ETSI TS 103 383 V12.1.0 (2013-06)

Smart Cards;
Embedded UICC;
Requirements Specification
(Release 12)

Petitioner Samsung Ex-1028, 0001

Reference
RTS/SCP-ReUICCvc10

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2013.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 4
Foreword 4
Introduction 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions and abbreviations 5
3.1 Definitions 5
3.1a Definitions for further study 7
3.2 Abbreviations 7
4 Abstract (informative) 7
5 Background (informative) 8
5.1 Overview of the use cases 8
5.2 Use Case: 1 - Provisioning of multiple eUICCs for M2M 8
5.2.1 Use case 1 - example a) - Utility Meters 8
5.2.2 Use case 1 - example b) - Security Camera 9
5.2.3 Use case 1 - example c) - Telematics 9
5.3 Use case 2 - Provisioning of an eUICC for a first subscription with a new connected device 9
5.3.1 Use case 2 - example a) - Provisioning of a new device 9
5.3.2 Use case 2 - example b) - Provisioning of multiple new devices for an enterprise 10
5.4 Use case 3 - Change of subscription for a device 10
5.4.1 Use case 3 - example a) - Change of subscription by consumer 10
5.4.2 Use case 3 - example b) - Change of subscriptions for devices for enterprise workforce 10
5.5 Use Case 4 - Change of SM-SR 10
6 Requirements 11
6.1 General 11
6.2 Profile, Application and File Structure 11
6.3 Procedural 12
6.4 Security 13
6.5 Profile Interoperability and Interactions 14
6.6 Policy Control 14
Annex A (informative): Void 15
Annex B (informative): States (see also annex D) 16
B.1 States of eUICC 16
B.2 States of Profiles 16
B.3 States of Applications in Profiles 16
Annex C (informative): Logical aspects of eUICC Architecture and associated Security Credentials 17
Annex D (informative): Profiles and NAA (Network Access Application) States 18
Annex E (informative): Change history 19
History 20

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 (http://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.

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

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.

2.1 Normative references

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".

2.2 Informative references

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".

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

EXAMPLE: A USIM application.

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

Network Access Credentials (NAC): 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 Profile: profile containing one or more network access applications and associated network access credentials

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

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 Loading: transfer of a profile into 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 Installer 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

Provisioning: container creation and initialisation, loading, and installation of a profile into an eUICC

Provisioning Profile: profile containing one or more network access applications, and associated network access credentials which, when installed on an eUICC, enables access to communication network(s), to provide transport capability for eUICC management and profile management between the eUICC and an SM-SR

Provisioning Subscription: subscription, with its associated provisioning 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 (SM-DP): role that prepares operational and provisioning profiles to be securely provisioned on the eUICC e.g. encryption of profile

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.

Subscription Manager - Secure Routing (SM-SR): role that securely performs functions which directly manage the operational and provisioning 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:

- **Initialised State:**

NOTE 1: This definition is required. Best proposal so far: "refers to the state the eUICC is in when an operational profile is either not active or not present, and the eUICC is only accessible for the purpose of management of operational profiles."

- **Profile Container Initialisation:**

NOTE 2: The definition of Profile Container Initialisation is needed and is FFS.

3.2 Abbreviations

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

ATR	Answer To Reset
CAT	Card Application Toolkit
eUICC	embedded UICC
FFS	For Further Study
IMSI	International Mobile Subscriber Identity
MNO	Mobile Network Operator
NAA	Network Access Application
NAC	Network Access Credentials.
OEM	Original Equipment Manufacturer
OTA	Over -The-Air
PCF	Policy Control Function
SM	Subscription Manager
SM-DP	Subscription Manager - Data Preparation
SM-SR	Subscription Manager - Secure Routing
SP	Service Provider

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 maybe 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

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.

5.2.1 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.

5.2.2 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.

5.2.3 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

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.

5.3.1 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.

5.3.2 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

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.

5.4.1 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.

5.4.2 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 doesn't 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.

6 Requirements

6.1 General

Identifier	Requirement
REQ-12-EU-01-01	The eUICC is a UICC conforming to TS 102 221 [1] and TS 102 671 [2] as well as, in particular, the requirements specified in the present document and the technical realisation based on them.
REQ-12-EU-01-02	The eUICC shall be identified with a globally unique and non-modifiable identifier.

6.2 Profile, Application and File Structure

NOTE: Security requirements associated with the following are found in clause 6.4.

