ETSI TS 103 465 V16.1.0 (2020-03)

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

Reference
RTS/SCP-RSSPvg10

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 0 early working draft;
  - 1 presented to TC SCP for information;
  - 2 presented to TC SCP for approval;
  - 3 or greater indicates TC SCP approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

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

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

1 Scope

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

2 References

2.1 Normative references

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

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

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

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

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

[4] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; 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 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".

[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: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[31] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); 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".

2.2 Informative references

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

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[i.1] 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

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

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 OFL [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 Recommendation ITU-T E.212 network [i.1]

EXAMPLE: A USIM application.

Network Access Credentials (NAC): data required to authenticate to an Recommendation 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

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 GSMA SGP.02 [32], GSMA SGP.22 [33] or 3GPP specification ETSI TS 131 102 [15] would be classified as a telecom bundle

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

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

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

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

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])

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
DNS	Domain Name System
DPA	Differential Power Analysis
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EF	Elementary File
EMA	Electromagnetic Attacks
EPC	Evolved Packet Core
eSSP	embedded SSP
eUICC	embedded UICC
FFS	For Further Study
GSMA	GSM Association
HCI	Host Controller Interface
HPSIM	Hosting Party Subscription Identity Module
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 for Standardization
iSSP	integrated SSP
M2M	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
MTC	Machine-Type Communication
MTU	Maximum Transport Unit
NAA	Network Access Application
NAC	Network Access Credentials
NIST	National Institute of Standards and Technology
NVM	Non Volatile Memory
OFL	Open Firmware Loader
OS	Operating System
OSI	Open Systems Interconnection

PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPI	Primary Platform Interface
RFM	Remote File Management
rNVM	remote Non-Volatile Memory
rSSP	removable SSP
SCL	SSP Common Layers
SE	Secure Element
SIM	Subscriber Identity Module
SMS	Short Message Service
SoC	System on Chip
SOG-IS	Senior Officials Group Information Systems Security
SP	Service Provider
SPB	Secondary Platform Bundle
SPBL	Secondary Platform Bundle Loader
SPBM	Secondary Platform Bundle Manager
SPI	Serial Peripheral Interface
SSP	Smart Secure Platform
SWP	Single Wire Protocol
TBD	To Be Defined
TLV	Tag Length Value
UE	User Equipment
UI	User Interface
URN	Uniform Resource Name
USAT	USIM Application Toolkit
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language

4 Abstract (informative)

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

Figure 1 shows the layout of the SSP protocol stack.

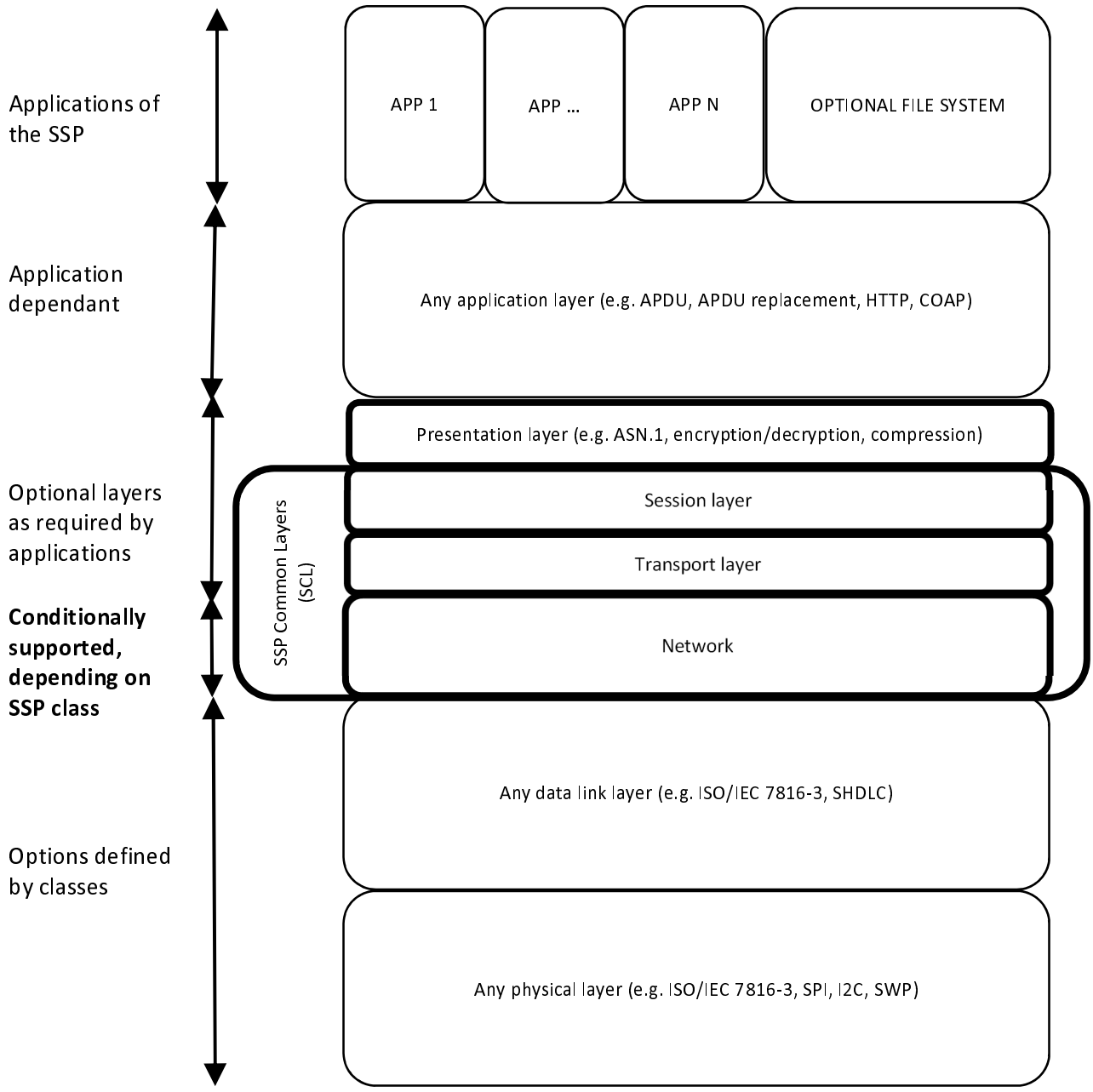

Figure 1: SSP protocol stack

This SSP is a modular platform allowing for its use in various use cases. In order to address these different contexts and in order to factorize the possible configuration some SSP classes will be defined. An SSP class will define a configuration of the SSP. One SSP class can correspond to the definition of the UICC.

5 SSP concept description

5.1 Introduction

The SSP is a secure platform intended for use in a number of use cases which may have very different requirements. For that reason, the SSP is designed to be a modular platform offering a core set of features as well as a number of options that need to be selected at the time of implementation based on the intended application. The goal is to enable the best fit for the targeted use case.

The physical interface(s) between the SSP and the device might be selected from a range of options including popular protocols in the industry (e.g. SPI, I2C, USB) as well as the legacy ETSI TS 102 221 [2] interface.

The data link layer and the transport protocols used over the physical interface might also be selected from a range of options.

In addition, a mandatory core set of security features will be provided, together with a number of optional security features which can be selected depending on the application.

It is expected that the technical specification for the SSP will provide a clear definition of the options available and describe a number of standard combinations of these options in what will be called SSP Classes.

5.2 Core features

A key element of the SSP is a logical interface allowing the support of different types of application protocols such as the ones used in the internet world (e.g. HTTP(S)), but also protocols used for secure elements such as banking cards or UICCs. This logical interface is able to transport these application protocols simultaneously between a secure application residing in the SSP and an application residing either in the device holding the SSP or in a remote location using the device as a proxy.

5.3 Security

A set of security features such as secure channel protocols, access control and secure storage needs to be defined. SSP class definitions will reference the required security features. A certification scheme targeting the different classes of SSP may also be defined. These certification schemes will help the secure application provider to assess the level of trust it can give to the SSP and thus assess if its secure applications can be hosted by this particular SSP. This assessment can be done by an offline process (contractual agreement between the SSP provider and the secure application provider), but also by an online process right before the loading of the secure application in the SSP. Some auditing capabilities may also be added to the SSP in order to help this assessment.

5.4 Electrical characteristics and physical interfaces

5.4.1 Unlinking electrical characteristics of the SSP from its physical interfaces

A secure element according to ETSI TS 102 221 [2] with an additional interface according to ETSI TS 102 613 [4] or ETSI TS 102 600 [9] lacks a clear separation of electrical characteristics which belong to the secure element (e.g. power supply, current consumption in different operational states, clock characteristics) and electrical characteristics which belong to a physical interface (e.g. input, output voltage levels, timing ranges).

For a modular system approach and to allow adding future interfaces in a quick manner it is very beneficial to separate electrical characteristics of the SSP from electrical characteristics of each physical interface.

Electrical characteristics of the SSP which are not directly linked to a physical interface (power supply, current consumption in different operational states) are defined independently from physical interfaces.

The electrical characteristics of each physical interface are defined independently from the electrical characteristics of other physical interfaces.

5.4.2 Operational stages

During device operation an SSP will not be used continuously in the same manner. There will be stages when the SSP performs high performance tasks like bulk encryption or key generation followed by stages where the SSP remains responsive to incoming service requests. Depending on the device which embeds the SSP it may also happen that the SSP remains unused for a longer period of time. During this period power saving is of topmost importance.

Since the SSP is a multi-application platform, its operational stages depend on the status of each individual application as well as on the status of each physical interface.

To offer quick responsiveness, highest computing power as well as lowest power consumption when not actively used, the SSP may offer the following operational modes:

- OPERATIONAL - providing highest computing power.
- IDLE - quick responsiveness on incoming requests with low power consumption.
- SUSPENDED - a powerless state: before entering the suspended state the application and security context are saved to a non-volatile memory inside the SSP; while resuming from SUSPENDED the same application and security context is restored.

Power consumption and timing behaviour when switching from one mode to another need to be clearly defined. In case additional SSP classes will be introduced in a later stage, those classes might define their proper characteristics with respect to power and timing. For some implementations of the SSP, the above features may not be required.

6 Background (informative)

6.1 Overview of the use cases

A range of use cases is identified in this clause to derive requirements for the specification of the SSP.

Use cases are provided as a means to understand and add context to the overall requirements.

6.2 Use Case 1 - Embedded secure element

6.2.1 Overview

An embedded secure element is a dedicated hardware component that is not intended to be removed from or replaced in the terminal. One example for an embedded secure element is an embedded UICC (eUICC). Such an embedded secure element is normally soldered into the terminal and is therefore an integral part of the terminal.

Secure elements are used in a wide range of terminals including mobile phones but also PC, car entertainment systems, etc. They are used to provide secure authentication in order to get access to a cellular network but are also used for other purposes, such as:

- Hosting of banking applications
- Generic authentication service in order to get access to a remote resource

A UICC as defined in ETSI TS 102 221 [2] specifies a specific interface between the UICC and the terminal which was developed to allow to easily exchange a single UICC between multiple terminals. For an embedded secure element it is not necessary to define an interface that allows easy exchange. Instead it would be beneficial if the interface between the terminal and the embedded secure element could re-use existing electrical and protocol interfaces already used inside the terminal.

One of the areas where embedded secure elements will be used is M2M. For many M2M applications very small and power efficient terminals are required. Specific use cases and related requirements are for example detailed in 3GPP specifications.

6.2.2 Sub use cases

6.2.2.1 Use case 1.1 - Embedded secure element, electrical interface

Using an electrical interface already used in the terminal would avoid implementing a specific power supply for the embedded secure element and would make the power management in the terminal much easier and more efficient.

6.2.2.2 Use case 1.2 - Embedded secure element, physical interface

Using an interface already available in the terminal would make the implementation inside the terminal more efficient as existing interfaces like e.g. I2C or SPI can be re-used and there is no need to develop a specific interface for communicating with an embedded secure element.

The Serial Peripheral Interface (SPI) is one of the most important of such interfaces and it is widely adopted in industrial and automotive markets. Despite its wide adoption in different industries, SPI is lacking commonly defined electrical and timing parameters.

6.2.2.3 Use case 1.3 - Embedded secure element, independence from hardware form factor

An embedded secure element forms an integral part in the terminal and therefore the design of the terminal can be optimized by using the optimal form factor for an embedded secure element.

6.2.2.4 Use case 1.4 - Embedded secure element, protocol interface

The existing UICC protocols couple the electrical interface and higher-layer functionality. In order to enable an appropriate decoupling of these components, the protocols would permit SSP power management while allowing different transports to be used, and the other use cases to be supported. The protocols would be decoupled from the transports.

