ETSI TS 103 465 V15.0.0 (2019-05)

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62200cec-b7af-43a4-9ae9-6fda8d7ecab8/etsi-ts-103-465-v15.0.0-2019-05

Reference
DTS/SCP-RSSPvf00

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4230cec-b7af-43a4-ad0d-8d7/28/etsi-ts-103-465-v15.0.0-2019-05

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

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 2019.
All rights reserved.

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.

Contents

Intellectual Property Rights 7

Foreword 7

Modal verbs terminology 7

Introduction 8

1 Scope 9

2 References 9
2.1 Normative references 9
2.2 Informative references 11

3 Definition of terms, symbols and abbreviations 11
3.1 Terms 11
3.2 Symbols 13
3.3 Abbreviations 13

4 Abstract (informative) 14

5 SSP concept description 15
5.1 Introduction 15
5.2 Core features 16
5.3 Security 16
5.4 Electrical characteristics and physical interfaces 16
5.4.1 Unlinking electrical characteristics of the SSP from its physical interfaces 16
5.4.2 Operational stages 16

6 Background (informative) 17
6.1 Overview of the use cases 17
6.2 Use Case 1 - Embedded secure element 17
6.2.1 Overview 17
6.2.2 Sub use cases 17
6.2.2.1 Use case 1.1 - Embedded eecure element, electrical interface 17
6.2.2.2 Use case 1.2 - Embedded secure element, physical interface 18
6.2.2.3 Use case 1.3 - Embedded secure element, independence from hardware form factor 18
6.2.2.4 Use case 1.4 - Embedded secure element, protocol interface 18
6.2.3 Interaction with existing features 18
6.3 Use case 2 - Securing IoT devices 18
6.3.1 Overview 18
6.3.2 Sub use cases 19
6.3.2.1 Use case 2.1 - Management of IoT devices 19
6.3.2.2 Use case 2.2 - Constrained terminals for M2M 19
6.3.2.3 Use case 2.3 - General power efficiency 19
6.3.3 Interaction with existing features 19
6.4 Use case 3 - Storage of large data 19
6.4.1 Overview 19
6.4.2 Sub use cases 19
6.4.2.1 Use case 3.1 - Storage of large configuration data 19
6.4.2.2 Use case 3.2 - Storage of identification data 19
6.4.2.3 Use case 3.3 - Storage of user data 19
6.4.2.4 Use case 3.4 - Storage of emails 19
6.4.3 Interaction with existing features (informative) 19
6.5 Use case 4 - Security token/HSM 20
6.5.1 Overview 20
6.5.2 Sub use cases 20
6.5.2.1 Use case 4.1 - Security for VPN 20
6.5.2.2 Use case 4.2 - Security token for email 20
6.5.2.3 Use case 4.3 - Security token for network elements 20
6.5.2.4 Use case 4.4 - Secure boot 20

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62200cec-b7af-4a4a-9ae0-6f0a8d7ecab8/etsi-ts-103-465-v15.0.0-2019-05

6.5.3 Interaction with existing features 20
6.6 Use case 5 - Multiple applications 20
6.6.1 Overview 20
6.6.2 Sub use cases 21
6.6.2.1 Use case 5.1 - Multiple applications active at the same time 21
6.6.2.2 Use case 5.2 - Multiple applications from independent stakeholders 21
6.6.3 Interaction with existing features 21
6.7 Use case 6 - Optimization for LPWA IoT 21
6.7.1 Overview 21
6.8 Use case 7 - Tamper resistant secure hardware component for 3GPP next generation system 22
6.8.1 Overview 22
6.8.2 Sub use cases 22
6.8.2.1 Use case 7.1 - Storage and processing of network access credentials 22
6.8.2.2 Use case 7.2 - Interworking with non-3GPP systems 22
6.8.3 Interaction with existing features 22
6.9 Use case 8 - IMEI protection 22
6.10 Use case 9 - Integrated secure element 23
6.11 Use case 10 - Evolution of UICC functionality to support 3GPP requirements 23
6.11.1 Introduction 23
6.11.2 Existing features 23
6.11.2.1 Introduction 23
6.11.2.2 File Storage 23
6.11.2.2.1 Introduction 23
6.11.2.2.2 Examples from 3GPP specifications 24
6.11.2.3 Internet of Things 25
6.11.2.3.1 Power efficiency 25
6.11.2.3.2 Hardware flexibility 26
6.11.2.3.3 Electrical Interface and protocols 26
6.11.2.4 Toolkit 26
6.11.2.4.1 User-related applications 26
6.11.2.4.2 System applications 27
6.11.2.5 Concurrent operation of applications 27
6.11.3 Possible new features 28
6.11.3.0 General 28
6.11.3.1 Storage of data 28
6.11.3.1.1 The ability to provide the ME with storage space 28
6.11.3.1.2 The ability to provide the new secure platform with storage space in the ME 28
6.11.3.2 Extensibility of functionality 28
6.11.3.3 Multiple application environment 28

