number of connected M2M devices to start telecommunication services with a first MNO. While it is expected that there will be a very great range of M2M applications, and many of these will have different parties and business models, it is likely that the key technical requirements will become clear through examining a few examples of this use case; the following examples are considered further in this clause:

a) Provisioning for a first subscription, and optional later change of subscription, for communication services for automated reading of utility (electricity, water, gas) meters; a M2M Service Provider will contract these subscriptions.

b) Provisioning for a first subscription and optional later change of subscription for a security camera.

c) Provisioning for a first subscription, and optional later change of subscription for communication services to vehicles (e.g. telematics); the vehicle vendor will provide the automotive services.

5.2.2 Use case 1 - example a) - Utility Meters

The Meter Reading M2M SP has a commercial contract to both supply meters and - once they have been installed - to provide regular meter readings of these meters to the utility company. The M2M SP selects the preferred MNO to provide a number of subscriptions after completing a tender process for the communication services as part of a defined service level agreement.

Once the MNO is selected, the M2M SP arranges for the utility meters to be installed and as part of the installation process for the communication services to start. While the physical installation is a manual process, the subscription management required for the communication services will be automated.

These contracts for communication services are negotiated to last for a given period of time e.g. several years; if a change of contract is negotiated, the change is likely to apply to multiple subscriptions. The changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period.

5.2.3 Use case 1 - example b) - Security Camera

A consumer purchases a security camera for monitoring his house. The security camera is supplied with a communication service so that recorded data is uploaded and stored as part of the service from a security (M2M) SP. The consumer (or M2M SP) installs the camera and sets up access to the security services online.

The M2M SP selects the MNO for the video camera service; the subscription management will be automated for the contracted number of subscriptions between the M2M SP and the MNO.

These contracts for communication services are negotiated to last for a given period of time e.g. several years; if a change of contract is negotiated, the change is likely to apply to multiple subscriptions. The changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period. Noting that the level of MNO coverage within individual properties can be different, an automated check of coverage for the target MNO may form part of any change of an operational profile.

5.2.4 Use case 1 - example c) - Telematics

A consumer purchases a new vehicle and this includes a number of vehicle manufacturer provided services delivered over wide area wireless communications to the vehicle and its occupants. The services will be delivered whether the vehicle is mobile or stationary, and whether or not the vehicle is in the country in which it was purchased. The vehicle manufacturer himself or a subcontractor acts as M2M SP, providing both vehicle related services (such as engine monitoring) and being a broker for services supplied by other SPs (such as infotainment).

The subscription starts at vehicle purchase to be operational as the customer drives the vehicle away; the subscription management will be automated for the contracted number of subscriptions between the M2M SP and the MNO. The M2M SP agrees to the commercial contract with MNO(s) in either the same or different countries for subscriptions for the communication services; the vehicle customer may not know which MNO is providing communication services.

These contracts for communication services are negotiated to last for a given period of time e.g. several years; if a change of contract is negotiated by the M2M SP, the change is likely to apply to multiple subscriptions. The changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period.

5.3 Use case 2 - Provisioning of an eUICC for a first subscription with a new connected device

5.3.1 Overview

An end user purchases a new type of communications or connected device from an OEM together with a subscription to provide first services to this device. While it is expected that there will be a range of consumer purchased devices for communication, media and Internet applications and more, and many of these will have different parties and business models, it is likely that the key technical requirements will become clear through examining a few examples; the following examples are considered further in this clause:

a) Provisioning an eUICC in a new device; the consumer will select the MNO to provide communication services.

b) Provisioning an eUICC in multiple connected new device for an enterprise workforce; the enterprise will select the MNO to provide the subscriptions.

5.3.2 Use case 2 - example a) - Provisioning of a new device

A consumer purchases a new device with an eUICC and then selects an MNO for communication services. The MNO might be selected at the same or another retailer, at an MNO shop or online and will be activated within a short period. First use of the new device will be with the first subscription already set-up, or if no subscription is set-up, the customer will select an MNO and, if required, after appropriate authorization a subscription will be set-up. The subscription management will be automated for this single consumer subscription between the consumer and the MNO. The consumer agrees to the contract with the MNO for the subscription for the communication services.

5.3.3 Use case 2 - example b) - Provisioning of multiple new devices for an enterprise

An enterprise (Purchasing Manager) purchases new devices for a set of employees. Contracts for multiple subscriptions will be negotiated for communication services, which enable a range of telecommunication and enterprise applications. The subscriptions will be activated as new employees start, at the latest on their first use of the device. The subscription activation may be followed by device management to configure enterprise specific applications and directories.

The subscription management will be automated for the contracted number of subscriptions between the enterprise and the MNO. The enterprise agrees to the commercial contract with MNO(s) for subscriptions for the communication services; the enterprise employees will be aware of which MNO is providing communication services.

5.4 Use case 3 - Change of subscription for a device

5.4.1 Overview

A subscriber changes the contract and thus subscription for the device to stop services with the current MNO and start services with a new MNO.

a) Change of a subscription for a device by the consumer.

b) Change of the subscriptions of multiple connected new devices for an enterprise workforce to a new MNO; the enterprise will select the MNO to provide the subscriptions.

5.4.2 Use case 3 - example a) - Change of subscription by consumer

A contract for communication services of a device is expected to last for a period of one or more years; if a change of contract is decided upon by the consumer, the change is likely to apply to a single subscription, or possibly a few subscriptions the consumer has for connected devices. The changeover is expected to be managed seamlessly in an automatic fashion at an agreed date. The changeover will be undertaken in accordance with relevant Policy Control Functions.

5.4.3 Use case 3 - example b) - Change of subscriptions for devices for enterprise workforce

Contracts for communication services for the workforce are expected to be negotiated to last for a period of one or more years. If a change of contract is negotiated by the enterprise, the change is likely to apply to multiple subscriptions, and the changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period. The changeover will be undertaken in accordance with relevant Policy Control Functions.