6.2.3 Interaction with existing features

Although for the above use cases it may be beneficial to re-use existing electrical and protocol interfaces, while it may for other use cases be beneficial to have a standardized interface defined. One of such use case is a removable SSP.

6.3 Use case 2 - Securing IoT devices

6.3.1 Overview

IoT devices are a special class of devices which are usually very constrained in terms of cost and power supply. But IoT devices are also the source of potential high risk for end user privacy and security. IoT devices are usually comprised of three main parts:

- Sensors
- Processing and management
- Remote connection

Remote communication usually requires the IoT device to contain a secure authentication mechanism containing credentials belonging to the network provider. The processing and management part will use the remote connection in order to securely communicate to a service backend (e.g. for data collection and/or system-wide management). This service backend could be provided by an independent service provider. Alternatively, the service backend could be provided directly by the end user's own equipment. In any case, communication with this service backend will need to be secured in order to avoid endangering end user's safety, security and privacy.

An SSP can be used in order to provide the security services associated with network authentication, network remote connection and the service backend communication. The credentials associated with these services could be independent and belong to different actors.

In order to minimize the cost and the overall power consumption of the system, the SSP can also be used to interface to the sensors, provide dedicated processing of the information coming from the sensors and manage the communication with the remote service backend. In that case, the SSP will need to provide a flexible interface to the different parts of the IoT device.

Energy saving is a general issue and should also be considered for the SSP. Although the SSP is probably not consuming a lot of energy in a terminal compared to other terminal features, it is a factor to consider. Especially for constrained terminals in M2M applications, power consumption is an important issue.

6.3.2 Sub use cases

6.3.2.1 Use case 2.1 - Management of IoT devices

The SSP will have the role of processing all the information contained into an IoT device in addition to provide secure authentication to be used to connect to a wireless network and to be used to securely connect to a remote service backend.

6.3.2.2 Use case 2.2 - Constrained terminals for M2M

Several use cases in the M2M area are requiring very power efficient terminals and procedures. Such terminals may only be active very infrequently, e.g. once a week, and only transmit a small amount of data.

6.3.2.3 Use case 2.3 - General power efficiency

In the light of the general need to save energy wherever possible it is also necessary to optimize the power consumption of small devices like an SSP.

6.3.3 Interaction with existing features

None.

6.4 Use case 3 - Storage of large data

6.4.1 Overview

Several use cases may require the SSP to store large amounts of data, possibly in one file and in an unstructured way.

6.4.2 Sub use cases

6.4.2.1 Use case 3.1 - Storage of large configuration data

In 3GPP, more and more configuration parameters need to be stored in the device. Also the complexity of these parameters is increasing.

6.4.2.2 Use case 3.2 - Storage of identification data

Applications making use of biometric security require to store biometric information (e.g. voice, facial, fingerprint) in a secure way. Such biometric data may require a big amount of data.

6.4.2.3 Use case 3.3 - Storage of user data

The SSP may be used to store user data that is considered by the user as relevant to be protected (e.g. documents, pictures, videos).

6.4.2.4 Use case 3.4 - Storage of emails

The SSP may be used to securely store emails.

6.4.3 Interaction with existing features (informative)

None.

6.5 Use case 4 - Security token/HSM

6.5.1 Overview

The SSP can be used to provide security services for various applications as described below. It will be the provider of security and cryptographic applications such as:

- Signature generation/verification
- Bulk encryption/decryption
- Hardware root of trust
- Secure boot

6.5.2 Sub use cases

6.5.2.1 Use case 4.1 - Security for VPN

The SSP acts as a security token to provide employees access to the VPN of their company. The data traffic over the VPN tunnel may be encrypted/decrypted online by the SSP.

6.5.2.2 Use case 4.2 - Security token for email

The SSP can be used as a security token to protect access to emails. The emails may also be stored securely in the SSP (see clause 6.4.2.4).

6.5.2.3 Use case 4.3 - Security token for network elements

Wide area networks, including cellular networks, make more and more usage of small distributed network equipment in order to provide more flexibility in the network deployment but also in order to improve performance by reducing the distance between the end user and this network equipment.

In order to secure all these pieces of network, each of them may contain a secure device that will be used to ensure that this equipment will remain secure.

6.5.2.4 Use case 4.4 - Secure boot

The security capability service could be centralized and managed by the SSP. During booting, the SSP could provide integrity protection to ensure that the signed image can be loaded, but prevent unauthorized third-party code from running on different processors or chips.

6.5.3 Interaction with existing features

FFS.

6.6 Use case 5 - Multiple applications

6.6.1 Overview

The SSP may support multiple applications for example multiple network access applications, multiple security token applications or combinations thereof.

6.6.2 Sub use cases

6.6.2.1 Use case 5.1 - Multiple applications active at the same time

An SSP supports several applications. One of them is a network access application e.g. a USIM, and in addition an ID application, e.g. a driver's license. When the driver's license application is being activated, e.g. during a control by the police, it needs to be activated in parallel to the still activated NAA and data exchange with both applications is required at the same time.

6.6.2.2 Use case 5.2 - Multiple applications from independent stakeholders

An SSP supports multiple applications. Those applications may belong to different stakeholders. For example an NAA may belong to an MNO, a payment application may belong to a payment institution, while a secure key storage may belong to a service provide who manages the device in which the SSP is embedded.

For easy deployment and easy management of those applications, it is highly desirable that application owners can access their applications independently from other applications on the SSP.

When applications from different stakeholders coexist on the same platform, integrity and confidentially are of highest importance. Furthermore, mutual trust between the different stakeholders cannot be postulated since those different stakeholders might not even be aware of each other. To establish trust, formal certification by an independent organization is a prerequisite for multi-application SSPs.

While a multi-application SSP requires certification to establish trust, there is a need to be able to manage the applications (loading, updating, revoking) on the SSP without impacting its certification status. This means the mechanisms to separate one application from another need to be secure enough that individual application cannot compromise the security level of an SSP and retrieve or manipulate other applications or data which do not belong to them.

To further support an easy application management, the applications themselves are excluded from a certification process. However the SSP needs to offer a mechanism to verify the signature of an application which allows checking its integrity.

Single application SSPs might not necessarily require formal certification.

6.6.3 Interaction with existing features

It needs to be clarified if also several NAAs can be active at the same time. Potential interferences between applications should be avoided.

6.7 Use case 6 - Optimization for LPWA IoT

6.7.1 Overview

Low-Power, Wide-Area (LPWA) wireless technology is a generic term for a group of technologies including NB-IoT, Cat-M, even 5G massive IoT technology, etc. Such LPWA technologies differentiate themselves from other technologies in terms of:

- Wide area coverage
- Low cost
- Long battery life
- Low data throughput

It is expected that large numbers of resource-constrained IoT devices based on LPWA technologies will be deployed. The optimization for this kind of devices will be considered from the above key resource constraints point of view.

LPWA IoT devices will get access to the wide-area network after security interactions with the remote network and backend server. A secure channel should be established for data transmission between IoT devices, remote network and backend server. All these security services can be supported by using SSP technology.

6.8 Use case 7 - Tamper resistant secure hardware component for 3GPP next generation system

6.8.1 Overview

The 3GPP next generation mobile communication system, also called 5G, is requiring to store the network access credentials in a tamper resistant secure hardware component. The processing of the credentials with the authentication algorithm is required to be performed inside the tamper resistant secure hardware component.

The 3GPP next generation system is targeting various improvements to fulfil the specific requirements of various use cases, including mission critical communication, M2M/IoT, vehicle to x (V2X), broadband, interworking with other, non-3GPP systems etc. Most of these services impose additional security requirements on the network and the 3GPP User Equipment (UE). These identified requirements are captured in the security specification for 5G (ETSI TS 133 501 [10]).

Several requirements lead to the need for a dedicated tamper resistant secure hardware component inside the UE.

6.8.2 Sub use cases

6.8.2.1 Use case 7.1 - Storage and processing of network access credentials

The next generation system requires the storage of credentials and identities (human and machine) in the UE.

Subscription (human and machine) credentials and identities allow the network operator to authenticate its subscribers. Subscription authentication is needed to identify the origin and destination of the communication, to guarantee the quality of service and fulfil contractual, legal and regulatory obligations.

6.8.2.2 Use case 7.2 - Interworking with non-3GPP systems

The 5G network is required to interwork with various non-3GPP systems. These include fixed line access, satellite access, WLAN access, etc. For authentication between the UE and the 5G network over a non 3GPP access the authentication methods defined in ETSI TS 133 501 [10] are 5G AKA or EAP AKA.

6.8.3 Interaction with existing features

The 5G system is supposed to interwork with existing 3GPP networks, e.g. in Phase 1 of 5G it is the interworking of the new radio technology with the existing LTE network core, EPC. This includes the authentication but also existing services that are supported by the existing UICC and the 3GPP applications (SIM, USIM, ISIM, HPSIM).

6.9 Use case 8 - IMEI protection

One issue identified by several governments is the high number of stolen mobile devices. The current mechanism of blacklisting stolen devices does not really solve the issue, as the mechanism relies on the equipment identifier (IMEI) which is not tamper resistant. Studies in the US have shown that it may take only several hours until attackers have found ways to tamper with the IMEI and change it. Thus the blocking of stolen IMEIs does not really work.

For devices that include a non-removable secure element (e.g. embedded UICC or SSP) this could be used to provide a reliable mechanism for storing or protecting the IMEI.

6.10 Use case 9 - Integrated secure element

An integrated secure element can be a secure element integrated in a larger hardware platform. One example is a system on chip that integrates modem, processing and security functionalities where the integrated secure element is part of such a SoC. The SoC is normally soldered into the terminal and is therefore an integral part of the terminal.

The integrated secure element is part of the SoC so it does not need standardized electrical and physical interfaces. However due to its integrated nature it needs the definition of hardware requirements that will define how it will work inside the SoC. To prove that an integrated secure element is not exposed to any vulnerability due to the interaction with the rest of the SoC, certification is needed. It should be possible to verify that any changes of the SoC would not impact the security level of the iSSP. The purpose of the integrated secure element is to:

- Store the SSP credentials.
- Process and protect the credentials (e.g. 3GPP credentials).
- Provide cryptographic means.
- Feature secure communication service.
- Cryptographic operations isolated from the rest of the SoC.
- Meet certification requirements to assure the targeted level of security.

6.11 Use case 10 - Evolution of UICC functionality to support 3GPP requirements

6.11.1 Introduction

3GPP has identified several features that require an evolution of the current UICC functionalities to support new or existing 3GPP features. The SSP is intended to be an alternative for the current UICC, which is already an agreed option in ETSI TS 133 501 [10] and thus needs to support the features required by 3GPP.

6.11.2 Existing features

6.11.2.1 Introduction

The following sections describe existing features in 3GPP that make use of the UICC applications defined in 3GPP (USIM, ISIM, HPSIM, etc.) and impose technical requirements that may not be optimally supported by the existing UICC as the platform.

6.11.2.2 File Storage

6.11.2.2.1 Introduction

In recent 3GPP releases, the number of configuration files for new 3GPP features that need to be stored in the UICC has consistently increased. In many of these cases, a complex and large XML schema is defined in 3GPP to provision the configuration into the device with OMA-DM. Due to existing requirements to have the possibility to configure the device also using the USIM, 3GPP CT WG6 had to define ways to store the same information in the files of the USIM application or ISIM application.

In the past, most configuration files were coded in proprietary ways defined by 3GPP CT WG6 (for example, using nested TLV objects). Anyway, that approach presented several drawbacks:

- A change in the specification that define the XML schema can have a potential large impact on the representation of the data in the UICC.
- A device vendor is forced to implement two separate parsing functions to read the same configuration (i.e. using the XML schema and using the method defined by 3GPP CT WG6).

- Some configuration files are so large and complex that it is difficult to convert them into a different format.

As a consequence of this, 3GPP CT WG6 has started storing the configuration directly in XML format in the files of the USIM application or ISIM application. While this certainly solves the problems described above, it introduces new ones. More specifically, the access to the configuration files becomes problematic, due to the large size of the XML files.

3GPP CT WG6 is currently widely using the BER-TLV files defined in ETSI TS 102 221 [2], but this approach has limitations, in the ability to retrieve the data. Access to the configuration files requires several commands that are performed in sequence. While the terminal can still perform some other operations that do not impact the file pointer (for example, authentication algorithm), the device would not be able to perform several other operations, thus leading to a potential bad user experience or even to failure of specific procedures.

