UMTS 21.11 V0.4.0 (1998-12)

Technical Report

Universal Mobile Telecommunication System (UMTS); USIM and IC Card Requirements

UMTS

Universal Mobile
Telecommunications System

Reference

<WORKITEM> (070000c3.PDF)

Keywords

<keyword[, keyword]>

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

Introduction

The UICC is a removable module containing a USIM. The USIM contains an identity which unambiguously identifies a subscriber.

1 Scope

This document defines the functional characteristics and requirements of the USIM (User Service Identity Module) and the IC card for UMTS (UICC). These are derived from the service and security requirements defined in UMTS 22.01 [2] and 22.00 [1]. The USIM is a UMTS application on an IC card. It inter-operates with a UMTS terminal and provides access to UMTS services.

This document is intended to serve as a basis for the specification of the USIM, the UICC, and the interface to the UMTS 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] UMTS 22.00: "Universal Mobile Telecommunications System (UMTS); UMTS phase 1"

[2] UMTS 22.01: "Universal Mobile Telecommunications System (UMTS); UMTS service aspects; Service principles".

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

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

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

[6] CEN EN 726-3: "Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements"

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

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

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

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 UMTS application on an IC card.

3.2 Symbols

V_{pp}	Programming voltage

3.3 Abbreviations

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

ADN	Abbreviated Dialling Number
ATR	Answer To Reset
CHV	Card Holder Verification information; access condition used by the SIM for the verification of the identity of the user
DF	Dedicated File (abbreviation formerly used for Data Field)
EF	Elementary File
ICC	Integrated Circuit Card
IMUI	International Mobile User Identity
ME	Mobile Equipment
MF	Master File
PPS	Protocol and Parameter Selection
SIM	Subscriber Identity Module
UICC	UMTS Integrated Circuit Card
USIM	User Service Identity Module

[general abbreviations doc in UMTS ?]

4 Security Requirements

The USIM shall be used to provide security features. For access to UMTS services a UICC containing a valid USIM shall be present at all times, except for emergency calls. If the UICC is removed from the UMTS terminal, the service is terminated immediately. The functions of the USIM include authenticating itself to the network and vice versa, authenticating the user and providing additional security functions (to be defined by ETSI SMG10).

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

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

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

4.1 File access conditions

Actions, e.g. read, update, on SIM data shall be controlled by access conditions, which shall be satisfied before the action can be performed.

Since a UICC may contain multiple (UMTS and non-UMTS) applications a flexible method of controlling file access will be required. Two different solutions are considered in the following subclauses.

4.1.1 The EF_{CHV} approach

Following a notion brought up in EN726-3 [6], for each file in a card there is a relevant CHV defined. CHVs are stored in an EF_{CHV}, and the relevant CHV file is a son of the current DF, or, if this one is not existing, the relevant CHV file is the relevant CHV of the parent of the current DF applies.

This sounds a bit complex, but in fact is simple because given any file xyz, you look for an EF_{CHV} at the same level. If there is none, you go one level up. If there is a CHV file at this level, it applies to xyz; if not, you go one further level up. If you end up at the master file without coming across any EF_{CHV}, then no CHV applies to xyz.

Example:

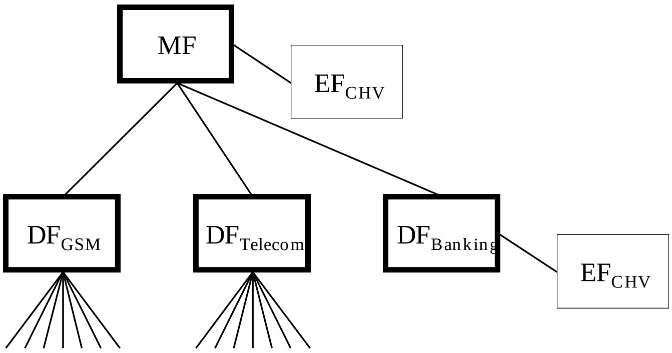

Figure 1: File / CHV structure

Here, the CHV related to the upper CHV file applies to the MF, DF_{GSM} and $DF_{Telecom}$. In contrast, $DF_{Banking}$ is protected by its own CHV stored in the lower CHV file.

According to this approach, it is possible to group several applications in a card, each potentially with its own CHV protection. It is, however, not possible to combine access conditions to a file (e.g. CHV of party x or CHV of party y).