5.5 Use Case 4 - Change of SM-SR

The M2M device manufacturer orders eUICCs from an eUICC Manufacturer. The eUICCs contain Profile Management Credentials which are associated with an SM-SR Y.

MNO A has to provide telecommunication services to a M2M service provider that has M2M devices equipped with eUICCs. The SM-SR Z is used by MNO A.

However, as MNO A usually manages their profiles with SM-SR Z, the management of the eUICCs will be handed over from SM-SR Y to SM-SR Z.

SM-SR Z will request the necessary data to manage the eUICCs (e.g. the appropriate access credentials, characteristics of the eUICCs, previous SM-SRs) in the M2M devices from SM-SR Y.

However, SM-SR Z does not want the SM-SR Y to have knowledge of the eUICC Profile Management Credentials it will have.

Therefore SM-SR Y and SM-SR Z perform a change of eUICC management responsibilities involving the eUICCs in the process.

As a consequence SM-SR Z becomes the entity managing the eUICCs on behalf of the MNO A.

5.6 Use Case 5 - Terminal state and capabilities reporting

As the eUICC may be mounted in a terminal, the profile build and provisioning may depend on the terminal capabilities and states. For instance, when the user asks the operator for a subscription, the build of the profile may depend on the network capabilities supported by the terminal, and the provisioning initialization may depend on the terminal state of the battery. As a possible approach, the terminal may therefore need to be able to provide such information to the eUICC in order to potentially adapt the profile build and its delivery.

5.7 Use Case 6 - Profile Update

When an eUICC is delivered, there may be a pre-loaded Profile from an MNO on the eUICC with Provisioning Attribute for profile provisioning and management. After a user purchases a device with the eUICC, the user may subscribe to the same MNO for normal services. The MNO may want to reuse the existing Profile on eUICC, e.g. reusing network access credentials (e.g. IMSI, Ki) and other common files (e.g. files under MF), add the Operational Attribute to the Profile and optionally update the content of the Profile (e.g. loading new EFs and applications) based on the user's subscription.

5.8 Use Case 7 - Provisioning of devices with only IP connectivity

3GPP MTC (Machine Type Communications) work items have defined PS-only MTC devices, that only have PS domain connectivity and possibility without MSISDN as specified in ETSI TS 123 682 [i.3].

This may make CS domain SMS-based device triggering infeasible, and the network would not be able to perform network-initiated provisioning if the system solely relies on CS domain SMS triggering.

From a specification point of view, SMS over NAS and SMS over IMS are both feasible. However, they are largely operators' deployment choice as specified in ETSI TS 123 682 [i.3].

In addition, there is always concern that delivering SMS via IMS, i.e. requiring the MTC modem to have IMS support and the MNO to configure IMS core for MTC usage, works against the principle of low-cost MTC as proposed by major MNOs and already defined in 3GPP Rel-12.

5.9 Use Case 8 - Provisioning a device in markets with multiple roots of trust (CAs)

Through the lifetime of a device, it may be provisioned multiple times. The provisioning may happen in different countries and markets if the device is nomadic, for example, a car, a personal health device, or a handheld device.

It is quite possible that a PKI security framework will be used in remote provisioning, where authorized network entities will be issued certificates by CA for authentication with the eUICC. The issue arises when sometimes different markets are using different roots of trust, e.g. root CAs, for issuing certificates. For example, this is already the case for today's online banking systems in Asia, North America and Europe markets. Thus it is a business requirement that the eUICC technology has to ensure provisioning is possible even in markets with different roots of trust.

6 Requirements

6.1 General

Identifier	Requirement
REQ-12-EU-01-01	The eUICC is a UICC that shall conform to either ETSI TS 102 221 [1] or ETSI TS 102 671 [2] and in particular to the technical realization of the requirements specified in the present document.
REQ-12-EU-01-02	The eUICC shall be identified with a globally unique and non-modifiable identifier.
REQ-12-EU-01-03	As far as feasible, the technical specification for the eUICC shall provide an option that allows its implementation on existing terminals, i.e. not mandate the support of Rel-12 features by the terminal (see note).
REQ-13-EU-01-04	There shall be a standardized, length-optimized, human readable representation of the eUICC identifier.
REQ-13-EU-01-05	The representation in REQ-13-EU-01-04 may be a subset of the eUICC identifier as long as it is still globally unique.
NOTE: The requirement does not exclude the specification of eUICC-specific mechanisms that require additional feature support by Rel-12 and beyond Terminals.	

6.2 Profile, Application and File Structure

Identifier	Requirement
REQ-12-EU-02-01	Each Profile shall be globally and uniquely identified.
REQ-12-EU-02-02	It shall be possible for the MNO to manage the contents of its Enabled Profile on the eUICC in the same manner as for a UICC; e.g. Remote File and Application Management.
REQ-12-EU-02-03	It shall be possible for a Profile to include data, such as identities, keys, PINs, certificates, and algorithm parameters, as well as first and second level applications.
REQ-12-EU-02-04	Void.
REQ-12-EU-02-05	Void.
REQ-12-EU-02-06	Void.
REQ-12-EU-02-07	A Profile with the Operational Attribute may be used for provisioning.
REQ-12-EU-02-08	The eUICC may contain one or more Profiles.
REQ-12-EU-02-09	It shall be possible to securely bind Profiles to specific Terminals.
REQ-12-EU-02-10	The Profile identifier associated with a Profile shall remain the same through the lifetime of the Profile.
REQ-12-EU-02-11	The Profile Attributes are part of the Profile and shall be defined, managed and updated by the Profile Access Credentials holder.
REQ-12-EU-02-12	A Profile shall be set with at least one of the following Attribute: Provisioning Attribute, Operational Attribute.
REQ-12-EU-02-13	Profiles shall include an indication of their Attributes.
REQ-12-EU-02-14	The eUICC shall be able to read the Profile Attributes.
REQ-12-EU-02-15	There shall be a mechanism in order to configure whether or not to enforce that there is always at least one Profile with the Provisioning Attribute in an eUICC.

