3GPP TS 22.048 V5.0.0 (2003-06)

3rd Generation Partnership Project;
Technical Specification Group Terminals;
Security mechanisms for the (U)SIM Application Toolkit;
Stage 1
(Release 5)

Keywords
GSM, UMTS, SIM, USIM, SMS, card, security

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

3GPP

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG 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 standardised security mechanisms in conjunction with the SIM Application Toolkit for the interface between a 3G or GSM PLMN 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 the stage 2 specification (TS 23.048).

The present document is the result of a feasibility study carried out on this topic, contained in GSM 11.15.

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

The ICC is considered as a platform, which is either based on TS 31.101 [13], here called "3G platform", or TS 51.011 [23], here called "2G platform".

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

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

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1]   3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2]   3GPP TS 23.048: "Security Mechanisms for the (U)SIM Application Toolkit - Stage 2".

[3]   3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[4]   ETR 330: "STAG; A guide to the legislative and regulatory environment".

[5]   3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics"

[6]   3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface"

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. 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. This could be realised as a sequence oriented or time stamp derived value maintaining a level of synchronisation.

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). 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.

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). 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: this is the entity to which the Application Message is destined.

Receiving Entity: this is the entity where the Secured Packet is received (e.g. SMS-SC, UICC, USSD entry point, or dedicated (U)SIM Toolkit Server) and where the security mechanisms are utilised. 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. 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 (e.g. counter, key identification, indication of security level, checksum or Digital Signature).

Sender Identification: this is the simple verification of the identity of the Sending Entity by the Receiving Entity comparing the sender identity with an apriori stored identity of the sender at the Receiving Entity.

Sending Application: entity generating an Application Message to be sent.

Sending Entity: this is the entity from which the Secured Packet originates (e.g. SMS-SC, UICC, USSD entry point, or dedicated (U)SIM Toolkit Server) and where the security mechanisms are invoked. The Sending Entity generates the Secured Packets to be sent.

Status Code: this is an indication that a message has been received (correctly or incorrectly, indicating reason for failure).

Transport Layer: this is the layer responsible for transporting Secured Packets through the 3G and/or GSM network. The transport layer implements one or more transport mechanisms, (e.g. SMS or USSD).

Unsecured Acknowledgement: this is a Status Code included in a response message.

3.2 Abbreviations

Abbreviations used in the present document are listed in TR 21.905 [1].

4 Introduction

The USIM Application Toolkit as described in TS 31.111 [3] is a set of commands and procedures for use during the network operation phase of 3G and GSM. It allows operators to create specific applications resident on the UICC. There exists a need to secure USIM Application Toolkit related communication over the 3G and GSM 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.
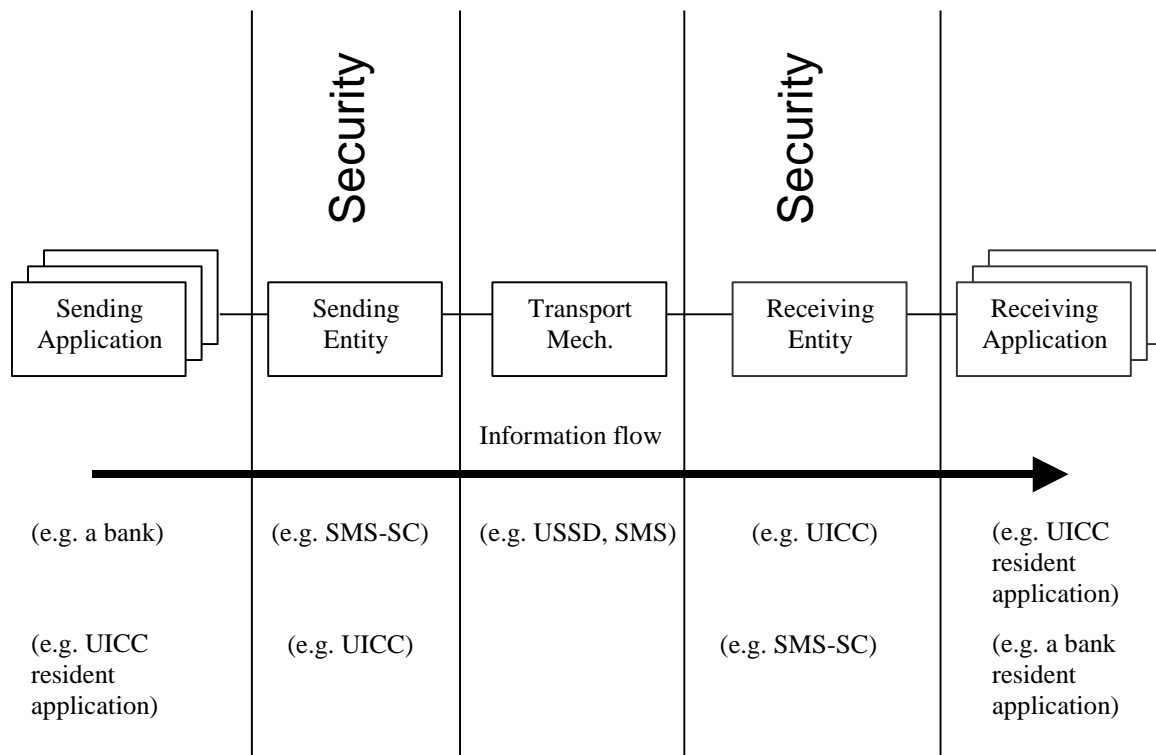
Figure 1: System overview