NOTE: The solutions offered by ISO and other non-ETSI card standards on these questions should be considered, e.g. VISA, MULTOS.

With this method, CHVs are clearly application-related. Normally they are stored locally within the application DF, which bears the advantage that adding or deleting applications to a card is straightforward.

4.1.2 A general solution for flexible multiple CHVs

If multiple CHVs are being used within one card, this represents a multi-user environment. In particular, in the general case there is no mapping between applications and CHVs as in clause 4.1.1, but rather a CHV is related to a specific user.

Consequently, in this case it is not sufficient to prompt for a CHV, but, as in multi-user computer systems, the user is prompted for username and password (i.e. CHV).

Clearly if there is no mapping between an application (i.e. a DF) and a specific CHV, then the GSM coding for the STATUS response is no more appropriate because the DF may be accessed by various CHVs and thus there is no clearly defined “number of false presentations remaining “ as in the GSM STATUS response.

In this scenario, each application DF would have a mandatory “CHV list” contained in it, with a list of pointers to the CHVs which are allowed to access the application. The CHVs itself would be stored together with some kind of username.

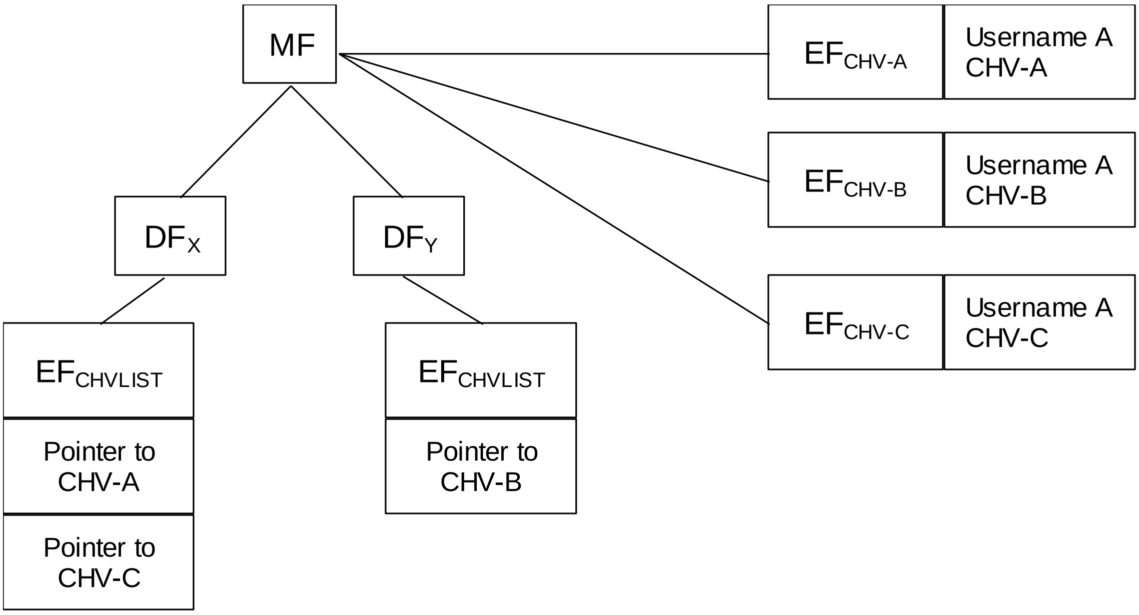

Figure 2: Example of multiple CHVs using the CHV list method

In this example, the card has three CHVs (A, B, C) in total; the application in DF_X can be accessed with either CHV-A or CHV-C, whereas the application in DF_Y can be accessed with CHV-B. When the user selects an application, he is prompted for a username and the corresponding CHV which are both stored in the EF_{CHV}. If the user successfully verifies a particular CHV, then all applications where this CHV is valid are accessible.

4.2 Subscriber data stored in ME

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

Subscriber related security codes (e.g. CHV and Unblock CHV) may be kept in the ME during the execution of the appropriate SIM/ME interface procedure (e.g. verifying or changing a CHV). They shall be deleted from the ME immediately after completion of the procedure.

Optionally, an ME may retain some less security critical data at SIM removal or MS switch-off. Such data are SMS, ADN/SSC, FDN/SSC, LND etc. These data, when stored in the ME, shall only be readable/retrievable if the same SIM 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.

