3GPP TSG-T (Terminals) Meeting #12
Stockholm, Sweden, 13 - 15 June 2001

Tdoc TP-010103

Source: T3

Title: Change Request to TS 02.48 "Security Mechanisms for the SIM application toolkit - Stage 1"

Document for: Approval

This document contains change requests to GSM 02.48 as agreed by T3. The change request will result in the creation TS 22.048 v4.0.0.

T3 Doc	Spec	CR	Rv	Rel	Subject
T3-010433	02.48	A001		rel-4	Alignment with 3G release-4 core specifications

3GPP TSG-T3 (USIM) Meeting #19
St John, USA, 8-11 May 2001

Tdoc T3-0104xx
(Technical content of this document is identical to T3-010433)

CR-Form-v4

CHANGE REQUEST

⌘ **02.48** **CR** **A001** ⌘ ev **-** ⌘ Current version: **8.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Alignment with 3G release-4 core specifications
Source:	⌘	T3
Work item code:	⌘	TEI4
Date:	⌘	11 May, 2001
Category:	⌘	**F**
Release:	⌘	REL-4

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	To create a release 4 version of 02.48 that covers both 2G and 3G.
Summary of change:	⌘	Terminology is changed to refer to both 2G and 3G
Consequences if not approved:	⌘	Two separate specifications for 2G and 3G instead of a combined one. This will lead to an increased risk of divergence between 2G and 3G.

Clauses affected:	⌘	
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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~~SIM~~.

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 (~~GSM~~ TS~~0~~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. ~~This application is called here Network Access Application (NAA).~~

The ICC is considered as a platform, which is either based on TS 31.101 [13], here called "3G platform", or GSM 11.11 [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] ~~GSM 01.04 (ETR 350): "Digital cellular telecommunications system; Abbreviations and acronyms".~~3GPP TR 21.905: "Vocabulary for 3GPP Specifications (Release 1999)".

[2] ~~GSM 03.48 (TS 101 181)~~3GPP TS 43.048~~: "Digital cellular telecommunications system (Phase 2+)~~; Security Mechanisms for the (U)SIM Application Toolkit - Stage 2".

[3] ~~GSM 11.14 (GTS 11.14)~~ 3GPP TS 31.111: "~~Digital cellular telecommunications system (Phase 2+); Specification of Subscriber Identity Module - Mobile Equipment (SIM - ME) Interface for~~ USIM Application Toolkit (USAT)".

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

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, ~~SIM~~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, ~~SIM~~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

~~In addition to those below,~~ A~~a~~bbreviations used in the present document are listed in ~~GSM 01.04.~~ 3GPP TR 21.905 [1].

~~SIM Subscriber Identity Module~~
~~SMS Short Message Service~~
~~SMS-SC Short Message Service - Service Centre~~
~~UICC Universal Integrated Circuit Card~~

~~USIM Universal Subscriber Identity Module~~
~~USSD Unstructured Supplementary Service Data~~

4 Introduction

The USIM Application Toolkit as described in ~~GSM 11.14~~ 3GPP 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~~SIM (Subscriber Identity Module)~~. 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~~SIM~~;
- unilateral authentication from UICC~~SIM~~ to network;
- message integrity;
- replay detection;
- proof of receipt;
- message confidentiality.