6.3 Procedural

Identifier	Requirement
REQ-12-EU-03-01	There shall be a mechanism to support the creation of Profile Containers.
REQ-12-EU-03-02	There shall be a mechanism to support Profile Container Initialization.
REQ-12-EU-03-03	There shall be a mechanism to support Profile Transport.
REQ-12-EU-03-03a	It shall be possible for the eUICC and the Terminal to exchange information required to initiate the loading of a Profile.
REQ-12-EU-03-04	Void.
REQ-12-EU-03-04a	The initial state of an installed Profile shall be the disabled state.
REQ-12-EU-03-04b	There shall be a mechanism to support Profile Loading.
REQ-12-EU-03-04c	There shall be a mechanism to support Profile Installation.
REQ-12-EU-03-05	There shall be a mechanism to support the deletion of disabled Profiles.
REQ-12-EU-03-05a	It shall not be possible to delete an enabled Profile.
REQ-12-EU-03-06	There shall be a mechanism to support the enabling of a disabled Profile.
REQ-12-EU-03-07	There shall be a mechanism to support the disabling of an enabled Profile.
REQ-13-EU-03-07a	After fulfilling the security requirements, it shall be possible to execute any one of the mechanisms in REQ-12-EU-03-05, REQ-12-EU-03-06, REQ-12-EU-03-07 by a single corresponding command using the Profile ID as a parameter.
REQ-12-EU-03-08	It shall be possible to load a Profile in one or multiple sessions.
REQ-12-EU-03-09	Void.
REQ-12-EU-03-10	There may be a mechanism on the eUICC that identifies a change of device.
REQ-12-EU-03-11	There shall be a mechanism to allow the eUICC to provide information on its capabilities and status (e.g. hosted algorithms, CAT, runtime environment and OTA capabilities, memory capacity and memory usage).
REQ-12-EU-03-11a	It shall be possible for an eUICC to provide the capabilities and state of the associated terminal to the Profile Management Credentials holder and/or the Profile Provisioning Credentials holder.
REQ-12-EU-03-11b	Terminal state and capabilities in REQ-12-EU-03-11a are the following: • The information provided in the CAT command "Terminal Profile". • Current Access Technology. • Radio Access Technologies supported by the terminal. Battery state.
REQ-12-EU-03-12	There shall be a mechanism to allow the eUICC to acknowledge the result of Profile Management Operations and Local Profile Management Operations.
REQ-12-EU-03-13	Activities on the eUICC related to any other Profile or the overall management of the eUICC, such as the mechanism defined in REQ-12-EU-03-11, shall not disrupt the services provided by the enabled Profile to the terminal, to the network or to the user.
REQ-12-EU-03-14	eUICC shall provide isolation of data and applications between Profiles.
REQ-12-EU-03-15	There shall be a mechanism for the eUICC to recover from interruptions of Profile management operations.
REQ-12-EU-03-15a	There shall be a mechanism for the eUICC to optionally ensure the Profile Loading, Installation and Deletion operations to be atomic, i.e. are either executed completely or return to the state before the start of the operation.
REQ-12-EU-03-16	There shall be a mechanism to allow the eUICC to provide Profile identifier information to an authorized PMC and/or LPMC holder.
REQ-12-EU-03-16a	There shall be a mechanism to allow the eUICC to provide Profile state information (enabled or disabled) to an authorized PMC and/or LPMC holder.
REQ-12-EU-03-16b	There shall be a mechanism to allow the eUICC to provide the Profiles Attributes to an authorized entity (see note 2).
REQ-12-EU-03-16c	There shall be a mechanism to allow the eUICC to provide meta-data information (e.g. Profile MNO name and ICCID) associated with a Profile to an authorized entity (see note 2).
REQ-12-EU-03-17	There shall be a mechanism to allow the eUICC to provide the information mentioned in REQ-12-EU-03-16/16a/16b/16c for all Profiles installed on the eUICC in an aggregated manner.
REQ-13-EU-03-18	It shall be possible for an authorized Profile Provisioning Credentials holder to determine that an eUICC contains a specific Profile, which that PPC holder has loaded and installed, identified by the Profile identifier.
REQ-12-EU-03-19	It shall be possible to switch between Profiles in a failsafe manner.

Identifier	Requirement
REQ-12-EU-03-20a	There shall be a mechanism to allow the eUICC to provide on demand the eUICC identifier to authorized PMC, LPMC, PPC and eUICC Management Credentials holders.
REQ-12-EU-03-20b	There shall be a mechanism to allow the eUICC to provide on demand the following information to an authorized PPC holder and/or eUICC Management Credentials holder: eUICC manufacturer, date of eUICC manufacture, eUICC operating system, and operating system version.
REQ-12-EU-03-21	There shall be a mechanism for an eUICC to resolve the network address of an associated Profile Management Credentials holder.
REQ-12-EU-03-22	It shall be possible to define within the Profile which entities are to receive acknowledgement of Profile management operations and Local Profile Management operations related to that Profile, as described in REQ-12-EU-03-12 (see note 3).
REQ-12-EU-03-23	Disabling a Profile on the eUICC shall have the same effect for the Terminal as powering off and removing a UICC, with the possible exception of the initial communication establishment procedures as specified in clause 6 of ETSI TS 102 221 [1] (i.e. the Terminal shall perform the procedures it would perform if a regular UICC had been removed, with the exception of the aspects that obviously would not require to be repeated since the eUICC has not been physically removed).
REQ-12-EU-03-24	Void.
REQ-12-EU-03-25	Toolkit resources (e.g. Menus entries, Event registration) shall be disabled for toolkit application in a disabled Profile, and enabled when the Profile is enabled, by the runtime environment defined in ETSI TS 102 241 [4].
REQ-12-EU-03-26	Void.
REQ-12-EU-03-27	It shall not be possible to select an application that is part of a disabled Profile on any interface.
REQ-12-EU-03-28	Void.
REQ-12-EU-03-29	It shall be possible for the terminal to obtain the eUICC identifier.
REQ-12-EU-03-30	It shall be possible for an authorized Profile Management Credentials holder to determine that an eUICC contains a specific Profile.
REQ-13-EU-03-31	The technical specification shall have an option that allows provisioning of the eUICC over mobile networks when there is neither SMS nor IMS service available.
REQ-13-EU-03-32	The terminal may implement Local Profile Management.
REQ-13-EU-03-33	There shall not be more than one enabled profile at any time on the eUICC.
NOTE 1: Void. NOTE 2: Requirement to be revised in order to define the authorized entity. Potential authorized entities include: Profile Provisioning Credentials holder, Profile Management Credentials holder, eUICC Management Credentials holder. NOTE 3: Requirement to be revised in order to define the entities. Potential entities include: Profile Provisioning Credentials holder, Profile Management Credentials holder, eUICC Management Credentials holder, Profile Access Credentials holder.	