Moreover, 3GPP had cases where the UICC was used as secure storage, to keep data that had to be transmitted to the server on the network while the device was unable to do (for example, out of coverage). When this occurs, the UICC needs to have sufficient space to internally store the data, waiting for the conditions to transmit it to the network.

6.11.2.2.2 Examples from 3GPP specifications

6.11.2.2.2.1 Configuration Parameters for MCPTT

The parameters stored in the USIM follow the specification of the management object for the ME as defined in ETSI TS 124 383 [20]. The structure of the management object is, depending on the required services, complex and may therefore contain a large amount of data. The description of the management object is in XML, and the structure of the data cannot be easily reflected with the current file system design.

6.11.2.2.2.2 ProSe (Proximity Services) - Usage information storage

In the case of direct device to device communication without network coverage, the UE has to store the usage information according to the related configuration as specified in ETSI TS 124 334 [21] and ETSI TS 132 277 [22]. Depending on the configuration of which information needs to be included in the report, the amount of data to be stored may be large. On top of this, the longer the UE is out of coverage while using direct communication, the more likely it is that more than one report will need to be stored in the USIM. The data to be stored follows the specification of the related usage information management object as specified in ETSI TS 124 333 [23]. With the current solution defined in ETSI TS 131 102 [15] the ME sends the usage information report to the USIM and the USIM has to cater for storing the data received. The structure of the data cannot be easily reflected with the current file system design and due to the potential large amount of data the transmission of data may take a long time with the current interface between ME and UICC.

6.11.2.2.2.3 V2X (Vehicle-to-Everything

V2X requires to store configuration to enable the communication between a vehicle and other elements, such as other vehicles or infrastructure. The structure of the configuration is defined in ETSI TS 124 385 [24]: its structure is complex and may therefore contain a large amount of data. The description of the management object is in XML, and the structure of the data cannot be easily reflected with the current file system design.

6.11.2.3 Internet of Things

6.11.2.3.1 Power efficiency

6.11.2.3.1.1 Introduction

In the recent years, power consumption of the UE has become a very important aspect due to the rise of several IoT use cases that require that the device remains active for long periods of time, without the possibility to re-charge it. The overall power consumption is obviously composed by the sum of the power consumption of the ME and the power consumption of the UICC.

6.11.2.3.1.2 UICC suspension

3GPP conducted a study on the power consumption of the UICC, available in ETSI TR 131 970 [i.3]. This study was shared with ETSI TC SCP and was the basis to define the UICC suspension mechanism, specified in release 14.

The UICC suspension mechanism allows the terminal to completely remove the power from the UICC and be able to restore the UICC status later on, when the UICC is required. Such a mechanism can significantly improve the power consumption when the duration of the suspension is sufficiently long, as described in ETSI TR 131 970 [i.3], and so it is suitable mostly for devices that are idle for long periods of time.

3GPP CT WG6 expects that power consumption will remain a critical aspect also for the future, with even more use cases enabled by 5G technology. For this reason, the new secure platform should continue to support the suspension mechanism already introduced for the UICC, even if this might be implemented in a different way.

Also, 3GPP CT WG6 encourages ETSI TC SCP to consider additional improvements to reduce the power penalty introduced by the UICC resume operation. This would have two benefits on the UE:

- further improve the power saving for devices that are idle for long periods of time;
- ability to potentially extend the optimization to new classes of IoT devices that are idle for shorter periods of time.

6.11.2.3.1.3 Polling

As described in ETSI TR 131 970 [i.3], the presence detection polling and the proactive polling performed by the ME are also causes of considerable power consumption. In the current 3GPP specifications, the presence detection polling can be suspended when the UE is idle, and the proactive polling can be disabled by the operator. These changes allows the device to avoid unnecessary polling, with the goal of saving power.

Polling should be taken into consideration while working on the new secure platform, in order to limit it only to cases where it is strictly required, trying to define solutions that allow complete disablement of polling, without compromising on the ability of the secure platform to initiate a proactive session or on the ability of the device to detect a removal of the secure platform (where the removal is possible at all).

6.11.2.3.1.4 Voltage

In the current 3GPP specifications, only two classes of operating condition are considered valid, that is class B (3 V) and class C (1,8 V). The voltage of the UICC has a clear impact on the amount of power that is consumed by the UICC itself and by the terminal.

Moreover, with the reduction in node technology on the terminals, support for class B has become more expensive, as it requires external power sources. For the same reason, also support for class C is currently at risk.

Since the new secure platform may potentially break backward compatibility with the UICC specification at electrical level, it is recommended to avoid including any requirements for 3 V.

3GPP CT WG6 is not aware of specific electrical interfaces that ETSI TC SCP is considering for the new secure element, and if the existing UICC interface specified in ETSI TS 102 221 [2] will continue to be used at all. In any case, if a specification for the electrical interface is defined, it is recommended to consider also the addition of a new class that works below 1,8 V.

6.11.2.3.1.5 UICC access operations

In the existing UICC platform, there are several cases where the device needs to send multiple commands to perform what is logically a single operation. A good example for this is the access of the emergency numbers, stored in the USIM application. The terminal needs to first perform a SELECT command to retrieve the properties of the EF, such as the total number of records and the length of each record, and then needs to perform separate READ RECORD commands for each record, regardless of the size of each one.

This access is inefficient in terms of delay and power, as it requires that the terminal is awake while it performs these operations, often waiting for the UICC to respond.

For this reason, ETSI TC SCP is encouraged to consider solutions that limit the number of commands required to access the content stored in the new secure platform, or to perform other operations.

6.11.2.3.1.6 Execution time

One of the aspects discussed in the recent years was the execution time of certain commands, as highlighted by 3GPP CT WG6 to ETSI TC SCP. As a solution for the problem, the maximum power consumption of the UICC was increased starting with Release 12.

A fast execution time of commands is an essential part for the new secure element. This is important not only to make sure that all procedures described by 3GPP are performed in a timely and correct way, but it also contributes to the overall power reduction, as the terminal needs to be awake waiting for a response from the UICC for a shorter time.

3GPP CT WG6 encourages ETSI TC SCP to consider solutions that minimize the execution time of commands sent to the new secure element, while still taking into consideration the requirements to save power.

6.11.2.3.2 Hardware flexibility

For many use cases in IoT, devices may be optimized in size, functionality and according to the specific needs of the IoT application they are intended for. Some devices may be very small, e.g. simple sensors and may have specific requirements related to size and power consumption.

For such devices it would be beneficial to have a flexible choice of form factor of a UICC that is optimally fitting to the design of such constraint devices. Due to the variety of IoT use cases a large variety of specialized device designs is envisaged. Aspects that are to be considered are for example the form factor, removability, the size, the location and number of contacts.

6.11.2.3.3 Electrical Interface and protocols

In several use cases for IoT it may also be beneficial for a device to not have to implement the current ISO interface to a UICC but rather rely on interfaces and protocols already in use inside the device. Examples of such interfaces are I2C or SPI.

Additional aspects to consider are:

- Number of wires
- Transmission speed
- Supply voltage
- Power efficiency (e.g. polling)

6.11.2.4 Toolkit

6.11.2.4.1 User-related applications

6.11.2.4.1.1 Interaction with user authentication

Issues found when using the USAT command on which user authentication is needed: no mean to retrieve the user authentication status. For instance ENVELOPE (ProSe report) requires user authentication.

The same issue is identified for second level applications.

6.11.2.4.1.2 User toolkit menu

The user toolkit menu can be implemented by a toolkit application by using the proactive commands defined in ETSI TS 102 223 [14]. At the time these commands were defined, the MEs had a different way to get the user input and to display the information if it is compared to state-of-the-art MEs (e.g. higher resolution screen, colour, touch enabled screen, etc.).

This results in that user toolkit menus used in the MEs do not provide the same user experience as applications running on these devices.

6.11.2.4.1.3 Timer

Timing features that may be used by a toolkit applet rely on the timer implementation of the ME and not on the UICC. This creates an external dependency where ME potentially could not manage the timer timely as it is described in clause 6.4.1 of ETSI TS 102 223 [14]: "The precision of the returned value cannot be relied upon in all cases due to potential terminal activities".

This could be managed more efficiently if the UICC platform provides timer functionalities instead of the ME. In addition, as a consequence, it would reduce the amount of commands exchanged.

6.11.2.4.2 System applications

6.11.2.4.2.1 Proactive commands

In the ME-UICC interface defined in the existing platform, the UICC plays a slave role in the communication with the ME in a way that the UICC cannot initiate by itself the communication with the ME in the case a command from the UICC to the ME is requested to be sent. To enable this case, it is defined in ETSI TS 102 223 [14] the command protocol in the CAT layer that enables the UICC to send the so-called proactive commands to the ME.

This requires the active intervention of the ME in order to give the chance to the UICC to be able to send a proactive command by sending periodically a STATUS command. This creates an additional exchange of commands that could potentially delay the execution of the proactive command by the terminal, thus limiting the extension of new potential features.

It would be beneficial if the new secure element supports interfaces providing remote wake up features e.g. as specified in ETSI TS 102 600 [9].

6.11.2.5 Concurrent operation of applications

The existing platform supports multiple applications on different channels, with the limitation of one command at a time. This may result in the interface to the card being blocked by one of these applications, potentially causing disruption in the operation of 3GPP applications.

For instance, some non-telecommunication applications require the execution of cryptographic algorithms that can potentially take a long time, sometimes in the order of tens of seconds. This possibility is supported by the standard, using NULL procedure bytes. The card can send NULL procedure bytes in order to request additional work waiting time and avoid that the transaction timer expires on the terminal.

It is critical and essential for the correct functionality of the terminal and of the telecommunication applications residing on the UICC that the interface between the terminal and the UICC is never blocked for a long time that exceeds a few seconds. Consequences of blocking this interface include, but are not necessarily limited to:

- User cannot originate any voice call or send any text messages due to the fact that the required call control ENVELOPE command cannot be sent to the UICC.
- Network authentication cannot be executed and this has some very strict timing requirements.
- User cannot access the content on the UICC (phonebook, SMS, etc.).
- User cannot navigate the toolkit menu (even if menu is present in the UI of the UE).

6.11.3 Possible new features

6.11.3.0 General

3GPP also considered additional use cases, describing new features that are not specified in 3GPP but may be considered during the definition of a new secure platform.

6.11.3.1 Storage of data

6.11.3.1.1 The ability to provide the ME with storage space

With such feature the new secure platform could provide a possibility for a device to store specific data, for example sensitive information inside the new secure platform. This would require an efficient mechanism to transfer data in a fast, efficient and secure way. Such a mechanism needs to ensure that only the authorized entities can access the data.

6.11.3.1.2 The ability to provide the new secure platform with storage space in the ME

Such a feature would enable the new secure platform to make use of memory available in the ME. This can be data that is encrypted and therefore stored in a secure way or data that is not sensitive. Such a feature could allow new use cases which are currently not possible due to the resource limitations in current UICCs.

6.11.3.2 Extensibility of functionality

An update of part of or the whole Secure Platform functionality may be triggered by the need to extend the set of supported features. This includes:

- Extension of the supported command set.

6.11.3.3 Multiple application environment

Multiple applications may be hosted by the Secure Platform and may be active at the same moment in some deployments. Multiple non-telecommunication applications may be communicating at the same moment. Another case is when a network authentication is processed at the same moment as an over-the-air update is performed.

In such a situation, multiple non-telecommunication applications in addition to the network access application may send or receive commands at the same moment in a time critical manner: For instance to perform authentication to their respective services or perform time critical transportation payment. An application cannot afford to wait for other applications to terminate their communications before starting or terminating the application's own transaction.

Consequently, it would be beneficial that:

- Communication protocols on the secure platform allow multiple concurrent application sessions.
- The secure platform allows the execution of multiple applications that are time critical.
- The execution of an application does not prevent execution of another application.

7 SSP Classes overview

7.1 Introduction

As the SSP covers a wide set of use cases, requirements for the SSP are split into requirements that are applicable to all types of SSPs and requirements that are specific to a particular SSP class. This clause provides an overview on the currently defined SSP classes. Those are iSSP, eSSP and rSSP as defined below.

7.2 iSSP: integrated SSP

An iSSP is integrated into a system on chip (SoC), so it does not have a standardized form factor.

7.3 eSSP: embedded SSP

7.3.0 General

An eSSP is implemented as a discrete tamper resistant hardware component, that is embedded, non-removable and may have a standardized form factor.

7.3.1 eSSP: Type 1

An eSSP Type 1 is an eSSP which supports the SCL and which may support different electrical interfaces.

