ETSI TS 103 666-3 V16.0.0 (2020-07)

Smart Secure Platform (SSP);
Part 3: Embedded SSP (eSSP) Type 1 characteristics
(Release 16)

Reference
DTS/SCP-T00TSSPvg00-3

Keywords
eSSP, SSP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - 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.

The present document is part 3 of a multi-part deliverable covering Smart Secure Platform (SSP), as identified below:

Part 1: "General characteristics";

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

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

Modal verbs terminology

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

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

1 Scope

The present document details the technical specifications for the Smart Secure Platform (SSP) in a discrete hardware non removable component, also known as eSSP. The present document defines specific attributes on top of the generic SSP specified in ETSI TS 103 666-1 [1] for eSSP Type 1, including the external interfaces (e.g. ISO/IEC 7816-3 [11], SPI, SWP). The eSSP Type 1 class implements an operating system directly accessing the SSP hardware platform, as described in ETSI TS 103 666-1 [1] in clause 5.2.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the 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] ETSI TS 103 666-1: "Smart Secure Platform (SSP); Part 1: General characteristics".

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

[3] ETSI TS 102 622: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)".

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

[5] ORACLE: "Application Programming Interface, Java Card™ Platform, 3.0.5 Classic Edition".

[6] ORACLE: "Runtime Environment Specification, Java Card™ Platform, 3.0.5 Classic Edition".

[7] ORACLE: "Virtual Machine Specification Java Card™ Platform, 3.0.5 Classic Edition".

NOTE: ORACLE Java Card™ Specifications can be downloaded at http://docs.oracle.com/javame/javacard/javacard.html.

[8] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Physical and data link layer characteristics".

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

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

[11] ISO/IEC 7816-3: "Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols".

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

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

[13] "Common Criteria for Information Technology Security Evaluation; Part 3: Security assurance components', April 2017 Version 3.1 Revision 5.

NOTE: Available at https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf.

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

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

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

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

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

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

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

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.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 666-1 [1], clause 3.1 apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

eSSP embedded SSP

4 Introduction

4.1 Background

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

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

4.2 Document layout

The present document specifies:

- the definition and overview of an eSSP Type 1;
- the eSSP Type 1 architecture and the possible transport protocol(s) used between the terminal and the eSSP Type 1;
- the eSSP Type 1 features and characteristics, including security requirements;
- the eSSP Type 1 possible physical interface(s).

4.3 External references

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

4.4 ASN.1 syntax

4.4.1 Introduction

The ASN.1 syntax defined in ETSI TS 103 666-1 [1], clause 4.4.1 shall apply. The ASN.1 code defined in this document are provided in addition to definitions of ETSI TS 103 666-1 [1].

The complete ASN.1 code is provided for reference in annex A.

4.4.2 Start of ASN.1

```
-- ASN1START

ESSPDefinitions { itu-t (0) identified-organization (4) etsi (0) smart-secure-platform (3666) part3
(3) }

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

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

-- ASN1STOP
```

5 eSSP Type 1 architecture

5.1 Overview

The eSSP Type 1 is a specific SSP class which is a non-removable discrete hardware component. The type and number of physical interface and the form factor depend of the implementation of the eSSP Type 1.

5.2 Software architecture

The eSSP Type 1 shall use the software architecture "SSP software running directly on SSP hardware platform" described in ETSI TS 103 666-1 [1], clause 5.2.

5.3 Hardware architecture

In addition to eSSP Type 1 example description in ETSI TS 103 666-1 [1], clause 5.3, an eSSP Type 1 has physical interface(s).

5.4 Protocol stacks

As described in ETSI TS 103 666-1 [1], clause 5.4, the eSSP Type 1 may have multiple physical interfaces.

The eSSP Type 1 shall support at least one physical interface that supports the SSP Common Layer (SCL) implementation, as described in ETSI TS 103 666-1 [1], clause 8.

An eSSP Type 1 may implement an ISO/IEC 7816-3 [11] interface. If an eSSP Type 1 supports an ISO/IEC 7816-3 [11] interface, only APDU shall be transmitted on this interface.

The eSSP Type 1 may support the UICC architecture as defined in ETSI TS 102 221 [2] and ETSI TS 102 622 [3].

If the UICC architecture is supported, an unique and dedicated APDU transport protocol shall be used for that architecture e.g. APDU protocol over an ISO/IEC 7816-3 [11] interface, or the UICC APDU Service gate as described in ETSI TS 103 666-1 [1].

If the eSSP Type 1 supports multiple APDU transport mechanisms (e.g. clause C.5.1), in addition to the APDU transport mechanism involved to support the UICC architecture, all other APDU transport mechanisms should convey APDUs to a dedicated and independent execution(s) framework(s).

5.5 Execution frameworks

The eSSP Type 1 should support an execution framework as defined for the UICC according to ETSI TS 102 241 [4] based on the Java Card™ Platform [5], [6] and [7].

If the eSSP Type 1 supports the contactless interface defined in ETSI TS 102 613 [8] and the protocol defined in ETSI TS 102 622 [3], the eSSP Type 1 shall support the execution framework defined in ETSI TS 102 705 [9].

The eSSP Type 1 may support additional execution frameworks, based on the Java Card™ Platform [5], [6] and [7] or others. In that case, such an additional execution framework should be independent from the others and shall be connected to a dedicated APDU transport mechanism.

6 eSSP Type 1 characteristics

6.1 Form factors

The eSSP Type 1 form factor may comply with ETSI TS 102 671 [10] with the exception of MFF1.

6.2 Power

6.2.1 Power mode

The power modes defined in ETSI TS 103 666-1 [1], clause 6.2.1 shall apply.

6.2.2 Power sources

6.2.2.1 Types of power sources

The type of power source defined in ETSI TS 103 666-1 [1], clause 6.2.2.1 shall apply.

6.2.2.2 Power source of type Interface

The power source of type interface defined in ETSI TS 103 666-1 [1], clause 6.2.2.2 shall apply.

6.2.2.3 Power source of type Independent

The power source of type independent defined in ETSI TS 103 666-1 [1], clause 6.2.2.3 shall apply.

