ETSI TS 102 484 V11.2.0 (2019-04)

Smart Cards;
Secure channel between a UICC and an end-point terminal
(Release 11)

Reference
RTS/SCP-T0312vb20

Keywords
security, smart card

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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.

1 Scope

The present document specifies the technical implementation of the secure channel requirements specified in ETSI TS 102 412 [8].

The present document includes the architecture, functional capabilities and characteristics of the Secure Channel protocol and its associated interfaces transported over the UICC interface specified in ETSI TS 102 221 [1] and over the UICC USB interface specified in ETSI TS 102 600 [15].

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 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[2] IETF RFC 4346 (2006): "The Transport Layer Security (TLS) Protocol Version 1.1".

NOTE: The reference to IETF RFC 4346 is intentional, even though the RFC is obsolete.

[3] IETF RFC 4366 (2003): "Transport Layer Security (TLS) Extensions".

NOTE: The reference to IETF RFC 4366 is intentional, even though the RFC is obsolete.

[4] IETF RFC 4279 (2005): "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[5] Void.

[6] Void.

[7] ETSI TS 133 110: "Universal Mobile Telecommunications System (UMTS); LTE; Key establishment between a Universal Integrated Circuit Card (UICC) and a terminal (3GPP TS 33.110)".

[8] ETSI TS 102 412: "Smart Cards; Smart Card Platform Requirements Stage 1".

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

[10] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".

[11] IETF RFC 6234: "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)".

[12] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".

[13] FIPS PUB 180-2: "Secure Hash Standard (SHS)".

[14] ETSI TS 102 225 (V7.3.0): "Smart Cards; Secured packet structure for UICC based applications (Release 7)".

[15] ETSI TS 102 600: "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface".

[16] ISO/IEC 9797-1: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher".

[17] Void.

[18] IETF RFC 3268 (2002): "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

NOTE: The reference to IETF RFC 3268 is intentional, even though the RFC is obsolete.

[19] IETF RFC 5996: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[20] IETF RFC 4301 (2005): "Security Architecture for the Internet Protocol".

[21] IETF RFC 4307 (2005): "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)".

NOTE: The reference to IETF RFC 4307 is intentional, even though the RFC is obsolete.

[22] Void.

[23] IETF RFC 4303 (2005): "IP Encapsulating Security Payload (ESP)".

[24] ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal".

[25] IETF RFC 4835 (2007): "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

NOTE: The reference to RFC 4835 is intentional, even though the RFC is obsolete.

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

[27] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

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 following terms apply:

encrypted blob: Binary Large Object resulting from encrypting plain data

endpoint: application or platform handler on either the terminal or UICC that is capable of being an end of a secure channel

nonce: number used once

NOTE: Random value that is used only once in a cryptographic message to protect against replay attacks.

security association: set of information required for the channel endpoints to start communicating securely

3.2 Symbols

Void.

3.3 Abbreviations

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

3DES	Triple DES
AES	Advanced Encryption Standard
AH	Authentication Header
APDU	Application Protocol Data Unit
ASCII	American Standard Code for Information Interchange
ATR	Answer To Reset
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
BIP	Bearer Independent Protocol
CAT	Card Application Toolkit
CBC	Cipher Block Chaining
CL	Counter Limit
CMAC	Cipher-based Message Authentication Code
CRL	Certificate Revocation List
CSA	Connection Security Association
CSAMAC	Connection Security Association Message Authentication Code
DES	Data Encryption Standard
ESP	Encapsulating Security Payload
FFS	For Further Study
FIPS	Federal Information Processing Standard
GBA	Generic Bootstrap Architecture
HMAC	Hash Message Authentication Code
ICCID	Integrated Circuit Card Identification
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKE_SA	Internet Key Exchange - Security Association
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol security
KIC	Key and algorithm Identifier for ciphering
KID	Key and algorithm IDentifier for RC/CC/DS
MAC	Message Authentication Code
MF	Master File
MODP	MODular exPonential

MS	Master Secret
MSA	Master Security Association
OCSP	Online Certificate Status Protocol
PPS	Protocol and Parameter Selection
PSK	Pre-Shared Key
SA	Security Association
SHA	Secure Hash Algorithm
SSCMAC	Start Secure Channel Message Authentication Code
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Tag Length Value
TSCA	Terminal-Supported Ciphering Algorithms
TSIM	Terminal-Supported Integrity Mechanisms
UCA	UICC Ciphering Algorithm
UIM	UICC Integrity Mechanism
USB	Universal Serial Bus
UTF	Universal Character Set Transformation Format

4 Overview

The present document defines several types of secured data transport protocols that can be used to deliver the secure channel usecases and requirements specified in ETSI TS 102 412 [8] and the associated mechanisms that can be used to setup these protocols.

The secured data transport protocols are:

- **TLS - Application to Application:** This protocol secures IP communication between an application in the UICC and an application in the terminal or in a device connected to the terminal. Using this protocol, IP communication by other applications to the UICC may be unsecured. This protocol may be used over the APDU interface specified in ETSI TS 102 221 [1] using the BIP - UICC Server mode commands specified in ETSI TS 102 223 [9] or over the Ethernet emulation class of the USB interface specified in ETSI TS 102 600 [15]. Support for this type of secure channel shall be indicated on per application basis.