7.3.2 eSSP: Type 2

An eSSP Type 2 inherits the eSSP Type 1 functionalities and, in addition, supports the primary/secondary platform architecture.

7.4 rSSP: removable SSP

An rSSP is implemented as a discrete tamper resistant hardware component. This component is removable and shall have a standardized form factor.

8 Requirements applicable for all SSP classes

8.1 General

8.1.0 Introduction

This clause defines the applicability of requirements:

Mandatory requirements in general section:

Any product, regardless of its class, shall support these features to be compliant with the SSP technical specification.

Optional requirements in general section:

The support of the respective features by a dedicated product is optional regardless of its class.

Class dependent requirements in general section:

It is up to each SSP class whether the class mandates the support of a particular feature to be mandatory or optional. If the feature is not present in the specific SSP class requirements it means that the feature is not supported for that class.

Mandatory requirements in class section:

Any product compliant with this SSP class shall support these features.

Optional requirements in class section:

The support of the respective features by a dedicated product is optional.

Use case specific requirements:

Any SSP which claims to support a defined use case (e.g. 3GPP) shall support all features related to this use case specified in the present document.

8.1.1 General - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.1.1-01	The SSP shall be optimized for power efficiency.
REQ-15-SSP-8.1.1-02	There shall be an option for the SSP to operate in different power modes (e.g. IDLE, SUSPENDED, OPERATIONAL).
REQ-15-SSP-8.1.1-03	The timing behaviour when switching between power modes shall be clearly defined.
REQ-15-SSP-8.1.1-04	Each SSP class shall take the following parts into account: • APIs. • Filesystem. • Platform applications. • Transport protocol. • Link layer protocol. • Physical and electrical interface. • Form factor. • Power modes and related timings. • Security.
REQ-15-SSP-8.1.1-05	SSP class definition shall include the definition of the binding between the different layers of the protocol stack.
REQ-15-SSP-8.1.1-06	(3GPP) The SSP shall allow for a flexible choice of protocol handling large payload.

8.1.2 General - optional requirements

Identifier	Requirement
REQ-15-SSP-8.1.2-01	There shall be an optional mechanism to negotiate the transmission rate between the terminal and the SSP.

8.1.3 General - use case specific requirements

Identifier	Requirement
REQ-15-SSP-8.1.3-01	(3GPP) The SSP shall provide a mechanism for the secure platform for 3GPP applications to initiate a proactive session with the ME.
REQ-15-SSP-8.1.3-02	(3GPP) The SSP shall provide a mechanism for rich user interface for applications on the secure platform.
REQ-15-SSP-8.1.3-03	(3GPP) The SSP shall provide the capability for the secure platform to manage timers internally.

8.2 Application and file structure

8.2.1 SSP applications

8.2.1.1 SSP applications - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.2.1.1-01	The activation and the usage of an SSP application shall be protected by access conditions as defined in clause 8.2.3.
REQ-15-SSP-8.2.1.1-02	The SSP shall provide a mechanism allowing to list the SSP application(s) available in the SSP.
REQ-16-SSP-8.2.1.1-03	It shall be possible for a terminal application to discover the SSP application(s) or service(s) available in the SSP.
REQ-16-SSP-8.2.1.1-04	It shall be possible for a terminal application to access an SSP application or a service available in the SSP after the terminal application has been authorized by the SSP and/or the SSP application.

8.2.1.2 SSP applications - optional requirements

Identifier	Requirement
REQ-15-SSP-8.2.1.2-01	There shall be an option for the SSP to support concurrent SSP applications.
REQ-15-SSP-8.2.1.2-02	There shall be an option for the SSP to support multiple active SSP applications.
REQ-15-SSP-8.2.1.2-03	There shall be an option for the SSP to support SSP applications using the HCI as defined in ETSI TS 102 622 [6].
REQ-15-SSP-8.2.1.2-04	There shall be an option for the SSP to support SSP applications using the APDU as defined in ISO/IEC 7816-4 [8] and ETSI TS 102 221 [2].
REQ-15-SSP-8.2.1.2-05	There shall be an option for the SSP to support SSP applications using HTTP(S) (see note).
REQ-15-SSP-8.2.1.2-06	There shall be an option for the SSP to support SSP applications using CoAP [17], including DTLS support (see note).
REQ-15-SSP-8.2.1.2-07	There should be an option for the SSP to support SSP applications using any streaming protocol.
REQ-15-SSP-8.2.1.2-08	There shall be an option for the SSP to support SSP application data structures using a presentation layer generated from a syntax notation based on ASN.1 [16].
NOTE: Both, server and client mode of these protocols shall be supported.	

8.2.1.3 SSP applications - use case specific requirements

Identifier	Requirement
REQ-15-SSP-8.2.1.3-01	CAT commands and protocols transported via SCL shall support payloads larger than 255 bytes.
REQ-15-SSP-8.2.1.3-02	Proactive commands transported via SCL shall be supported without the need for proactive polling.

8.2.2 File system

8.2.2.1 File system - mandatory requirements

None.

8.2.2.2 File system - optional requirements

Identifier	Requirement
REQ-15-SSP-8.2.2.2-01	Support of file systems as described in this clause is optional for the SSP.
REQ-15-SSP-8.2.2.2-02	The SSP file system shall be able to handle large files (100 MB or larger).
REQ-15-SSP-8.2.2.2-03	The SSP shall provide an option for supporting UICC file system as defined in ETSI TS 102 221 [2] and ETSI TS 102 671 [3].
REQ-15-SSP-8.2.2.2-04	Access to the SSP file system from an external entity shall be provided using an interface independent of the physical and low protocols layers used by the SSP.
REQ-15-SSP-8.2.2.2-05	Access to files shall be protected by access conditions as defined in clause 8.2.3.

8.2.2.3 File system - class dependent requirements

None.

8.2.2.4 File system - use case specific requirements

Identifier	Requirement
REQ-15-SSP-8.2.2.4-01	(3GPP) The SSP shall support efficient access to large and complex configuration data in the sense that an ME does not need to read the complete content if only a part of the configuration data needs to be read at a time.

8.2.3 SSP application and file system access conditions

8.2.3.1 SSP application and file system access conditions - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.2.3.1-01	The SSP shall provide an access condition mechanism based on end user verification.
REQ-15-SSP-8.2.3.1-02	Access to the SSP applications and file system from a remote entity shall use a strong authentication and authorization mechanism.
REQ-16-SSP-8.2.3.1-03	The SSP shall support a mechanism to authorize a terminal application before granting access to an SSP application and/or service as per requirement REQ-16-SSP-8.2.1.1-04.

8.2.3.2 SSP application and file system access conditions - optional requirements

Identifier	Requirement
REQ-15-SSP-8.2.3.2-01	The end user verification mechanisms may include PIN code verification.
REQ-15-SSP-8.2.3.2-02	The end user verification mechanisms may include biometric.
REQ-15-SSP-8.2.3.2-03	The SSP shall provide an option for supporting application and file system access conditions as defined in ETSI TS 102 221 [2].

8.2.4 Terminal support for SSP applications

8.2.4.1 Terminal support for SSP applications - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.2.4.1-01	The terminal that supports IP shall support a mechanism to relay IP network connections from SSP applications.
REQ-15-SSP-8.2.4.1-02	The mechanism as described in REQ-15-SSP-8.2.4.1-01 shall be able to use currently available IP network connection in the terminal.
REQ-15-SSP-8.2.4.1-03	There shall be an option for the terminal to relay DNS resolution for SSP applications using the currently configured DNS servers.
REQ-15-SSP-8.2.4.1-04	There shall be an option for the SSP application to request the terminal to initiate an IP network connection.
NOTE: The IP network connection parameters shall only be used for the SSP application requesting the connection and shall not affect the other connections of the terminal.	

8.2.4.2 Terminal support for SSP applications - optional requirements

Identifier	Requirement
REQ-15-SSP-8.2.4.2-01	There shall be an option for the SSP application to provide IP network connection parameters such as an APN to the terminal (see note).
NOTE: The IP network connection parameters shall only be used for the SSP application requesting the connection and shall not affect the other connections of the terminal.	

8.3 Protocols

8.3.1 Protocols - mandatory requirements

None.

8.3.2 Protocols - optional requirements

8.3.2.1 SCL network layer requirements

Identifier	Requirement
REQ-15-SSP-8.3.2.1-01	The SSP should support the SCL network layer as defined in the present document.
REQ-15-SSP-8.3.2.1-02	The SCL network layer shall provide a means to address a targeted SSP application without additional application selection mechanisms (e.g. SELECT AID).
REQ-15-SSP-8.3.2.1-03	The SCL network layer shall support addressing multiple applications active at the same time.
REQ-15-SSP-8.3.2.1-04	The SCL network layer shall support the interleaving of protocol data units.
REQ-15-SSP-8.3.2.1-05	The SCL network layer shall be independent of all the underlying layers (physical and link layers).
REQ-15-SSP-8.3.2.1-06	The SCL network layer shall be independent of all its upper layers.
REQ-15-SSP-8.3.2.1-07	The SCL network layer shall support the requirements related to the under-layers of the tunnelled protocols.
REQ-15-SSP-8.3.2.1-08	The SCL network layer shall provide a means for tunnelling any protocols including the legacy UICC protocols at an equal or higher OSI model level.
REQ-15-SSP-8.3.2.1-09	The SCL network layer shall support communication between an SSP application and multiple end points.

8.3.2.2 SCL Transport layer requirements

Identifier	Requirement
REQ-15-SSP-8.3.2.2-01	The SSP may support the SCL transport layer as defined in the present document.
REQ-15-SSP-8.3.2.2-02	The SCL transport layer shall be independent of all the underlying layers (network, physical and link layers).
REQ-15-SSP-8.3.2.2-03	The SCL transport layer shall be independent of all its upper layers.
REQ-15-SSP-8.3.2.2-04	The SCL transport layer shall provide an optional mechanism for segmentation and reassembly.

8.3.2.3 SCL session layer requirements

Identifier	Requirement
REQ-15-SSP-8.3.2.3-01	The SSP may support the SCL session layer as defined in the present document.
REQ-15-SSP-8.3.2.3-02	The SCL session layer shall provide an optional means to manage (open, close) a session to a targeted application hosted by the SSP.
REQ-15-SSP-8.3.2.3-03	The SCL session layer shall be able to handle multiple sessions addressing SSP applications.
REQ-15-SSP-8.3.2.3-04	The SCL session layer shall be independent of all the underlying layers (transport, network physical and link layers).
REQ-15-SSP-8.3.2.3-05	The SCL session layer shall be independent of all its upper layers.

8.3.2.4 Presentation layer requirements

Identifier	Requirement
REQ-15-SSP-8.3.2.4-01	The SSP may support the presentation layer as defined in the present document.
REQ-15-SSP-8.3.2.4-02	The presentation layer may be application specific or generic as defined in the present document.
REQ-15-SSP-8.3.2.4-03	The generic presentation layer shall provide a means to serialize an unlimited number of parameters.
REQ-15-SSP-8.3.2.4-04	The generic presentation layer shall provide a means to serialize a parameter as scalar or objects having any size.
REQ-15-SSP-8.3.2.4-05	The presentation layer shall be independent of all the underlying layers (session, transport, network, physical and link layers).

8.3.2.5 Common underlying protocol stack requirements

Identifier	Requirement
REQ-15-SSP-8.3.2.5-01	The SSP shall provide a means for managing the SCL underlying data flow control.
REQ-15-SSP-8.3.2.5-02	The SSP shall provide a means for getting the MTU of the SCL underlying protocols.
REQ-15-SSP-8.3.2.5-03	The SSP shall provide an optional means for controlling (e.g. activating, deactivating) the underlying protocols.
REQ-15-SSP-8.3.2.5-04	The SSP shall provide an optional means for getting the notifications from an underlying protocol (e.g. activation/deactivation of the interface by the terminal).
REQ-15-SSP-8.3.2.5-05	The data packets delivery by the SSP underlying protocol stack to the network layer shall be reliable (i.e. data packets delivered error free and in sequence).

8.3.3 Protocols - class dependent requirements

8.3.3.1 Protocols - requirements for SPI

Identifier	Requirement
REQ-15-SSP-8.3.3.1-01	The SSP shall support the SPI interface if required by the corresponding SSP class.
REQ-15-SSP-8.3.3.1-02	The SSP may represent the SPI slave or master.
REQ-15-SSP-8.3.3.1-03	Once defined the layers "1. Physical", "2.Data Link", "3.Network", "4.Transport" shall comply with the OSI model.
REQ-15-SSP-8.3.3.1-04	The SPI interface shall support SPI mode 0.
REQ-15-SSP-8.3.3.1-05	The SPI interface shall support a minimum bit rate of 1 Mbps at the physical layer.
REQ-15-SSP-8.3.3.1-06	The SPI interface shall provide a technical means to allow proactivity (i.e. to allow the slave to initiate a communication sequence).