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;

- there should be the ability to turn mechanisms on and off on a per Application Message basis, with an indication of the status transmitted with the message;

- security related information used should be independent of that used with existing 3G or GSM network keys;

- third party applications may have access to the Sending Entity, however this is considered to be an internal network security issue and therefore outside of the scope of the present document.

5.1 Authentication

5.1.1 Definition

Authentication is the verification of an entity's claimed identity by another entity. A first level of authentication is "unilateral authentication" which provides the receiver with proof of the sender's identity. A higher level is "mutual authentication", where both entities are provided with proof of each other's identity.

For mutual authentication purposes the Sending and/or Receiving Entities have to generate and exchange dedicated authentication messages. Due to the unidirectional nature of current transport mechanisms mutual authentication is not considered in the present document.

5.1.2 Purpose

The purpose of authentication is to protect Sending and Receiving Entities and Applications against unauthorised use. Authentication assures that only authorised parties can perform actions at the UICC, and it prevents unauthorised parties from having access to entities on the network side (or even behind it) via a (U)SIM Application Toolkit feature.

5.1.3 Functional requirements

For the purposes of Sender Identification and unilateral authentication the Sending Entity shall be uniquely defined and addressed, as an example a GSM SIM already satisfies this requirement.

Unilateral authentication can be achieved by the use of a Cryptographic Checksum or Digital Signature attached to the message. The distinguishing identifications of the Receiving and Sending Entities should be linked to them for the entire life time of these entities. (If for some reason, the identity of any of the entities is changed, then all other entities involved in the authentication procedure shall be informed of the new identity.)

5.2 Message integrity

5.2.1 Definition

Message Integrity ensures that no corruption, accidental or intentional, of the content of the message has occurred.

5.2.2 Purpose

The purpose of this mechanism is to detect any corruption of the Application Message or the whole Secured Packet.

5.2.3 Functional requirements

The integrity of the Application Message or whole Secured Packet may be achieved as follows:

- by adding a Redundancy Check in the Security Header to protect against accidental corruption (The Redundancy Check mechanism on it's own only protects against accidental corruption. In conjunction with encryption it can be used to provide message integrity);

- by adding a Cryptographic Checksum in the Security Header. In certain circumstances the authentication of the Sending Entity is achieved implicitly by the verification of the Cryptographic Checksum;

- by calculating and verifying a Digital Signature on the Application Message to be transferred. In this case the authentication of the Sending Entity is achieved implicitly by the verification of the Digital Signature.

5.3 Replay detection and sequence integrity

5.3.1 Definition

Replay detection is a mechanism which provides the Receiving Entity with a means of recognising that it has received the same Secured Packet(s) previously.

Sequence integrity is a mechanism which ensures that no changes, accidental or intentional, have occurred to the intended sequence of Secured Packets.

