ETSI TS 103 666-4 V17.0.0 (2022-04)

TECHNICAL SPECIFICATION

Smart Secure Platform (SSP);
Part 4: Embedded SSP (eSSP) Type 2 characteristics
(Release 17)

Reference
DTS/SCP-T00TSSPvh00-4

Keywords
eSSP, SSP

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

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

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

ETSI

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Secure Element Technologies (SET).

The contents of the present document are subject to continuing work within TC SET and may change following formal TC SET approval. If TC SET 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 SET for information;

2 presented to TC SET for approval;

3 or greater indicates TC SET 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 4 of a multi-part deliverable covering Smart Secure Platform (SSP), as identified below:

Part 1: "General characteristics";

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

Part 3: "Embedded SSP (eSSP) Type 1 characteristics";

Part 4: "Embedded SSP (eSSP) Type 2 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) in a discrete non removable hardware component, also known as eSSP. The present document defines specific attributes on top of the generic SSP specified in ETSI TS 103 666-1 [1] for eSSP Type 2, including the external interfaces (e.g. ISO 7816 [9], SPI, SWP). More in details the physical layer and related features are inherited from ETSI TS 103 666-3 [3] and the software architecture with virtualization interface, based on ETSI TS 103 666-2 [2].

2 References

2.1 Normative references

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

- In the case of a reference to a TC SET 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] ETSI TS 103 666-1: "Smart Secure Platform (SSP); Part 1: General characteristics".

[2] ETSI TS 103 666-2: "Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics".

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

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

[5] GlobalPlatform® Technology: "Virtual Primary Platform - Network Protocol", Version 2.0.

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

[6] GlobalPlatform® Technology: "Virtual Primary Platform - Concepts and Interfaces", Version 2.0.

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

[7] GlobalPlatform® Technology: "Virtual Primary Platform - VPP Firmware Format", Version 2.0.

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

[8] GlobalPlatform® Technology: "Virtual Primary Platform - OFL VNP Extension", Version 2.0.

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

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

[10] 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.

2.2 Informative references

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

- In the case of a reference to a TC SET 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.

Not applicable.

2.3 External references

The present document contains several references to other specifications, therefore required replacements as defined in ETSI TS 103 666-1 [1], clause 4.3 shall apply. As the present document targets the eSSP Type 2 class, word "SSP" from ETSI TS 103 666-1 [1] and the word "iSSP" from ETSI TS 103 666-2 [2] shall be replaced with "eSSP Type 2" as needed.

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 [1], clause 3.1, ETSI TS 103 666-2 [2], clause 3.1 and ETSI TS 103 666-3 [3], clause 3.1 apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 666-1 [1], clause 3.3, ETSI TS 103 666-2 [2], clause 3.3 and ETSI TS 103 666-3 [3], clause 3.3 apply.

3.4 References to GlobalPlatform

The present document contains references to the GlobalPlatform VPP specifications: either with direct references or with indirect references through ETSI TS 103 666-1 [1], ETSI TS 103 666-2 [2] or ETSI TS 103 666-3 [3]. Where the GlobalPlatform VPP specifications are referred, the documents VPP - Concepts and Interfaces [6], Virtual Primary Platform - Firmware Format [7], VPP - OFL VNP Extension [8] and Virtual Primary Platform - Network Protocol [5] shall apply.

NOTE: Care should be taken due to the fact that some clause numbers in the GlobalPlatform VPP specifications [5], [6], [7] and [8] may have changed compared to previous versions.

The provisions of ETSI TS 103 666-2 [2], clause 5.3 shall apply with the following exception:

- Tamper Resistant Element (TRE) refers to the eSSP Type 2.

4 Introduction

4.1 Overview

The present document defines an embedded secure element which allows different combinations of form factors, physical and electrical interfaces, transport layers, file system and security requirements based on the targeted use-case.

This secure element is called embedded Smart Secure Platform (eSSP) Type 2 and is a specific class of SSP defined in ETSI TS 103 666-1 [1]. This platform is defined to be flexible to use multiple physical interfaces and transport protocols.

The eSSP Type 2 implements virtualization interface as described in ETSI TS 103 666-1 [1], clause 5.2 and inherits all characteristics of eSSP Type-1 defined in ETSI TS 103 666-3 [3].

4.2 Document layout

The present document specifies:

- the eSSP Type 2 architecture, features and characteristics;

- 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 eSSP Type 2.

4.3 ASN.1 syntax

4.3.1 Introduction

The ASN.1 syntax defined in ETSI TS 103 666-1 [1], clause 4.4.1 shall apply.