8.4 Electrical and physical Interface

8.4.1 Electrical and physical Interface - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.4.1-01	The SSP shall support a mechanism to suspend and resume.
REQ-15-SSP-8.4.1-02	The electrical and physical interface shall be independent from the form factor.
REQ-15-SSP-8.4.1-03	Electrical characteristics of the SSP which are not directly linked to a physical interface (e.g. current consumption in different operational states) shall be defined independently from physical interfaces.
REQ-15-SSP-8.4.1-04	The electrical characteristics of each physical interface (input/output voltages, timings and bitrates) shall be defined independently from the electrical characteristics of other physical interfaces.
REQ-15-SSP-8.4.1-05	The SSP definition shall not prevent the adoption of new evolved electrical and physical interfaces.
REQ-15-SSP-8.4.1-06	There shall be a mean for the SSP to trigger a communication over the physical interface.

8.4.2 Electrical and physical Interface - class dependent requirements

8.4.2.1 Electrical and physical Interface requirements

Identifier	Requirement
REQ-15-SSP-8.4.2.1-01	There shall be an option for the SSP to support the ISO/IEC 7816 [1] electrical and physical interface as defined in ISO/IEC 7816-3 [7].
REQ-15-SSP-8.4.2.1-02	There shall be an option for the SSP to support the SPI electrical and physical interface.
REQ-15-SSP-8.4.2.1-03	There shall be an option for the SSP to support the SWP electrical and physical interface as defined in ETSI TS 102 613 [4].
REQ-15-SSP-8.4.2.1-04	There shall be an option for the SSP to support the I2C electrical and physical interface.
REQ-15-SSP-8.4.2.1-05	There shall be an option for the SSP to support the I3C electrical and physical interface.

8.4.2.2 Electrical and physical Interface: SPI requirements

Identifier	Requirement
REQ-15-SSP-8.4.2.2-01	The electrical parameters of the SPI interface shall be clearly defined (e.g. signalling levels, slew rates, input & output driver characteristics).
REQ-15-SSP-8.4.2.2-02	The timing parameters of the SPI interface shall be clearly defined (e.g. clock rates, bit lengths, signal transitions).
REQ-15-SSP-8.4.2.2-03	The SPI interface shall support supply voltage class B and C.
REQ-15-SSP-8.4.2.2-04	The SPI interface shall have a dedicated SPI chip select (CS#) signal.
REQ-15-SSP-8.4.2.2-05	The SPI clock signal CLK shall be independent from an SSP internal clock.
REQ-15-SSP-8.4.2.2-06	The SPI interface shall support the full duplex mode.

8.4.2.3 Electrical and physical Interface: I2C requirements

Identifier	Requirement
REQ-15-SSP-8.4.2.3-01	The I2C interface shall support I2C master mode.
REQ-15-SSP-8.4.2.3-02	The I2C interface shall support I2C slave mode.
REQ-15-SSP-8.4.2.3-03	The I2C interface shall support I2C multi-master mode.

8.5 Form factor

8.5.1 Form factor - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.5.1-01	The SSP definition shall be independent of the form factor (see note).
NOTE: The form factors used for SSP may include the form factors defined in ETSI TS 102 221 [2] and ETSI TS 102 671 [3].	

8.6 Security

8.6.1 Security - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.6.1-01	It shall be possible for the SSP to go through a high level of certification and advanced attacks testing with high level qualified labs.
REQ-15-SSP-8.6.1-02	Such certification process shall include the SOG-IS protection profiles [5].
REQ-15-SSP-8.6.1-03	The SSP shall be tamper resistant.
REQ-15-SSP-8.6.1-04	It shall be possible for applications owners to securely manage their respective applications independent from other owners.
REQ-15-SSP-8.6.1-05	Only the application owner shall be able to manage its application unless the application owner has granted this access to others.
REQ-15-SSP-8.6.1-06	The SSP shall be a secure element.
REQ-15-SSP-8.6.1-07	The SSP shall process/execute its data/software in a dedicated secure CPU contained within the SSP (see note 1).
REQ-15-SSP-8.6.1-08	All the security functions in the present document shall be based on non-deprecated algorithms published by recognized standardization bodies.
REQ-15-SSP-8.6.1-09	Any entity within the SSP ecosystem receiving a certificate shall be able to verify it and determine the revocation status of the certificate when it receives it from another entity in the SSP ecosystem.
REQ-15-SSP-8.6.1-10	The SSP shall be resistant to hardware and software side-channel attacks (e.g. DPA, cache-timing attacks, EMA, etc.) (see note 2).
REQ-15-SSP-8.6.1-11	All SSP software and data shall be exclusively processed within the SSP.
REQ-15-SSP-8.6.1-12	The SSP shall use only self contained cryptographic mechanisms.
REQ-15-SSP-8.6.1-13	All security mechanisms within the SSP shall withstand state of the art attacks.
NOTE 1: Secure CPU will be defined in the protection profile. NOTE 2: The level of security shall be determined by a specific protection profile.	

8.6.2 Security - optional requirements

Identifier	Requirement
REQ-15-SSP-8.6.2-01	The SSP shall include an optional mechanism in order to allow remote auditing of its security state.
REQ-15-SSP-8.6.2-02	The SSP shall include an optional secure mechanism in order to allow remote provisioning of its software components, including applications, part of or all the operating system.
REQ-15-SSP-8.6.2-03	The SSP may contain a dedicated secure co-processor.

8.7 SSP management

8.7.1 SSP management - mandatory requirements

Identifier	Requirement
REQ-15-SSP-8.7.1-01	There shall be a mechanism to discover the services available in the SSP by the terminal (see note).
NOTE: Examples of services are: card application toolkit, support for suspension mechanism, ability to exchange IP data.	

8.7.2 SSP management - optional requirements

Identifier	Requirement
REQ-15-SSP-8.7.2-01	There shall be an optional mechanism for the SSP to discover the services available for its use in the terminal.

8.8 Backwards compatibility

8.8.1 Backwards compatibility - mandatory requirements

None

8.8.2 Backwards compatibility - optional requirements

Identifier	Requirement
REQ-15-SSP-8.8.2-01	There shall be an option for the SSP to support the transport of APDU.
REQ-15-SSP-8.8.2-02	There shall be an option for the SSP to support the ISO/IEC 7816-3 [7] interface.
REQ-15-SSP-8.8.2-03	An SSP implemented according to one of the existing form factors in ETSI TS 102 221 [2] and ETSI TS 102 671 [3] shall support the ISO/IEC 7816-3 [7] interface and the transport of APDUs.
REQ-15-SSP-8.8.2-04	There shall be an option for the SSP to support the contactless interface as defined in ETSI TS 102 613 [4] and ETSI TS 102 622 [6] (see note).
REQ-15-SSP-8.8.2-05	There shall be an option for the SSP to support UICC applications (e.g. USIM as defined in ETSI TS 131 102 [15]).
REQ-15-SSP-8.8.2-06	There shall be an option for the SSP to support UICC card application toolkit (CAT) applications as defined in ETSI TS 102 223 [14].
REQ-15-SSP-8.8.2-07	There shall be an option for the SSP to support applications based on ETSI TS 102 241 [18].
REQ-15-SSP-8.8.2-08	There shall be an option for the SSP to support applications based on ETSI TS 102 705 [19].
REQ-15-SSP-8.8.2-09	There shall be an option for the SSP to support Remote File Management (RFM) and remote application management based on ETSI TS 102 225 [25] and ETSI TS 102 226 [26].
NOTE: To be reviewed in the light of the identified classes/configurations for the SSP.	

8.9 Primary/secondary platform architecture

8.9.1 Primary/secondary platform architecture - class dependent requirements

8.9.1.1 General

The primary/secondary platform architecture shall be comprised of 4 parts:

- **Primary Platform:** The hardware platform, a low-level operating system managing the exceptions, the hardware platform resources and their accesses. The primary platform should provide forward compliance, subject to limitations of resources. The primary platform is use case independent.
- **Primary Platform Interface (PPI):** An abstraction layer between the primary platform and the secondary platform. The PPI provides a standard interface that makes any primary platform virtually equivalent for a secondary platform.
- **Secondary Platform:** A software platform using the primary platform interface and containing the high-level operating system on top of which the SSP applications are running.
- **SSP Application:** Application running on top of the secondary platform. The SSP application may be defined in other organizations and may not be part of the SSP specification.

The secondary platform along with its SSP applications is named Secondary Platform Bundle (SPB).

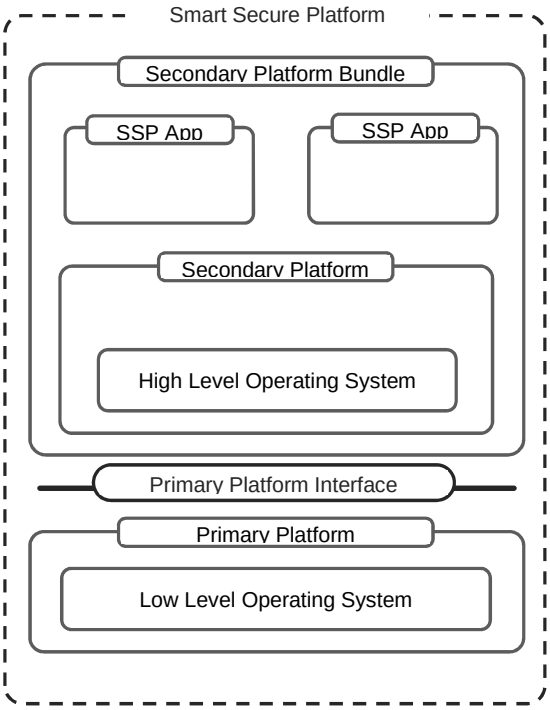

Figure 2: Primary/secondary platform architecture

The different states of the secondary platform bundle during its life are described in figure 3.

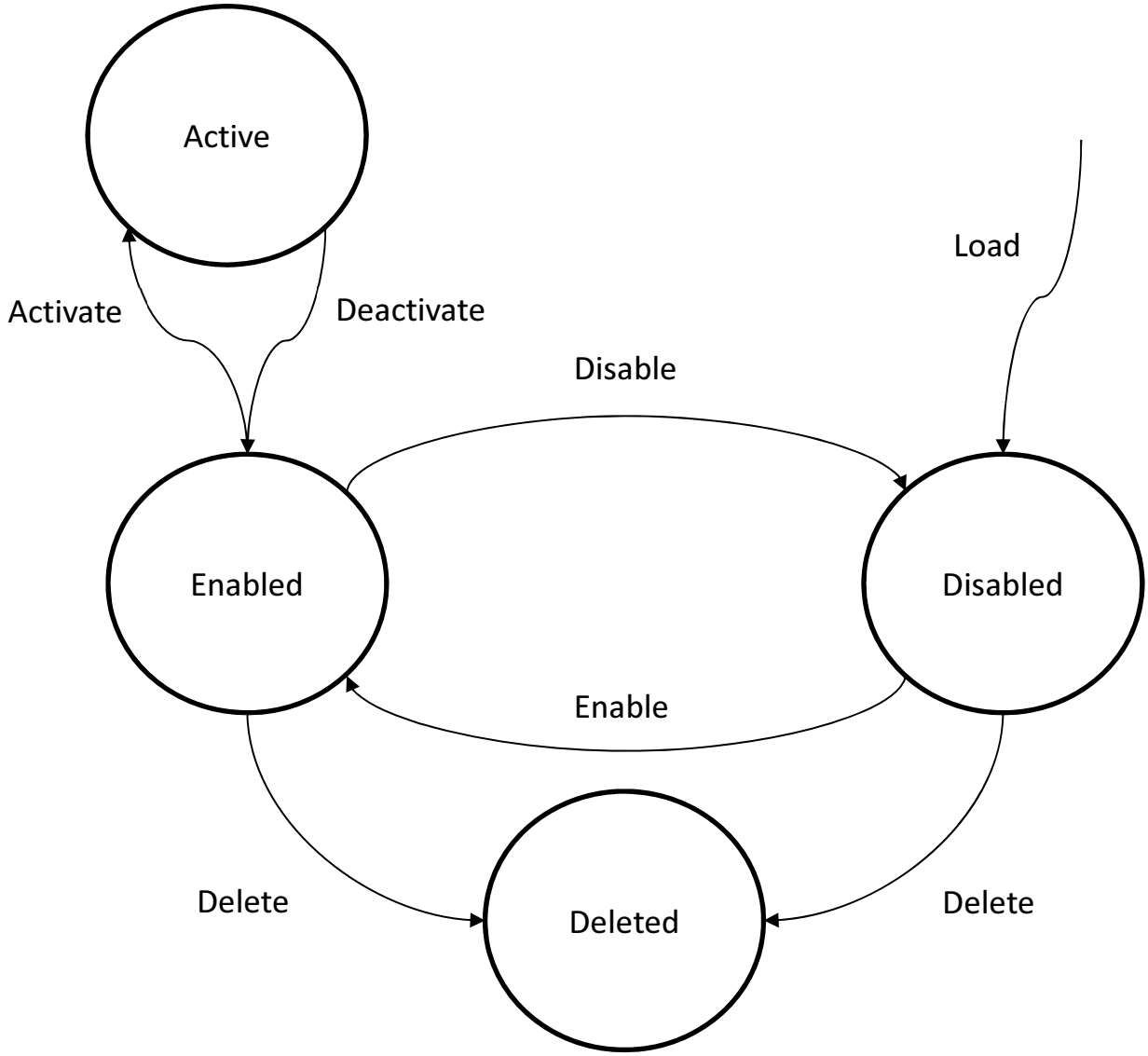

Figure 3: Secondary platform bundle states

The secondary platform bundle shall support the following states:

- **Active:** The secondary platform is running.
- **Enabled:** The secondary platform bundle can be activated.
- **Disabled:** The secondary platform bundle cannot be activated.
- **Deleted:** The secondary platform bundle, and all its associated resources are deleted from the SSP.

