

ETSI TS 103 666-2 V17.1.0 (2024-12)



Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics (Release 17)

Document Preview

[ETSI TS 103 666-2 V17.1.0 \(2024-12\)](https://standards.iteh.ai/catalog/standards/etsi/8fbcc90d-f092-4365-961d-8d72e5173680/etsi-ts-103-666-2-v17-1-0-2024-12)

[https://standards.iteh.ai/catalog/standards/etsi/8fbcc90d-f092-4365-961d-8d72e5173680/etsi-ts-103-666-2-v17-1-0-2024-](https://standards.iteh.ai/catalog/standards/etsi/8fbcc90d-f092-4365-961d-8d72e5173680/etsi-ts-103-666-2-v17-1-0-2024-12)

Reference

RTS/SET-T103666-2vh10

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 - 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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	8
Foreword.....	8
Modal verbs terminology.....	9
1 Scope	10
2 References	10
2.1 Normative references	10
2.2 Informative references.....	12
3 Definition of terms, symbols and abbreviations.....	12
3.1 Terms.....	12
3.2 Symbols.....	13
3.3 Abbreviations	13
4 Introduction	14
4.1 Document Layout	14
4.2 ASN.1 syntax	14
4.2.1 Introduction.....	14
4.2.2 Start of ASN.1	14
5 Overview	14
5.1 Description	14
5.2 Security requirements.....	15
5.3 References to GlobalPlatform	15
6 iSSP Architecture	15
6.1 Overview	15
6.2 Functional architecture	16
6.3 Security perimeters.....	16
6.4 Unprivileged execution model	16
6.5 Unprivileged virtual address space	16
6.6 Run time model.....	16
7 Primary Platform	17
7.1 Hardware Platform	17
7.1.1 Architecture	17
7.1.2 Form factor	17
7.1.3 Security functions	17
7.1.3.1 Hardware Platform isolation	17
7.1.3.2 Memory Management Function	17
7.1.3.3 Key protection function.....	17
7.1.3.4 Data protection hardware function.....	17
7.1.3.5 Memory transfer function	18
7.1.3.6 Test functions	18
7.1.3.7 Remote audit	18
7.1.3.8 Security sensor function	18
7.1.4 Memories	18
7.1.4.1 Non Volatile Memories.....	18
7.1.4.2 Volatile memory	18
7.1.5 Communication functions.....	18
7.1.6 Power.....	18
7.1.7 Cryptographic functions	18
7.1.8 Clock.....	19
7.1.9 SSP internal interconnect.....	19
7.1.10 Secure CPU.....	19
7.1.11 Random Number Generator.....	19
7.2 Low-level Operating System.....	19
7.2.1 Introduction.....	19

7.2.2	Kernel objects	19
7.2.3	Global requirements and mandatory Access Control rules	19
7.2.4	Process states diagram	19
7.2.5	Definition of the process states	19
7.2.6	Mandatory access control	19
7.3	Services	20
7.3.1	Secondary Platform Bundle Loader	20
7.3.1.1	Overview	20
7.3.1.2	Registries	20
7.3.1.3	Commands	21
7.3.1.4	Responses	21
7.3.1.5	Firmware session	22
7.3.2	Communication service	22
7.3.3	Management service	22
7.4	Minimum level of interoperability	22
7.5	Primary Platform identification	22
7.6	Provisioning of Primary Platform software	23
7.7	Part Number Identifier	23
8	Primary Platform Interface	23
8.1	Kernel functions ABI/API	23
8.2	Communication service interface	23
8.3	Secondary Platform Bundle management service interface	24
9	Secondary Platform Bundle	24
9.1	Introduction	24
9.2	States	24
9.3	Secondary Platform Bundle container format	25
9.4	Secondary Platform	25
9.4.1	High-level OS	25
9.4.2	Execution framework	25
9.4.3	UICC platform as a Secondary Platform	25
9.4.4	Capability exchange	26
9.4.5	Identifiers of Secondary Platform Bundle	26
9.5	SSP Application	26
9.5.1	Overview	26
9.5.2	Lifecycle management	26
9.6	Lifecycle management of Secondary Platform Bundles	27
9.7	Secondary Platform Bundle family identifier	27
10	Communication interface	27
10.1	Low level protocol layers	27
10.1.1	Physical layer	27
10.1.2	Link layer	27
10.2	SSP Common Layer	27
10.3	Communication layers above SCL	27
11	Certification	28
11.1	Introduction	28
11.2	Primary Platform certification	28
11.2.1	Overview	28
11.2.2	Security Capabilities	28
11.3	Secondary Platform Bundle certification	29
12	iSSP ecosystem and interfaces	30
12.1	General architecture	30
12.1.1	Introduction	30
12.1.2	Architecture overview	30
12.1.3	Entities	30
12.1.4	Interfaces	31
12.2	Security overview	31
12.2.1	Public key infrastructures	31
12.2.1.1	Public key infrastructure for Si4 interface	31
12.2.1.1.1	Certificate chains	31