6.2.3 Power consumption

The power consumption defined in ETSI TS 103 666-1 [1], clause 6.2.3 shall apply.

6.3 Clock

The eSSP Type 1 shall support a clock as defined in ETSI TS 103 666-1 [1], clause 6.3.

6.4 SSP initialization

6.4.1 SSP interface session

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

6.4.2 Capability exchange

6.4.2.1 Overall description

The capability exchange procedure is used to inform the eSSP Type 1 of the capabilities of the terminal and for the terminal to retrieve the capabilities of the eSSP Type 1.

The capability exchange for eSSP Type 1 supporting SCL as defined in ETSI TS 103 666-1 [1], clause 6.4.2.3. shall apply.

6.4.2.2 Capabilities of the terminal

The data field sent by the terminal to the eSSP Type 1 during the capability exchange procedure shall contain the data structure defined in ETSI TS 103 666-1 [1], clause 6.4.2.4, with the following modifications:

- aPhysicalInterfaces in the TerminalCapability should be present.

6.4.2.3 Capabilities of the eSSP Type 1

The data field sent by the eSSP Type 1 to the terminal contains the data structure defined in ETSI TS 103 666-1 [1],clause 6.4.2.5, with the following modification:

- SSPClass field shall have the eSSPClass-Embedded-Type1 (1) value.
- aPhysicalInterfaces and aSspExternalMaxPowerConsumption into the SSPCapability should be provided.
- aClassSpecificCapabilities into the SSPCapability shall have the following structure:

```
-- ASN1START

ESSPCapabilities ::= SEQUENCE
{
    aSupportforSspSuspension [3] BOOLEAN DEFAULT FALSE
}

-- ASN1STOP
```

aSupportforSspSuspension: it indicates if the eSSP Type 1 supports the suspension mechanism, as defined in clause 6.9. It shall have the value FALSE if suspension is not supported, TRUE otherwise.

6.5 Storage

The storage capabilities of the eSSP Type 1 interface defined in ETSI TS 103 666-1 [1], clause 6.5 shall apply with the following modifications:

- An eSSP Type 1 shall use only its own dedicated internal non-volatile memory (NVM) for code and data.

6.6 Data management

6.6.1 UICC file system

The eSSP Type 1 may support the UICC file system as specified in ETSI TS 102 221 [2], clauses 8.1, 8.2 and 8.3, and the associated security features described in ETSI TS 102 221 [2], clause 9.

6.6.2 eSSP Type 1 file system

The eSSP Type 1 may support the SSP file system defined in ETSI TS 103 666-1 [1], clause 6.6.2 and its sub-clauses.

6.7 eSSP Type 1 identification

The eSSP Type 1 shall be identified with an identifier based on the definition in ETSI TS 103 666-2 [16], clause 7.5 with the following exceptions:

- **SSP Type** identifies the type of eSSP Type 1 and is coded as follows:

Base-32 character	Value	Description
E	'00100'	Embedded SSP Type 1 (eSSP Type 1)

- **SSP Manufacturer identifier:** identifies the eSSP Type 1 maker which manufactures and provides the eSSP Type 1.
- **Manufacturer proprietary information:** is a field under the responsibility of the eSSP Type 1 manufacturer.

NOTE 1: This field may contain information about the eSSP Type 1.

- The UUID is computed using UUID version 5 as defined in IETF RFC 4122 [18] from the string "urn:etsi.org:esspt1id:<eSSP Type 1 maker OID>:<ISN>" (without quotes), where:
  - <**eSSP Type 1 maker OID**> is the OBJECT IDENTIFIER of the eSSP Type 1 maker which manufactures and provides the eSSP Type 1.

- <**ISN**> is the individual serial number of the eSSP Type 1 and is defined by the eSSP Type 1 maker. <ISN> shall be unique and immutable within the scope of the eSSP Type 1 maker for products of this class.

NOTE 2: It is for further study if the uniqueness of <ISN> within the scope of the eSSP Type 1 maker needs to be for all products of the SSP maker or only for eSSP Type 1 products of that SSP maker.

6.8 Runtime environment

6.8.1 CAT Runtime Environment

If the eSSP Type 1 support the CAT Runtime Environment as specified in ETSI TS 102 241 [4] the provisions defined in ETSI TS 103 666-1 [1] clause 6.8.1 for eSSP Type 1 supporting SCL shall apply.

6.9 eSSP Type 1 suspension

If the eSSP Type 1 support the suspension mechanism, the provisions defined in ETSI TS 103 666-1 [1], clause 6.9 shall apply.

6.10 eSSP Type 1 Applications

The eSSP Type 1 support for eSSP Type 1 applications is defined in ETSI TS 103 666-1 [1], clause 6.10 and its sub-clauses.

6.11 eSSP Type 1 security

6.11.1 eSSP Type 1 security architecture

The eSSP Type 1 security architecture overview and requirement provided in ETSI TS 103 666-1 [1], clause 6.11.1 shall apply.

6.11.2 Mandatory requirements

The eSSP Type 1 mandatory security requirement provided in ETSI TS 103 666-1 [1], clause 6.11.2 and its sub-clauses shall apply.

6.11.3 Optional requirements

The eSSP Type 1 optional security requirement provided in ETSI TS 103 666-1 [1], clause 6.11.3 and its sub-clauses may apply.

6.11.4 Security certification

The eSSP Type 1 may accommodate different security features and may meet different security levels depending on the targeted applications. The different security levels are evaluated by independent evaluation labs based on industry specific Protection Profiles.

The eSSP Type 1 shall be common criteria certified at least to the Evaluation Assurance Level (EAL) 4 augmented with AVA_VAN.5 and ALC_DVS.2. The security target of the eSSP Type 1 shall claim the certified protection profile under the reference BSI-CC-PP-0084-2014 [12]. The Evaluation Assurance Level may be augmented if one or more Assurance Families exceed their minimal level.

The Evaluation Assurance Level is defined in table 1 in Common Criteria for Information Technology Security Evaluation Part 3 [13] according to the level of the different Assurance Families and Assurance Classes.

AVA_VAN.5 tests shall be performed in accordance with the JIL Application of Attack potential to Smartcards documentation [14].

