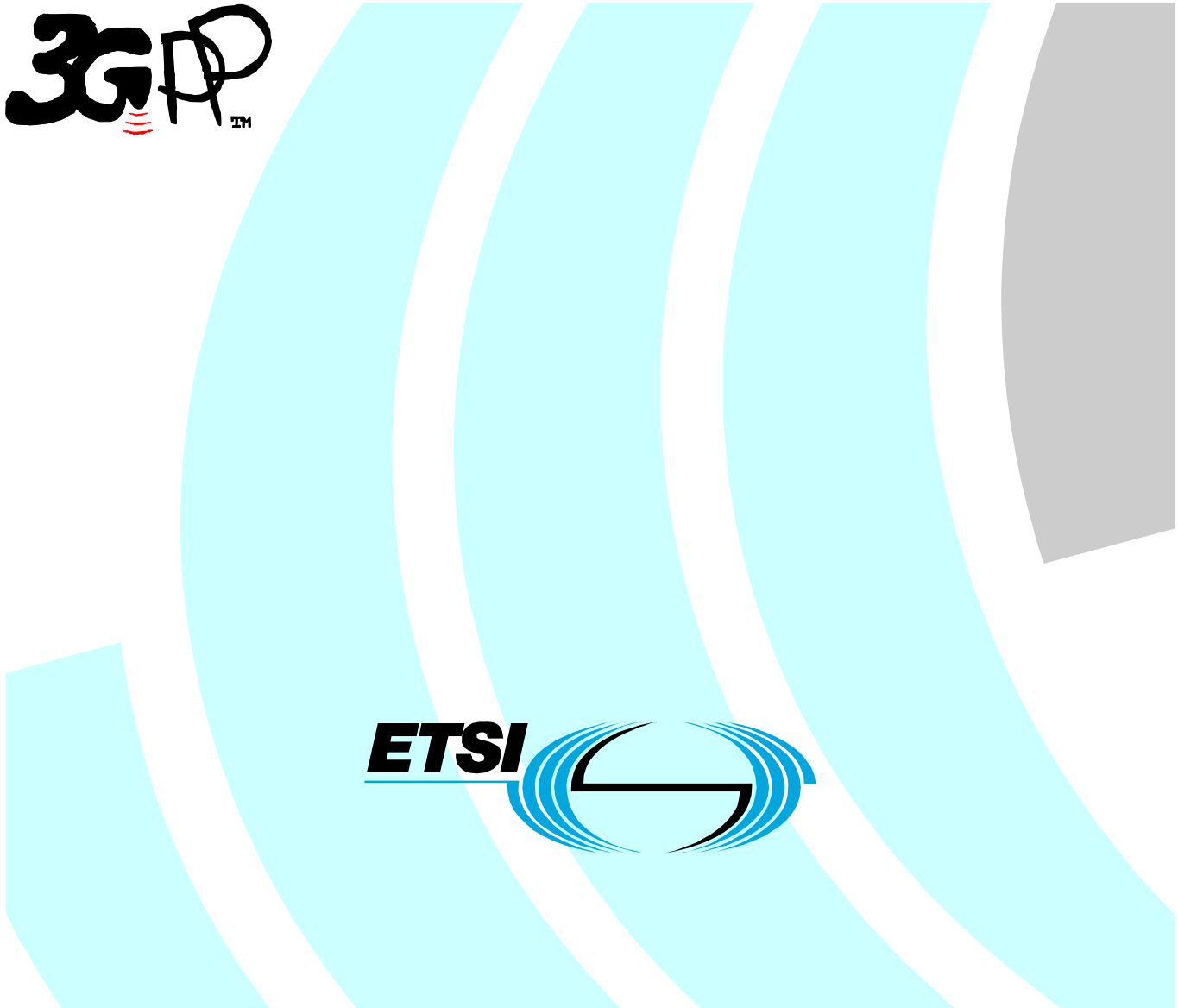
ETSI TS 121 111 V8.1.0 (2008-01)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
USIM and IC card requirements
(3GPP TS 21.111 version 8.1.0 Release 8)



Reference
RTS/TSGC-0621111v810

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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 ETSI 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

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

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 x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater 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 document.

