ETSI TS 103 383 V13.2.0 (2016-05)

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

Reference
RTS/SCP-REUICCVD20

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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.

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 referenced 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 referenced 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, local Profile disabling or local Profile deletion

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

Network Access Credentials: data required to authenticate to an Recommendation 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 Recommendation ITU E.212 [i.1] network for the purpose of accessing telecommunication and related services

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: Also known as Profile Provisioning Credentials holder.

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

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

3.1a Void

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
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.