Technical Specification Group Terminals
Meeting #6, Nice, France, 13-15 December 1999

TSGT#6(99)255

Source: **T3**

Agenda item: **8.3**

TSG-T3 (USIM) #11
Sophia Antipolis, France, 8-10 December 1999

Document ***T3-99429***
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** **001** Current Version: V 3.0.0

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

For submision to: TSG-T #6 *list approval meeting # here ↑*

for approval	X	strategic	
for information		non-strategic	

(for SMG use only)

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	ME	UTRAN / radio	Core Network
X	X		

Source: TSG-T3 **Date:** 10.12.1999

Subject: References to new specifications and editorial changes

Work item:

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

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

Reason for change: The current version of 21.111 does not comprise any reference to the new T3 specifications; editorial modifications to align with new terminology were incorporated

Clauses affected: all

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:

Foreword

This Technical Specification has been produced by the 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 this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 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 specification;

1 Scope

This document defines the requirements of the USIM (Universal Subscriber Identity Module) and the IC card for ~~3GPP~~3G (UICC). These are derived from the service and security requirements defined in 3G~~PP~~ TS 22.100 [1] and 3G TS 22.101 [2]. The USIM is a 3G~~PP~~ application on an IC card. It inter-operates with a 3G~~PP~~ terminal and provides access to 3G~~PP~~ services.

This document is intended to serve as a basis for the detailed specification of the USIM and the UICC, and the interface to the 3G~~PP~~ terminal.

2 References

~~References may be made to:~~

~~a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or~~

~~b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or~~

~~c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or~~

~~d) publications without mention of a specific version, in which case the latest version applies.~~

~~A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.~~

2.1 Normative 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.
- ~~A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.~~

[1] 3G TS 22.100: "~~Universal Mobile Telecommunications System (UMTS);~~ 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; UMTS phase 1 Release 99".

[2] 3G TS 22.101: "~~Universal Mobile Telecommunications System (UMTS); UMTS s~~3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

[3] 3G TS 31.101: "3rd Generation Partnership Project; Technical Specification Terminals; UICC-Terminal Interface; Physical and Logical Characteristics".

[4] 3G TS 31.102: "3rd Generation Partnership Project; .Technical Specification Terminals; Characteristics of the USIM application"

[5] 3G TS 31.110: "3rd Generation Partnership Project; Technical Specification Terminals; Numbering system for telecommunication IC card applications".

[6] 3G TS 31.111: "3rd Generation Partnership Project; Technical Specification Terminals; USIM Application Toolkit (USAT)".

[7] 3G TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security: Security Architecture".

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

[9] 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".

[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~~3~~] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[12~~[4~~] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[13~~5~~] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".

~~[6] ETSI EG 201 220: "Integrated Circuits Cards (ICC); ETSI numbering system for telecommunication; Application providers (AID)".~~

~~[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~~3G 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~~3G Integrity Algorithm
USIM	Universal Subscriber Identity Module

4 General Requirements

The UICC shall be a removable module containing a USIM. The USIM shall contain an identity which unambiguously identifies a subscriber.

For access to ~~3GPP~~3G services, a UICC containing a valid USIM shall be present at all times, other than for emergency calls.

The specifications shall support the security requirements as defined in 33.102 [7~~11~~].

The USIM shall provide storage for subscription and subscriber related information.

The UICC/USIM may also contain applications which use the features defined in the USIM Application Toolkit specification ~~GSM 11.14 [9]~~ 3G TS 31.111 [6].

5 Security Requirements

The USIM shall be used to provide security features. If the UICC is removed from the ~~3GPP~~3G terminal, the service shall be terminated immediately. The functions of the USIM include authenticating itself to the network and vice versa, authenticating the user and providing additional security functions as defined in 3G TS 33.102 [7].~~by 3GPP TSG SA WG3.~~

The USIM shall be unambiguously identified, also in the case of pre-paid subscriptions.

Means shall be provided to prevent fraudulent use of stolen IC Cards.

It shall not be possible to access data intended for USIM internal use, e.g. authentication keys.

Further details of the following requirements are given in 33.102 [7~~11~~].

5.1 File access conditions

Actions, such as READ, UPDATE on UICC data shall be controlled by access conditions. These shall be satisfied prior to the action being performed.

Since a UICC may contain multiple (~~3GPP~~3G and non-~~3GPP~~3G) applications, a flexible method of controlling file access shall be provided.

5.2 User authentication

The USIM shall support means to authenticate the user, to provide, for example, protection against the use of stolen cards. For the USIM, authentication shall be performed by the verification of a numeric PIN of four (4) to eight (8) decimal digits.

A function to disable user authentication may exist which may be inhibited by the application provider, in which case the user shall always use the PIN. Otherwise, the user may decide whether or not to make use of the user authentication function. If disabled, the user authentication function remains disabled until the user specifically re-enables it.

Following correct PIN presentation, the ME may perform functions and actions on USIM data, which are protected by the relevant access condition.

