Technical Specification Group Terminals ***Tdoc TP-000017***
Meeting #7, Madrid, Spain, 13-15 March 2000

Source: T3

Title: Change Requests to TS 21.111 "USIM and IC card requirements"

Agenda item: 5.3.3

Document for: Approval

This document contains one change request to TS 21.111 v3.0.1 agreed by T3.

T3 Doc	Spec	CR	Rv	Cat	Rel	Subject
T3-000095	21.111	002		F	R99	Alignment with 33.102 regarding the data integrity of signalling elements and user identity confidentiality

3GPP TSG-T3 #13
Tokyo, Japan, 21.-24. 2. 2000

Document T3-000095
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

21.111	CR	002	Current Version:	3.0.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T #7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: T3 **Date:** 22.02.00

Subject: Alignment with 33.102, alignment with terminology

Work item:

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: 1. The location of the UIA (3GPP integrity algorithm) and was changed in 33.102 (security architecture) and alignment is required. 2. The user identity is called IMSI (not IMUI).

Clauses affected: 5.5, 5.6

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

[7] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[8] GSM 11.12 (ETS 300 641): "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] GSM 11.18: "Digital cellular telecommunications system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[11] 3G TS 33.102: "3G security: Security Architecture".

2.2 Informative references

[20] GSM 02.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 1".

[21] GSM 03.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

UICC: A removable IC card containing a USIM.

USIM: A 3GPP application on an IC card.

3.2 Symbols

Vpp Programming voltage

3.3 Abbreviations

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

ADN	Abbreviated Dialling Number
ATR	Answer To Reset
DF	Dedicated File
EF	Elementary File
FFS	For Further Study
ICC	Integrated Circuit Card
IK	Integrity Key
~~IMUI~~	~~International Mobile User Identity~~
IMSI	International Mobile Subscriber Identity
ME	Mobile Equipment
MF	Master File
PIN	Personal Identification Number
PPS	Protocol and Parameter Selection
SIM	Subscriber Identity Module
UIA	3GPP Integrity Algorithm
USIM	Universal Subscriber Identity Module

5 Security Requirements

...

5.3 User data stored in ME

Subject to the exception below, all user related information transferred into the ME during network operations shall be deleted from the ME after removal of the UICC, deselection of the USIM, deactivation of the ME, or following an electrical reset of the UICC. [This includes any data that was transferred to the ME by SIM Application Toolkit commands. FFS]

User related security codes such as PIN and Unblock PIN may only be stored by the ME during the procedures involving such a code and shall be discarded by the ME immediately after completion of the procedure.

Optionally, an ME may retain some less security-critical data at UICC removal, USIM deselection or ME switch-off. Such data are SMS, ADN/SSC, FDN/SSC, LND. These data, when stored in the ME, shall only be readable/retrievable if the same USIM is reactivated (as determined by the ~~IMUI~~IMSI). If the ~~IMUI~~IMSI is retained in the ME for this purpose, it shall be stored securely and shall not be able to be read out.

5.4 Authentication

A means shall be specified to mutually authenticate the USIM and the network by showing knowledge of a secret key K which is shared between and available only to the USIM and in the user's Home Environment. The method is composed of a challenge/response protocol identical to the GSM user authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication.

5.5 Data integrity of signalling elements

Some signalling information elements are considered sensitive and must be integrity protected. An integrity function shall be applied on certain signalling information elements transmitted between the ME and the network.

~~The 3GPP Integrity Algorithm (UIA) shall be implemented in the USIM.~~

The 3GPP Integrity Algorithm (UIA) ~~shall be~~ is used with an Integrity Key (IK) to compute a message authentication code for a given message. The setting of IK is triggered by the authentication procedure. IK shall be stored on the USIM.

5.6 User identity confidentiality

A mechanism shall be specified to provide user identity confidentiality by means of a temporary identity. If a temporary identity is not available in the serving network, a means of encrypting the permanent user identity (IMSI)~~IMUI)~~ with a group key may be used. ~~The requirement for this mechanism is still under study by TSG SA WG3.~~