- **Secured APDU - Application to Application:** This protocol secures the APDU communication between an application in the UICC and an application in the terminal or in a device connected to the terminal. Using this protocol, APDU communication by other applications to the UICC may be unsecured. This protocol may be used over the APDU interface specified in ETSI TS 102 221 [1] or the APDU class of the USB interface specified in ETSI TS 102 600 [15]. Support for this type of secure channel shall be indicated on per application basis.

- **IPsec - USB class to USB class:** This protocol secures all IP communication between the UICC and the terminal when ETSI TS 102 483 [24] is supported over the Ethernet emulation class of the USB interface specified in ETSI TS 102 600 [15].

- **Secured APDU - Platform to Platform:** This protocol secures all APDU communication between the UICC and the terminal. This protocol may be used over the APDU interface specified in ETSI TS 102 221 [1] or the APDU class of the USB interface specified in ETSI TS 102 600 [15]. Support for this type of secure channel shall be indicated in the ATR.

- **Secured APDU - Platform to Platform CAT:** This protocol secures all CAT APDU communication between the UICC and the terminal and is reusing the Secured APDU - Platform to Platform mechanism but restricted to CAT related APDUs. This protocol may be used over the APDU interface specified in ETSI TS 102 221 [1] or the APDU class of the USB interface specified in ETSI TS 102 600 [15]. Support for this type of secure channel shall be indicated in the MF file control parameters. A terminal and a UICC claiming conformance to the present document may support this secured data transport protocol.

- **eCAT Secure Channel:** This protocol secures the eCAT communication between the UICC and an eCAT client in the terminal as specified in ETSI TS 102 223 [9]. Support for this type of secure channel shall be indicated on per application basis.

Terminals/applications in the terminal/eCAT clients and UICCs/UICC applications claiming conformance to the present document shall explicitly state which of these secured data transport protocols they support.

Secured platform to platform channels between the Terminal and a device connected to the terminal are out of scope of the present document.

To manage the security aspects of these secure channel protocols, Security Contexts are setup which contain security settings and key material. The present document defines four mechanisms to agree key material using:

- **Strong Pre-shared Keys - GBA:** Key material is agreed using the GBA procedures specified in ETSI TS 133 110 [7]. The UICC and the terminal shall support this mechanism if GBA is supported.
- **Strong Pre-shared Keys - Proprietary Pre-agreed keys:** These are keys with an entropy of at least 128 bits. The UICC and the terminal may support this mechanism. An eCAT client and the related application on the UICC using the eCAT secure channel shall support this mechanism.
- **Weak Pre-shared Keys - Proprietary Pre-agreed keys:** These are keys with an entropy of less than 128 bits (such as password based keys). The UICC and the terminal may support this mechanism.
- **Certificate exchange:** A UICC or a terminal that does not support the GBA mechanism shall support this mechanism. A UICC or a terminal that does support the GBA mechanism may support this mechanism.

5 Secure channel properties

5.0 General

This clause defines common properties for secure channels and details the secure channel lifecycle of each secure channel type defined in the present document.

A secure channel, within the present document, is characterized as having:

- an endpoint on a terminal or connected device;
- an endpoint on a UICC;
- a means of secure bidirectional communication between these endpoints;
- security policy management at each endpoint that prevents insecure communication between these two points.

5.1 Secure Channel Lifecycle

5.1.0 General

The lifecycle of each secure channel will include the following steps:

- Discovery of support for secure channels by the terminal and the UICC as detailed in the present document.
- Discover endpoints that can communicate securely on the UICC.
- Negotiate secure channel parameters.
- Create a secure channel.
- Communicate over a secure channel.
- Suspend and resume a secure channel.
- Terminate a secure channel.

5.1.1 Secure channel support discovery

Support for the mandatory procedures defined in the present document and support for the Secured APDU - Platform to Platform secure channel shall be indicated in the ATR as defined in ETSI TS 102 221 [1].

Support for the Secured APDU - Platform to Platform CAT secure channel shall be indicated in the MF file control parameters as defined in ETSI TS 102 221 [1].

A terminal shall only indicate that it supports the procedures in the present document if it is able to execute applications as a trusted platform. Definition of a trusted platform is out of scope of the present document.

5.1.2 Discovery of available endpoints

Each secure channel type defines the mechanisms by which the terminal or the UICC can dynamically discover the available endpoints on the other entity.

NOTE: By their nature, endpoints can dynamically change their availability depending on the activation state of their associated applications.

5.1.3 Negotiate secure channel parameters

5.1.3.0 General

For a secure channel to be setup, both ends of the secure channel shall agree on the parameters to be used for this channel. The present document defines these parameters as a "Security Association".

5.1.3.1 Security Associations

A Security Association has the following parameters:

- Identified and authenticated endpoints for both the terminal and the UICC.
- Cryptographic keys.
- Protection algorithms.
- Any additional parameters to be used for securing data transmissions.
- Mechanisms and parameters for identifying secure connections and managing the secure channel.

There are two types of Security Association defined in the present document:

- Master SA.
- Connection SA.

Each secure channel shall have one Master SA and at least one Connection SA.

The terminal and the UICC shall be able to securely store all of the parameters for a minimum of 4 Master SAs and 4 Connection SAs. These Security Association parameters shall not be visible or editable by any process outside of the present document.

5.1.3.2 Master SA

The main security association set up between the channel endpoints is the Master SA. This SA records the following information:

- Channel endpoints.
- Master SA identifier.
- Master SA cryptographic keys (defined as the Master Secret (MS)).