6.4 Security

Identifier	Requirement
REQ-12-EU-04-01	There shall be a secure mechanism providing the capability for authorization, authentication, integrity and confidentiality for the management of Profiles, as per REQ-12-EU-03-03, REQ-12-EU-03-05, REQ-12-EU-03-06 and REQ-12-EU-03-07.
REQ-12-EU-04-02	The mechanism in REQ-12-EU-04-01 shall use Profile Management Credentials.
REQ-12-EU-04-03	There shall be an additional secure mechanism providing the capability for authorization, authentication, integrity and confidentiality for the loading and installation of Profiles, as per REQ-12-EU-03-04b and REQ-12-EU-03-04c.
REQ-12-EU-04-03a	All information required for loading and installation of Profiles protected by the mechanism in REQ-12-EU-04-03 shall be transported to the eUICC using the mechanism defined in REQ-12-EU-04-01.
REQ-12-EU-04-04	The mechanism in REQ-12-EU-04-03 shall use Profile Provisioning Credentials.
REQ-12-EU-04-05	There shall be a secure mechanism providing the capability for authorization and authentication for the creation of a container for Profiles, as per REQ-12-EU-03-01.
REQ-12-EU-04-06	There shall be a secure mechanism providing the capability for authorization, authentication, integrity and confidentiality for the initialization of a container for Profiles, as per REQ-12-EU-03-02.
REQ-12-EU-04-07	The mechanism in REQ-12-EU-04-05 shall use Profile Management credentials.
REQ-12-EU-04-08	The mechanism in REQ-12-EU-04-06 shall use credentials (see note 1).
REQ-12-EU-04-09	There shall be a safeguard mechanism against Profile installation error that may leave devices unintentionally without connectivity.

Identifier	Requirement
REQ-12-EU-04-10	There shall be mechanisms to protect all Profiles against unauthorized access, unauthorized deletion or unauthorized modification.
REQ-12-EU-04-11	The eUICC shall support Profile Provisioning Credentials to be used for decrypting Profiles.
REQ-12-EU-04-12	The Profile Provisioning Credentials used in REQ-12-EU-04-11 shall also be used for integrity checking of a Profile.
REQ-13-EU-04-13	The eUICC shall be able to host multiple algorithms for network authentication external to Profiles.
REQ-12-EU-04-14	The eUICC shall be able to provide MNO algorithm capabilities to the Network Access Applications (NAA) hosted in an enabled Profile.
REQ-13-EU-04-15	There shall be a mechanism on the eUICC whereby NAA parameters from an enabled Profile are used to select and customize the corresponding MNO algorithm(s) hosted on the eUICC.
REQ-12-EU-04-16	The eUICC shall ensure the confidentiality and integrity of algorithm parameters.
REQ-12-EU-04-16a	The security mechanism used to protect the algorithm parameters (especially the key K) during provisioning of the Profile shall provide at least the same security strength as the strength of the algorithm key itself.
REQ-12-EU-04-17	There shall be a mechanism that allows mutual authentication between an eUICC and the Profile Management Credentials holder.
REQ-12-EU-04-18	The mechanism in REQ-12-EU-04-17 shall use Profile Management Credentials.
REQ-12-EU-04-19	Mutual authentication between the eUICC and the Profile Management Credentials holder shall be mandatory.
REQ-12-EU-04-20	There shall be a mechanism that allows mutual authentication between the eUICC and the Profile Provisioning Credentials holder.
REQ-12-EU-04-21	Mutual authentication between the eUICC and the Profile Provisioning Credentials holder shall be mandatory.
REQ-12-EU-04-22	There shall be a secure mechanism to allow the Profile Provisioning Credentials to be installed, replaced or deleted.
REQ-12-EU-04-23	The overall solution shall prevent replay attacks for the management of Profiles.
REQ-12-EU-04-24	It shall be possible to establish new Profile Management Credentials and/or Profile Provisioning Credentials on the eUICC.
REQ-12-EU-04-25	It should be possible to revoke Profile Management Credentials and Profile Provisioning Credentials on the eUICC in a secure way.
REQ-12-EU-04-26	It shall be possible for an eUICC to host multiple sets of Profile Provisioning Credentials at a given time for the loading and installation of multiple Profiles.
REQ-12-EU-04-27	There shall be only one set of Profile Provisioning Credentials per Profile.
REQ-12-EU-04-28	The Profile Provisioning Credentials used to provide confidentiality and integrity protection of a Profile payload shall be unique to a specific Profile and to a specific eUICC.
REQ-12-EU-04-28a	The Profile Provisioning Credentials used to provide authentication of the eUICC for Profile loading and installation shall be unique to a specific eUICC
REQ-12-EU-04-29	The eUICC shall use a mechanism ensuring that a Profile prepared for a given eUICC can be installed only on that eUICC.
REQ-12-EU-04-30	The eUICC shall use a secure mechanism ensuring that, each time a Profile is prepared by a Profile Provisioning Credential holder for loading and installation on the eUICC, that Profile shall be successfully installed only once on the eUICC.
REQ-12-EU-04-31	The mutual authentication defined in REQ-12-EU-04-20 and REQ-12-EU-04-21 shall be performed directly between Profile Provisioning Credential holder and the eUICC.
REQ-12-EU-04-32	The mechanism for REQ-12-EU-04-24 shall provide confidentiality, integrity and authentication of the new credentials.
REQ-12-EU-04-33	Authorization for the mechanism for REQ-12-EU-04-24 shall use the eUICC Management Credentials.
REQ-12-EU-04-34	There shall be a secure mechanism to provide authentication and integrity protection for the acknowledgements defined in REQ-12-EU-03-12 and REQ-12-EU-03-22.
REQ-12-EU-04-35	There shall be a mechanism providing authentication and authorization for the changing of the eUICC Policy Control Credentials on the eUICC.
REQ-12-EU-04-36	The mechanism for REQ-12-EU-04-35 shall use the eUICC Management Credentials.
REQ-12-EU-04-37	It shall be possible for multiple Profile Management Credentials (PMCs) to exist on the eUICC, with only one PMC authorized for the Profile Container creation and Profile Transport operations, only one PMC authorized for the Profile Enabling/Disabling operations, and only one PMC authorized for the Profile Deletion operation. The PMC authorized for one operation may be the same PMC authorized for another operation.
REQ-13-EU-04-38	The confidentiality protection on Profile content via Profile Provisioning Credentials shall provide Perfect Forward Secrecy.