Identifier	Requirement
REQ-15-SSP-8.9.1.1-01	There shall be a clear separation of functionalities between the primary platform and the secondary platform allowing the different stakeholders to act independently.
REQ-15-SSP-8.9.1.1-02	There shall be a means for the secondary platform to restore its context and the context of its SSP applications if any when entering the active state (see note 1).
REQ-15-SSP-8.9.1.1-03	There shall be a means for the secondary platform to save its context and the context of its SSP applications if any before leaving the active state (see note 1).
REQ-15-SSP-8.9.1.1-04	There shall be a means to inform a secondary platform bundle that it has been previously disabled when entering in the active state.
REQ-15-SSP-8.9.1.1-05	Upon reception of the information as described in REQ-15-SSP-8.9.1.1-04, the secondary platform shall erase its context and the context of its SSP applications if any (see note 1).
REQ-15-SSP-8.9.1.1-06	Each regulated Industry sector (e.g. the financial, transport, public service, telecom, etc.) may have a reserved family identifier in order to implement its own management principles.
REQ-15-SSP-8.9.1.1-07	A family identifier shall be a UUID computed from a URN using IETF RFC 4122 [27] (see note 2).
REQ-15-SSP-8.9.1.1-08	At most one secondary platform bundle shall be in active state at any given time.
REQ-15-SSP-8.9.1.1-09	An enabled SPB shall be activated at the earliest opportunity whenever an event addressing this SPB is received by the primary platform (e.g. reception of a data packet addressed to this SPB, timer event, exception).
REQ-15-SSP-8.9.1.1-10	The SSP may contain multiple secondary platform bundles in enabled state.
REQ-15-SSP-8.9.1.1-11	There shall be a means to deactivate an SPB if it becomes unresponsive.
NOTE 1: The context of a secondary platform bundle includes all data required to resume the SPB in the exact condition so it is equivalent as if the SPB was not deactivated. NOTE 2: The family identifier values are TBD.	

8.9.1.2 Primary/secondary platform external interfaces and SPB provisioning and management

8.9.1.2.1 General description

This clause specifies the roles, interfaces and requirements associated with the SSP for the provisioning of a secondary platform bundle.

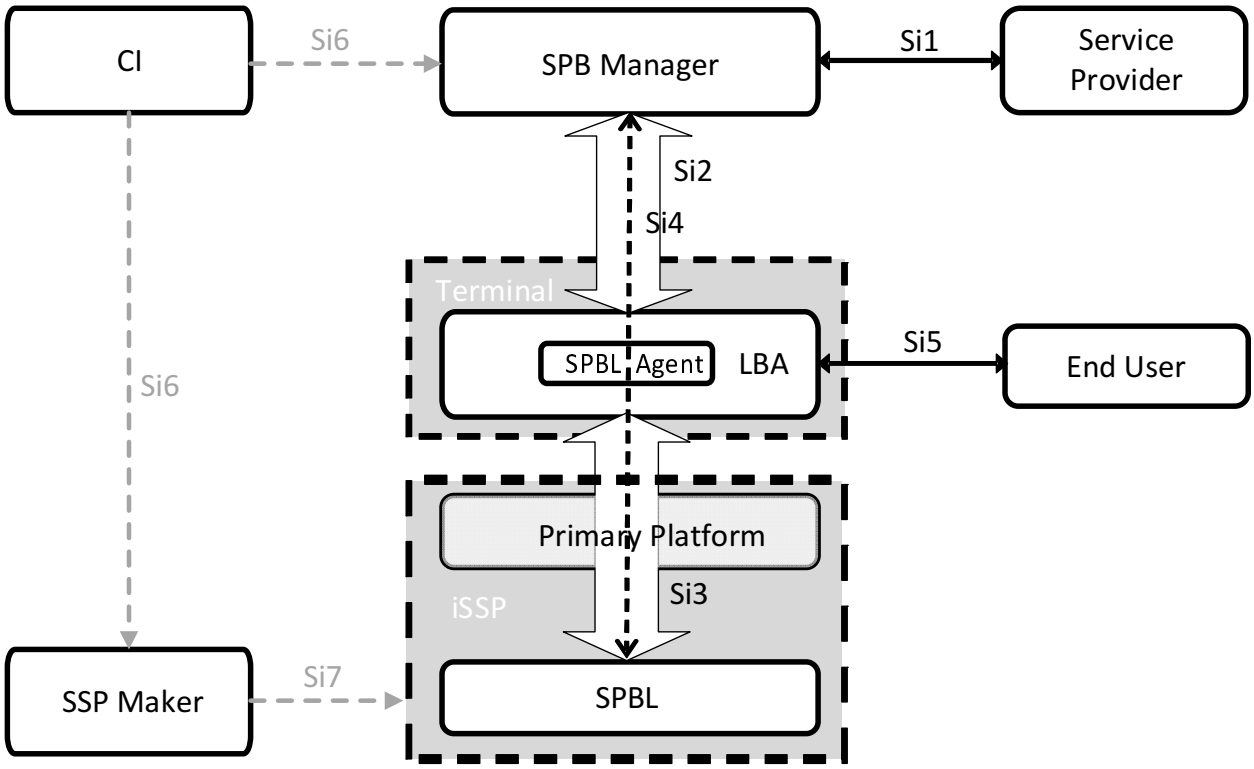

Figure 4: SSP external interfaces

The following interfaces are defined in the present document:

- Si1: Interface between a service provider and the SPB manager.
- Si2: Interface between the SPB manager and the LBA running on the terminal.
- Si3: Interface between the LBA and the SPBL in the SSP.
- Si4: Interface between the SPB manager and the SPBL in the SSP. This interface is tunnelled through the LBA.
- Si5: Interface between the end user and the LBA.
- Si6: Interface between the CI and the entities which request certificate signing (out of scope).
- Si7: Interface between the SSP maker and the SSP (out of scope).

8.9.1.2.2 Primary/secondary platform external interfaces requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.2.2-01	The SPB manager shall securely bind an SPB to a specific SSP instance.
REQ-15-SSP-8.9.1.2.2-02	The service provider shall have a means to control the SPB binding via Si1 interface.
REQ-15-SSP-8.9.1.2.2-03	The SPBL shall use a secure mechanism ensuring that, each time an SPB is prepared by an SPB manager for loading and installation on the SSP, that SPB shall be successfully installed only once on the SSP instance that it is bound to.
REQ-15-SSP-8.9.1.2.2-04	The Si4 interface shall provide authorization, mutual authentication (see note 1), integrity and confidentiality for loading and installation of an SPB.
REQ-15-SSP-8.9.1.2.2-05	The format of the digital certificates shall be compliant with X.509 version 3 format [30].
REQ-15-SSP-8.9.1.2.2-06	It shall be possible for an SPBL to support loading and installation of an SPB generated by any SPB manager.
REQ-15-SSP-8.9.1.2.2-07	The LBA and the SPB manager shall be certified according to some specific industry requirement (see note 5).
REQ-15-SSP-8.9.1.2.2-08	The SSP ecosystem shall be interoperable so that actors can choose the SPB manager independent of the target SSP and LBA.
REQ-15-SSP-8.9.1.2.2-09	Si3 interface shall provide a standardized protocol between the LBA and SPBL.

Identifier	Requirement
REQ-15-SSP-8.9.1.2.2-10	Si1 interface shall provide a means for the service provider to request the loading of an SPB.
REQ-15-SSP-8.9.1.2.2-11	Si1 interface shall provide a means for the service provider to cancel the request for the loading of an SPB.
REQ-15-SSP-8.9.1.2.2-12	Si1 interface shall provide confidentiality and integrity protection.
REQ-15-SSP-8.9.1.2.2-13	The Si2 interface shall provide a means to obtain a bound SPB from the SPB manager
REQ-15-SSP-8.9.1.2.2-14	The Si2 interface shall provide confidentiality and integrity protection.
REQ-15-SSP-8.9.1.2.2-15	The Si2 interface shall provide authentication of the SPB manager.
REQ-15-SSP-8.9.1.2.2-16	There shall be a means to locally enable, disable and delete an SPB via Si3 interface.
REQ-15-SSP-8.9.1.2.2-17	There shall be a means to send a notification for the change of bundle state on an SPB to the recipient(s) indicated by the SPB (see note 4).
REQ-15-SSP-8.9.1.2.2-18	Each notification shall be uniquely identifiable.
REQ-15-SSP-8.9.1.2.2-19	The notification shall be authenticity, integrity and replay protected by the SPBL.
REQ-15-SSP-8.9.1.2.2-20	The service provider shall be able to configure which state changes shall be notified as well as to which recipient(s) (see note 4).
REQ-15-SSP-8.9.1.2.2-21	Each SPB shall have exactly one family identifier.
REQ-15-SSP-8.9.1.2.2-22	Si4 interface shall provide perfect forward secrecy for SPB loading and installation.
REQ-15-SSP-8.9.1.2.2-23	The SSP information shall include the primary platform identifier.
REQ-15-SSP-8.9.1.2.2-24	The SSP information shall include the specification version of the SPBL.
REQ-15-SSP-8.9.1.2.2-25	The SSP information shall include the list of supported CIs, algorithms and parameters for signature verification which are associated with the family identifier(s) and custodian(s) the SSP intends to download (see note 6).
REQ-15-SSP-8.9.1.2.2-26	The SSP information shall include a means for identifying the primary platform manufacturer.
REQ-15-SSP-8.9.1.2.2-27	The SSP information shall include a means for identifying the model of the primary platform.
REQ-15-SSP-8.9.1.2.2-28	The SSP information shall include the maximum size of an SPB supported by the SSP (see note 6).
REQ-15-SSP-8.9.1.2.2-29	The terminal information shall include the specification version of the LBA.
REQ-15-SSP-8.9.1.2.2-30	The terminal information shall include the type allocation code (see ETSI TS 123 003 [31]) of the terminal, if available.
REQ-15-SSP-8.9.1.2.2-31	The terminal information shall be provided to the SPB manager via Si2 interface, before download of a bound SPB.
REQ-15-SSP-8.9.1.2.2-32	The SSP information shall be provided to the SPB manager via Si4 interface, before download of a bound SPB.
REQ-15-SSP-8.9.1.2.2-33	Some parts of the SSP information that are necessary to establish the Si4 interface (e.g. supported CIs, algorithms and parameters) shall be provided to the SPB manager via Si2 interface, before establishing the Si4 interface between the SSP and the SPB manager.
REQ-15-SSP-8.9.1.2.2-34	SPBs and SSPs shall be interoperable so that any SPB can be downloaded and installed on any SSP (memory permitting) and be fully functional to the extent supported by the SSP.
REQ-16-SSP-8.9.1.2.2-35	The default SPB manager address shall be accessible by the LBA.