12.2.1.1.2	Certificate description	32
12.2.1.1.3	Algorithm identifiers and parameters	35
12.2.1.1.4	Certification path verification.....	36
12.2.1.1.5	Certificate revocation status verification	37
12.2.2	Cryptographic algorithms	37
12.2.2.1	Elliptic curve domain parameter sets	37
12.2.2.2	Digital signature algorithm	37
12.2.2.3	Key agreement algorithm.....	37
12.2.2.4	Block cipher algorithm.....	38
12.3	Secondary Platform Bundle provisioning procedure.....	38
12.3.1	Overview	38
12.3.2	Preparation procedure	39
12.3.2.1	Overview	39
12.3.2.2	Secondary Platform Bundle selection process	40
12.3.2.3	Service provider reference creation process.....	40
12.3.2.4	Cancellation of the preparation procedure	41
12.3.3	Download procedure.....	41
12.3.3.1	Capability negotiation	41
12.3.3.2	Bound SPB image download.....	44
12.3.4	Installation procedure	46
12.3.5	SSP activation code	47
12.4	Secondary Platform Bundle management procedure.....	48
12.4.1	Enable a Secondary Platform Bundle	48
12.4.2	Disable a Secondary Platform Bundle	48
12.4.3	Delete a Secondary Platform Bundle	49
12.4.4	SPB metadata retrieving procedure	50
12.4.5	SPB state retrieving procedure.....	50
12.5	Notification procedure.....	51
12.5.1	Overview	51
12.5.2	Notification of the service provider	51
12.5.3	Notification from the LBA	52
12.6	Interfaces and functions.....	53
12.6.1	Overview	53
12.6.2	Common features.....	53
12.6.2.1	Common data types.....	53
12.6.2.2	SSP information	54
12.6.2.2.1	Introduction	54
12.6.2.2.2	Public SSP information	54
12.6.2.2.3	Protected SSP information.....	55
12.6.2.3	SPBM credential	56
12.6.2.4	SSP credential	56
12.6.2.5	Bound SPB image	58
12.6.2.6	SPB metadata	59
12.6.2.7	Terminal information	60
12.6.2.8	Notification token	61
12.6.3	Si1 interface	62
12.6.3.1	Overview	62
12.6.3.2	Si1 common headers	62
12.6.3.2.1	Si1 command header	62
12.6.3.2.2	Si1 response header	62
12.6.3.3	Si1 error codes	62
12.6.3.4	Si1.SelectSpb	63
12.6.3.4.1	Command	63
12.6.3.4.2	Procedure.....	64
12.6.3.4.3	Response.....	65
12.6.3.5	Si1.CreateSPReference	65
12.6.3.5.1	Command	65
12.6.3.5.2	Procedure.....	66
12.6.3.5.3	Response.....	67
12.6.3.6	Si1.FinalizePreparation	67
12.6.3.6.1	Command	67
12.6.3.6.2	Procedure.....	68

12.6.3.6.3	Response.....	68
12.6.3.7	Si1.CancelPreparation.....	69
12.6.3.7.1	Command	69
12.6.3.7.2	Procedure.....	69
12.6.3.7.3	Response.....	70
12.6.3.8	Si1.HandleNotification.....	70
12.6.3.8.1	Command	70
12.6.3.8.2	Procedure.....	72
12.6.4	Si2 interface	72
12.6.4.1	Overview	72
12.6.4.2	Si2.GetSpbmCertificate	72
12.6.4.2.1	Command	72
12.6.4.2.2	Procedure.....	73
12.6.4.2.3	Response.....	74
12.6.4.3	Si2.GetBoundSpbImage.....	75
12.6.4.3.1	Command	75
12.6.4.3.2	Procedure.....	76
12.6.4.3.3	Response.....	78
12.6.4.4	Si2.HandleNotification.....	79
12.6.4.4.1	Command	79
12.6.4.4.2	Procedure.....	79
12.6.4.4.3	Response.....	80
12.6.5	Si3 interface	80
12.6.5.1	Overview	80
12.6.5.2	Registries.....	80
12.6.5.3	Commands	80
12.6.5.4	Responses.....	80
12.6.5.5	Functions.....	80
12.6.5.5.1	Si3.GetSpInfo	80
12.6.5.5.2	Si3.SetSpbmCredential.....	82
12.6.5.5.3	Si3.LoadBoundSpbInfo	83
12.6.5.5.4	Si3.LoadBoundSpbSds	84
12.6.5.5.5	Si3.LoadBoundSpbSeg.....	84
12.6.5.5.6	Si3.GetSpCredential.....	85
12.6.5.5.7	Si3.EnableSpb	85
12.6.5.5.8	Si3.DisableSpb	85
12.6.5.5.9	Si3.DeleteSpb	86
12.6.5.5.10	Si3.GetSpbMetadata	86
12.6.5.5.11	Si3.UpdateSpbState	86
12.6.5.5.12	Si3.GetSpbState	86