The eSSP Type 1 shall embed an autonomous and independent clock system in conformance with the Protection Profile BSI-CC-PP-0084-2014 [12].

If the eSSP Type 1 includes a loader, the eSSP Type 1 shall be conformant to the Loader Package 2, as defined in BSI-CC-PP-0084-2014 [12].

The eSSP Type 1 may claim in its Security Target the conformance with Protection Profile BSI-CC-PP-0089-2015 [15].

6.12 User interface

The eSSP Type 1 may support an web-based user interface, in that case clause 6.12 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply.

6.13 Accessor authentication service

The eSSP Type 1 shall support the accessor authentication service described in ETSI TS 103 666-1 [1], clause 6.13 and its sub-clauses.

7 Physical interfaces

7.1 Overview

The eSSP Type 1 physical interface description clause 7.1 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply, with the following additions:

- At least one physical interface shall be used to convey SCL.

If the eSSP Type 1 has multiple interfaces that support SCL, theses interfaces should be able to work concurrently.

7.2 Reset

The eSSP Type 1 description clause 7.2 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply.

7.3 ISO 7816 interface

The eSSP Type 1 may support an interface ISO/IEC 7816-3 [11], in that case clause 7.3 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply, with the following additions:

- the eSSP Type 1 should support the T=0 protocol.

7.4 SPI interface

The eSSP Type 1 may support an SPI interface, in that case clause 7.4 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply.

7.5 I2C interface

The eSSP Type 1 may support an I2C interface, in that case clause 7.5 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply.

7.6 SWP interface

The eSSP Type 1 may support an SWP interface, in that case clause 7.6 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply. In addition:

- the eSSP Type 1 should support extended resume time;
- the terminal should deactivate the SWP line only prior to a global eSSP Type 1 deactivation;
- the values for power mode given in ETSI TS 102 613 [8], clause 7.1.2 are not applicable;
- if the eSSP Type 1 supports the interfaces defined in ETSI TS 102 221 [2] and ETSI TS 102 613 [8] used by the same execution environment, the following clauses shall apply:
  - ETSI TS 102 613 [8] clauses 5.3, 5.4, 6.2.2.0, 6.2.2.3, 6.2.3.4, 6.2.6, 8.3.2 and clause 8.4 to support "low power mode" and interfaces interworking;
  - ETSI TS 102 221 [2] clauses 4.5.1, 4.5.2, 4.5.3, 6.3.3, 11.1.19 and clause 11.1.22;
- if the SWP interface operates independently of an ETSI TS 102 221 [2] interface, the interface activation may depend on other physical interfaces and is out of the scope of the present document.

7.7 USB interface

The eSSP Type 1 may support an USB interface, in that case clause 7.7 and its sub-clauses in ETSI TS 103 666-1 [1] shall apply.

8 SSP Common Layer (SCL)

8.1 introduction

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

- The SCL network controller host and SCL router need not to share the same security perimeter of the eSSP Type 1, i.e. the security perimeter of the SCL network controller host and SCL router is not required to be shared.

8.2 eSSP Type 1 with only one SCL interface

If the eSSP Type 1 has only one SCL interface, this interface should convey packets to multiple SCL hosts outside the SSP host domain, as illustrated in clause B.1.

8.3 eSSP Type 1 with multiple SCL interfaces

If the eSSP Type 1 has multiples SCL interfaces, all these interfaces should belong to the same SCL network. Furthermore, the eSSP Type 1 should implement the SCL router and SCL network controller host, as illustrated in clause B.2.

SCL hosts of an host domain should be accessible only through one SCL interface. The communication inside the eSSP Type 1 between the eSSP Type 1 Host, the router and the SCL network controller host are out of the scope of the present document.

9 Secure SCL

The eSSP Type 1 should support, on top of the secure SCL protocol as defined in ETSI TS 103 666-1 [1], clause 9 and its sub-clauses.

10 Communication layers above SCL

The eSSP Type 1 may support, on top of the SCL protocol, any protocol defined in ETSI TS 103 666-1 [1] clause 10 and its sub-clauses, e.g. APDU protocol, file system protocol, TCP control protocol support, UDP control protocol support, CRON service, contactless communications, CAT over SCL.

Annex A (normative): ASN.1 definitions

A.1 End of ASN.1

```
-- ASN1START

END

-- ASN1STOP
```

A.2 Complete ASN.1 file

The complete ASN.1 definition, as generated merging all the ASN.1 snippets present in this document is available at the following URL:

- https://forge.etsi.org/rep/scp/ts_103666-3_essp_type1/raw/v16.0.0/asn1/asn1_syntax.asn1.

Annex B (informative): SCL topologies

B.1 eSSP Type 1 with one SCL interface

In this example, the eSSP Type 1 has only one physical interface that convey all SCL packets. The SCL router is in charge of conveying each packet to the destination host. Host domains and communications means between the SCL router and the SCL network controller are not represented in figure B.1.