Storage for other data such as ADN/SSC, SMS etc., storage may also exist in the ME. These data stored in the ME, which have not been transferred from a SIM during a card session, are not subject to the above security restriction.

4.3 CHV management

The U SIM shall support the use of Card Holder Verifications (CHV) to authenticate the user to the card e.g. to provide protection against the use of stolen cards. For the USIM the CHV information takes the form of a numeric CHV of 4 to 8 decimal digits.

A CHV disabling function may exist. This function may be inhibited at card issue. In this case the subscriber shall always use the CHV. Otherwise the subscriber may decide whether or not to make use of the CHV function. If disabled, the CHV remains disabled until the subscriber specifically re-enables CHV checking.

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

If an incorrect CHV is entered, an indication is given to the user. After three consecutive incorrect entries the relevant CHV is blocked, i.e. functions, and actions on data, protected by the CHV access condition are no longer possible, even if between attempts the SIM has been removed or the MS has been switched off. Once a CHV is blocked, further CHV verifications cannot be performed.

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

CHVs shall be changeable by the subscriber following correct entry of either the current CHV or Unblock CHV.

The Unblock CHVs shall consist of 8 decimal digits and are not changeable by the user. If an incorrect Unblock CHV is presented, an indication is given to the user. After 10 consecutive incorrect entries, the Unblock CHV is itself blocked, even if between attempts the UICC has been removed or the MS has been switched off. Unblocking of the relevant CHV is now impossible.

It shall not be possible to read the CHV(s) or Unblock CHV(s).

5 Logical issues

5.1 Application selection

In a multiapplication environment, a flexible application selection method is an obvious requirement. The application identifier defined in ISO 7816-5 [5] and EG 201 220 [7] should be used for application selection. Direct application selection defined in ISO 7816-4 [4], and the EF_{DIR} concept of ISO 7816-4 [4], and EN 726-3 [3], shall be followed.

5.2 Logical channels

The mechanism of logical channels according to ISO 7816-4 [4] shall be supported. The support is mandatory for the terminal and mandatory for the card if multiple applications are present.

5.3 File structures

It has to be investigated whether the inclusion of linear variable EF structures offers a benefit.

6 Service Requirements

6.1 User Profiles

Each USIM shall contain at least one user profile which is associated with at least one user address.

[To be re-checked against 22.01 , successor of V3.3.0 as soon as it becomes available]

6.2 Data Download

A standardised mechanism allowing highly secure transfer of applications and/or associated data to/from the UICC shall be supported in UMTS phase 1, as required in UMTS 22.01 [1]. This comprises a secure download mechanism.
GSM 02.48 and GSM 03.48 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 e.g. a new USIM has to be downloaded has to be studied.

It is envisaged that in UMTS phase 1, the download of subscription-related applications (e.g. SIM application toolkit) can be achieved. The generic application download (e.g. download of a new USIM) is considered to be a UMTS phase 2 issue.

Moreover, application creation comprises file creation and other administrative operations on the card (SMG9 generics subgroup), as well as negotiation of code type or language (SMG9 API subgroup, JAVA card forum).

6.3 Application Execution Environment

An application execution environment may exist on the UICC which includes the functionality defined in GSM 11.14 [10].

7 Physical Characteristics

7.1 Dimensions

The ID-1 and plug-in format used for the GSM SIM shall be adopted. A third, even smaller format is currently under consideration within ETSI SMG9. A possibility would be to define a size which covers just the contact area (for six contacts) defined by ISO; however, the size reduction with respect to the plug-in size is limited, and in a few years the need for even smaller modules may arise. Thus also a smaller contact area could be taken into consideration. For the new card size, a mechanical means shall be provided in order to prevent an incorrect insertion of the card.

7.2 Contacts

The USIM shall not provide any connection to the V_{PP} contact. The contact shall be provided on the UICC. The UMTS terminal 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 [3] the V_{PP} contact is RFU for ICCs operating at 3V.

8 Electrical Characteristics and Transmission Protocols

Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3 [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] and GSM 11.18 [11]. Lower voltages may be added in the future. UMTS 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 [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 with at least the values defined in GSM 11.11 [8].

The ME shall have the capabilities of initiating a warm reset as defined in ISO/IEC 7816-3 [3]. The USIM shall support warm reset as defined in ISO/IEC 7816-3 [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 fields caused by user actions or network data downloading.

