ETSI TS 103 465 V16.3.0 (2020-11)

TECHNICAL SPECIFICATION

Smart Cards;
Smart Secure Platform (SSP);
Requirements Specification
(Release 16)

Reference

RTS/SCP-RSSPvg30

Keywords

interface, secure element, security, UICC

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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

The current specification of the (e)UICC is based on the ISO/IEC 7816 series [1] of specifications for IC-cards. This series of specifications has been developed in the 1980s and was suitable at that point in time but today limits the capabilities that are required by the market. The current (e)UICC specifications also link the form factor to the electrical interface and the logical protocol. This link limits the (e)UICC implementations to specified form factors.

New requirements are emerging, for example, inspired by embedded secure elements in terminals that are intended to provide security services or store data securely. Such embedded secure elements may come in different form factors and are intended to be integrated into the terminals architecture and using electrical and physical interfaces other than those used by the (e)UICC. Such secure elements could also provide the capability to store large amount of data to be protected which requires new and more efficient ways to store and manage data.

1 Scope

The present document defines the use cases and requirements for the definition of the interfaces and protocols for interfacing with a secure element. This secure element is called Smart Secure Platform (SSP).

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 https://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] ISO/IEC 7816 (all parts): "Identification cards -- Integrated circuit cards".

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

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

[4] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Physical and data link layer characteristics".

[5] SOG-IS: "Protection Profiles".

NOTE: Available at https://www.sogis.eu/uk/pp_en.html.

[6] ETSI TS 102 622: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)".

[7] ISO/IEC 7816-3: "Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols".

[8] ISO/IEC 7816-4: "Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange".

[9] ETSI TS 102 600: "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface".

[10] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System (3GPP TS 33.501 Release 15)".

[11] Security IC Platform BSI Protection Profile 2014 with Augmentation Packages.

NOTE: Available at https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf.

[12] Application of Attack Potential to Smartcards (V2.9) (01-2013).

NOTE: Available at https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v2-9.pdf.

[13] GlobalPlatform Card Technology: "Open Firmware Loader for Tamper Resistant Element".

NOTE: Available at https://globalplatform.org/specs-library/open-firmware-loader-for-tamper-resistant-element-v1-3/.

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

[15] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102)".

[16] Recommendation ITU-T X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[17] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

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

[19] ETSI TS 102 705: "Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications".

[20] ETSI TS 124 383: "LTE; Mission Critical Push To Talk (MCPTT) Management Object (MO) (3GPP TS 24.383)".

[21] ETSI TS 124 334: "Universal Mobile Telecommunications System (UMTS); LTE; Proximity-services (ProSe) User Equipment (UE) to ProSe function protocol aspects; Stage 3 (3GPP TS 24.334)".

[22] ETSI TS 132 277: "Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Charging management; Proximity-based Services (ProSe) charging (3GPP TS 32.277)".

[23] ETSI TS 124 333: "Universal Mobile Telecommunications System (UMTS); LTE; Proximity-services (ProSe) Management Objects (MO) (3GPP TS 24.333)".

[24] ETSI TS 124 385: "LTE; V2X services Management Object (MO) (3GPP TS 24.385)".

[25] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

[26] ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications".

[27] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[28] ETSI TS 134 108: "Universal Mobile Telecommunications System (UMTS); LTE; Common test environments for User Equipment (UE); Conformance testing (3GPP TS 34.108)".

[29] GSMA TS.37 (V4.0) (06/2018): "Requirements for Multi SIM Devices".

[30] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[31] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Numbering, addressing and identification (3GPP TS 23.003)".

[32] GSMA SGP.02 (V3.2) (06/2017): "Remote Provisioning Architecture for Embedded UICC Technical Specification".

[33] GSMA SGP.22 (V2.2.1) (12/2018): "RSP Technical Specification".

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

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] Void.

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

[i.3] ETSI TR 131 970: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; UICC power optimisation for Machine-Type Communication (MTC) (3GPP TR 31.970)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Certificate Issuer (CI): root CA which issues digital certificates to the certified entities in the SSP ecosystem

custodian: organization that defines family identifier specific requirements (e.g. trusted CIs, product certification) within its SSP ecosystem (e.g. iSSP and SPB Manager)

family identifier: identifier specified by GP OFL [13] that can be used to categorize secondary platform bundles

image: generic data format encapsulating a secondary platform bundle version and its cryptographic data to be used by the SPBL

internal Non Volatile Memory (iNVM): non volatile memory physically located inside an SSP