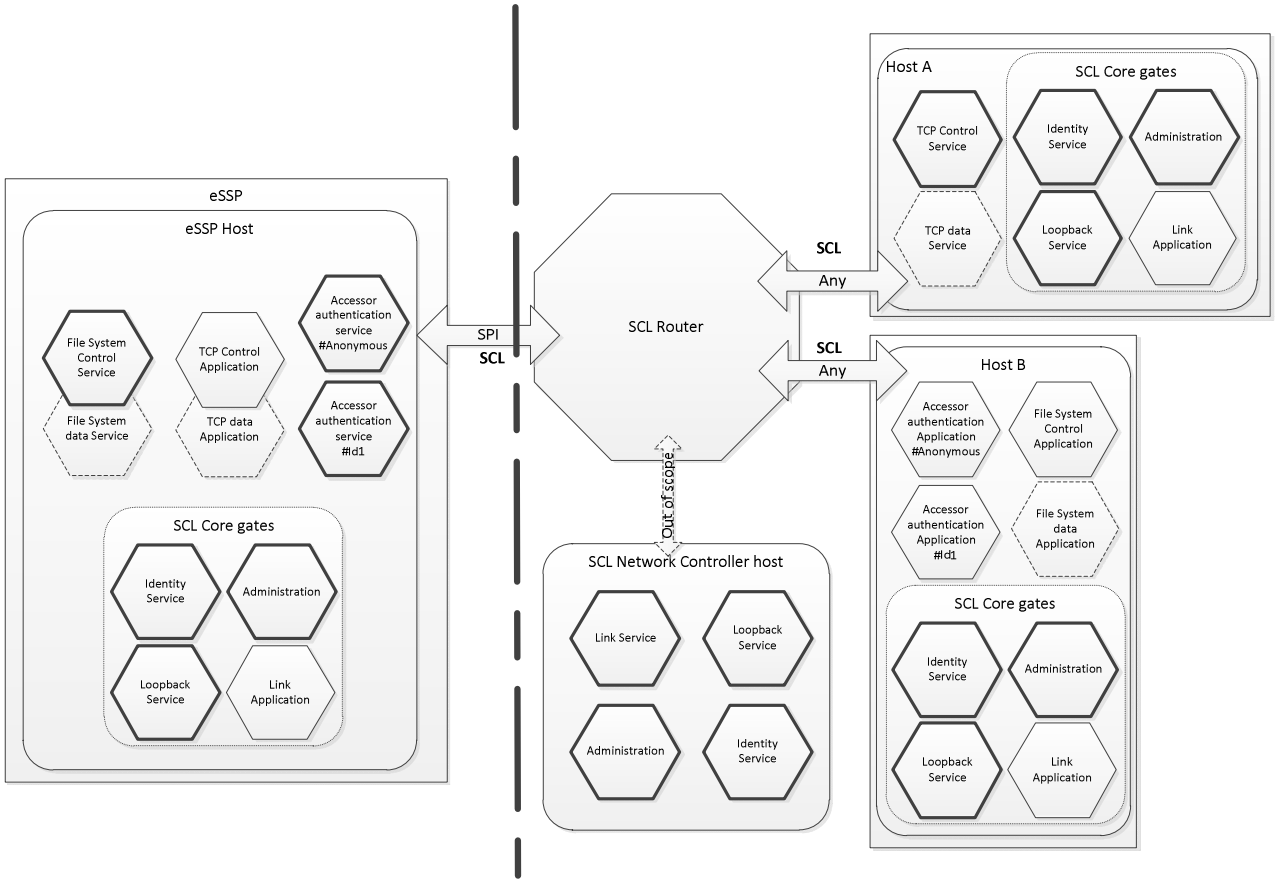

Figure B.1: eSSP Type 1 with one SCL interface

B.2 eSSP Type 1 with two SCL interfaces

In this example, the eSSP Type 1 has two physical interfaces that convey SCL packets. The SCL router in the eSSP Type 1 is in charge of conveying each packet to the destination host through the proper physical interface. The communication inside the eSSP Type 1 between the eSSP Type 1 host, the SCL router and the SCL network controller host are out of the scope of the present document. Host domains are not represented in figure B.2.