1 Scope

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

2 References

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. 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] 3GPP TS 22.100 v3.x.x: "UMTS phase 1" (Release 99).

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[4] Void

[5] ETSI TS 101.220: "ETSI Numbering System for AIDs".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] 3GPP TS 33.102: "3G Security: Security Architecture".

[8] 3GPP TS 51.011, Rel-4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] Void.

[10] Void.

[11] Void.

[12] ISO/IEC 7816-4 : "Identification cards - Integrated circuit cards, Part 4: Organization, security and commands for interchange".

2.2 Void

3 Definitions, symbols and abbreviations

3.1 Definitions

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

3.2 Void

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
ICC	Integrated Circuit Card
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
ME	Mobile Equipment
MF	Master File
PIN	Personal Identification Number
PPS	Protocol and Parameter Selection
SIM	Subscriber Identity Module
USIM	Universal Subscriber Identity Module

4 General requirements

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

For access to 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].

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 TS 31.111 [6].

5 Security requirements

The USIM shall be used to provide security features. If the UICC is removed from the 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].

The USIM shall be unambiguously identified.

Means shall be provided to prevent fraudulent use of stolen UICCs.

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 TS 33.102 [7].

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 (3G and non-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.

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-sensitive data at UICC removal, USIM deselection or ME switch-off. Such data are e.g. 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 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.

5.7 Length of security parameters

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

- all security-related parameters for 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 3G security, fixed length security parameters according to TS 51.011 [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 ETSI TS 101 220 [5] should be used for application selection. Direct application selection, including selection by partial DF name and the EF_{DIR} concept of ISO/IEC 7816-4 [12] 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 application 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 Void

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 3G TS 22.101 [2]. This requires a secure transfer mechanism.

7.3 Application execution environment

An application execution environment may exist on the UICC/USIM which includes functionality defined in 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.

7.5 Version identification

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

8 Physical Characteristics

The physical characteristics shall be in accordance with the specifications in TS 31.101 [3].

8.1 Void

8.2 Void

9 Electrical characteristics and transmission protocols

Electronic signals and transmission protocols shall be in accordance with the specifications in TS 31.101.

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 [10]. Lower voltages may be added in the future. 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].

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] 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 [11]. The UICC shall support warm reset as defined in ISO/IEC 7816-3 [11].

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 [8] shall be supported by both the ME and the UICC.

9.1 Void

10 Contents of the Elementary Files

10.1 USIM information storage requirements

The USIM shall contain information elements for 3G network operations. The USIM may contain information elements related to the subscriber, 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;
    - IMSI;
    - Language indication;
    - Location information;
    - Cipher key (Kc) and cipher key sequence number;
    - Access control class(es);
    - Forbidden PLMNs;
    - 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;
    - Higher Priority PLMN search period;
    - list of carrier frequencies to be used for cell selection.
- 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

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 UICC 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).

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 Void

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;

- mobile originated calls:
  called party number, date and time, called party's name and duration;

- accumulated duration of preceding calls, separately for mobile originated and mobile terminated calls.

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.

10.4 Void

11 3G/GSM interworking

11.1 Void

11.2 3G subscribers in a GSM network

3G 22.101 [2] requires that UMTS shall provide some mechanisms which permit UMTS subscribers to roam easily onto pre-UMTS systems and access the services.

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

12 Contact Manager

12.1 General

The Contact Manager provides an interface for the management of contact information including rich content without any structural limitations.

There shall be a mechanism for the ME to detect that the UICC containing the Contact Manager has changed. This mechanism may be used by the ME to ask the user whether synchronization of data between the ME and the UICC Contact Manager should occur.

This section defines the functional requirements of the Contact Manager. An ME and a 3GPP application supporting the Contact Manager shall comply with all these requirements.

12.2 Security requirements

The Contact Manager may contain personal information. It shall be possible to restrict the access to this information to authorized users or entities (e.g. by binding the access to the verification of the USIM PIN).

12.4.3 Interworking with the 3G Phone Book

In case both the ME and the 3GPP application support both the 3G Phone Book (i.e. as defined in section 10.2 of the present document) and the Contact Manager the Contact Manager shall be used. There shall be a mechanism for the 3GPP application to indicate the support of the Contact Manager.