5.3.2 Purpose

Replay detection protects the Receiving Entity against replay attack and Secured Packet duplication.

Sequence integrity protects the Receiving Entity against message suppression and loss of Secured Packets.

5.3.3 Functional requirements

The implementation of these mechanisms shall be achieved by including a counter in the Security Header. The protection of the counter shall be achieved by including it in the calculation of the checksum (Cryptographic Checksum or encrypted Redundancy Check) or Digital Signature when used.

The Sending Entity and the Receiving Entity shall maintain synchronisation for their counters.

5.4 Proof of receipt and proof of execution

5.4.1 Definition

Proof of receipt proves to the Sending Entity that the Receiving Entity has correctly received a Secured Packet, has performed the necessary security checks and forwarded the contents to the Receiving Application.

Proof of execution proves to the Sending Application that the Receiving Application has performed an action that the Sending Application initiated. Proof of execution is not applicable at the Transport Layer.

5.4.2 Purpose

The purpose of proof of receipt is to prove delivery of a Secured Packet to the Receiving Entity in an unambiguous way. This allows detection of non-delivery due to network error, message corruption, validation failure etc. to be indicated to the Sending Entity using a Status Code in the proof of receipt response.

5.4.3 Functional requirements

Proof of receipt must be requested by the Sending Entity. Proof of receipt is returned from the Receiving Entity in an acknowledgement to a Secured Packet transmitted by the Sending Entity. The acknowledgement shall take the form of a Status Code in a response message, which may be secured by either a Cryptographic Checksum or Digital Signature.

The Sending Entity shall send an indication of proof of receipt to the Sending Application upon successful delivery of the Application Message, or indicate the reason for failure upon unsuccessful delivery of the Application Message. The behaviour at the Receiving Entity is elaborated in the stage 2 document [2].

The Sending and Receiving Entity shall be uniquely defined and addressed.

In the case of SMS transport, proof of receipt could be carried in the short message acknowledgement as defined in TS 31.111 [3] (SMS data download mechanism).

The case of other transport mechanisms is for further study.

5.5 Message confidentiality

5.5.1 Definition

Message confidentiality ensures that the messages exchanged are not made available or disclosed to unauthorised individuals, entities, or processes.

5.5.2 Purpose

This security function prevents any external party from extracting any useable information from Secured Packets.

5.5.3 Functional requirements

Message confidentiality is achieved by encrypting the message. In order for the recipient to use the content of the message it has to be decrypted.

Some of the security parameters that make up the Security Header (Digital Signatures, Counters and other security parameters) may be encrypted.

NOTE: There may be legal constraints for the implementation of message confidentiality mechanisms entirely resident on the UICC, see ETSI Technical Report (ETR) 330 [4]

5.6 Security management

The security mechanism applied to the Secured Packet shall be indicated in the Security Header, and this indication may be integrity protected to prevent it from malicious alteration.

Security parameters (e.g. counters, keys) at the Receiving and Sending Entity shall be stored in a secure manner such that no unauthorised parties or applications can read, modify or use these parameters.

Procedures for key management (e. g. key update) should be foreseen for transport level.

6 Normal procedures

6.1 Security mechanisms

From the security requirements described in clause 5, the following subclauses define security mechanisms on the Transport Layer. Some of the security mechanisms fulfil more than one security requirement.

6.1.1 Authentication mechanisms

Mechanisms ensuring authentication are:

- Cryptographic Checksum (b1);

- Digital Signature (b2).

The Cryptographic Checksum mechanism is suitable for authentication when the secret information is shared only by the communicating entities.

6.1.2 Message integrity mechanisms

Mechanisms ensuring message integrity are:

- Redundancy Check;

- Cryptographic Checksum (b1);

- Digital Signature (b2).

The Redundancy Check mechanism on it's own only protects against accidental corruption. In conjunction with encryption it can be used to provide message integrity.

6.1.3 Replay detection and sequence integrity mechanisms

Mechanisms ensuring replay detection and sequence integrity are:

- Simple Counter;

- A counter included in the calculation of the Cryptographic Checksum (d1);

- A counter included in the calculation of the Digital Signature (d2).

