ETSI TS 102 224 V8.0.0 (2008-10)

Technical Specification

Smart Cards;
Security mechanisms for UICC based Applications - Functional requirements
(Release 8)

Reference
RTS/SCP-R0282v800

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://webapp.etsi.org/IPR/home.asp).

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.

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.

1 Scope

The present document provides standardized security mechanisms in conjunction with the Card Application Toolkit for the interface between a Network Entity and a UICC.

The security mechanisms which are specified are independent of applications.

The present document describes the functional requirements of the security mechanisms with the implementation detail of these mechanisms being described in TS 102 225 [2].

Within the scope of the present document, the UICC refers here to an ICC which support at least one application in order to access a cellular network.

The ICC is considered as a platform, which is based on TS 102 221 [5].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- 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.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

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

[3] ETSI TS 131 111: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Universal Subscriber Identity Module Application Toolkit (USAT) (3GPP TS 31.111)".

[4] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

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

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

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

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

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

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

For the purpose of the present document, the following terms and definitions apply:

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.

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.

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 (MAC).

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.

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

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 header: that part of the secured packet which consists of all security information

EXAMPLE: 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 Abbreviations

For the purposes of the present document the abbreviations given in TR 121 905 [1] and the following apply:

CAT	Card Application Toolkit
CAT_TP	Card Application Toolkit Transport Protocol

4 Introduction

The Card Application Toolkit (CAT) as described in TS 102 223 [6] is a set of applications and related procedures that may be used during a card session. It allows operators to create specific applications resident on the UICC. There exists a need to secure Card Application Toolkit (CAT) related communication over the network, (e.g. SMS, USSD, and future transport mechanisms) with the level of security chosen by the network operator or the application provider.

It is assumed in the present document that the sending and receiving entities are in a secure environment.

The appropriate security mechanisms are described in the present document.

The security mechanisms cover the following security requirements:

- unilateral authentication from network to UICC;
- unilateral authentication from UICC to network;
- message integrity;
- replay detection;
- proof of receipt;
- message confidentiality.

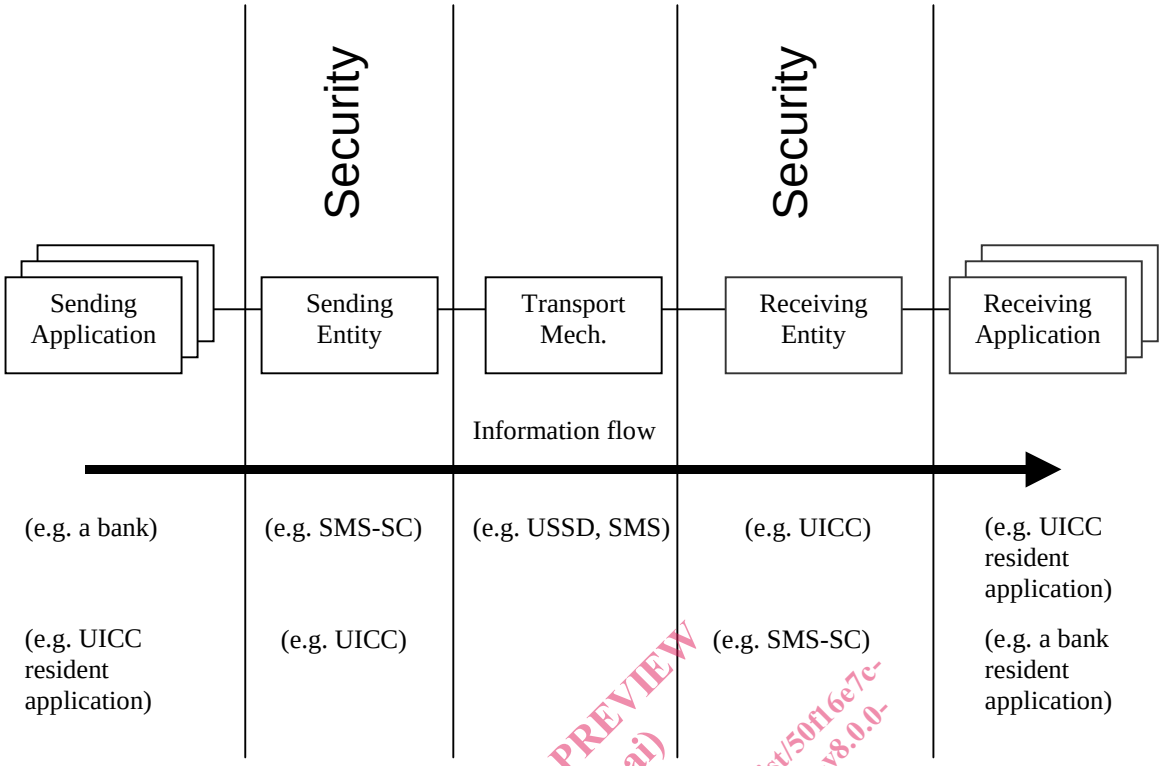

Figure 1: System overview

5 Security requirements

The application message is transferred from the sending application to the receiving application in one or more secured packets via a sending entity and a receiving entity, or group of receiving entities. The receiving entity is then responsible for reconstructing the application message from the received secured packets for presentation to the target receiving application. It is possible that there are several receiving entities and applications.

The sending application shall indicate to the sending entity the security mechanisms to be applied to the application message. This shall be indicated in the secured packet. The receiving entity shall indicate to the receiving application the security mechanisms applied to the secured packet, in a secure manner. The interface between the sending application and the sending entity, and the interface between the receiving entity and receiving application are not defined.

The security requirements to satisfy when transferring application messages from the sending entity to the receiving entity that have been considered are:

- authentication;
- message integrity;
- replay detection and sequence integrity;
- proof of receipt and proof of execution;
- message confidentiality;
- indication of the security mechanisms used.

Mechanisms to satisfy the above requirements will be governed by the following assumptions:

- in general, security is provided for each secured packet transmitted (an application message may be broken into several secured packets, each of which shall have identical security mechanisms applied to it);