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	The eUICC shall support two types of Profile: Operational Profile and Provisioning Profile (see note).
REQ-12-EU-02-05	Profiles shall have an indication of the profile type.
REQ-12-EU-02-06	The eUICC shall be able to read the profile types.
REQ-12-EU-02-07	An Operational Profile may be used for provisioning.
REQ-12-EU-02-08	The eUICC may contain one or more Profiles regardless of their type.
REQ-12-EU-02-09	It shall be possible to securely bind Operational Profiles to specific Terminals.
NOTE: The technical solution shall not preclude future support for other standardised types of Profiles.	

6.3 Procedural

Identifier	Requirement
REQ-12-EU-03-01	There shall be a mechanism to support the creation of the container of Profiles.
REQ-12-EU-03-02	There shall be a mechanism to support the initialisation of the container of Profiles.
REQ-12-EU-03-03	There shall be a mechanism to support the loading of Profiles.
REQ-12-EU-03-04	There shall be a mechanism to support the installing of Profiles.
REQ-12-EU-03-05	There shall be a mechanism to support the deletion of Profiles.
REQ-12-EU-03-06	There shall be a mechanism to support the enabling of Profiles.
REQ-12-EU-03-07	There shall be a mechanism to support the disabling of Profiles.
REQ-12-EU-03-08	It shall be possible to load a Profile in one or multiple sessions.
REQ-12-EU-03-09	There shall be a mechanism to allow the eUICC to provide information on the type of the enabled Profile (i.e. provisioning or operational).
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-03-12	There shall be a mechanism to allow the eUICC to acknowledge the result of Profile management operations (e.g. loading, deleting, enabling, disabling) (see note 1).
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-03-16	There shall be a mechanism to allow the eUICC to provide Profile identifier information.
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 for all Profiles loaded on the eUICC in an aggregated manner.
REQ-12-EU-03-18	It shall be possible for an authorized entity to determine that an eUICC contains a specific Profile (see note 2).
REQ-12-EU-03-19	It shall be possible to switch between Profiles in a failsafe manner.

NOTE 1: Insert placeholder for a definition for "Profile management operations", when this definition is there, we can remove the e.g. part of the requirement.
NOTE 2: Requirement to be revised in order to define the authorized entity.

6.4 Security

Identifier	Requirement
REQ-12-EU-04-01	There shall be a secure mechanism providing the capability for authorisation, authentication, integrity and confidentiality for the management of Operational or Provisioning Profiles, as per REQ-12-EU-03-03, REQ-12-EU-03-05, REQ-12-EU-03-06, 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 a secure mechanism providing the capability for authorisation, authentication, integrity and confidentiality for the installation of Operational or Provisioning Profiles, as per REQ-12-EU-03-04.
REQ-12-EU-04-04	The mechanism in REQ-12-EU-04-03 shall use Profile Installer Credentials.
REQ-12-EU-04-05	There shall be a secure mechanism providing the capability for authorisation and authentication for the creation of a container for Operational or Provisioning Profiles, as per REQ-12-EU-03-01.
REQ-12-EU-04-06	There shall be a secure mechanism providing the capability for authorisation, authentication, integrity and confidentiality for the initialisation of a container for Operational or Provisioning 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).
REQ-12-EU-04-09	There shall be a safeguard mechanism against profile installation error that may leave devices unintentionally without connectivity.
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 Installer Credentials to be used for decrypting profiles; e.g. Provisioning or Operational Profiles.
REQ-12-EU-04-12	The Profile Installer Credentials used in REQ-12-EU-04-11 shall also be used for integrity checking of a Profile.
REQ-12-EU-04-13	The eUICC shall be able to host 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 Operational or Provisioning Profile.
REQ-12-EU-04-15	There shall be a mechanism on the eUICC whereby algorithm parameters from an NAA of a Profile which is enabled are used to customize the corresponding MNO algorithm hosted on the eUICC.
REQ-12-EU-04-16	The eUICC shall ensure the confidentiality and integrity of algorithm parameters.
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 Installer Credentials holder.
REQ-12-EU-04-21	Mutual authentication between the eUICC and the Profile Installer Credentials holder shall be mandatory.
REQ-12-EU-04-22	There shall be a secure mechanism to allow the Profile Installer Credentials to be installed, replaced or deleted.
REQ-12-EU-04-23	The overall solution shall prevent replay attacks for the management of Operational and Provisioning Profiles.
REQ-12-EU-04-24	It shall be possible to load new Profile Management Credentials and Profile Installer Credentials on the eUICC in a secure way.
REQ-12-EU-04-25	It should be possible to revoke Profile Management Credentials and Profile Installer 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 Installer Credentials at a given time for the installation of multiple Profiles.
REQ-12-EU-04-27	There shall be only one set of Profile Installer Credentials per Profile.
REQ-12-EU-04-28	A set of Profile Installer Credentials shall be unique to a specific Profile and 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.
NOTE: The type of credentials used is FFS.	