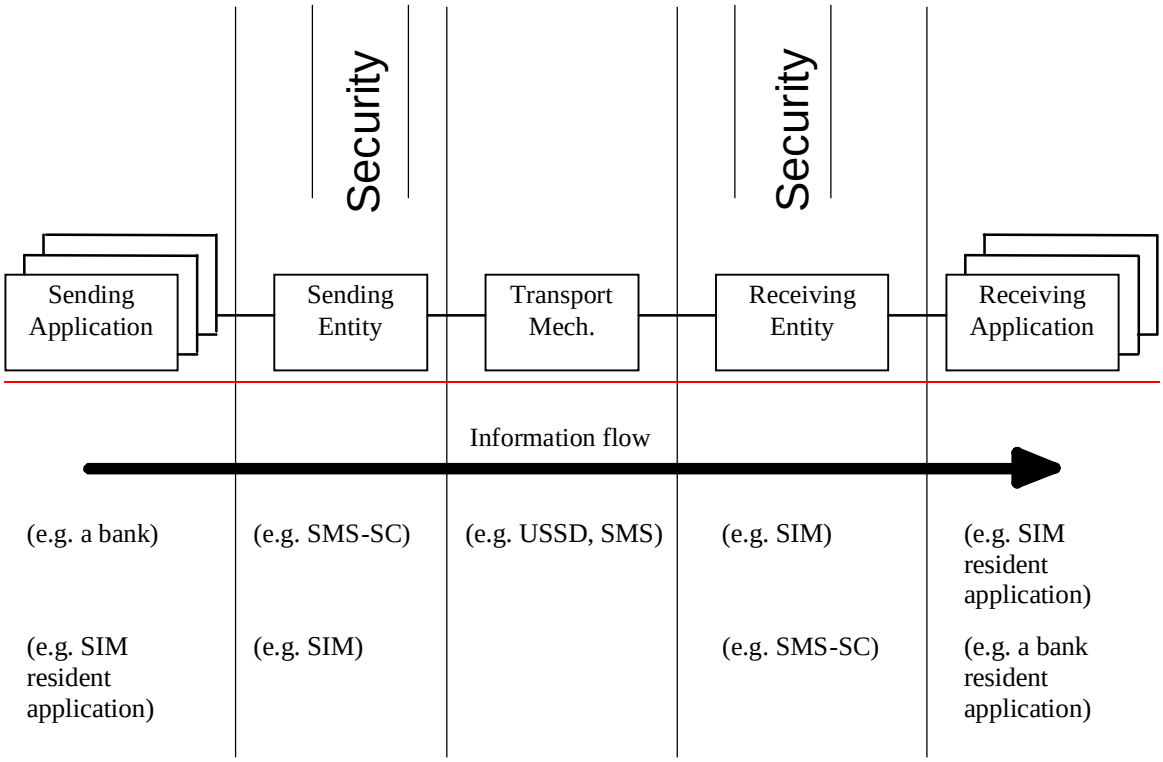

Diagram above to be deleted and replaced with diagram below

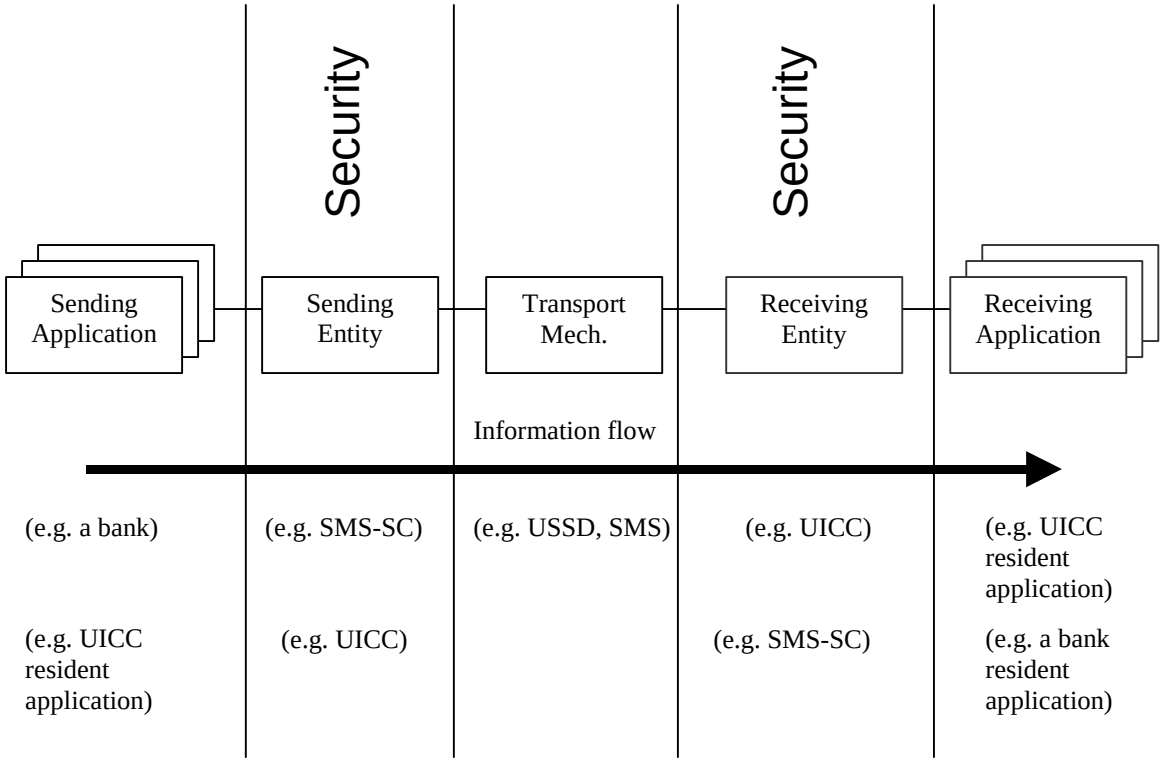

Figure 1: System overview

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~~SIM~~, 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 ~~GSM 11.14~~ 3GPP 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 ~~SIM~~UICC, see ETSI Technical Report (ETR) 330 [4].