4.3.2 Start of ASN.1

```
The complete ASN.1 code is provided for reference in Annex B.-- ASN1START

ESSPDefinitions { itu-t (0) identified-organization (4) etsi (0) smart-secure-platform (3666) part4 (4) }

DEFINITIONS
AUTOMATIC TAGS
EXTENSIBILITY IMPLIED ::=
BEGIN
IMPORTS
  /* Basic types */
  maxUInt32, UInt32,
  /* Common types */
  UUID, URI, Certificates, VersionType

FROM
  SSPDefinitions { itu-t (0) identified-organization (4) etsi (0) smart-secure-platform (3666) part1 (1) };

-- ASN1STOP
```

5 eSSP Type 2 architecture

5.1 Overview

The provisions of ETSI TS 103 666-2 [2], clause 6.1 shall apply.

5.2 Functional Architecture

The provisions of ETSI TS 103 666-2 [2], clause 6.2 shall apply.

5.3 Security Perimeters

The provisions of ETSI TS 103 666-2 [2], clause 6.3 shall apply.

5.4 Unprivileged Execution Mode

The provisions of ETSI TS 103 666-2 [2], clause 6.4 shall apply.

5.5 Unprivileged Virtual Address Space

The provisions of ETSI TS 103 666-2 [2], clause 6.5 shall apply.

5.6 Run time Model

The provisions of ETSI TS 103 666-2 [2], clause 6.6 shall apply.

6 Primary Platform

6.1 Hardware Platform

6.1.1 Architecture

The provisions of GlobalPlatform VPP - Concepts and Interfaces [6], clause 3.1 shall apply with the following exceptions:

- the eSPP Type 2 shall contain an autonomous and independent clock system;

- the eSPP Type 2 shall contain communication functions;

- the eSPP Type 2 may contain the data protection hardware function.

6.1.2 Form factor

The eSSP Type 2 form factor may comply with ETSI TS 102 671 [4] with the exception of MFF1.

6.1.3 Security functions

6.1.3.1 Hardware Platform isolation

The provisions of ETSI TS 103 666-2 [2], clause 7.1.3.1 shall apply.

6.1.3.2 Memory Management Function

The provisions of ETSI TS 103 666-2 [2], clause 7.1.3.2 shall apply.

6.1.3.3 Key protection function

The provisions of ETSI TS 103 666-2 [2], clause 7.1.3.3 shall apply.

6.1.3.4 Remote audit

The provisions of ETSI TS 103 666-2 [2], clause 7.1.3.7 shall apply.

6.1.3.5 Security sensor function

The provisions of ETSI TS 103 666-2 [2], clause 7.1.3.8 shall apply.

6.1.4 Memories

6.1.4.1 Non Volatile Memories

The Primary Platform shall provide the Secondary Platform with direct memory-mapped access to its embedded NVM.

6.1.4.2 Volatile memory

The Primary Platform shall provide the Secondary Platform with direct memory-mapped access to its embedded volatile memory.

6.1.5 Communication functions

The physical communication interfaces between the Primary Platform and the hardware it is integrated with is outside the scope of the present document. These are abstracted from the Secondary Platform by the interface defined in clause 7.2.

6.1.6 Power

6.1.6.1 Power mode

The power modes defined in ETSI TS 103 666-3 [3], clause 6.2.1 shall apply.

6.1.6.2 Power sources

6.1.6.2.1 Types of power sources

The type of power source defined in ETSI TS 103 666-3 [3], clause 6.2.2.1 shall apply.

6.1.6.2.2 Power source of type Interface

The power source of type interface defined in ETSI TS 103 666-3 [3], clause 6.2.2.2 shall apply.

6.1.6.2.3 Power source of type Independent

The power source of type independent defined in ETSI TS 103 666-3 [3], clause 6.2.2.3 shall apply.

6.1.6.3 Power consumption

The power consumption defined in ETSI TS 103 666-3 [3], clause 6.2.3 shall apply.

6.1.7 Cryptographic functions

The provisions of ETSI TS 103 666-2 [2], clause 7.1.7 shall apply.

6.1.8 Clock

The eSSP Type 2 shall support a clock as defined in ETSI TS 103 666-3 [3], clause 6.3.

6.1.9 Secure CPU

The characteristics of the CPUs (e.g. endianness) are implementation dependent and outside the scope of the present document. The CPU(s) shall be based at least on a 32-bit architecture.

6.1.10 Random Number Generator

The provisions of ETSI TS 103 666-2 [2], clause 7.1.11 shall apply.