If an incorrect PIN is entered, an indication shall be given to the user. After three (3) consecutive incorrect entries the relevant PIN is blocked, i.e. functions and actions on data protected by the access condition shall no longer be possible, even if between attempts the UICC has been removed, the USIM has been deselected or the ME has been switched off. Once a PIN is blocked, further PIN verifications shall be denied.

The USIM shall support a mechanism for unblocking a blocked PIN. Unblocking of a PIN is performed by using the relevant PIN Unblocking Key.

PINs, but not Unblock PINS, shall be changeable by the user following correct entry of either the current PIN or Unblock PIN.

The Unblock PIN shall consist of eight (8) decimal digits and shall not be changeable by the user. If an incorrect Unblock PIN is presented, an indication shall be given to the user. After ten (10) consecutive incorrect entries, the Unblock PIN shall be blocked, even if between attempts the UICC has been removed, the USIM has been deselected or the ME has been switched off. Unblocking of a blocked PIN shall not be possible.

It shall not be possible to read PINs or Unblock PINs.

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 USIM 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~~sensitive 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~~3G Integrity Algorithm (UIA) shall be implemented in the USIM.

The UIA shall be 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.

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 (~~IMUI~~IMSI) with a group key may be used. ~~The requirement for this mechanism is still under study by TSG SA WG3.~~

5.7 Length of security parameters

In order to allow for enhancements of the security level in ~~3GPP~~3G, the following requirements shall be covered:

- all security-related parameters for ~~UMTS~~ 3G shall be accompanied by a length indicator;
- the USIM shall support variable-length security parameters.

If the USIM supports the GSM security mechanisms in addition to ~~3GPP~~3G security, fixed length security parameters according to GSM 11.11 ~~[7~~[8] shall be supported in addition.

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~~[13] and ~~EG 201 220 [6]~~3G TS 31.110 [5] should be used for application selection. Direct application selection and the EF_{DIR} concept of ISO/IEC 7816-4 [12~~4~~] shall be followed.

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~~3G TS 22.101 [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]~~ 3G TS 31.111 [6].

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;
- USIM/UICC services capabilities may be provided to the ME (and thus potentially to the network);
- network services capabilities may be provided to the USIM/UICC via the ME.

Editors note: This requirement needs to be ratified by the TSG-SA1 (services) group.

7.5 Version identification

A means for identification of the version of the USIM shall be provided.

8 Physical Characteristics

8.1 Dimensions

The ID-1 and Plug-in format used for the GSM SIM shall be adopted. A third format, smaller than the Plug-in format, is for further study. If a new format is defined, a means shall be specified in order to prevent an incorrect insertion of the card into the ME.

8.2 Contacts

The UICC shall not provide any connection to the V_{PP} contact. The contact shall be provided on the UICC. The ME may support the V_{PP} contact in the reader. The ME shall not have this contact connected; neither to ground nor to the UICC supply voltage.

NOTE: According to ISO/IEC 7816-3 [11~~3~~] the V_{PP} contact is RFU for ICCs operating at 3V.

9 Electrical characteristics and transmission protocols

Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3 [11~~3~~] unless specified otherwise.

The electrical specifications shall at least cover the 1.8V and 3V voltage ranges as specified in GSM 11.12 [9~~8~~] and GSM 11.18 [10]. Lower voltages may be added in the future. ~~3GPP~~3G terminals shall not support 5V on the ME-UICC interface. Both ME and UICC shall support operational class indication as defined in ISO/IEC 7816-3 [11~~3~~]. Both ME and UICC shall support at least two voltage classes.

Both UICC and ME shall support PPS as defined in ISO/IEC 7816-3 [11~~3~~] with at least the values defined in GSM 11.11 ~~[7~~[8].

The ME shall have the capabilities of initiating a warm reset as defined in ISO/IEC 7816-3 [11~~3~~]. The UICC shall support warm reset as defined in ISO/IEC 7816-3 [11~~3~~].

NOTE: The warm reset is used during a session when there is a need to restart the USIM due to internal modifications of data caused by user actions or network data downloading.

The UICC may indicate in the ATR to the warm reset that the specific mode is entered automatically, using the parameters that were used prior to the warm reset. In case of a cold reset, the UICC shall enter the negotiable mode.

In addition to the T=0 protocol which is mandatory for the UICC and the ME, the T=1 protocol shall be mandatory for the ME. It is optional for the UICC.

The speed enhancement as specified in GSM 11.11 [~~7~~8] shall be supported by both the ME and the UICC. Higher interface bit rates than those specified in GSM 11.11 [8~~7~~] should be considered.

9.1 Power consumption indication

Power consumption figures are to be revised based on the need for more secure authentication algorithms, utilising crypto co-processors. In order to be compatible with the GSM specifications, the UICC shall meet the power consumption specifications set in GSM 11.12 [9~~8~~] and GSM 11.18 [10] during the ATR. The USIM status information shall contain power consumption information, which is related to the operational class indicated in the ATR and the operating frequency indicated for running the authentication algorithm.