Local Bundle Assistant (LBA): entity in the terminal managing the secondary platform bundles

non-shareable memory regions: memory space that is declared by, and accessed by a single program

primary platform: hardware platform along with a low-level operating system managing the exceptions, the hardware platform resources and their accesses

NOTE: The primary platform is use case independent and technology dependent.

remote Non Volatile Memory (rNVM): non volatile memory physically located outside an iSSP

secondary platform: software platform using the primary platform interface and containing the high-level operating system on top of which the SSP applications are running

Secondary Platform Bundle (SPB): secondary platform along with its SSP applications

Secondary Platform Bundle Loader (SPBL): application, requiring system specific privileges, used to load a secondary platform bundle

Secondary Platform Bundle Loader agent: part of the local bundle assistant managing the communication with the secondary platform bundle manager and the transfer of the image to secondary platform bundle loader on the SSP

Secondary Platform Bundle Manager (SPBM): entity which builds an image on behalf of the service provider this image belongs to and securely delivers it to the SPBL on the target iSSP through the SPBL agent

Secondary Platform Bundle metadata: information belonging to a secondary platform bundle used for the purpose of management of the SPB

Secure Element (SE): tamper-resistant dedicated platform, consisting of hardware and software, capable of securely hosting applications and their confidential and cryptographic data and providing a secure application execution environment

SSP activation code: information issued by a Service Provider used by the LBA to initiate the download of an SPB

SSP application: application running on the top of an SSP OS (e.g. USIM)

SSP class: configuration of the SSP in accordance with a business requirement

SSP information: information of the primary platform and the SPBL which is used for the eligibility checking of the iSSP by the SPB manager

SSP maker: entity which manufactures the SSP

SSP OS: operating system compliant with the SSP specifications

telecom bundle: secondary platform bundle which contains or is intended to contain at least one 3GPP NAA

EXAMPLE: A secondary platform bundle providing functions as defined in the GSMA remote SIM provisioning specifications GSMA SGP.02 [32], GSMA SGP.22 [33] or 3GPP specification ETSI TS 131 102 [15] would be classified as a telecom bundle.

telecom bundle class: indicates the sort of a telecom bundle (e.g. operational, provisioning, test, eSIM), with which the iSSP and the terminal can handle the telecom bundle appropriately

telecom bundle concurrency capability: parameter which is set on the iSSP, indicating the number of distinct concurrent 3GPP/3GPP2 network registrations based on different subscriber identifier, supported by the cellular baseband capability inside the SoC containing the iSSP

EXAMPLE: "1" for a baseband supporting single-SIM, and "2" for a baseband supporting dual-SIM (either dual-SIM dual-active or dual-SIM dual-standby).

telecom family identifier: family identifier having a reserved value, used to class a secondary platform bundle as a telecom bundle

terminal information: information of the terminal which is used for the eligibility checking of the terminal by the SPB Manager

test telecom bundle: telecom bundle containing a 3GPP NAA which is intended to access a 3GPP test network (e.g. a network compliant with ETSI TS 134 108 [28])

3.2 Symbols

Void.

3.3 Abbreviations

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

CI	Certificate Issuer
eSSP	embedded SSP
HPSIM	Hosting Party Subscription Identity Module
iNVM	internal Non-Volatile Memory
iSSP	integrated SSP
LBA	Local Bundle Assistant
LPWA	Low Power Wide Area

M2M	Machine to Machine (communication)
MCPTT	Mission Critical Push ToTalk
NVM	Non Volatile Memory
OFL	Open Firmware Loader
PPI	Primary Platform Interface
rNVM	remote Non-Volatile Memory
rSSP	removable SSP
SCL	SSP Common Layers
SE^{TS}	Secure Element
SOG-IS	Senior Officials Group - Information Systems Security
SPB	Secondary Platform Bundle
SPBL	Secondary Platform Bundle Loader
SPBM	Secondary Platform Bundle Manager
SSP	Smart Secure Platform

4 Abstract (informative)

The present document describes the use case and requirements for the definition of a new secure element and its interfaces, superseding the interfaces currently defined for a UICC. By defining these interfaces, a new type of secure element will be defined called a Smart Secure Platform (SSP). The present document aims at defining the requirements for the SSP interfaces related security, the power management, the access to common protocol layer and a common protocol layer in the protocol stack of the SSP which is independent of any of its optional underlying and upper communication layers. This common layer will be supported by several underlying communication layers defined in optional SSP classes. The goal is also to solve the obsolescence of the ISO/IEC 7816-4 [8].

Figure 1 shows the layout of the SSP protocol stack.