Identifier	Requirement
REQ-13-EU-04-39	Where certificates are required for the authentication of the Profile Provisioning Credentials holder, the technical solution shall ensure the capability of performing such authentication in an ecosystem with certificates signed by different off-card CAs. (See note 2.)
REQ-13-EU-04-40	If Local Profile Management is implemented, there shall be a secure mechanism providing authentication and authorization for the Local Profile Management Operations.
REQ-13-EU-04-41	The mechanism in REQ-13-EU-04-40 shall use Local Profile Management Credentials.
REQ-13-EU-04-42	The secure mechanism described in REQ-13-EU-04-40 shall be an integral part of the terminal and authorized by the user through an explicit human being validation process (see note 3).
REQ-13-EU-04-43	The combination of Local Profile Management operations, consisting of disabling a Profile and enabling another Profile, shall require a single dedicated human authorization each time it is performed.
REQ-13-EU-04-44	The Local Profile Management operation consisting of disabling a Profile shall require a single dedicated human authorization each time it is performed.
REQ-13-EU-04-45	The Local Profile Management operation consisting of enabling a Profile shall require a single dedicated human authorization each time it is performed.
REQ-13-EU-04-46	The security level required for the Local Profile Management Operations shall be similar to the security level required for the other Profile Management Operations (see note 4).
REQ-13-EU-04-47	It shall be possible to have a Local Profile Management Credential on the eUICC authorized for the Profile Enabling/Disabling operations in the case of Local Profile Management is implemented. (see note 5).
NOTE 1: The type of credentials used is FFS. NOTE 2: It is FFS whether the eUICC supports one CA public key, multiple CA public keys, or multiple CA public keys but only one active CA public key at any point in time. NOTE 3: The appropriate explicit validation process for human being authorization is TBD. NOTE 4: The appropriate security level is TBD. NOTE 5: It is FFS whether LPMC and PMC for the same type of operation can be present together on the eUICC.	

6.5 Profile Interoperability and Interactions

Identifier	Requirement
REQ-12-EU-05-01	It shall be possible for an eUICC to support loading and installing of Profiles generated by different Profile Provisioning Credential holders.
REQ-12-EU-05-01a	A Profile shall use a standardized description format to allow its loading and installation on any compliant eUICC.
REQ-12-EU-05-01b	A Profile may contain proprietary elements (see note).
REQ-12-EU-05-01c	An eUICC may support proprietary elements in a Profile. Proprietary elements that are not supported shall be ignored by the eUICC.
REQ-12-EU-05-01d	The standardized description format shall provide for at least the following standardized items: NAA parameters, NAA algorithm parameters and keys, OTA keys, RAM and RFM parameters, as well as PINs/PUKs.
REQ-12-EU-05-02	The interface, in terms of file structure and metadata, for a Profile to be remotely provisioned onto an eUICC shall be common.
NOTE: Proprietary elements may contain, for instance, Profile extensions adding features not initially included by the eUICC platform or data for features not specified by the implemented standard description format.	

6.6 Policy Enforcement

NOTE: The following describes the requirements for Policy Enforcement Functions necessary to be present on the eUICC. This does not exclude or define any PCF capabilities in the external eco-system also associated with eUICC and profile management.

Identifier	Requirement
REQ-12-EU-06-01	The eUICC shall provide Policy Enforcement Functions.
REQ-12-EU-06-02	The Policy Rules defined in clause 6.8 shall be enforced by the eUICC.
REQ-12-EU-06-03	Policy Rules contained in the eUICC inside of Profiles shall be enforced by the eUICC (see note).
REQ-12-EU-06-04	Policy Rules contained in the eUICC outside of Profiles shall be enforced by the eUICC (see note).
REQ-12-EU-06-05	It shall be possible for an eUICC to enforce policy rules in a disabled Profile.
NOTE: This requirement might be refined according to the decision about the need to have Policy Rules defined inside and/or outside Profiles.	

6.7 Policy Control

Identifier	Requirement
REQ-12-EU-07-01	The Profile Access Credentials holder shall be able to update the Policy Rules inside that Profile using its secured Over The Air access (see note 1).
REQ-12-EU-07-02	Updating the Policy Rules inside a given Profile can only be done when this Profile is in enabled state (see note 1).
REQ-12-EU-07-03	There shall be a secure mechanism to establish and change Policy Rules stored on the eUICC outside of Profiles (see note 1).
REQ-12-EU-07-04	The Policy Rules contained in a Profile shall be able to be updated only by the owner of the Profile (see note 1).
REQ-12-EU-07-05	The mechanism defined in REQ-12-EU-07-03 shall use and only use eUICC Policy Control Credentials (see notes 1 and 2).
NOTE 1: This requirement might be refined according to the decision about the need to have Policy Rules defined inside and/or outside Profiles. NOTE 2: The eUICC Policy Control Credentials holder needs to be defined.	

