ETSI TS 103 666-2 V15.0.0 (2019-11)

Smart Secure Platform (SSP);
Part 2: Integrated SSP (iSSP) characteristics
(Release 15)

Reference
DTS/SCP-00TSSPvf00-2

Keywords
M2M, MFF

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

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.

The present document is part 2 of a multi-part deliverable covering Smart Secure Platform (SSP), as identified below:

Part 1: "General characteristics";

Part 2: "Integrated SSP (iSSP) characteristics".

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.

1 Scope

The present document details the technical specifications for the Smart Secure Platform (SSP) integrated into an SoC, also known as iSSP. The present document defines specific attributes on top of the generic SSP specified in ETSI TS 103 666-1 [3].

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

[3] ETSI TS 103 666-1: "Smart Secure Platform (SSP); Part 1: General characteristics".

[4] BSI-CC-PP-0084-2014: "Security IC Platform Protection Profile with Augmentation Packages".

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

[5] BSI-CC-PP-0089-2015: "Embedded UICC Protection Profile, Version 1.1 25.08.2015".

NOTE: Available at https://www.commoncriteriaportal.org/files/ppfiles/pp0089a_pdf.pdf.

[6] GlobalPlatform Card Technology: "Open Firmware Loader for Tamper Resistant Element", Version 1.3.

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

[7] GlobalPlatform Technology: "VPP - Concepts and Interfaces", Version 1.0.1.

NOTE: Available at https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform-v1-0-1/.

[8] GlobalPlatform Technology: "Virtual Primary Platform - Firmware Format", Version 1.0.1.

NOTE: Available at https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform-v1-0-1/.

[9] GlobalPlatform Technology: "VPP - OFL VNP Extension", Version 1.0.1.

NOTE: Available at https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform-v1-0-1/.

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

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

[12] NISTIR 7298: "Glossary of Key Information Security Terms".

[13] NIST 800-108: "Recommendation for Key Derivation Using Pseudorandom Functions".

[14] BSI: "Functionality classes and evaluation methodology for deterministic random number generators", Reference: AIS20, version 1, 02/12/1999.

[15] BSI: "Functionality classes and evaluation methodology for physical random number generators", Reference:AIS31, version 1, 25/01/2001.

[16] "Application of Attack Potential to Smartcards and Similar Devices", v3.0, April 2019.

NOTE: Available at https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-0.pdf.

[17] "Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components", September 2012 Version 3.1 Revision 4.

NOTE: Available at https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf.

[18] NIST 800-56A: "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revision 2)", May, 2013.

[19] IETF RFC 5639: "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation".

[20] ANSI X9.62-2005: "Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)".

[21] ISO/IEC 14888-3:2018: "IT Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms".

[22] ISO/IEC 10118-3:2018: "IT Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions".

[23] BSI TR-03111: "Elliptic Curve Cryptography", Version 2.10.

[24] IETF draft-shen-sm2-ecdsa-02: "SM2 Digital Signature Algorithm".

[25] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[26] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[27] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[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] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

[30] IETF RFC 5758: "Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA".

[31] Recommendation ITU-T X.501 (ISO/IEC 9594-2:2005): "Information technology - Open Systems Interconnection - The Directory: Models".

[32] IETF RFC 4868: "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec".

[33] NIST SP 800-38B (May 2005): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

NOTE: Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38B.pdf.

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

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

[36] ISO 7816: "Identification cards -- Integrated circuit cards".

[37] IETF RFC 5754: "Using SHA2 Algorithms with Cryptographic Message Syntax".

[38] GlobalPlatform Technology: "Card Specification", Version 2.3.1.

NOTE: Available at https://globalplatform.org/specs-library/card-specification-v2-3-1/.

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.