Annex A (normative): Additions for Telecom Secondary Platform Bundles88

A.1	Telecom family identifier.....	88
A.2	Data types for telecom family identifier.....	88
A.2.1	Introduction	88
A.2.2	SSP information	88
A.2.3	Terminal information	88
A.3	SPB metadata for the telecom family identifier	89
A.4	Terminal behaviour	89
A.5	Telecom Secondary Platform Bundle management	89
A.5.1	Introduction	89
A.5.2	Switch Telecom Secondary Platform Bundles	90
A.6	Si3 interface function for telecom family identifier	90
A.6.1	Introduction	90
A.6.2	Si3.SwitchSpb	90

Annex B (normative): ASN.1 definitions92

B.1	End of ASN.1	92
-----	--------------------	----

B.2 Complete ASN.1 file92

Annex C (normative): Bundle eligibility check93

C.1 Introduction93

C.2 Basic eligibility check93

C.2.1 Summary93

C.2.2 Version compatibility check.....93

C.2.3 Bundle compatibility check93

C.2.4 Primary platform identifier check93

C.3 Family identifier-specific eligibility check94

Annex D (informative): UML code of figures95

Annex E: Void96

Annex F (informative): Change history97

History98

i T h S t a n d a r d s
(h t t p s : / / s t a n d a r d s . i t
D o c u m e n t i e P w r

h t t p s : / / s t a n d a r d s . i t e h . a i / c a t a l o g / s t a n d
E T T S S I 1 0 3 6 6 6 . 2 (2 0 2 4 - 1 2)
1 2

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 IPR online database](https://standards.itsc.ai).

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™**, **LTE™** and **5G™** logo 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 2 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.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 103 666-2 V17.1.0 \(2024-12\)](#)

<https://standards.iteh.ai/catalog/standards/etsi/8fbcc90d-f092-4365-961d-8d72e5173680/etsi-ts-103-666-2-v17-1-0-2024-12>

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 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 in the [ETSI docbox](#).

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".
- [5] [BSI-CC-PP-0089-2015](#): "Embedded UICC Protection Profile, Version 1.1 25.08.2015".
- [6] GlobalPlatform Technology: "[Open Firmware Loader for Tamper Resistant Element](#)", Version 1.3.
- [7] GlobalPlatform Technology: "[Virtual Primary Platform - Concepts and Interfaces](#)", Version 2.0.
- [8] GlobalPlatform Technology: "[Virtual Primary Platform - Firmware Format](#)", Version 2.0.
- [9] GlobalPlatform Technology: "[Virtual Primary Platform - OFL VNP Extension](#)", Version 1.0.
- [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] Void.
- [13] [NIST 800-108](#): "Recommendation for Key Derivation Using Pseudorandom Functions".
- [14] [BSI AIS 20, version 1 \(02/12/1999\)](#): "Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators".
- [15] [BSI AIS 31, version 3.1 \(25/09/2001\)](#): "Functionality classes and evaluation methodology for true (physical) random number generators".
- [16] Joint Interpretation Library: "[Application of Attack Potential to Smartcards and Similar Devices](#)", v3.1, June 2020.

- [17] [CCMB-2017-04-003](#): "Common Criteria for Information Technology Security Evaluation; Part 3: Security assurance components", April 2017 Version 3.1 Revision 5.
- [18] [NIST 800-56A Revision 2](#): "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography", May 2013.
- [19] [IETF RFC 5639](#): "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation".
- [20] [ANSI X9.142-2020](#): "Financial services - 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] [draft-sca-cfrg-sm3-02](#): "The SM3 Cryptographic Hash Function".
- [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] Void.
- [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 \(10/2019\) \(ISO/IEC 9594-2:2020\)](#): "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".
- [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 \(all parts\)](#): "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.
- [39] [IETF RFC 4648](#): "The Base16, Base32, and Base64 Data Encodings".
- [40] [ETSI TS 123 003](#): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification (3GPP TS 23.003)".
- [41] [ETSI TS 129 002](#): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Mobile Application Part (MAP) specification (3GPP TS 29.002)".
- [42] [IETF RFC 3986](#): "Uniform Resource Identifier (URI): Generic Syntax".

- [43] [Recommendation ITU-T E.212](#): "The international identification plan for public networks and subscriptions".
- [44] [ISO/IEC 18033-3:2010/Amd 1:2021](#): "Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers — Amendment 1: SM4".

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 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.

- [i.1] BSI-DSZ-CC-0827-V7-2018: "Security IC Platform Protection Profile", Version 1.0, 15 June 2007.
- [i.2] Void.
- [i.3] [NIST IR 7298](#): "Glossary of Key Information Security Terms".
- [i.4] [ETSI TS 134 108](#): "Universal Mobile Telecommunications System (UMTS); LTE; Common test environments for User Equipment (UE); Conformance testing (3GPP TS 34.108)".

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

NOTE: 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 NIST IR 7298 [i.3])

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

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

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 [i.4])

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
ISN	Individual Serial Number
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.