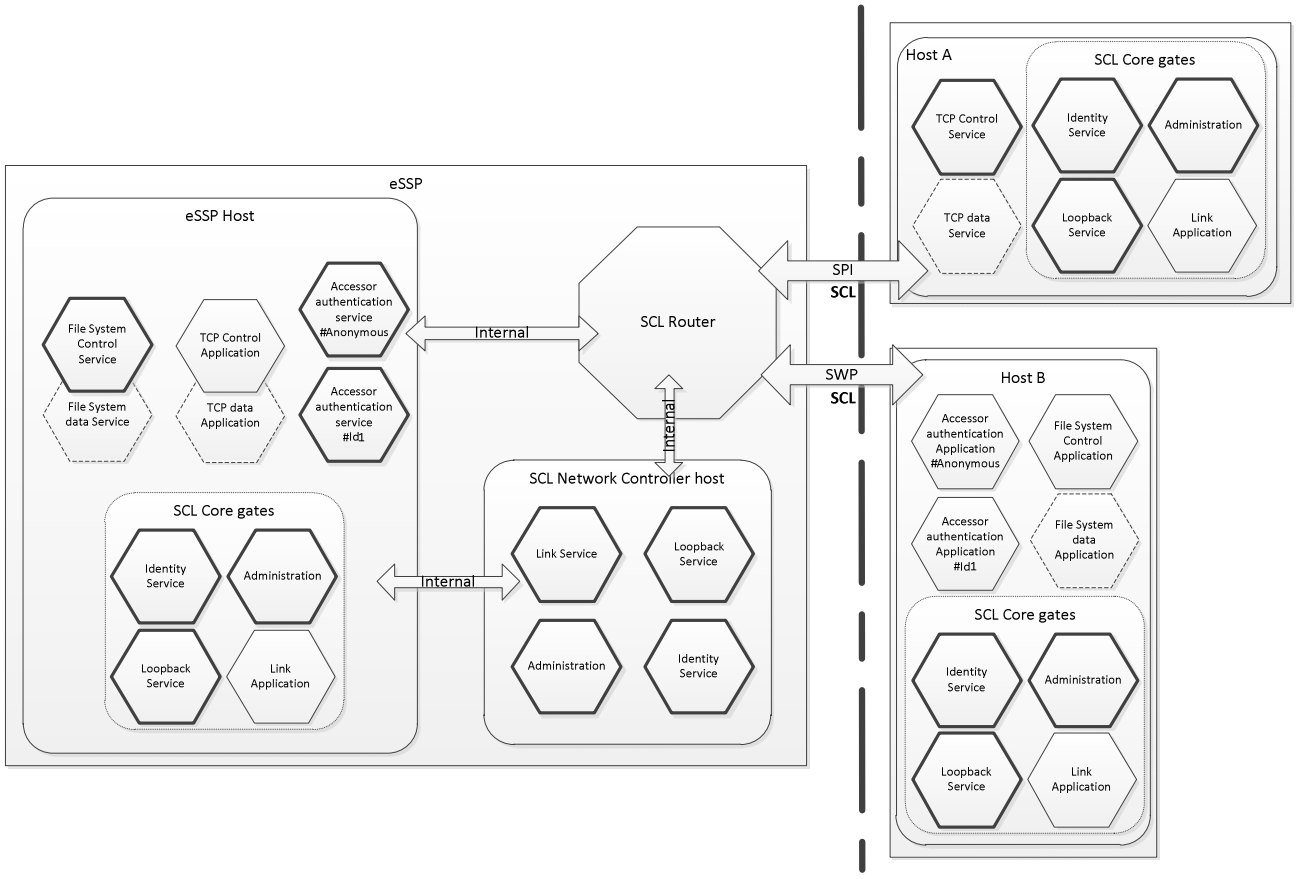

Figure B.2: eSSP Type 1 with multiple SCL interfaces

Annex C (informative): UICC architecture

C.1 UICC Architecture description

C.1.1 Introduction

The support of an eSSP Type 1 with an UICC architecture implies to support the APDU protocol and the UICC file system as defined in ETSI TS 102 221 [2]. The toolkit mechanisms, as defined in ETSI TS 102 223 [17] and/or the HCI protocol as defined in ETSI TS 102 622 [3] may also be supported.

The UICC may support execution(s) framework(s) linked to the supported protocols listed above.

C.1.2 Protocols stacks and execution frameworks

Supported protocols allow different types of execution frameworks to be supported.

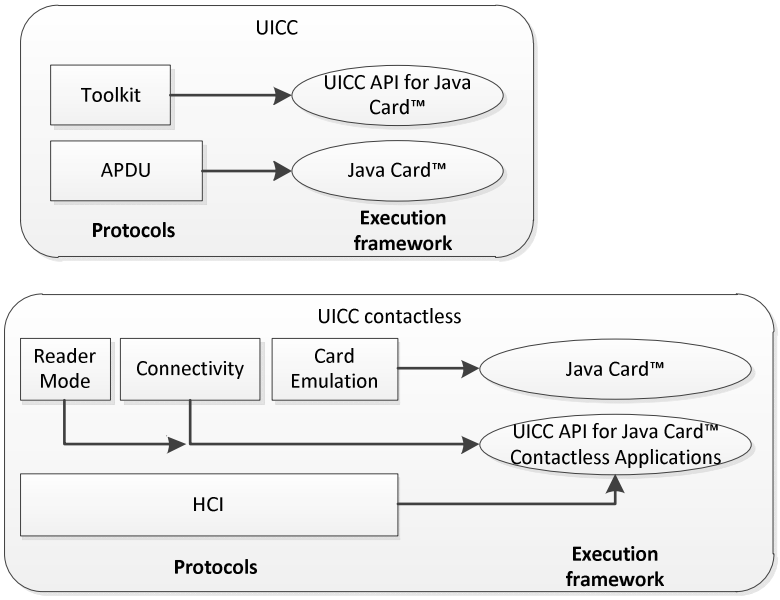

Figure C.1: Protocols and applications

Each type of protocol may support a dedicated execution framework: first level applications with the Java Card™ Platform [5], [6] and [7], toolkit application and access to the file system with the ETSI TS 102 241 [4], and for HCI protocol, the ETSI TS 102 705 [9].

C.2 eSSP Type 1 example without UICC features

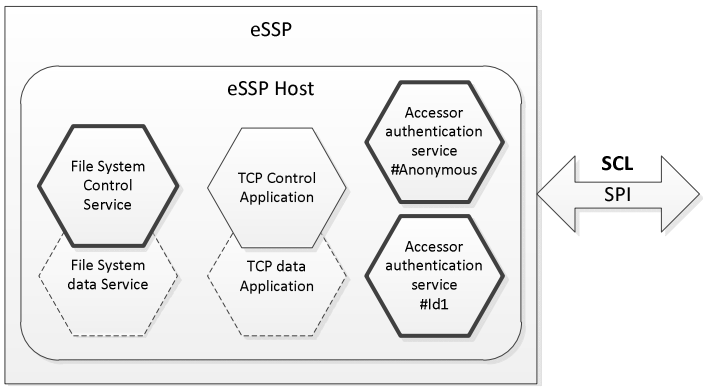

Figure C.2: SCL only eSSP Type 1 no UICC legacy

In this example, the eSSP Type 1 has one SCL interface, which provides support for functions over SCL as described in ETSI TS 103 666-1 [1] in clause 10. Capability exchange is done via the SCL interface through the Identity gate, not represented (as all SCL Core gates).

C.3 eSSP Type 1 Example with UICC support on an legacy physical interface

C.3.1 UICC with no contactless

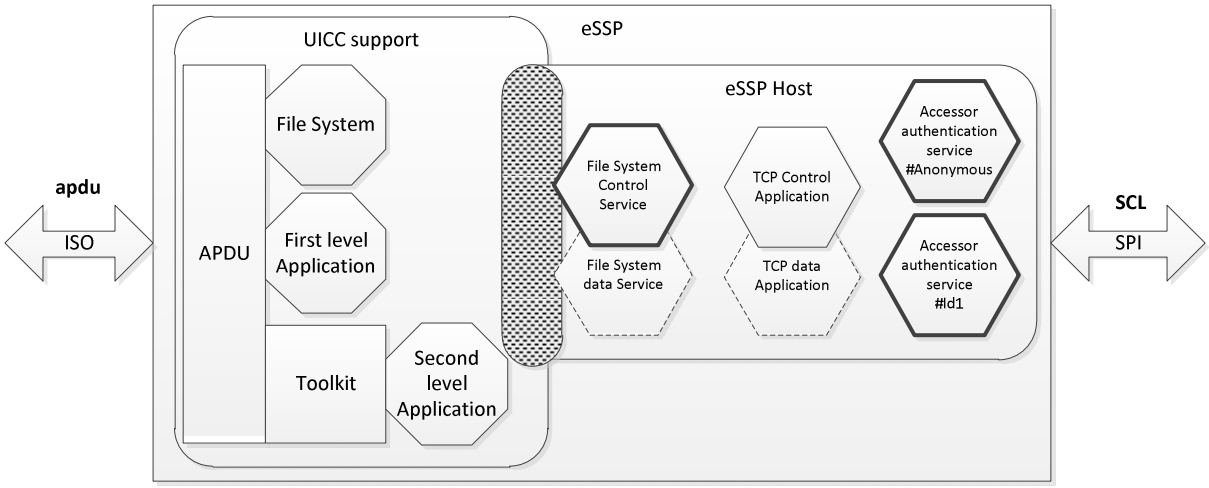

Figure C.3: SCL and APDU physical interface on eSSP Type 1 with UICC legacy support

In this example, the eSSP Type 1 has one SCL interface, which provides support for functions over SCL as described in ETSI TS 103 666-1 [1] in clause 10. In addition, this eSSP Type 1 has one ISO/IEC 7816-3 [11] interface which supports the APDU transport protocol to an UICC architecture. That UICC architecture may support protocols and execution framework as described in clause C.1.2. Inter dependencies between functions in the UICC architecture and functions in the eSSP Type 1 host are out of scope of the present document. Capability exchange is done via the SCL interface through the Identity gate, not represented (as all SCL Core gates).