NOTE: The power consumption figure may differ between different applications on the UICC; thus a particular ME may support some applications in a card and reject others, depending on the power consumption values.

The ME may reject the USIM if it can not supply the current indicated in the status information and if this current is above the maximum value defined for use by the UICC for running the USIM.

10 Contents of the Elementary Files

10.1 USIM information storage requirements

The USIM shall contain information elements for ~~3GPP~~3G network operations. The USIM may contain information elements related to the subscriber, ~~3GPP~~3G services and home environment or service provider related information.

The UICC shall provide storage capability for the following:

- UICC related information:
  - IC card identification: a number uniquely identifying the UICC and the card issuer;
  - Preferred language(s);
  - Directory of applications.
- USIM related information:
  - Administrative information: indicates mode of operation of the USIM, e.g. normal, type approval;
  - USIM service table: indicates which optional services are provided by the USIM;
  - ~~IMUI~~IMSI;
  - Language indication;
  - Location information;
  - Cipher key (Kc) and cipher key sequence number;
  - Access control class(es);
  - Forbidden PLMNs;
  - Phase identification;
  - Ciphering Key for GPRS;
  - GPRS location information;
  - Cell Broadcast related information;
  - Emergency call codes;
  - Phone numbers (ADN, FDN, SDN);
  - Short messages and related parameters;

  - Capability and Configuration parameters;
  - HPLMN search period [FFS];
  - BCCH information: list of carrier frequencies to be used for cell selection [FFS].

- Information accessible to the USIM and other applications:

  - ADN.

In addition, the USIM shall manage and provide storage for the following information in accordance with the security requirements of clause 5:

- PIN;
- PIN enabled/disabled indicator;
- PIN error counter;
- Unblock PIN;
- Unblock PIN error counter;
- Data integrity keys;
- Subscriber authentication keys.

10.2 Phone Book

The Phone Book feature is based on the ADN functionality as defined in GSM 11.11 [8~~7~~]. Additional features are identified in the following subclauses. A Phone Book entry consists of a record in an ADN file and, optionally, additional records which are placed in different EFs. In the latter case, a mechanism shall be defined to link all records in the same Phone Book entry. These features shall be supported by the ME while their support by the USIM is optional.

10.2.1 Support of two name fields per entry

The support of two name fields per entry shall be specified to allow, for example, for two different representations of the same name (~~,~~ for example, in Japanese characters and in Latin characters~~English~~).

10.2.2 Support of multiple phone numbers per entry

The support of multiple phone numbers per entry shall be specified, for example, office, home, fax, mobile or pager. In addition to that, information for identifying those attributes are needed.

10.2.3 Support of email address

The support of email addresses linked to Phone Book entries shall be specified. In addition to that, information for identifying these addresses is needed.

10.2.4 Support of user definable groupings

The specification shall support the grouping of Phone Book entries into groups defined by the user, for example, business and private.

10.2.5 Support of hidden entries

The specification shall support means of marking Phone Book entries as "hidden".

10.2.6 Number of entries

The specification shall support storage of at least 500 entries.

10.2.7 Mode of alerting

[FFS]

10.3 Storage of call details

The specification shall support provision of storage for call detail information. The call detail information consists of the following attributes:

- mobile terminated calls:
  calling party number, date and time, calling party's name and status of call (i.e. answered or missed), duration and [FFS] charge;
- mobile originated calls:
  called party number, date and time, called party's name, duration and [FFS] charge;
- accumulated duration of preceding calls, separately for mobile originated and mobile terminated calls;
- accumulated charge information of preceding calls [FFS].

Call detail attributes are optional. A value to mark them as "undefined" shall be available.

NOTE 1: The calling/called party's name may be available from the Phone Book.

NOTE 2: The storage of multiparty call information is FFS.

11 ~~3GPP~~3G/GSM interworking

11.1 GSM subscribers in a ~~3GPP~~3G network

~~3GPP~~3G 22.101 [2]: "UMTS shall provide some mechanisms which permit pre UMTS subscribers to roam easily onto UMTS and access the services."

~~3GPP~~3G 22.100 [1]: "The UMTS mobile terminal shall support phase 2 and phase 2+ GSM SIMs as access modules to UMTS networks. The services that can be provided in this case may be limited to GSM like services provided within that UMTS network. It shall be up to the UMTS network operator whether or not to accept the use of GSM SIM as access modules in its network".

11.2 ~~3GPP~~3G subscribers in a GSM network

The following requirement is made in ~~3GPP~~3G 22.101 [2]: "UMTS shall provide some mechanisms which permit UMTS subscribers to roam easily onto pre-UMTS systems and access the services."

This may be achieved by providing all mandatory elements as defined in GSM 11.11 [8~~7~~] in the UICC.

The specification shall allow the UICC to be used with a dual mode (GSM/ ~~3GPP~~3G) ME and a GSM ME for the provision of GSM service.

NOTE: This does not, for example, preclude the support of the PDC application on a UICC.

History

Document history		
3.0.0	April 1999	Approved at TSG #3, Yokohama, April 1999