6.2 Low-level Operating System

The provisions of ETSI TS 103 666-2 [2], clause 7.2 shall apply.

6.3 Services

The provisions of ETSI TS 103 666-2 [2], clause 7.3 shall apply.

6.4 Minimum level of interoperability

The provisions of ETSI TS 103 666-2 [2], clause 7.4 shall apply.

6.5 Primary Platform identification

The eSSP Type 2 shall be identified with an identifier based on the definition in ETSI TS 103 666-2 [2], clause 7.5 with the following exceptions:

- **SSP Type** identifies the type of SSP and is coded as follows:

Base-32 character	Value	Description
F	'00101'	Embedded SSP Type 2 (eSSP Type 2)

6.6 Provisioning of Primary Platform software

The provisions of GlobalPlatform VPP - Concepts and Interfaces [6], clause 5.7 REQ85 shall apply.

6.7 Part Number Identifier

The provisions of ETSI TS 103 666-2 [2], clause 7.7 shall apply.

7 Primary Platform Interface

7.1 Kernel functions ABI/API

The provisions of ETSI TS 103 666-2 [2], clause 8.1 shall apply.

7.2 Communication service interface

The provisions of ETSI TS 103 666-2 [2], clause 8.2 shall apply with the exception listed below:

- One of the end points of any dynamic pipe may be out the SSP host domain.

7.3 Secondary Platform Bundle management service interface

The provisions of ETSI TS 103 666-2 [2], clause 8.3 shall apply.

8 Secondary Platform Bundle

8.1 Introduction

The Secondary Platform Bundle refers to either the data container or the runtime instance of the container.

8.2 States

The provisions of ETSI TS 103 666-2 [2], clause 9.2 shall apply.

8.3 Secondary Platform Bundle container format

The provisions of ETSI TS 103 666-2 [2], clause 9.3 shall apply.

8.4 Secondary Platform

8.4.1 High-level OS

The provisions of ETSI TS 103 666-2 [2], clause 9.4.1 shall apply.

8.4.2 Execution framework

The provisions of ETSI TS 103 666-2 [2], clause 9.4.2 shall apply.

8.4.3 UICC platform as a Secondary Platform

The provisions of ETSI TS 103 666-2 [2], clause 9.4.3 shall apply.

8.4.4 Capability exchange

8.4.4.1 Overall description

The capability exchange procedure is used to inform the eSSP Type 2 of the capabilities of the terminal and for the terminal to retrieve the capabilities of the eSSP Type 2.

The capability exchange for eSSP Type 2 supporting SCL as defined in ETSI TS 103 666-1 [1], clause 6.4.2 apply with modifications provided below.

8.4.4.2 Capabilities of the terminal

The data field sent by the terminal to the eSSP Type 2 contains the data structure defined in ETSI TS 103 666-3 [3], clause 6.4.2.2.

8.4.4.3 Capabilities of the eSSP Type 2

The provisions of ETSI TS 103 666-3 [3], clause 6.4.2.3 shall apply with the following exception:

- SSPClass field shall have the eSSPClass-Embedded-Type2 (2) value.

8.4.5 Identifiers of Secondary Platform Bundle

The provisions of ETSI TS 103 666-2 [2], clause 9.4.5 shall apply.

8.5 SSP Application

The provisions of ETSI TS 103 666-2 [2], clause 9.5 and subclauses shall apply.

8.6 Lifecycle management of Secondary Platform Bundles

The provisions of ETSI TS 103 666-2 [2], clause 9.6 shall apply.

8.7 Secondary Platform Bundle family identifier

The provisions of ETSI TS 103 666-2 [2], clause 9.7 shall apply.

8.8 eSSP Type 2 suspension

If the eSSP Type 2 indicates it supports the suspension mechanism as defined in clause 8.4.4.3, the provisions defined in ETSI TS 103 666-1 [1], clause 6.9 shall apply with the modifications listed below:

- The suspension of the SSP should only be used if, in addition to the Secondary Platform Bundle Loader, only one Secondary Platform Bundle is Enabled on an eSSP Type 2.

- The Secondary Platform Bundle Enabled shall support the suspension mechanism.

- The Terminal shall not suspend the eSSP Type 2 if a Secondary Platform Bundle provisioning procedure is ongoing.

    NOTE: Suspension of eSSP Type 2 with multiple Secondary Platform Bundle is FFS.

9 Communication interface

9.1 eSSP Type 2 initialization

The eSSP Type 2 interface session defined in ETSI TS 103 666-1 [1], clause 6.4.1 shall apply.