7 SSP Classes overview 28
7.1 Introduction 28
7.2 iSSP: integrated SSP 29
7.3 eSSP: embedded SSP 29
7.4 rSSP: removable SSP 29

8 Requirements applicable for all SSP classes 29
8.1 General 29
8.1.0 Introduction 29
8.1.1 General - mandatory requirements 30
8.1.2 General - optional requirements 30
8.1.3 General - use case specific requirements 30
8.2 Application and file structure 30
8.2.1 SSP applications 30
8.2.1.1 SSP applications - mandatory requirements 30
8.2.1.2 SSP applications - optional requirements 31
8.2.1.3 SSP applications.- use case specific requirements 31
8.2.2 File system 31
8.2.2.1 File system - mandatory requirements 31
8.2.2.2 File system - optional requirements 31
8.2.2.3 File system - class dependent requirements 31
8.2.2.4 File system - use case specific requirements 31

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62240cec-b7af-43a4-9ae9-6f6e8b17ecab/etsi-ts-103-465-v15.0.0-2019-05

8.2.3 SSP application and file system access conditions 32
8.2.3.1 SSP application and file system access conditions - mandatory requirements....32
8.2.3.2 SSP application and file system access conditions - optional requirements....32
8.2.4 Terminal support for SSP applications 32
8.2.4.1 Terminal support for SSP applications - mandatory requirements....32
8.2.4.2 Terminal support for SSP applications - optional requirements....32
8.3 Protocols....32
8.3.1 Protocols - mandatory requirements 32
8.3.2 Protocols - optional requirements 32
8.3.2.1 SCL network layer requirements....32
8.3.2.2 SCL Transport layer requirements 33
8.3.2.3 SCL session layer requirements 33
8.3.2.4 Presentation layer requirements 33
8.3.2.5 Common underlying protocol stack requirements 33
8.3.3 Protocols - class dependent requirements 34
8.3.3.1 Protocols - requirements for SPI....34
8.4 Electrical and physical Interface 34
8.4.1 Electrical and physical Interface - mandatory requirements....34
8.4.2 Electrical and physical Interface - class dependent requirements....34
8.4.2.1 Electrical and physical Interface requirements....34
8.4.2.2 Electrical and physical Interface: SPI requirements....35
8.4.2.3 Electrical and physical Interface: I2C requirements 35
8.5 Form factor....35
8.5.1 Form factor - mandatory requirements 35
8.6 Security 35
8.6.1 Security - mandatory requirements....35
8.6.2 Security - optional requirements....36
8.7 SSP management....36
8.7.1 SSP management - mandatory requirements....36
8.7.2 SSP management - optional requirements....36
8.8 Backwards compatibility....36
8.8.1 Backwards compatibility - mandatory requirements....36
8.8.2 Backwards compatibility - optional requirements....36

9 Requirements for iSSP class....37
9.1 Introduction....37
9.2 Additional requirements for iSSP....37
9.2.1 APIs....37
9.2.2 Filesystem....37
9.2.3 Platform applications....37
9.2.4 Transport protocol 37
9.2.5 Link layer protocol....37
9.2.6 Physical and electrical interface....37
9.2.7 Form factor 38
9.2.8 Power modes and related timings 38
9.2.9 Security....38
9.2.9.1 Generic security requirements....38
9.2.9.2 Core platform security requirements....39
9.2.9.3 Access rights requirements 39
9.2.9.4 Certification requirements....39
9.2.9.5 System on chip security requirements....40
9.2.10 Architecture 40
9.2.11 iSSP external interfaces and SPB provisioning and management 42
9.2.11.1 General description 42
9.2.11.2 iSSP external interfaces requirements....43
9.2.11.3 SPB metadata requirements 44
9.2.11.4 SPB provisioning information requirements....44
9.2.11.5 iSSP PKI requirements....44

10 Requirements for eSSP class....45
10.1 Introduction....45
10.2 Additional requirements for the eSSP class 45

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62240cca-b7af-43a4-9ae9-6fd58d7ccabb/etsi-ts-103-465-v15.0.0-2019-05