C.3.2 UICC with contactless support on legacy physical interfaces

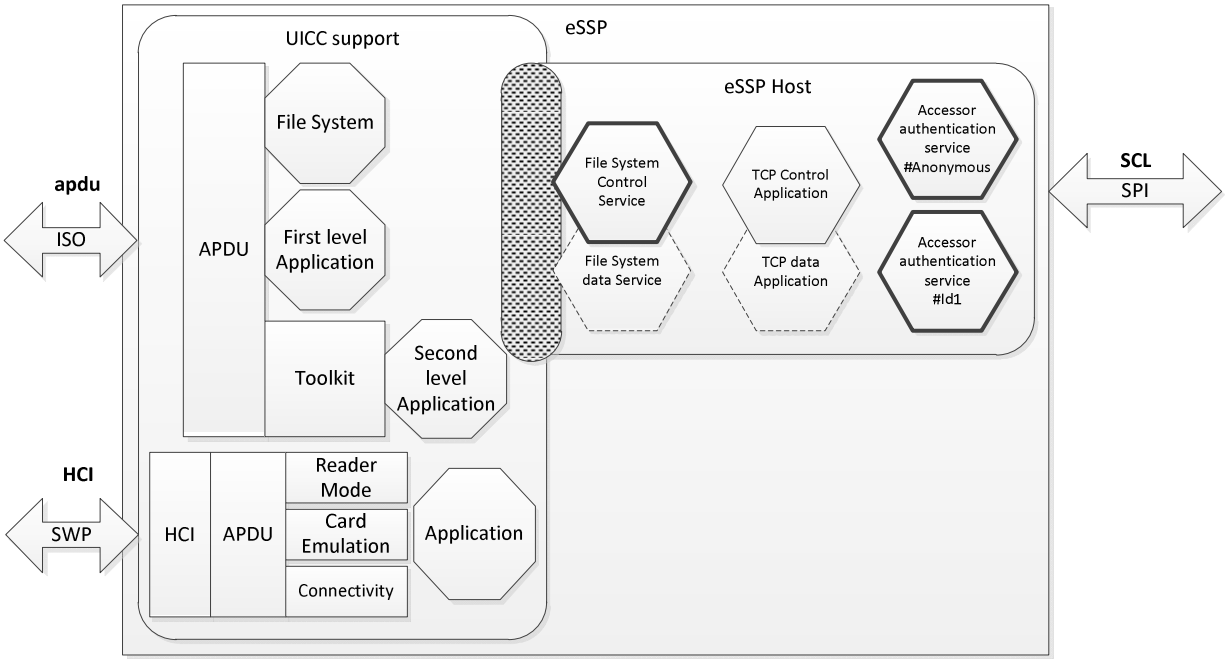

Figure C.4: SCL and APDU physical interface on eSSP Type 1 with UICC legacy support

In this example, the eSSP Type 1 has one SCL interface, which provides support for functions over SCL as described in ETSI TS 103 666-1 [1] in clause 10. In addition, this eSSP Type 1 has one ISO/IEC 7816-3 [11] interface which supports the APDU transport protocol and an SWP interface described in ETSI TS 102 613 [8] supporting the HCI protocol described in ETSI TS 102 622 [3] to an UICC architecture. That UICC architecture may support protocols and execution framework as described in clause C.1.2. Inter dependencies between functions in the UICC architecture and functions in the eSSP Type 1 host are out of scope of the present document. Capability exchange is done via the SCL interface through the Identity gate, not represented (as all SCL Core gates).

