ETSI TS 102 225 V16.0.1 (2020-12)

Smart Cards;
Secured packet structure for UICC based applications
(Release 16)

Reference
RTS/SCP-T0284VG01

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

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).

It is based on work originally done in the 3GPP in TSG-terminals WG3 and ETSI SMG.

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 structure of Secured Packets for different transport and security mechanisms.

It is applicable to the exchange of secured packets between an entity in a network and an entity in the UICC.

Secured Packets contain application messages to which certain mechanisms according to ETSI TS 102 224 [1] have been applied. Application messages are commands or data exchanged between an application resident in or behind the network and on the UICC. The Sending/Receiving Entity in the network and the UICC are responsible for applying the security mechanisms to the application messages and thus turning them into Secured Packets.

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 102 224: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements".

[2] Void.

[3] ISO 16609:2012: "Financial services - Requirements for message authentication using symmetric techniques".

[4] Void.

[5] ETSI TS 131 115: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (3GPP TS 31.115)".

[6] GlobalPlatform: "GlobalPlatform Technology Card Specification", Version 2.3.1.

NOTE: Available at https://globalplatform.org/specs-library/.

[7] Applied Cryptography: "Protocols, Algorithms, and Source Code in C", 2nd Edition, Bruce Schneier, John Wiley & Sons.

[8] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

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

[10] ETSI TS 102 127: "Smart Cards; Transport protocol for CAT applications; Stage 2".

[11] ISO/IEC 13239:2002: "Information technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures".

[12] NIST Special Publication FIPS-197 (2001): "Advanced Encryption Standard (AES)".

NOTE: Available at http://csrc.nist.gov/publications/fips/index.html.

[13] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation - Methods and Techniques".

NOTE: Available at http://csrc.nist.gov/publications/nistpubs/.

[14] NIST Special Publication 800-38B (2005): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

NOTE: Available at http://csrc.nist.gov/publications/nistpubs/.

[15] GlobalPlatform: "GlobalPlatform Card UICC Configuration", Version 1.2.0.

[16] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

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

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

[19] GlobalPlatform: "Remote Application Management over HTTP, Card Specification v2.2 - Amendment B", Version 1.1.3.

NOTE: Available at https://globalplatform.org/specs-library/.

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] ETSI TR 102 216: "Smart Cards; Vocabulary for Smart Card Platform specifications".

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.1] and the following apply:

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI TR 102 216 [i.1].

Advanced Encryption Standard (AES): standard cryptographic algorithm specified in FIPS-197 [12]

application layer: layer above the Transport Layer on which the Application Messages are exchanged between the sending and receiving applications

application message: package of commands or data sent from the Sending Application to the Receiving Application, or vice versa, independently of the transport mechanism

NOTE: An Application Message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more secured packets.

card manager: generic term for the 3 card management entities of a GlobalPlatform card i.e. the OPEN, Issuer Security Domain and the Cardholder Verification Method Services provider as defined in the GlobalPlatform Card Specification [6]

command header: security header of a command packet

NOTE: It includes all fields except the Secured Data.

command packet: secured packet transmitted by the Sending Entity to the Receiving Entity, containing a secured Application Message

counter: mechanism or data field used for keeping track of a message sequence

NOTE: This could be realized as a sequence oriented or time stamp derived value, maintaining a level of synchronization between the Sending Entity and the Receiving Entity.

cryptographic checksum: string of bits derived from some secret information, (e.g. a secret key), part or all of the Application Message, and possible further information (e.g. part of the Security Header)

NOTE: The secret key is known to the Sending Entity and to the Receiving Entity. The Cryptographic Checksum is often referred to as Message Authentication Code.

Data Encryption Key (DEK): key identifier for ciphering keys as defined in ETSI TS 102 226 [9]

Data Encryption Standard (DES): standard cryptographic algorithm specified as DEA in ISO 16609 [3]

digital signature: string of bits derived from some secret information, (e.g. a secret key), the complete Application Message, and possible further information (e.g. part of the Security Header)

NOTE: The secret information is known only to the Sending Entity. Although the authenticity of the Digital Signature can be proved by the Receiving Entity, the Receiving Entity is not able to reproduce the Digital Signature without knowledge of the secret information owned by the Sending Entity.

issuer security domain: on-card entity providing support for the control, security, and communication requirements of the Card Issuer as defined in the GlobalPlatform Card Specification [6]

receiving application: entity to which the Application Message is destined

receiving entity: entity where the Secured Packet is received (e.g. SMS-SC, UICC, USSD entry point, or dedicated Toolkit Server) and where the security mechanisms are utilized