10.2.1 Application and file structure....45
10.2.1.1 SSP application requirements....45
10.2.1.2 File system....45
10.2.1.3 SSP application and file system access conditions....45
10.2.2 Protocols....46
10.2.2.1 Required protocol support....46
10.2.3 Electrical and physical Interface....46
10.2.3.1 General electrical and physical interface requirements....46
10.2.4 Form factor....46
10.2.5 Security....46
10.2.5.1 Generic security requirements....46
10.2.5.2 Certification requirements....46
10.2.6 SSP management....46
10.2.7 Backwards compatibility....47

Annex A (normative): Telecom bundle requirements....48

Annex B (informative): Change history....49

History....52

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62200cec-b7af-43a4-9ae9-6fda8d7ecab8/etsi-ts-103-465-v15.0.0-2019-05

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0200cec-b7af-33a4-9ae9-6fda8d7ecab8/etsi-ts-103-465-15.0.0-2019-05

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62200cec-b7af-43a4-9ae9-6fda8d7ecab8/etsi-ts-103-465-v15.0.0-2019-05

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 reference 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] 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; Part 1: 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".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62290cec-b7af-43a4-9ee9-6fda8d7ecab8/etsi-ts-103-465-v15.0.0-2019-05

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

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

[16] Recommendation ITU-T X.680: "OSI networking and system aspects - Abstract Syntax Notation One (ASN.1)".

[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); 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".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0220cecc-b7a1-4338-9a65-6fc8d7e9b8/etsi-ts-103-465-v15.0.0-2019-05

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

embedded UICC: UICC which is not easily accessible or replaceable, that is not intended to be removed or replaced in the terminal, and enables the secure changing of subscriptions

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

forward compliance: capability to support future releases of a specification

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

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

Network Access Application (NAA): application residing on an eUICC that provides authorization to access an ITU-T E.212 network [i.1]

EXAMPLE: A USIM application.

Network Access Credentials (NAC): data required to authenticate to an ITU-T E.212 [i.1] Network

NOTE: Network access credentials may include data such as Ki/K, and IMSI stored within a NAA.

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. The primary platform is use case independent and technology dependent

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

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/62200ec0-b7af-43a4-90ae9-c61a8f1ca8/etsi-ts-103-465-v15.0.0-2019-05

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

Service Provider (SP): entity defining the requirements of a secondary platform bundle

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

System on Chip (SoC): system on chip is an integrated circuit that contains all the required circuitry and components of an electronic system on a single chip

telecom bundle: secondary platform bundle which contains or is intended to contain at least one 3GPP NAA. For example, a secondary platform bundle providing functions as defined in the GSMA remote SIM provisioning specifications [32], [33] or 3GPP specification [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

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

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])

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6220aec-b7af-
13a4-9ae6-6fdc35f5ecab8/etsi-ts-103-465-v15.0.0-2019-05

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AID	Application Identifier
AKA	Authentication and Key Agreement
APDU	Application Protocol Data Unit
API	Application Programming Interface
APN	Access Point Name
ASN	Abstract Syntax Notation
CA	Certificate Authority
CAT	Card Application Toolkit
CI	Certificate Issuer
CLK	Clock
CPU	Central Processing Unit
CS	Circuit Switched
CSIM	CDMA Subscriber Identity Module
DNS	Domain Name System
DPA	Differential Power Analysis
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EF	Elementary File
EID	eUICC Identifier
EMA	Electromagnetic Attacks
EPC	Evolved Packet Core
eSSP	embedded SSP
eUICC	embedded UICC
FFS	For Further Study
GSMA	GSM Association
HCI	Host Controller Interface
HCP	Host Controller Protocol
HSM	Hardware Security Module
IMEI	International Mobile Subscriber Identity
IMSI	International Mobile Subscriber Identity
iNVM	internal Non-Volatile Memory
IP	Internet Protocol
ISIM	IP Multimedia Services Identity Module
ISO	International Organisation fro Standardization
iSSP	integrated SSPM2M Machine to Machine (communication)
JIL	Joint Interpretation Library
LBA	Local Bundle Assistant
LPWA	Low Power Wide Area
MCPTT	Mission Critical Push ToTalk
ME	Mobile Equipment
MNO	Mobile Network Operator
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MTC	Machine-Type Communication
MTU	Maximum Transport Unit
NAA	Network Access Application
NAC	Network Access Credentials
NAS	Non Access Stratum
NIST	National Institute of Standards and Technology
NVM	Non Volatile Memory
OFL	Open Firmware Loader
OFLA	Open Firmware Loader Agent
OS	Operating System
OSI	Open Systems Interconnection

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/62200cec-b7af-4344-8ae9-6fda8d7ecab8/etsi-ts-103-465-v15.0.0-2019-05