C.3.3 UICC on an legacy physical interfaces and contactless support over SCL

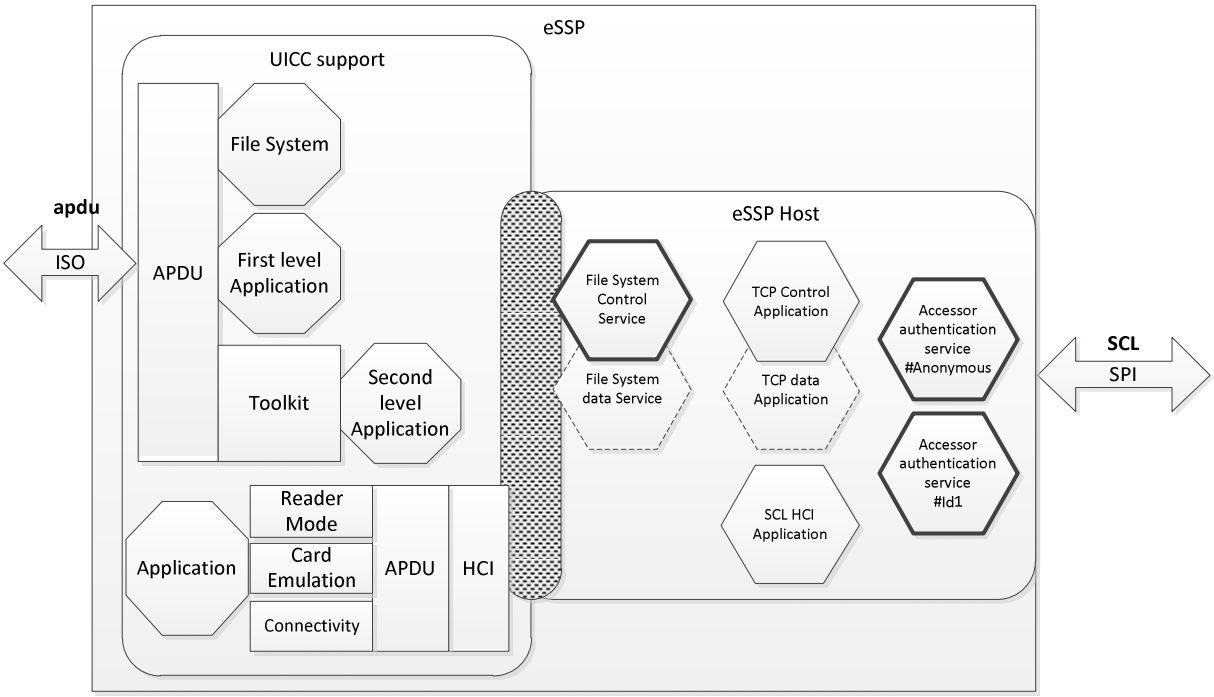

Figure C.5: APDU physical interface on eSSP Type 1 with UICC legacy support and contactless support over SCL

In this example, the eSSP Type 1 has one SCL interface, which provides support for functions over SCL as described in ETSI TS 103 666-1 [1] in clause 10. In addition, this eSSP Type 1 has one ISO/IEC 7816-3 [11] interface which supports APDU transport protocol and an SCL HCI Application gate which provides an interface that supports HCI protocol described in ETSI TS 102 622 [3] to an UICC architecture. That UICC architecture may support protocols and execution framework as described in clause C.1.2. Inter dependencies between functions in the UICC architecture and functions in the eSSP Type 1 host are out of scope of the present document. Capability exchange is done via the SCL interface through the Identity gate, not represented (as all SCL Core gates).

C.4 eSSP Type 1 Example with UICC support on SCL

C.4.1 UICC support on SCL, toolkit on APDU

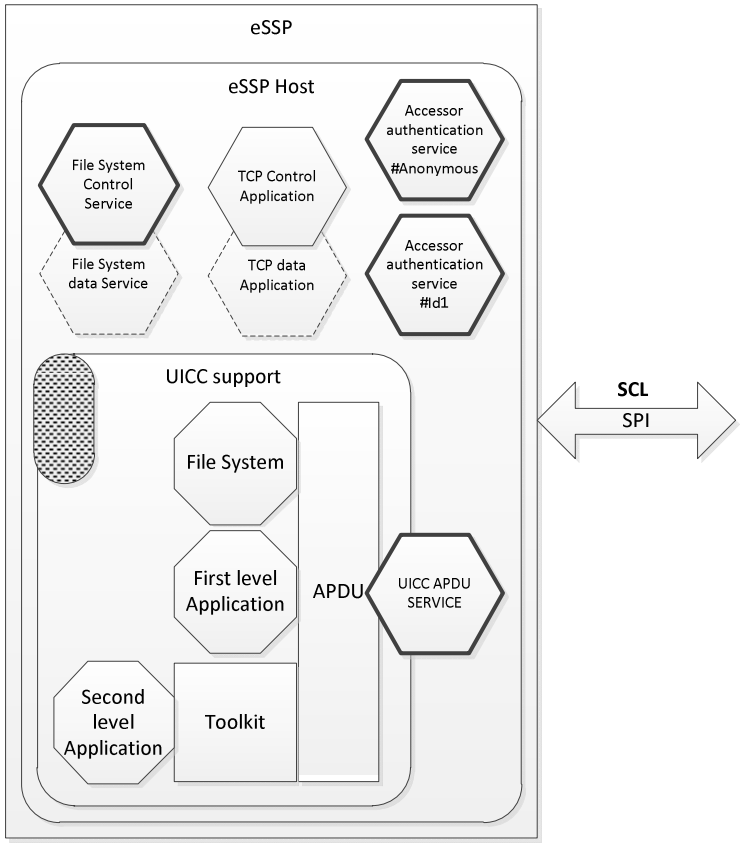

Figure C.6: SCL only eSSP Type 1 with UICC legacy support

In this example, the eSSP Type 1 has one SCL interface, which provides support for functions over SCL as described in ETSI TS 103 666-1 [1] in clause 10. In particular, this eSSP Type 1 has an UICC APDU service gate which provides an interface that supports APDU protocol communication to an UICC architecture. That UICC architecture may support protocols and execution framework as described in clause C.1.2. Inter dependencies between functions in the UICC architecture and functions in the eSSP Type 1 host are out of scope of the present document. Capability exchange is done via the SCL interface through the UICC APDU service gate. SCL Core gates are not represented.