6.8 Policy Rules

NOTE 1: The following describes Policy Rules necessary to be present on the eUICC. This does not exclude or define any PCF capabilities in the external eco-system also associated with eUICC and profile management.

NOTE 2: This clause requires further study in order to specify the type of rules to be enforced.

Identifier	Requirement

Annex A (informative): Void

Annex B (informative): States (see also annex D)

B.0 Foreword

All entities have states, and entities which interact may have combined states.

B.1 States of eUICC

Initialized	Contains Profile Management Credentials; it will also contain Profile Provisioning Credentials or the capability for their generation
Provisioned	Contains an enabled Profile
Terminated	End of Life

B.2 States of Profiles

Disabled	Installed, but applications within the Profile are not selectable
Enabled	Installed, and applications within the Profile are selectable

B.3 States of Applications in Profiles

Inactive	Not selected using 'Select' command
Active	Selected using 'Select' command

NOTE 1: Existing ETSI Smartcard Platform specifications allow for multiple applications to exist on a UICC. Available applications are indicated when EFDIR is 'Selected' and 'Read' following the ATR as per ETSI TS 102 221 [1]. The capability for multiple applications to be 'Selected' and utilized is achieved though the mechanism of Logical Channels, also defined in ETSI TS 102 221 [1].

NOTE 2: For the specific case of an Active NAA Application, the state of the subscription associated with the NAA is active if the MNO's Network Access Credentials e.g. IMSI, K are also active in HLR/AuC.

Annex C (informative): Logical aspects of eUICC Architecture and associated Security Credentials

NOTE: Figure C.1 requires updates in order to align with the definitions in the present document.

