3GPP TSG-T (Terminals) Meeting #8
Düsseldorf, Germany, 21 - 23 June, 2000

Tdoc TP-000097

Source: T3

Title: Change Requests to TS 21.111 "USIM and UICC characteristics"

Agenda item: 6.3.3

Document for: Approval

This document contains several change requests to TS 21.111 v3.1.0 agreed by T3.

T3 Doc	Spec	CR	Rv	Rel	Subject
T3-000303	21.111	003		R99	Clarification of USIM application selection
T3-000304	21.111	004		R99	Alignment with 33.102: Enhanced User Identity Confidentiality (EUIC)

3GPP TSG-T3 (USIM) #14
Visby, 24 – 26 May, 2000

Document ***T3-000303***
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.

3G 21.111	**CR**	**003**	Current Version:	V 3.1.0

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

For submision to: TSG-T #8 *list approval meeting # here ↑*	for approval	X	strategic		*(for SMG use only)*
	for information		non-strategic		

Form: CR cover sheet, version 1.1 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CRF-11.rtf*

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

Source: T3 **Date:** 26 May 2000

Subject: Clarification of USIM application selection

Work item: TEI

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

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

(releases phase2, 96, 97 and 98 apply only to GSM specifications)

Reason for change: Alignment with proposed S1 R'99 CR to 22.101 (S1-000326).

Clauses affected: 6.1

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.

6 Logical issues

6.1 Application selection

In a multiapplication environment, a flexible application selection method is required. The application identifier defined in ISO/IEC 7816-5 [5] and EG 201 220 [6] should be used for application selection. Direct application selection and the EF_{DIR} concept of ISO/IEC 7816-4 [4] shall be followed. In particular, a mechanism for the ME and the UICC shall be specified in order to allow the user, when the ME is in idle mode, to select and activate one amongst those which are available and supported by the ME (this will permit the user to choose, for instance, between 2 different USIM applications). At switch on, the last active USIM shall be automatically selected. The last active USIM shall be stored on the UICC. By default if there is no last active USIM defined in the UICC, the user shall be able to select the active USIM amongst those available on the UICC.

6.2 Simultaneous access

A mechanism shall be specified for simultaneous access to several files or applications.

7 Service Requirements

7.1 User profiles

Each USIM shall contain at least one user profile [FFS].

7.2 Data transfer

A mechanism allowing highly secure transfer of applications and/or associated data to/from the UICC/USIM shall be specified in line with the requirements in 3GPP 22.01 [2]. This requires a secure transfer mechanism. GSM 02.48 [20] and GSM 03.48 [21] could be considered here, however this is limited to the case where the application to be downloaded runs in the context of an existing subscription. The security requirements in the case where, for instance, a new USIM or other application has to be downloaded, requires further study.

It is envisaged that in early USIM specifications, the transfer of subscription-related applications (e.g. SIM application toolkit applications) will be specified. The generic application download (e.g. download of a new USIM) is not likely to be included in these early specifications.

Application creation comprises file creation and other administrative operations on the, as well as negotiation of code type or language.

7.3 Application execution environment

An application execution environment may exist on the UICC/USIM which includes the functionality defined in GSM 11.14 [9].

7.4 Profile exchange

A mechanism for the ME, the USIM and the network to exchange service capabilities shall be specified. The following exchange of service capabilities may occur:

- ME services capabilities may be provided to the USIM/UICC;

3GPP TSG-T3 #13
Visby, Sweden, 24. – 26. 5. 2000

Document T3-000304
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	004	Current Version:	3.1.0

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

For submission to:	TSG-T #8	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: *(at least one should be marked with an X)* (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T3 **Date:** 26 May 2000

Subject: Alignment with 33.102: Enhanced User Identity Confidentiality (EUIC)

Work item: TEI

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: EUIC has been postponed to R'2000 by TSG-SA and is subject to further study. Consequently, it is removed from 21.111.

Clauses affected: 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.

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 IMSI). If the 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) 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) with a group key may be used.~~