C.4.2 UICC support on SCL, toolkit on SCL

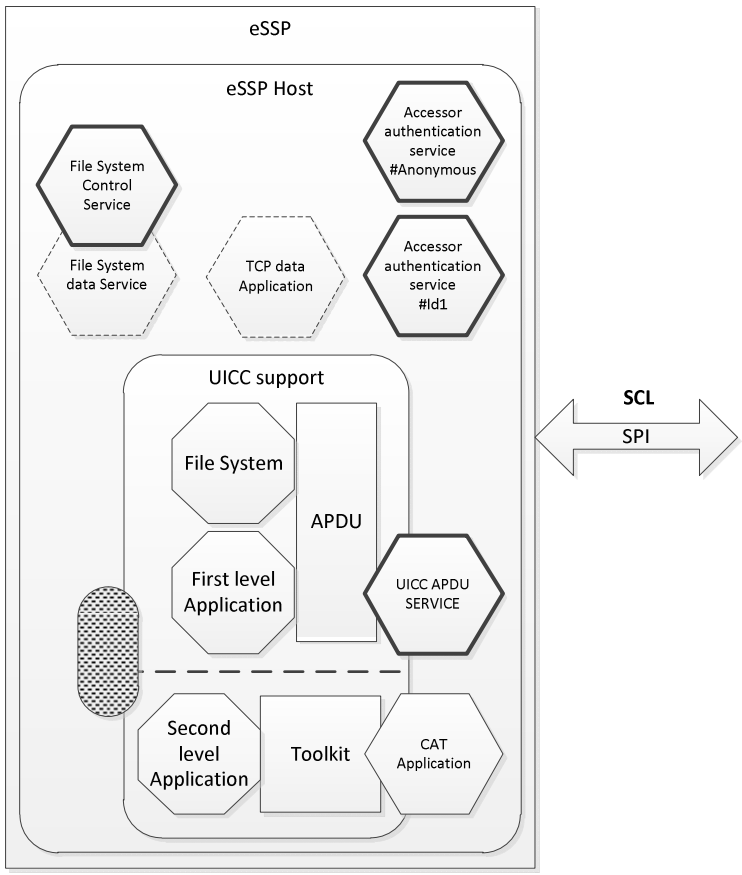

Figure C.7: SCL only eSSP Type 1 with UICC legacy support, toolkit on SCL

In this example, the eSSP Type 1 has one SCL interface, which provides support for functions over SCL as described in ETSI TS 103 666-1 [1] in clause 10. In particular, this eSSP Type 1 has an UICC APDU service gate which provides an interface that supports APDU protocol communication to an UICC architecture. That UICC architecture may support protocols and execution framework as described in clause C.1.2. However, toolkit related communication is supported by a dedicated CAT Application service. Inter dependencies between functions in the UICC architecture and functions in the eSSP Type 1 host are out of scope of the present document. Capability exchange is done via the SCL interface through the UICC APDU service gate. SCL Core gates are not represented.

C.5 eSSP Type 1 Example with UICC support and additional APDU execution framework

C.5.1 UICC support on an legacy physical interface and additional ADPU interface over SCL

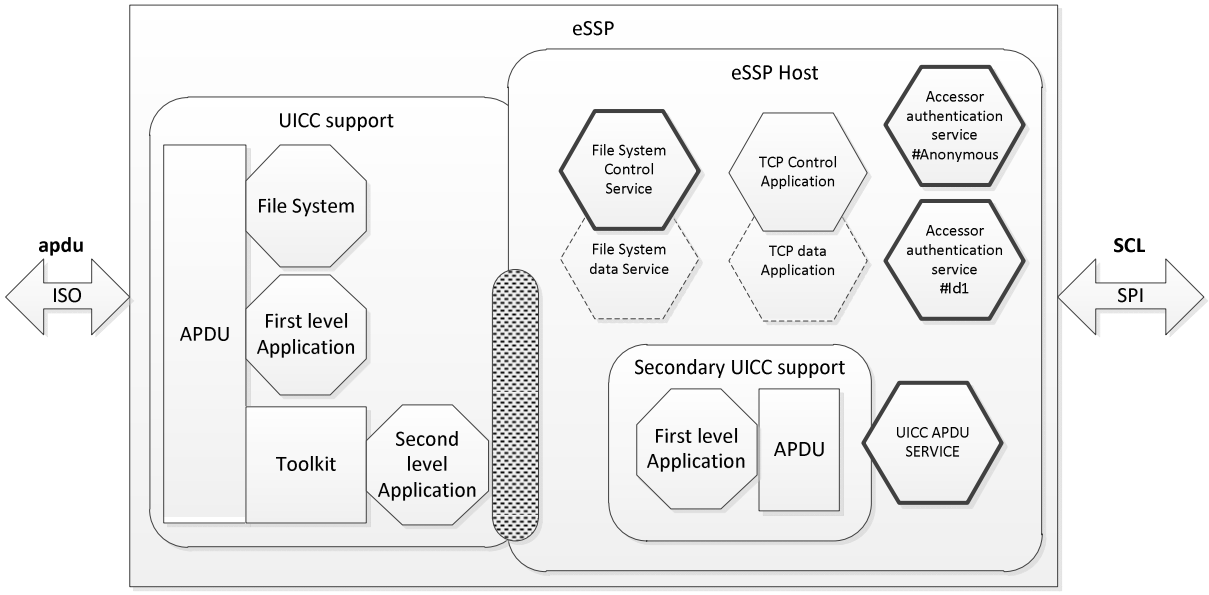

Figure C.8: eSSP Type 1 with UICC support and an additional APDU support

In this example, the eSSP Type 1 has one ISO/IEC 7816-3 [11] interface which supports APDU transport protocol to an UICC architecture. That UICC architecture may support protocols and execution framework as described in clause C.1.2.

The eSSP Type 1 has one SCL interface, which provides support for functions other SCL as described in ETSI TS 103 666-1 [1] in clause 10. In particular, this eSSP Type 1 has an UICC APDU service gate which provides an interface that supports APDU protocol communication to a secondary UICC architecture. That secondary UICC architecture need not to support protocols and execution framework as described in clause C.1.2, as these functions executions could be provided to another domain than the for primary UICC architecture.

Inter dependencies between functions in the UICC architectures and functions in the eSSP Type 1 host are out of scope of the present document. Capability exchange is done via the SCL interface through the UICC APDU service gate. SCL Core gates are not represented.

Annex D (informative): Change history

The table below indicates all changes that have been incorporated into the present document since it was placed under change control.

Change history								
Date	**Meeting**	**Plenary Doc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
	TEC#78					Creation of the specification		
	TEC#81					SCPTEC(19)000178r1		0.2.0
						Modification of the url in clause A.2		0.2.1
	TEC#84					SCPTEC(20)000028	0.2.1	0.3.0
	TEC#84					SCPTEC(20)000029r2	0.2.1	0.3.0
	TEC#84					SCPTEC(20)000032	0.2.1	0.3.0
	TEC#84					SCPTEC(20)000033r1	0.2.1	0.3.0
	TEC#84					Explicit name "eSSP Type 1" in all the document	0.2.1	0.3.0
	TEC#85					SCPTEC(20)000031r4	0.3.0	0.4.0
	TEC#85					SCPTEC(20)000075r1	0.3.0	0.4.0
	TEC#85					SCPTEC(20)000030r6	0.4.0	0.5.0
						Conversion of editor’s note in clause 6.7 to a note	0.4.0	0.5.0
						Editorial corrections for references	0.5.0	0.5.1
June 2020	SCP#93					Approval of draft specification	2.0.0	16.0.0

History

Document history		
V16.0.0	July 2020	Publication