NOTE: The Receiving Entity processes the Secured Packets.

redundancy check: string of bits derived from the Application Message and possible further information for the purpose of detecting accidental changes to the message, without the use of any secret information

response header: security header of a response packet

response packet: secured packet transmitted by the Receiving Entity to the Sending Entity, containing a secured response and possibly application data

secured data: this field contains the secured application message and possibly padding octets

secured packet: information flow on top of which the level of required security has been applied

NOTE: An Application Message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more Secured Packets.

security domain: As defined in the GlobalPlatform Card Specification [6].

security header: that part of the secured packet which consists of all security information (e.g. counter, key identification, indication of security level, checksum or Digital Signature)

sender identification: simple verification of the identity of the Sending Entity by the Receiving Entity comparing the sender identity with an a priori stored identity of the sender at the Receiving Entity

sending application: entity generating an Application Message to be sent

sending entity: entity from which the Secured Packet originates (e.g. SMS-SC, UICC, USSD entry point, or dedicated Toolkit Server) and where the security mechanisms are invoked

NOTE: The Sending Entity generates the Secured Packets to be sent.

status code: indication that a message has been received (correctly or incorrectly, indicating reason for failure)

transport layer: layer responsible for transporting Secured Packets through the network

NOTE: The transport layer implements one or more transport mechanisms, (e.g. SMS or USSD).

unsecured acknowledgement: status code included in a response message

3.2 Symbols

Void.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
AID	Application IDentifier
API	Application Programming Interface
ARD	Additional Response Data
BER	Basic Encoding Rules
BIP	Bearer Independent Protocol
CAT_TP	Card Application Toolkit Transport Protocol
CBC	Cipher Block Chaining
CC	Cryptographic Checksum
CHI	Command Header Identifier
CHL	Command Header Length
CMAC	Cipher-based Message Authentication Code
CNTR	CouNTeR
CPI	Command Packet Identifier
CPL	Command Packet Length
CRC	Cyclic Redundancy Check
DEA	Data Encryption Algorithm
DEK	Data Encryption Key
DES	Data Encryption Standard
DS	Digital Signature
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
ISO	International Organization for Standardization
KIc	Key and algorithm Identifier for ciphering
KID	Key and algorithm IDentifier for RC/CC/DS
NIST	National Institute of Standards and Technology
PCNTR	Padding CouNTeR
PoR	Proof of Receipt
RAM	Remote Application Management
RC	Redundancy Check
RE	Receiving Entity
RFM	Remote File Management

RHI	Response Header Identifier
RHL	Response Header Length
RPI	Response Packet Identifier
RPL	Response Packet Length
RSC	Response Status Code
SE	Sending Entity
SMG	Special Mobile Group
SMS	Short Message Service
SMS-CB	Short Message Service - Cell Broadcast
SMS-SC	Short Message Service - Service Centre
SP	Special Publication
SPI	Security Parameters Indication
TAR	Toolkit Application Reference
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Tag/Length/Value (data structure)
USSD	Unstructured Supplementary Services Data

4 Overview of security system

4.0 Overview

An overview of the secure communication related to the Card Application Toolkit together with the required security mechanisms is given in ETSI TS 102 224 [1] (see figure 1). Standardized applications for remote management of the UICC, which make use of the secure communication defined in the present document, are specified in ETSI TS 102 226 [9].