NOTE 1: Supported only in unicast mode as defined in GlobalPlatform Open Firmware Loader for Tamper Resistant Element [13].
NOTE 2: Whether REQ-15-SSP-8.9.1.2.2-03 to REQ-15-SSP-8.9.1.2.2-08 apply to provisioning of SPBs during the terminal manufacturing process is FFS.
NOTE 3: Si5 interface description is FFS.
NOTE 4: These requirements are not applicable to the transition between the active and enabled state.
NOTE 5: The meaning of "specific industry requirement" needs to be further clarified.
NOTE 6: The recommended association(s) between a family identifier and a CI are to be defined by a/the custodian of that family identifier. There may be more than one custodian for a specific family identifier.

8.9.1.2.3 SPB metadata requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.2.3-01	The SPB shall have associated SPB metadata.
REQ-15-SSP-8.9.1.2.3-02	The SPB metadata for an installed SPB shall be stored in the SSP.
REQ-15-SSP-8.9.1.2.3-03	The SPB metadata shall be readable by the LBA via Si2 interface during loading process of the SPB before the installation of the bound SPB.
REQ-15-SSP-8.9.1.2.3-04	The SPB metadata shall be readable by the LBA via Si3 interface irrespective of the state of the SPB (see note 2).
REQ-15-SSP-8.9.1.2.3-05	The SPB metadata shall be readable by the SPBL irrespective of the state of the SPB (see note 2).

Identifier	Requirement
REQ-15-SSP-8.9.1.2.3-06	The SPB metadata shall include the identifier of the SPB.
REQ-15-SSP-8.9.1.2.3-07	The SPB metadata shall include the family identifier of the SPB.
REQ-15-SSP8.9.1.2.3-08	The SPB metadata shall be extensible (see note 1).
NOTE 1: The extensions may be provided by industry specific organizations. NOTE 2: These requirements shall not apply to the deleted state.	

8.9.1.2.4 SPB provisioning information requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.2.4-01	The SPB manager shall have means to securely determine the manufacturer and the model (hardware and software version) of the primary platform instance.
REQ-16-SSP-8.9.1.2.4-02	There shall be a means to set a default SPB manager address in the SSP by an authorized entity (see note).
NOTE: It is FFS how the LBA handles (e.g. uses or ignores) the default SPB manager address and who is authorized to set it.	

8.9.1.2.5 Primary/secondary platform PKI requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.2.5-01	The SPBL end entity certificate(s) shall end a certification path originating from a CI trusted by the SPBM (see note 1).
REQ-15-SSP-8.9.1.2.5-02	The SPBM end entity certificate(s) shall end a certification path originating from a CI trusted by the SPBL (see note 2).
REQ-15-SSP-8.9.1.2.5-03	With regard to REQ-15-SSP-8.9.1.2.5-01 and REQ-15-SSP-8.9.1.2.5-02, there may be additional certificate(s) between the end entity certificate(s) and the trusted CI certificate in a given certification path.
REQ-15-SSP-8.9.1.2.5-04	With regard to REQ-15-SSP-8.9.1.2.5-01 and REQ-15-SSP-8.9.1.2.5-02, the algorithm and algorithm parameter set shall be the same for all the certificates belonging to a given certification path.
REQ-15-SSP-8.9.1.2.5-05	The SPBL and SPBM shall be able to support more than one certification path in REQ-15-SSP-8.9.1.2.5-01 and in REQ-15-SSP-8.9.1.2.5-02, respectively (see note 3).
REQ-15-SSP-8.9.1.2.5-06	The SPBL and SPBM shall be able to support the case where the trusted CI, algorithm and algorithm parameter set used for a certification path in REQ-15-SSP-8.9.1.2.5-01 are different from those used for a certification path in REQ-15-SSP-8.9.1.2.5-02.
REQ-15-SSP-8.9.1.2.5-07	When generating signature(s) for loading of an SPB to an SSP, the SPBM shall use a certification path associated with the family identifier of that SPB (see note 4).
REQ-15-SSP-8.9.1.2.5-08	The SPBL shall allow loading of an SPB if both the certification path used by the SPBM in REQ-15-SSP-8.9.1.2.5-07 is associated with the family identifier of that SPB and the certification path validation by the SPBL is successful (see note 5).
REQ-15-SSP-8.9.1.2.5-09	There shall be a means to identify a custodian.
REQ-15-SSP-8.9.1.2.5-10	There shall be a means for a Service Provider to indicate within its SPB one or more custodian(s) (see note 4).
REQ-15-SSP-8.9.1.2.5-11	When generating signature(s) for loading of an SPB to an iSSP, the SPBM shall use one of the certification path(s) associated with one of the custodian(s) if indicated in the SPB as per REQ-15-SSP-8.9.1.2.5-10
REQ-15-SSP-8.9.1.2.5-12	There shall be a means for a Service Provider to indicate the preferred custodian to be used by the SPBM, for an SPB having more than one custodian.
NOTE 1: Refer to IETF RFC 5280 [30] for the definition of the end entity certificate and the certification path. In the SSP PKI, the certification path described in REQ-15-SSP-8.9.1.2.5-01 is used by the SPBL to generate a signature and is used by the SPBM to verify that signature. NOTE 2: The certification path described in REQ-15-SSP-8.9.1.2.5-02 is used by the SPBM to generate a signature and is used by the SPBL to verify that signature. NOTE 3: One digital certificate can support only one algorithm parameter set for signature generation. It means, for example, in order for an SPBL to support 2 algorithm parameter sets for signature generation, 2 certification paths are required on the SPBL (e.g. one for NIST and the other for Brainpool). NOTE 4: The recommended association(s) between a family identifier and a certification path are to be defined by a/the custodian of that family identifier. There may be more than one custodian for a specific family identifier. NOTE 5: The certification path used by the SPBM shall be associated with a custodian if indicated by the service provider as per REQ-15-SSP-8.9.1.2.5-10.	

8.9.1.3 APIs

Identifier	Requirement
REQ-15-SSP-8.9.1.3-01	SSPs shall provide an abstraction layer on top of the hardware platform, the low-level operating system managing the exceptions, the hardware platform resources and their accesses, providing a standardized interface that enables development of high level OS solely based on this interface.
REQ-15-SSP-8.9.1.3-02	The PPI shall provide a means to notify the secondary platform when a shutdown request occurs.
REQ-15-SSP-8.9.1.3-03	The PPI shall provide a means for the secondary platform to notify the primary platform when the secondary platform is ready to be shutdown.
REQ-15-SSP-8.9.1.3-04	The primary platform shall support a standardized API, as part of the PPI, for the management (loading, unloading, updating, deleting, etc.) of secondary platform bundles.

8.9.1.4 Platform applications

Identifier	Requirement
REQ-15-SSP-8.9.1.4-01	SSPs shall contain a secondary platform bundle loader compliant with GlobalPlatform Open Firmware Loader for Tamper Resistant Element [13].

8.9.1.5 Primary/secondary platform security requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.5-01	The primary platform shall provide a means to be securely and uniquely identified.
REQ-15-SSP-8.9.1.5-02	The SSP shall be able to support a certification by composition of a secondary platform bundle on top of the primary platform certification.
REQ-15-SSP-8.9.1.5-03	There shall be one universally unique, immutable primary platform identifier which identifies the primary platform instance.
REQ-15-SSP-8.9.1.5-04	The primary platform identifier as defined in REQ-15-SSP-8.9.1.5-3 shall have a standardized format.
REQ-15-SSP-8.9.1.5-05	There shall be a means for the SPB Manager to authenticate the primary platform instance using the primary platform identifier via Si4 interface.
REQ-15-SSP-8.9.1.5-06	There shall be a means for the LBA to get the primary platform identifier from the SSP via Si3 interface.

8.9.1.6 Primary/secondary platform core security requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.6-01	Privacy by design shall be enforced by the primary platform specification.
REQ-15-SSP-8.9.1.6-02	It shall be possible for the primary platform to support multiple secondary platform bundles provided by different issuers.
REQ-15-SSP-8.9.1.6-03	The primary platform shall provide a means for preventing dependency between the secondary platform design and the memory addressing (e.g. paging).
REQ-15-SSP-8.9.1.6-04	The primary platform shall notify the active secondary platform when a software or hardware exception is encountered (e.g. access rights violation or hardware security sensors activated).
REQ-15-SSP-8.9.1.6-05	The primary platform shall provide strong isolation between processes.

8.9.1.7 Access rights requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.7-01	The primary platform shall provide a mechanism to securely destroy the contents of the private working set of the secondary platform bundle before the memory is reallocated.
REQ-15-SSP-8.9.1.7-02	The API defined in REQ-15-SSP-8.9.1.3-04 shall be accessible only to the secondary platform bundle loader.
REQ-15-SSP-8.9.1.7-03	The primary platform shall ensure the confidentiality and integrity of the contents of non-shareable memory regions.
REQ-15-SSP-8.9.1.7-04	The primary platform shall provide a mechanism to restrict access to its hardware units to authorized accessors only.
REQ-15-SSP-8.9.1.7-05	The primary platform shall provide a mechanism to ensure that access to its hardware units, including its input and output, is exclusive and confidential to each accessor.
REQ-15-SSP-8.9.1.7-06	The low-level operating system shall only have non-shareable memory regions.
REQ-15-SSP-8.9.1.7-07	All primary platform access control rules shall be enforced by the low-level operating system in the primary platform.

8.9.1.8 Certification requirements

Identifier	Requirement
REQ-15-SSP-8.9.1.8-01	The certification of the primary platform shall claim in its security target the conformance with protection profile BSI-CC-PP-0084-2014 [11] including loader package 2.
REQ-15-SSP-8.9.1.8-02	The security target of a primary platform shall support all the security requirements included in the present document.
REQ-15-SSP-8.9.1.8-03	The certification minimum assurance level is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.
REQ-15-SSP-8.9.1.8-04	AVA_VAN.5 tests shall be performed in accordance with the JIL Application of Attack potential to Smartcards documentation [12].
REQ-15-SSP-8.9.1.8-05	The secondary platform bundle manager shall have a means to securely determine the assurance level of the primary platform together with the secondary platform bundle loader.
REQ-15-SSP-8.9.1.8-06	The SSP shall be able to support a certification by composition compliant with EAL4+ using BSI-CC-PP-0084-2014 [11].
REQ-15-SSP-8.9.1.8-07	Any change of the primary platform (hardware or software) shall require an updated certification in accordance with the requirements REQ-15-SSP-8.9.1.8-01 to REQ-15-SSP-8.9.1.8-04.
REQ-15-SSP-8.9.1.8-08	The addition of a secondary platform bundle shall not impact the certification, if existing, of any other secondary platform bundle present on the SSP.

9 Requirements for iSSP class

9.1 Introduction

This clause specifies the requirements for the iSSP class.

Some use cases for an integrated secure element are described in clause 6.

There should be common principles of operation for the management framework across all industry sectors.

9.2 Additional requirements for iSSP

9.2.0 General Requirements

Identifier	Requirement
REQ-15-SSP-9.2-01	The iSSP shall support the requirements defined in clause 8.9.

9.2.1 Void (Clause is now 8.9.1.3)

9.2.2 Filesystem

No additional requirement

9.2.3 Void (Clause is now 8.9.1.4)

9.2.4 Transport protocol

Identifier	Requirement
REQ-15-SSP-9.2.4-01	A transport protocol may be defined to allow testing and debugging of the SSP functionality (see note 2).
REQ-15-SSP-9.2.4-02	The iSSP shall support the SCL network layer as defined in clause 8.3.1 (see note 1).
NOTE 1: This requirement does not mandate the usage of the SCL network layer for the purpose of internal communication within the SPB. NOTE 2: The definition of this transport protocol shall not allow any tampering of the SSP security (e.g. access to SSP memory).	

9.2.5 Link layer protocol

None.

9.2.6 Physical and electrical interface

Any electrical and physical interfaces of an iSSP are out of scope of the present document.

9.2.7 Form factor

None.

9.2.8 Power modes and related timings

None.