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

[i.1] BSI-DSZ-CC-0827-V7-2018: "Security IC Platform Protection Profile, Version 1.0, 15 June 2007".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 666-1 [3] and the following apply:

3GPP network registration: procedure defined by 3GPP allowing a terminal to get access to services provided by telecommunication networks compliant with 3GPP specifications, using the subscription information stored within the said terminal in a SIM, a USIM or an ISIM application

address space: set of addresses that can be used by a particular program or functional unit

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

family identifier: UUID identifying a family of Secondary Platform Bundles. It is equivalent to Firmware Family in GP OFL specification [6]

plaintext: intelligible data that has meaning and can be understood without the application of decryption (see NISTIR 7298 [12])

process: independent sequences of execution running within independent virtual address space and which may have shared virtual memories with other processes (e.g. virtual shared memory for communication between processes)

program: independent set of instructions executed by CPU

Secondary Platform Bundle (SPB) container: packaged code and data to create a Secondary Platform Bundle instance

Secondary Platform Bundle (SPB) image: data encapsulating an encrypted Secondary Platform Bundle container and cryptographic data to extract a Secondary Platform Bundle container

Secondary Platform Bundle (SPB) instance: runtime instance of the container, running on top of the Primary Platform Interface

Secondary Platform Bundle (SPB) loader: Secondary Platform Bundle instance with special privileges that enable managing Secondary Platform Bundle containers

Secondary Platform Bundle (SPB) management operation: operation related to the state of the Secondary Platform Bundle, including its enablement, its disablement and its deletion

Secondary Platform Bundle (SPB) provisioning: sequence of operations related to the downloading of a Secondary Platform Bundle from a SPB Manager, its loading and its installation within the iSSP

service: hardware dependent low level software running in unprivileged mode

telecom Secondary Platform Bundle (SPB): Secondary Platform Bundle (SPB) which contains or is intended to contain at least one 3GPP NAA

telecom family identifier: family identifier having a reserved value, used to identify a Secondary Platform Bundle as a Telecom Secondary Platform Bundle

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])

user intent: direct, real time acquisition and validation of the end user input on the LBA to trigger locally a Secondary Platform Bundle provisioning or a Secondary Platform Bundle management operation

virtual address: in a virtual storage system, the address assigned to a storage location in external storage (i.e. outside the SE) to allow that location to be accessed as though it were part of main storage (i.e. inside the SE)

virtual address space: set of virtual addresses that can be used by a particular program or functional unit

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 666-1 [3] and the following apply:

ABI	Application Binary Interface
API	Application Programming Interface
HLOS	High Level Operating System
iNVM	(internal NVM) Non-Volatile Memory inside the SSP
iRAM	(internal RAM) volatile random access memory inside the SSP
MMF	Memory Management Function
OID	Object IDentifier
PRF	Pseudorandom Function family
rNVM	(remote NVM) Non-Volatile Memory outside the SE
rRAM	(remote RAM) volatile random access memory outside the SSP
SPB	Secondary Platform Bundle

4 Introduction

4.1 Document Layout

The present document specifies:

- an overview of the iSSP;
- the iSSP architecture;
- the Primary Platform, including the hardware platform requirements and services;
- the Primary Platform Interface;
- the Secondary Platform Bundle;
- the communication interface, including the protocol stack layers;
- the certification requirements for the iSSP.

4.2 ASN.1 syntax

4.2.1 Introduction

The provisions of ETSI TS 103 666-1 [3], clause 4.4.1 shall apply.

The complete ASN.1 code is provided for reference in Annex B.

4.2.2 Start of ASN.1

```
-- ASN1START

ISSPDefinitions { itu-t (0) identified-organization (4) etsi (0) smart-secure-platform (3666) part2
(2) }
DEFINITIONS
AUTOMATIC TAGS
EXTENSIBILITY IMPLIED ::=
BEGIN

/* Imports */

IMPORTS
    Certificate, Time, AlgorithmIdentifier
        FROM PKIX1Explicit88 {iso(1) identified-organization(3) dod(6) internet(1) security(5)
mechanisms(5) pkix(7) id-mod(0) id-pkix1-explicit(18)}
    SubjectKeyIdentifier
        FROM PKIX1Implicit88 {iso(1) identified-organization(3) dod(6) internet(1) security(5)
mechanisms(5) pkix(7) id-mod(0) id-pkix1-implicit(19)};

-- ASN1STOP
```


5 Overview

5.1 Description

An iSSP is an integrated SSP confined in a dedicated sub-system within an SoC. The SoC is usually soldered in the terminal and so the SSP is an integral part of the terminal.

The iSSP is a composition of three parts as described in clause 6.1.