9.2 Low level protocol layers

9.2.1 Physical layer

9.2.1.1 Overview

The provisions of ETSI TS 103 666-3 [3], clause 7.1 shall apply.

9.2.1.2 Reset

The eSSP Type 2 description in ETSI TS 103 666-3 [3], clause 7.2 shall apply.

9.2.1.3 SPI interface

The eSSP Type 2 may support an SPI interface, in that case the clauses ETSI TS 103 666-3 [3], clause 7.4 and subclauses shall apply.

9.2.1.4 I2C interface

The eSSP Type 2 may support an I2C interface, in that case the clauses ETSI TS 103 666-3 [3], clause 7.5 and subclauses shall apply.

9.2.1.5 SWP interface

The eSSP Type 2 may support an SWP interface, in that case the clauses ETSI TS 103 666-3 [3], clause 7.6 and subclauses shall apply.

9.2.1.6 USB interface

The eSSP Type 2 may support an USB interface, in that case the clauses ETSI TS 103 666-3 [3], clause 7.7 and subclauses shall apply.

9.2.2 Link layer

The provisions of ETSI TS 103 666-1 [1], clause 8.3.1 shall apply.

9.3 SSP Common Layer

9.3.1 introduction

The eSSP Type 2 shall support the SCL protocol, therefore the provisions defined in ETSI TS 103 666-1 [1], clause 8 and subclauses shall apply, with the exception listed below:

- The SCL network controller host and SCL router need not to share the same security perimeter of the eSSP Type 2, i.e. the SCL network controller host and SCL router are not required to have an equivalent level of security when compared with the eSSP Type 2.

Each Secondary Platform Bundle is responsible for the implementation of the SCL protocol as needed for its operation.

9.3.2 eSSP Type 2 with only one SCL interface

If the eSSP Type 2 has only one SCL interface, this interface should convey packets to multiple SCL hosts outside the SSP host domain, as illustrated in ETSI TS 103 666-3 [3], clause B.1.

9.3.3 eSSP Type 2 with multiple SCL interfaces

If the eSSP Type 2 has multiples SCL interfaces, all these interfaces should belong to the same SCL network. Furthermore, the eSSP Type 2 should implement the SCL router and SCL network controller host, as illustrated in ETSI TS 103 666-3 [3], clause B.2.

SCL hosts of an host domain should be accessible only through one SCL interface. The communication inside the eSSP Type 2 between the eSSP Type 2 Host, the router and the SCL network controller host are out of the scope of the present document.

9.4 Communication layers above SCL

The definition and usage of protocols layers above the SCL (e.g. ISO 7816 [9] APDUs) are defined in ETSI TS 103 666-1 [1], clause 10.

10 Certification

10.1 Introduction

The eSSP Type 2 shall be able to support a certification by composition of a Secondary Platform Bundle from the Primary Platform certification.

10.2 Primary Platform certification

10.2.1 Overview

The provisions of GlobalPlatform VPP - Concepts and Interfaces [6], clause 4 shall apply. The certification of the Primary Platform shall include the Loader Package 2, as defined in BSI-CC-PP-0084-2014 [10].

10.2.2 Security Capabilities

The provisions of ETSI TS 103 666-2 [2], clause 11.2.2 shall apply.

10.3 Secondary Platform Bundle certification

The provisions of ETSI TS 103 666-2 [2], clause 11.3 shall apply.

11 eSPP Type 2 ecosystem and interfaces

The provisions of ETSI TS 103 666-2 [2], clause 12 and subclauses shall apply.

Annex A (normative):
Additions for Telecom Secondary Platform Bundles

The provisions of ETSI TS 103 666-2 [2], Annex A shall apply.

Annex B (normative):
ASN.1 definitions

B.1 End of ASN.1

```
-- ASN1START

END

-- ASN1STOP
```

B.2 Complete ASN.1 file

The complete ASN.1 definition, as generated merging all the ASN.1 snippets present in the present document is available here:

```
ESSPDefinitions { itu-t (0) identified-organization (4) etsi (0) smart-secure-platform (3666) part4
(4) }

DEFINITIONS
AUTOMATIC TAGS
EXTENSIBILITY IMPLIED ::=
BEGIN
IMPORTS
                /* Basic types */      maxUInt32, UInt32,                /* Common types
*/              UUID, URI, Certificates, VersionType

FROM
                SSPDefinitions { itu-t (0) identified-organization (4) etsi (0) smart-secure-
platform (3666) part1 (1) };

END
```

History

Document history		
V17.0.0	April 2022	Publication