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 SM-DP entities (see note).
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: The knowledge of an SM-DP is not applicable to the eUICC, but this requirement serves to indicate that a generic mechanism is required.	

6.6 Policy Control

NOTE 1: The following describes 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.

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

Identifier	Requirement
REQ-12-EU-06-01	The eUICC shall provide Policy Enforcement Functions.

Annex A (informative): Void

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

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

B.1 States of eUICC

Initialised	Contains Profile Management Credentials; it will also contain Profile Installer 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 TS 102 221 [1]. The capability for multiple applications to be 'Selected' and utilised is achieved though the mechanism of Logical Channels, also defined in 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.

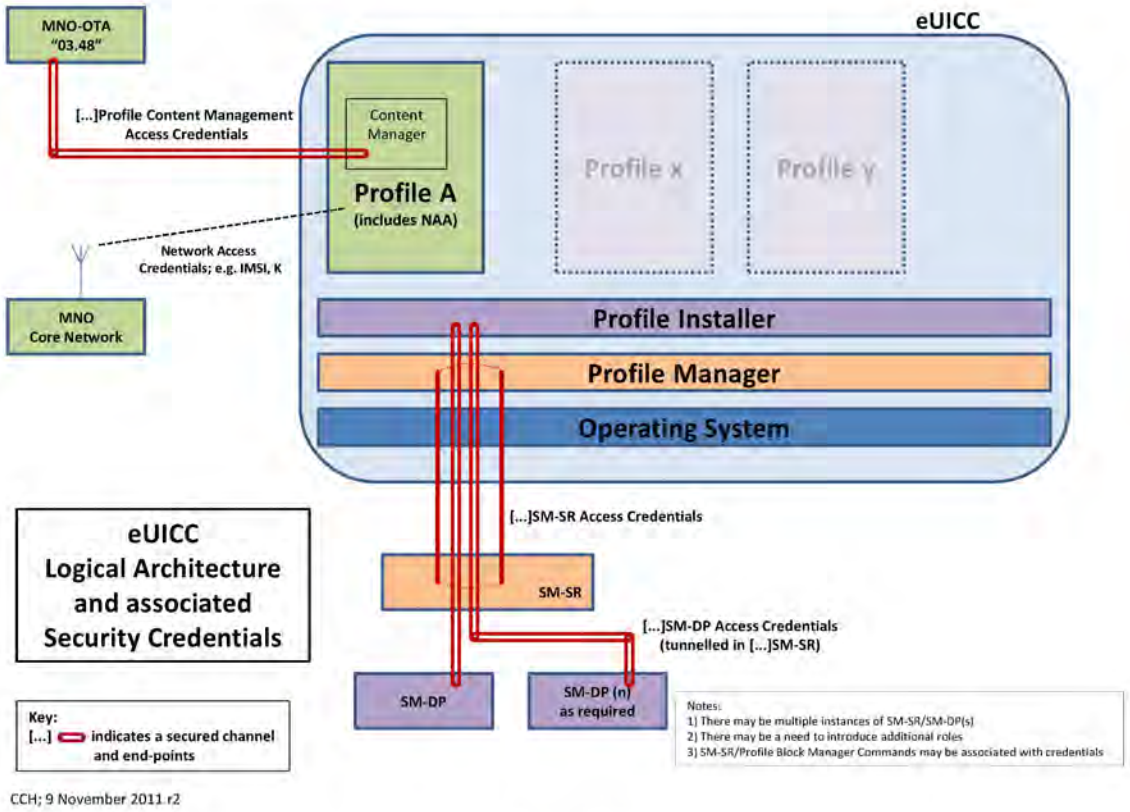