9.2.9 Security

9.2.9.1 Generic security requirements

Identifier	Requirement
REQ-15-SSP-9.2.9.1-01	The iSSP shall be isolated from all other SoC components such that no other SoC components can have access to the iSSP owned assets.
REQ-15-SSP-9.2.9.1-02	iSSP software and data shall never be exposed outside the iSSP in clear text (see note 2).
REQ-15-SSP-9.2.9.1-03	All iSSP software and data stored outside an iSSP shall be protected by the iSSP in order to ensure their confidentiality, their integrity, the perfect forward secrecy support, software side channel protection and their privacy (see note 2).
REQ-15-SSP-9.2.9.1-04	All iSSP software and data, including context, shall only be stored in protected memory as requested in paragraph 36 in BSI-CC-PP-0084-2014 [11].
REQ-15-SSP-9.2.9.1-05	All iSSP software and data stored outside an iSSP shall be protected against rollback attacks.
REQ-15-SSP-9.2.9.1-06	The iSSP instruction and data buses shall be isolated from other SoC buses by a firewall under the control of the iSSP (see note 2).
REQ-15-SSP-9.2.9.1-07	The other SoC components shall have no direct access to the iSSP buses.
REQ-15-SSP-9.2.9.1-08	The iSSP shall be able to use the rNVM, dedicated to the SoC, to store encrypted data.
REQ-15-SSP-9.2.9.1-09	Access to the rNVM as defined in REQ-15-SSP-9.2.9.1-08 shall be managed by the primary platform using a means which is independent of the rNVM implementation.
REQ-15-SSP-9.2.9.1-10	All iSSP software and data stored outside an iSSP shall be securely bound to that given iSSP instance (see note 2).
REQ-15-SSP-9.2.9.1-11	All the credentials used to protect the data stored in the rNVM as per requirements REQ-15-SSP-9.2.9.1-04 and REQ-15-SSP-9.2.9.1-08, shall only be stored and used in the iSSP.
REQ-15-SSP-9.2.9.1-12	The primary platform shall enforce that the credentials described in REQ-15-SSP-9.2.9.1-11 shall not be accessed in test mode.
REQ-15-SSP-9.2.9.1-13	The iSSP shall use only self-contained cryptographic mechanisms.
REQ-15-SSP-9.2.9.1-14	The iSSP shall have a hardware protection means that controls the access to every SSP functional domain.
REQ-15-SSP-9.2.9.1-15	Void. See requirement REQ-15-SSP-8.9.1.5-01.
REQ-15-SSP-9.2.9.1-16	Any transaction, that writes, updates or deletes persistent data that belongs to the secondary platform and its SSP applications, shall only be acknowledged after it has been committed (see note 1).
REQ-15-SSP-9.2.9.1-17	The iSSP shall be a secure element integrated within a SoC.
REQ-15-SSP-9.2.9.1-18	Void. See requirement REQ-15-SSP-8.9.1.5-02.
REQ-15-SSP-9.2.9.1-19	Void. See requirement REQ-15-SSP-8.9.1.5-03.
REQ-15-SSP-9.2.9.1-20	Void. See requirement REQ-15-SSP-8.9.1.5-04.
REQ-15-SSP-9.2.9.1-21	Void. See requirement REQ-15-SSP-8.9.1.5-05.
REQ-15-SSP-9.2.9.1-22	Void. See requirement REQ-15-SSP-8.9.1.5-06.
NOTE 1: Commitment in this context means that the iSSP NVM has been successfully updated. NOTE 2: This requirement does not apply to the communication protocol data.	

9.2.9.2 Core platform security requirements

Identifier	Requirement
REQ-15-SSP-9.2.9.2-01	Void. See requirement REQ-15-SSP-8.9.1.6-01.
REQ-15-SSP-9.2.9.2-02	Void. See requirement REQ-15-SSP-8.9.1.6-02.
REQ-15-SSP-9.2.9.2-03	Void. See requirement REQ-15-SSP-8.9.1.6-03.
REQ-15-SSP-9.2.9.2-04	The primary platform shall provide a means to preserve the integrity of the contents stored in its NVM across power-cycles.
REQ-15-SSP-9.2.9.2-05	The means provided in REQ-15-SSP-9.2.9.1-04 shall be at least equivalent to the means protecting the internal memory of a discrete SE during the life cycle of the SoC.
REQ-15-SSP-9.2.9.2-06	Void. See requirement REQ-15-SSP-8.9.1.6-04.
REQ-15-SSP-9.2.9.2-07	Void. See requirement REQ-15-SSP-8.9.1.6-05.

9.2.9.3 Void (Clause is now 8.9.1.7)

9.2.9.4 Void (Clause is now 8.9.1.8)

9.2.9.5 System on chip security requirements

Identifier	Requirement
REQ-15-SSP-9.2.9.5-01	It should be possible for the iSSP to allocate a private logical partition of the rNVM.
REQ-15-SSP-9.2.9.5-02	It may be possible for the rNVM controller to dynamically manage the size of the private logical partition as define in REQ-15-SSP-9.2.9.5-01.
REQ-15-SSP-9.2.9.5-03	A means shall be provided to prevent the access to the private logical partition as defined in REQ-15-SSP-9.2.9.5-01 by any part of the SoC outside the iSSP.

9.2.10 Void (Clause is now 8.9.1.1)

9.2.11 Void (Clause is now 8.9.1.2)

9.2.11.1 Void (Clause is now 8.9.1.2.1)

9.2.11.2 Void (Clause is now 8.9.1.2.2)

9.2.11.3 Void (Clause is now 8.9.1.2.3)

9.2.11.4 Void (Clause is now 8.9.1.2.4)

9.2.11.5 Void (Clause is now 8.9.1.2.5)

10 Requirements for eSSP class

10.1 Introduction

This clause specifies the requirements for the eSSP class.

Some use cases for an embedded secure element are described in clause 6. There are two types of the eSSP class using different architectures: eSSP Type 1 and eSSP Type 2.

10.2 Additional requirements for the eSSP Type 1 class

10.2.1 Application and file structure

10.2.1.1 SSP application requirements

Identifier	Requirement
REQ-15-SSP-10.2.1.1-01	There shall be an option for the eSSP Type 1 to support SSP applications using the APDU as defined in ISO/IEC 7816-4 [8] and ETSI TS 102 221 [2].
REQ-15-SSP-10.2.1.1-02	There shall be an option for the eSSP Type 1 to support SSP applications using HTTP(S).

10.2.1.2 File system

No additional requirement.

10.2.1.3 SSP application and file system access conditions

No additional requirement.

10.2.2 Protocols

10.2.2.1 Required protocol support

Identifier	Requirement
REQ-15-SSP-10.2.2.1-01	The eSSP Type 1 shall support SCL network layer, as described in clause 8.3.1.
REQ-15-SSP-10.2.2.1-02	If the eSSP Type 1 supports the ISO/IEC 7816-3 [7] interface as per REQ-15-SSP-8.4.2.1-01, it shall support the APDU protocol according to ISO/IEC 7816-4 [8] over the ISO/IEC 7816-3 [7] interface.
NOTE: Concurrent processing of APDUs received on both interfaces is not required.	

10.2.3 Electrical and physical Interface

10.2.3.1 General electrical and physical interface requirements

Identifier	Requirement
REQ-15-SSP-10.2.3.1-01	The eSSP Type 1 shall support at least one of the electrical and physical interfaces described in the requirements REQ-15-SSP-8.4.2.1-02, REQ-15-SSP-8.4.2.1-04 and REQ-15-SSP-8.4.2.1-05.
REQ-15-SSP-10.2.3.1-02	In addition to REQ-15-SSP-B3.1-01 requirements, the eSSP Type 1 may also support the electrical and physical interface described in requirements REQ-15-SSP-8.4.2.1-01.

10.2.4 Form factor

No additional requirement.

10.2.5 Security

10.2.5.1 Generic security requirements

No additional requirement.

10.2.5.2 Certification requirements

Identifier	Requirement
REQ-15-SSP-10.2.5.2-01	The certification of the eSSP Type 1 integrated chip shall claim in its security target the conformance with protection profile BSI-CC-PP-0084-2014 [11] (see note).
REQ-15-SSP-10.2.5.2-02	If the eSSP Type 1 integrated chip includes a loader then it shall claim in its security target the conformance with protection profile BSI-CC-PP-0084-2014 [11] including loader package 2 (see note).
REQ-15-SSP-10.2.5.2-03	The certification minimum assurance level is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.
REQ-15-SSP-10.2.5.2-04	AVA_VAN.5 tests shall be performed in accordance with the JIL Application of Attack potential to Smartcards documentation [12].
NOTE: In case this protection profile is deprecated, another protection profile that provides at least equal protection shall be used.	

10.2.6 SSP management

No additional requirement.

10.2.7 Backwards compatibility

Identifier	Requirement
REQ-15-SSP-10.2.7-01	The eSSP Type 1 may support legacy logical architecture as defined in ETSI TS 102 221 [2] and ETSI TS 102 671 [3].
REQ-15-SSP-10.2.7-02	The eSSP Type 1 should support the contactless interface as defined in ETSI TS 102 613 [4] and ETSI TS 102 622 [6].
REQ-15-SSP-10.2.7-03	The eSSP Type 1 should support UICC applications (e.g. USIM as defined in ETSI TS 131 102 [15]).
REQ-15-SSP-10.2.7-04	The eSSP Type 1 should support UICC card application toolkit (CAT) applications as defined in ETSI TS 102 223 [14].
REQ-15-SSP-10.2.7-05	The eSSP Type 1 should support applications based on ETSI TS 102 241 [18].
REQ-15-SSP-10.2.7-06	The eSSP Type 1 should support applications based on ETSI TS 102 705 [19].

10.3 Additional requirements for the eSSP Type 2 class

10.3.1 General requirements

Identifier	Requirement
REQ-15-SSP-10.3.1-01	The eSSP Type 2 shall support the requirements defined in clause 10.2 (see note).
REQ-15-SSP-10.3.1-02	The eSSP Type 2 shall support the requirements defined in clause 8.9.
NOTE: ISO/IEC 7816-3 [7] physical interface is not applicable.	

Annex A (normative): Telecom bundle requirements

The following requirements apply to Telecom Bundles.

Identifier	Requirement
REQ-15-SSP-XA-01	A telecom bundle shall have a telecom family identifier.
REQ-15-SSP-XA-02	There shall be a telecom bundle class to classify a telecom bundle as a test telecom bundle.
REQ-15-SSP-XA-03	The terminal shall use only a telecom bundle to establish access to Recommendation ITU-T E.212 [i.1] network.
REQ-15-SSP-XA-04	The terminal shall ensure that the IMSI value of the test telecom bundle complies with the test USIM IMSI defined in clause 8.3.2.2 of ETSI TS 134 108 [28].
REQ-15-SSP-XA-05	There shall be a means within the telecom bundle to configure whether end user/subscriber intent shall be required when switching this telecom bundle from disabled to enabled state and vice versa, as well as from enabled/disabled to deleted states.
REQ-15-SSP-XA-06	If configured in the telecom bundle, end user/subscriber intent shall be required when switching this telecom bundle from disabled to enabled state and vice versa, as well as from enabled/disabled to deleted states.
REQ-15-SSP-XA-07	Telecom bundle concurrency capability shall be set on the iSSP at the time of manufacturing (see note 1).
REQ-15-SSP-XA-08	If the telecom bundle concurrency capability in REQ-15-SSP-XA-07 is set to greater than one, the behaviour of the terminal shall be compliant with the operational modes as described in GSMA TS.37 [29] (see note 2).
REQ-15-SSP-XA-09	The iSSP shall enforce that the number of telecom bundles in the enabled or active state is not greater than the telecom bundle concurrency capability.
NOTE 1: iSSP inside the SoC containing no cellular baseband is FFS. NOTE 2: According to the GSMA TS.37 [29], 2 concurrent network registrations are maintained by the baseband with the following connection modes: - DSDS(Dual SIM Dual Standby): idle+idle or idle+connected mode. - DSDA(Dual SIM Dual Active): idle+idle, idle+connected or connected+connected mode.	

Annex B (informative): Change history

The table below indicates changes that have been incorporated into the present document since it was published.

Change history								
Date	**Meeting**	**TC SCP Doc.**	**CR**	**Rv**	**Cat**	**Subject/Comment**	**Old**	**New**
2019-06	SCP#88	SCP(19)000128	001		D	Primary/Secondary Platform Architecture - restructuring of requirements.	15.0.0	15.0.1
2019-06	SCP#88	SCP(19)000129r1	002	1	B	Introduction of eSSP Type 1 and eSSP Type 2.	15.0.1	15.1.0
2019-06	SCP#88	SCP(19)000131	004		B	Introduction of the definition of Custodian and the related requirements.	15.0.1	15.1.0
2019-06	SCP#88	SCP(19)000130	003		B	Secure access to SSP applications.	15.1.0	16.0.0
2019-09	SCP#89	SCP(19)000205r1	005	1	B	Requirements on storage of default SPB Manager address.	16.0.0	16.1.0

History

Document history		
V16.0.0	August 2019	Publication
V16.1.0	March 2020	Publication