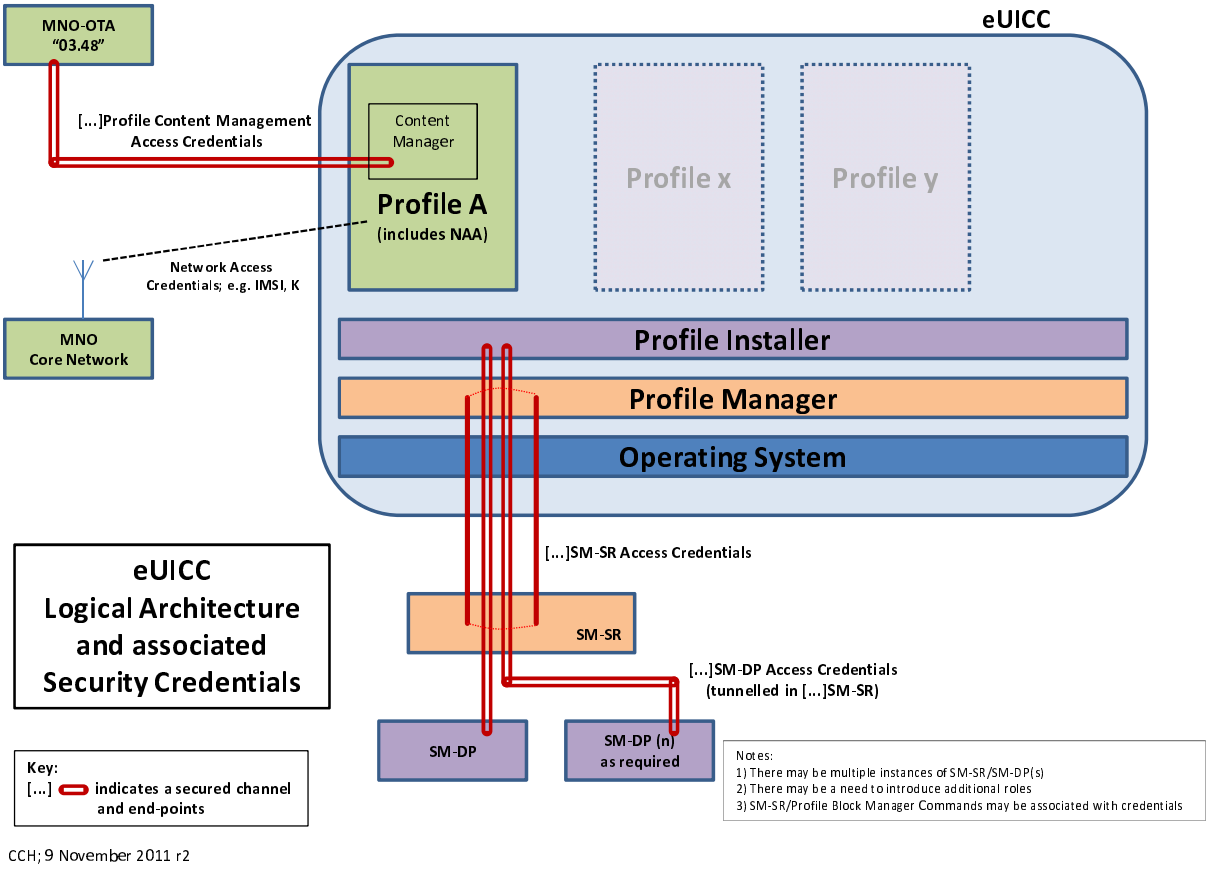

Figure C.1

Annex D (informative): Profiles and NAA (Network Access Application) States

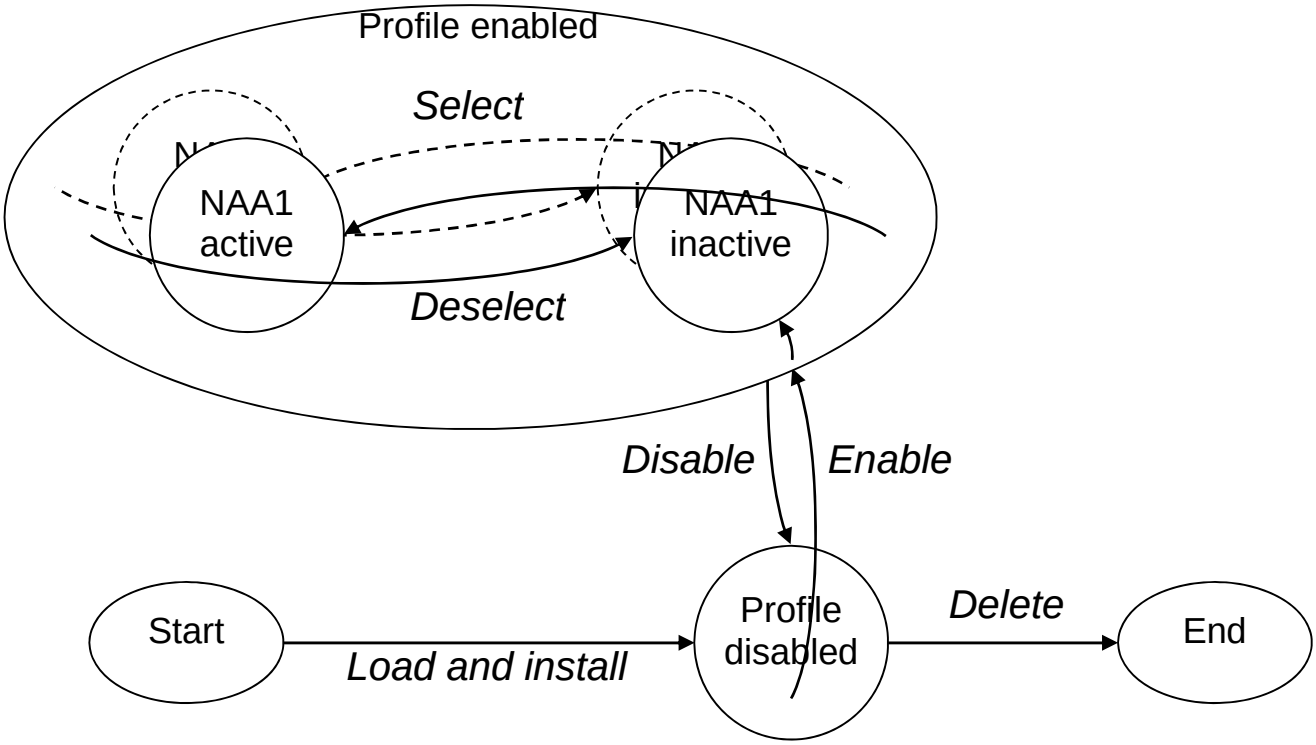

Figure D.1

Annex E (informative): Profile Aspects

E.0 Foreword

The following considerations outline the understanding of the Profile during its transfer to the eUICC and how it is expected to work on eUICCs in an interoperable manner.

E.1 Profile Content

Generally, a Profile is the representation of parameters and data which, when installed on an eUICC, deliver the functionality and features of a UICC according to ETSI TS 102 221 [1] and ETSI TS 102 671 [2]. Unless otherwise specified in the eUICC specifications, any element that is optional for the UICC continues to be optional for the eUICC.

A Profile is made up from the following main components:

1) One or more sets of parameters for Network Access Applications (NAAs), such as:
   - SIM = Parameters and Content of the SIM File System + Keys and Parameters for network access authentication, PINs and PUKs.
   - USIM = Parameters and Content of the USIM File System + Keys and Parameters for network access authentication, PINs and PUKs.
   - ISIM = Parameters and Content of the ISIM File System + Keys and Parameters for network access authentication, PINs and PUKs.
   - CSIM = Parameters and Content of the CSIM File System + Keys and Parameters for network access authentication, PINs and PUKs.
2) Mandatory and optional NAA-Independent Parameters and Data, such as:
   - Parameters and content of application independent files.
   - Standardized parameters under MNO control.
   - Universal PIN and PUK.
   - Keysets and Keys.
   - SD structure.
   - Policy Rules.
3) Optional Java Card™ applets and respective parameters.
4) Optional proprietary elements, e.g. applications, files or parameters that have a meaning only in combination with specific eUICCs.

E.2 Profile Related Principles

The following principles were identified to guarantee a level of interworking between Profiles and eUICCs similar to UICCs and Terminals in the classical UICC environment. This allows Profiles and eUICCs to evolve while backwards compatibility (advanced Profile on old eUICC or old Profile on advanced eUICC) is maintained. At the same time it is possible for Profiles in combination with particular eUICCs (and Terminals) to realize particular proprietary features.

1) A Profile contains at least the mandatory NAA Independent Parameters and the parameter set for an NAA.

NOTE 1: Standardization bodies in charge of NAAs may mandate a specific NAA for Profiles within their context, e.g. 3GPP may require at least a USIM.

2) An eUICC supports at least a Profile containing the mandatory NAA Independent Parameters and the parameter set for an NAA. Other mandatory elements are TBD. Unsupported elements in a Profile are ignored.

NOTE 2: Standardization bodies in charge of NAAs may mandate specific NAA support for eUICCs within their context, e.g. 3GPP may require to support at least a USIM.

3) Profiles may contain proprietary elements. These are out of scope for ETSI SCP.

4) eUICCs may support proprietary elements in a Profile. This is out of scope for ETSI SCP. Proprietary elements that are not supported are ignored by the eUICC.

Annex F (informative): Change history

The table below indicates changes that have been incorporated into the present document since it was created by TC SCP.