The USIM 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 USIM shall always 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 is mandatory for both the UMTS ME and the USIM to support. Higher interface bit rates than those specified in GSM 11.11 [8] should be considered.

8.1 Power consumption indication

Power consumption figures are to be revised based on the need for more secure authentication algorithms to be used, utilising crypto co-processors. In order to be compatible with the GSM specification the USIM shall meet the power consumption specifications set in 11.12 [9] and 11.18 [11] during the ATR. The USIM status information data field 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 mobile 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. The power consumption (current) shall be indicated on one byte with the unit in mA.

NOTE: This mechanism, although not needed for first generation UICCs, provides a measure of future-proofing for as yet unknown future requirements.

9 Contents of the Elementary Files

9.1 USIM information storage requirements

The USIM shall contain information elements for UMTS network operations. The SIM may contain information elements related to the mobile subscriber, UMTS services and home environment or service provider related information.

The UICC provides storage capability for the following:

1. Files at MF level

- IC card identification: a number uniquely identifying the UICC and the card issuer.
- Extended Language preference; subscriber preferred language(s) of MMI.
- Directory of applications

2. Files at USIM level

- 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.
- IMSI or IMUI.
- Location information
- Cipher key (Kc) and cipher key sequence number.
- *BCCH information: list of carrier frequencies to be used for cell selection. (? t.b.d.)*
- Access control class(es)
- Forbidden PLMNs
- *HPLMN search period (? t.b.d.)*
- Phase identification.
- Ciphering Key for GPRS
- GPRS location information
- Cell Broadcast related information
- Emergency call codes

- Phonenumbers (FDN, SDN, BDN)
- Short messages and related parameters,
- Capability and Configuration parameters.

3. Files at Telecom level

- ADN
- Short messages and related parameters,

In addition the USIM shall manage and provide storage for the following information in accordance with the security requirements of clause 4:

- CHV;
- CHV enabled/disabled indicator;
- CHV error counter;
- Unblock CHV;
- Unblock CHV error counter;
- Subscriber authentication keys

9.2 ADN

From the user's perspective, the ADN feature is one of the most important visible functionality delivered by the card. The GSM ADN may be enhanced e.g. by being able to group users, in order to separate between business and private numbers, or by assigning a class identifier to users in order to associate them with a particular mode of alerting. Another possible extension to the ADN functionality could be the ability to have a second name field (i.e. two names for one number).

For all these enhancements, additional information needs to be stored , e.g. by appending it to the existing data structure of the records of the GSM ADN file, or by adding additional files which carry the necessary information and are linked to the ADNs.

10 UMTS/Pre-UMTS interworking

10.1 Pre-UMTS subscribers in UMTS network

UMTS 22.01 [2]: "UMTS shall provide some mechanisms which permit pre UMTS subscribers to roam easily onto UMTS and access the services."

UMTS 22.00 [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".

10.2 UMTS subscribers in Pre-UMTS network

The following requirement is made in UMTS 22.01 [2]: "UMTS shall provide some mechanisms which permit UMTS subscribers to roam easily onto pre-UMTS systems and access the services."

For GSM, this may be achieved by providing all mandatory elements as defined in GSM 11.11 [8] in the card., however this GSM application does not necessarily reside below the DF_{7F20}, but rather may be part of, or below, the USIM.

10.3 Linking of GSM and UMTS application

The implications of the requirement to allow for GSM-UMTS handover need to be studied. For example, protecting GSM and USIM applications with different CHVs will cause problems .A possible solution for this problem would be to place the GSM application as a daughter, or as a subset, of the UMTS application thus allowing access to both applications with a single CHV.

NOTE: This is a solution which will work in a dual-mode GSM-UMTS terminal, but not necessarily in a GSM ME (which is not a requirement).

History

Document history		
0.1.0	2 October, 1998	Produced by the rapporteur for consideration at SMG9 UMTS #5 (6-7 October, 1998)
0.2.0	26 October, 1998	Inclusion of material agreed at SMG9 UMTS #5 (6 - 7 October, 1998) in tdoc 98u044. Abbreviations and references section also expanded.
0.3.0	5 November, 1998	Inclusion of material agreed at SMG9 UMTS #6 (4 - 5 November, 1998)
0.4.0	22 November, 1998	Inclusion of material agreed at SMG9 UMTS #7 (15 – 16 December, 1998)