The Simple Counter mechanism protects against accidental loss or replay. In conjunction with encryption it can be used to protect against malicious loss or replay. There shall exist a specific counter value which indicates that the replay detection and sequence integrity mechanisms are inactive.

6.1.4 Proof of receipt mechanisms

NOTE: The proof of receipt mechanisms may frequently be used in conjunction with replay detection and sequence integrity.

Mechanisms ensuring proof of receipt are:

- unsecured acknowledgement;

- acknowledgement included in the calculation of the Cryptographic Checksum (f1);

- acknowledgement included in the calculation of the Digital Signature (f2).

6.1.5   Message confidentiality mechanisms

- Encryption mechanism (g).

6.2   Security mechanisms and recommended combinations

6.2.1   Non-cryptographic mechanisms

In the following a number of mechanisms are listed which are based on non-cryptographic mechanisms. These mechanisms offer no security against any deliberate attack, only detection of accidental corruption.

- Redundancy Check;

- Unsecured Acknowledgement;

- Simple Counter.

6.2.2   Cryptographic mechanisms

The Security Header, except the Cryptographic Checksum/Digital Signature, shall always be included in the calculation of the Cryptographic Checksum/Digital Signature.

- Cryptographic Checksum (d1) or Digital Signature (d2);

   This security mechanism addresses the following security requirements: authentication, message integrity, replay detection and sequence integrity.

- Acknowledgement as Cryptographic Checksum (f1) or Digital Signature (f2);

   This security mechanism satisfies the security requirement proof of receipt.

- Encryption of the Application Data and possibly part of the Security Header (g);

   The encryption of the Application Data and possibly part of the Security Header corresponds to the requirement of message confidentiality.

Table 1: Overview of cryptographic mechanisms

Requirements	Mechanisms		
	Cryptographic Checksum	**Digital Signature**	**Encryption**
authentication	(b1)	(b2)	
message integrity	(b1)	(b2)	
replay detection and sequence integrity	(d1)	(d2)	
proof of receipt	(f1)	(f2)	
confidentiality			(g)

6.2.3 Recommended combinations of cryptographic mechanisms

Whilst it is recognised that many combinations of the above described security mechanisms are possible and feasible, for the purpose of the present document, in order to limit the complexity of implementation, a limited number of combinations is recommended.

- combinations employing Cryptographic Checksum:

  combination 1: d1

  combination 2: d1 + f1

  combination 3: d1 + f1 + g

  combination 4: d1 + g

- combinations employing Digital Signature:

  combination 5: d2

  combination 6: d2 + f2

  combination 7: d2 + f2 + g

  combination 8: d2 + g

It is recommended that encryption is employed only in conjunction with either a Redundancy Check, Cryptographic Checksum or Digital Signature in order to allow verification of the decryption.

If only authentication and message integrity are required this is indicated by a special counter value as described in subclause 6.1.3.

7 Exceptional procedures

7.1 Authentication or integrity failure

In the case of authentication or integrity failure, the received message shall be discarded. If proof of receipt has been requested, then a Status Code indicating the reason for failure shall be returned to the Sending Entity.

7.2 Sequence and replay detection failure

There are several mechanisms whereby counter value synchronisation can be maintained, or regained if synchronisation is lost If synchronisation cannot be regained, the Receiving Entity shall discard any Secured Packet with an unsynchronised counter value. In addition, if proof of receipt has been requested, then a Status Code indicating the reason for failure shall be returned to the Sending Entity.

7.3 Proof of receipt failure

The Sending Entity shall inform the Sending Application of the failure to deliver the Application Message, indicating the reason for failure.

Annex A (informative):
Change History

This annex lists all changes made to the present document since its initial approval.

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2001-06	TP-12	TP-010103	001		Alignment with 3G release-4 specifications *NOTE: This CR converts the terminology in TS 02.48 v8.0.0 to apply to both GSM and 3G. With this change, the specification number changes from TS 02.48 to TS 23.048.*		4.0.0
2003-06	TP-20				The specification was upgraded to Rel-5 with no CR in order to have a complete set of Rel-5 specifications. The contents is equal to the Rel-4 version 4.0.0.	4.0.0	5.0.0