Figure C.1

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

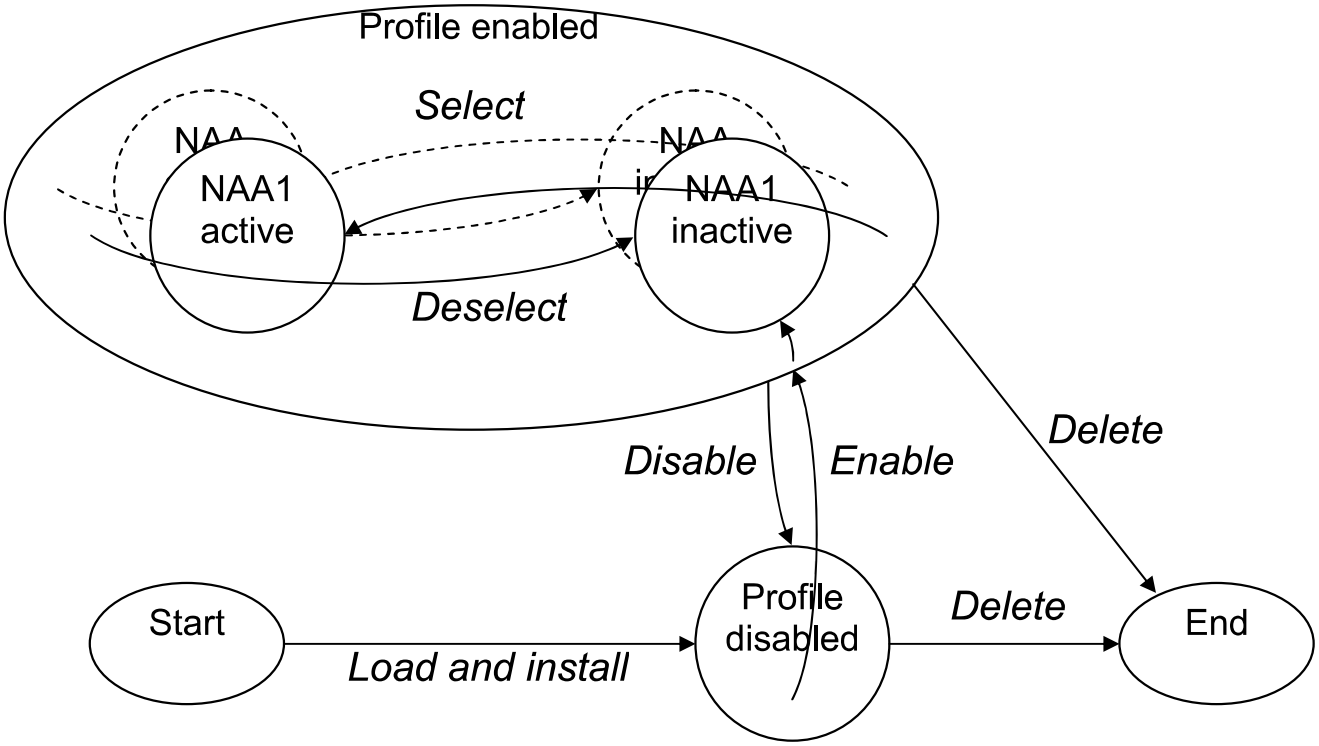

Figure D.1

Annex E (informative): 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	Old Version	CR	Rev	Cat	Subject	Resulting Version
SCP-58	SCP(13)000049r1	2.0.0	-	-	-	Initial publication	12.0.0
SCP-59	SCP(13)000103	12.0.0	001	-	F	Definition of subscriber	12.1.0
SCP-59	SCP(13)000104	12.0.0	002	-	F	Management of the content of provisioning profiles	12.1.0
SCP-59	SCP(13)000105	12.0.0	003	-	F	Clarification of "platform-related commands"	12.1.0
SCP-59	SCP(13)000106	12.0.0	004	-	F	Clarification of "unexpected interruptions"	12.1.0
SCP-59	SCP(13)000107r1	12.0.0	005	1	F	Removal of redundant requirements	12.1.0
SCP-59	SCP(13)000108r1	12.0.0	006	1	F	Definitions of container term and container related activities	12.1.0
SCP-59	SCP(13)000109r1	12.0.0	007	1	B	Missing requirement on anti-cloning of profiles	12.1.0
SCP-59	SCP(13)000110r1	12.0.0	008	1	F	Credentials for container creation	12.1.0

History

Document history		
V12.0.0	February 2013	Publication
V12.1.0	June 2013	Publication