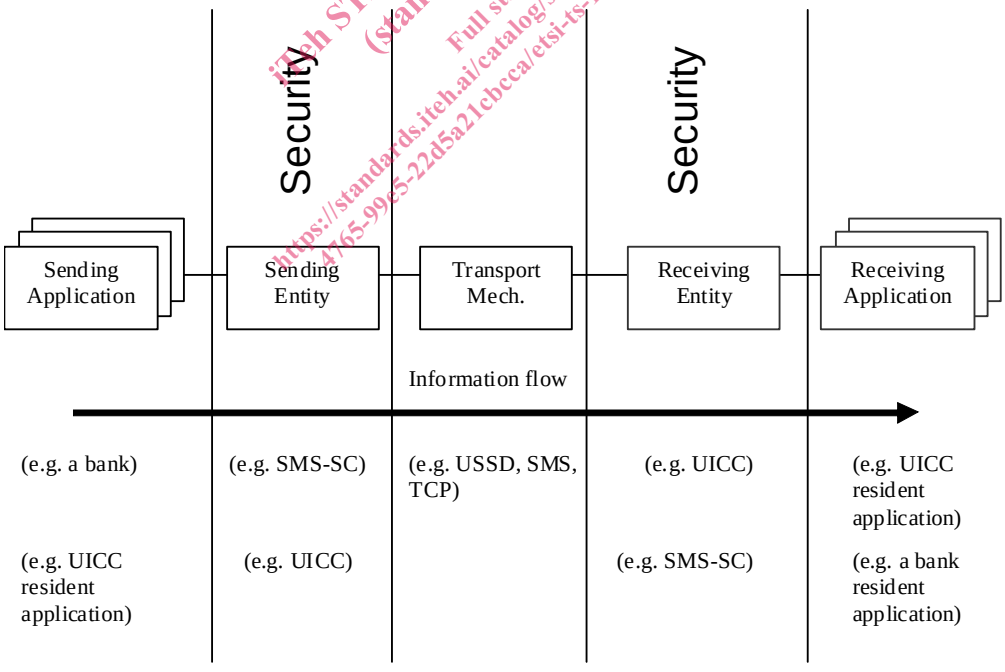

Figure 1: System overview

4.1 Protocol for generalized secured packets

This clause applies if messages are protected using an implementation of the generalized secured packet format.

The Sending Application prepares an Application Message and forwards it to the Sending Entity, with an indication of the security to be applied to the message.

The Sending Entity prepends a Security Header (the Command Header) to the Application Message. It then applies the requested security to part of the Command Header and all of the Application Message, including any padding octets. The resulting structure is here referred to as the (Secured) Command Packet.

Under normal circumstances the Receiving Entity receives the Command Packet and unpacks it according to the security parameters indicated in the Command Header. Additional security conditions may apply (e.g. a Minimum Security Level as defined in ETSI TS 102 226 [9]) before unpacking it. The Receiving Entity subsequently forwards the Application Message to the Receiving Application indicating to the Receiving Application the security that was applied. The interface between the Sending Application and Sending Entity and the interface between the Receiving Entity and Receiving Application are proprietary and therefore outside the scope of the present document.

If so indicated in the Command Header, the Receiving Entity shall create a (Secured) Response Packet. The Response Packet consists of a Security Header (the Response Header) and optionally, application specific data supplied by the Receiving Application. Both the Response Header and the application specific data are secured using the security mechanisms indicated in the received Command Packet. The Response Packet will be returned to the Sending Entity, subject to constraints in the transport layer (e.g. timing).

Although in some cases there might be no direct acknowledgement mechanism (i.e. for SMS-CB) the Sending Application may have requested a response. In this case a (Secured) Response Packet could be sent using a different bearer by the Receiving Application.

In some circumstances a security related error may be detected at the Receiving Entity. In such circumstances the Receiving Entity shall react according to the following rules:

1) nothing shall be forwarded to the Receiving Application, i.e. no part of the Application Message, and no indication of the error;

2) if the Sending Entity does not request a response (in the Command Header) the Receiving Entity discards the Command Packet and no further action is taken;

3) if the Sending Entity requests a response and the Receiving Entity can authenticate the Sending Entity, the Receiving Entity shall create a Response Packet indicating the error cause. This Response Packet shall be secured according to the security indicated in the received Command Packet;

4) if the Sending Entity requests a response and the Receiving Entity cannot authenticate the Sending Entity, the Receiving Entity shall:

   - either send a Response Packet indicating the error cause without any security being applied to the Response Packet and the Counter (CNTR) field set to zero; or

   - not send any Response Packet and discard the Command Packet with no further action being taken;

NOTE: The option to be adopted may depend on the bearer and the security policy of the UICC issuer.

5) if the Receiving Entity receives an unrecognizable Command Header (e.g. an inconsistency in the Command Header), the Command Packet shall be discarded and no further action taken.

4.2 Protocol for secured messages based on HTTPS

The security for data exchange over TCP is provided by TLS. The HTTP protocol is used on top of TLS to provide encapsulation of the data and information about the receiving entity.

The processing rules for messages that are protected using HTTPS are specified in Amendment B of the Global Platform Card Specification v2.2 [19].

TCP/IP transport is provided by the Bearer Independent Protocol of ETSI TS 102 223 [18] or a direct IP connection as specified in ETSI TS 102 483 [17].

If a TLS connection with the receiving entity is not already established, the sending entity shall send a triggering message as specified in Amendment B of the Global Platform Card Specification v2.2 [19] to the security domain handling the TLS connection for itself or for an associated application.