Meeting	Plenary Tdoc	CR	Rev	Cat	Subject	Old Version	Resulting Version
SCP #58	SCP(13)000049r1	-	-	-	Initial publication	2.0.0	12.0.0
SCP #59	SCP(13)000103	001	-	F	Definition of subscriber	12.0.0	12.1.0
	SCP(13)000104	002	-	F	Management of the content of provisioning profiles		
	SCP(13)000105	003	-	F	Clarification of "platform-related commands"		
	SCP(13)000106	004	-	F	Clarification of "unexpected interruptions"		
	SCP(13)000107r1	005	1	F	Removal of redundant requirements		
	SCP(13)000108r1	006	1	F	Definitions of container term and container related activities		
	SCP(13)000109r1	007	1	B	Missing requirement on anti-cloning of profiles		
	SCP(13)000110r1	008	1	F	Credentials for container creation		
SCP #60	SCP(13)000174	009	-	F	Two-layer encryption for profile loading and installation	12.1.0	12.2.0
	SCP(13)000178	013	-	B	Requirement on anti-cloning part 2		
	SCP(13)000179	014	-	B	Requirement for direct mutual authentication between eUICC and Profile Installer Credential holder		
	SCP(13)000180	015	-	B	eUICC Information Requirements		
	SCP(13)000181	016	-	C	Clarification of profile state transitions		
	SCP(13)000182r1	017	-	B	Address resolution of profile management credentials holder		
SCP #61	SCP(13)000262r1	018	2	D	Potential Authorized Entities	12.2.0	12.3.0
	SCP(13)000257	019		F	Correction of MNO management of profile requirement		
	SCP(13)000261	020		B	Requirements for authorization and credentials establishment		
	SCP(13)000260r1	021	1	C	Obtain profile information		
	SCP(13)000258	022		C	Deletion only of disabled profiles		
	SCP(13)000263	023		D	Addition of Profile Container Initialization definition		
	SCP(13)000259	024		C	State of a successfully installed profile		
	SCP(13)000256r1	025	1	B	Clarification about the uniqueness of Profile Installer Credentials		
SCP #62	SCP(14)000071	029		B	New requirements for Policy Control and Policy Enforcement	12.3.0	12.4.0
	SCP(14)000068	030		B	Enforcement of Policy Rules in disabled Profiles		
	SCP(14)000066r1	031	1	B	Procedure to define the entities to receive acknowledgement of management operations.		
SCP #63	SCP(14)000125r1	032	1	C	Definition of authorized entity	12.4.0	12.5.0
	SCP(14)000126	033		D	Section 6.2 Clean-up		
	SCP(14)000127r1	034	1	F	Definition of Profile Management Operations and clean-up of Procedural section		
	SCP(14)000128	035		D	Section 6.1 Clean-up		
	SCP(14)000129r1	036	1	C	Section 6.4 Clean-up		
	SCP(14)000130r1	037	1	D	Replace Profile Installer by Profile Provisioner		
	SCP(14)000131	038		D	Consistent use of term loading and installation		
	SCP(14)000132r1	039	1	B	Transport for Profile Management		
	SCP(14)000133	040		C	Introduction of eUICC Policy Control Credentials and related requirements		
	SCP(14)000134	041		C	Security protection of acknowledgements		
	SCP(14)000135r1	042	1	B	Visibility of application in a Profile		
	SCP(14)000143	043		B	Profile Interoperability		
SCP #64	SCP(14)000184	044		C	eUICC identifier access by the Terminal	12.4.0	12.5.0
	SCP(14)000185	045		B	Protection of Profile identifier		
	SCP(14)000181r1	046	1	B	Change of eUICC Policy Control Credentials		
	SCP(14)000183	048		B	Description of Profile		
SCP #65	SCP(14)000251	049			Applicable range of terminals	12.5.0	12.6.0
	SCP(14)000253	050			Definitions of profile loading and transport		
	SCP(14)000258	052			Standardized profile format for loading and installation		
	SCP(14)000259r1	053	1		Profile determination by a PMC holder		
	SCP(14)000255	054			Security level for profile provisioning		
	SCP(14)000254	056			Requirement on atomic operations		
	SCP(14)000256	057			Human-readability of eUICC identifier		
	SCP(14)000252	058			Preventing deletion of an enabled Profile		

Meeting	Plenary Tdoc	CR	Rev	Cat	Subject	Old Version	Resulting Version
Online Vote	SCP(14)000248r1	059			Multiple PMC function split	12.5.0	12.6.0
SCP #66	SCP(14)000339	062		D	Replace SM-DP by Profile Provisioning Credentials holder in section 6.5	12.6.0	12.7.0
	SCP(14)000340r1	063		F	Correction of a void reference		
	SCP(14)000341r1	064	1	B	Terminal state and capabilities reporting through eUICC		
	SCP(14)000342r1	065	1	B	Initiation of Profile Provisioning		
SCP #67	SCP(15)000056	066	1	F	Clarification of definition of Profile Container Initialization	12.7.0	12.8.0
SCP #69	SCP(15)000187r1	051	5	F	Clarification on application behaviour for dis/enabled profiles		
	SCP(15)000188r1	069	6	F	Removal of the notion of Profile type and addition of Profile Update use case		
2015-09	-	-	-	-	To comply with latest ETSI drafting rules: removal of hanging paragraphs through addition of clause headers where appropriate (source ETSI Secretariat + Rapporteur)		
SCP #67	SCP(15)000057	067	1	B	Addition of Perfect Forward Secrecy	12.8.0	13.0.0
	SCP(15)000058	068	1	B	eUICC Profile Management Commands		
	SCP(15)000060r1	070	2	B	Provisioning on IP connectivity only		
SCP #69	SCP(15)000134r1	072	1	C	Definition and requirements of Certificate Authority		
	SCP(15)000132r1	073		C	Multiple Network Authentication		
SCP #70	SCP(15)000195r1	075		B	Requirements for a local management of the profiles hosted in the embedded UICC by the end user	13.0.0	13.1.0
SCP #70	SCP(15)000243r1	074	1	C	Clarification of EID Requirements	13.0.0	13.1.0
SCP #71	SCP(15)000283	075		C	eUICC Cleanup of Authorized Entities	13.0.0	13.1.0
SCP #71	SCP(15)000284	077		C	Clarification of Profile	13.0.0	13.1.0

Annex G (informative): Bibliography

- ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT)".

History

Document history		
V13.0.0	October 2015	Publication
V13.1.0	February 2016	Publication