12.4.4 Content description

12.4.4.1 Number of contacts

The Contact Manager specification shall not unreasonably restrict the number of contacts.

12.4.4.2 Contact structure

The Contact Manager shall consist of contacts, which are made up of various fields (e.g. phone number, name, photo). A filtering mechanism according to OMA DS Field Filtering shall be supported.

It shall be possible to have several instances of a field in a contact when appropriate (e.g. a contact may have two fax numbers).

An extensible coding scheme shall be defined which allows to describe a contact including all its fields. An existing scheme (e.g. "vcard") shall be used, if appropriate.

A minimum set of field types recognised by the 3GPP application and the ME shall be defined (e.g. name, phone number, URL, Email address, address, sound, pictures, notes).

It shall be possible to store and associate multimedia information (stored on the 3GPP application) with a contact (e.g. photo, logo, video, ring tone, voice tag).

It shall be possible to associate an icon or a label to each contact field type (e.g. associate an icon representing a phone to the number field. "Home address" could be configured as the label of the "mailing address" field type).

It shall be possible to configure the structure and the display order of the contact fields (e.g. first name then Instant Messaging address then number, etc) depending on ME capabilities.

12.4.4.3 Group management

It shall be possible to define new groups (e.g. My Tennis Club).

It shall be possible to pre-define groups (e.g. Friend, Work, Family and VIP).

It shall be possible to store and associate multimedia information (stored on the 3GPP application) with a group (e.g. photo, logo, video, ring tone, icon).

It shall be possible to bind contacts to one or several groups.

12.4.4.4 User Action Management

It shall be possible to configure a list of possible actions that could be proposed to the user when the contact is selected (e.g. Launch Browser, Send SMS, Send MMS, Instant messaging, Make a voice over IP call, Make a video call, Make a conference call, Game player, Send Email).

12.4.5 Interface capabilities description

An external and an internal interface to the Contact Manager shall be defined.

The external interface between the Contact Manager and a UICC external entity, i.e. the ME, shall rely on a transport protocol layer that is independent of the physical interface (i.e. the ISO interface and the new high-speed interface). This is to allow the definition of one solution that can use either the existing ISO interface or the new high-speed interface. The external interface definition shall also ease interfacing the PC applications with the Contact Manager.

Both the ME and the UICC shall be capable of initiating contact information synchronization based on a configurable policy.The internal interface allows other UICC resident applications to access the Contact Manager e.g. through a dedicated API. This enables the creation of additional services utilizing the Contact Manager data and properties. There shall be a mechanism for the user to allow or prevent remote access to the Contact Manager.

The external and internal interface shall provide means to:

- identify Contact Manager capabilities

- perform the following operations on a contact or a group: create, retrieve, modify, delete, search

In addition the internal interface shall provide mechanisms to:

- register/deregister an UICC resident application to the Contact Manager.

- allow a resident UICC application to access Contact Manager data and properties based on user permission.

- allow the Contact Manager to notify events to registered UICC application and to pass event related information when applicable. Events notifying the applications shall include:

    - contact information is modified locally

    - contact information is modified remotely

- change of contact manager configuration

12.4.6 Efficient browsing and searching

The Contact Manager interfaces should allow efficient searching and browsing of the contacts (i.e. the user experience browsing the Contact Manager should be acceptable).

12.4.7 Associated services

12.4.7.1 Memory management

It shall be possible to determine the number of stored contacts and the amount of the available and used Contact Manager memory.

Annex A (informative): Change history

The table below indicates all change requests that have been incorporated into the present document since it was initially approved by 3GPP TSG T and subsequently 3GPP TSG CT.

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
1999-06	TP-03	TP-99085				Draft specification first approved at TSG-T #3	2.0.0	3.0.0
1999-12	TP-06	TP-99255	001		D	References to new specifications and editorial changes	3.0.0	3.0.1
2000-04	TP-07	TP-000017	002		F	Location of the UIA (3GPP integrity algorithm) aligned with 33.102	3.0.1	3.1.0
2000-07	TP-08	TP-000097	003		F	Clarification of USIM application selection	3.1.0	3.2.0
		TP-000097	004		F	Alignment with 33.102: removal of Enhanced User Identity Confidentiality (EUIC) from R99		
2000-10	TP-09	TP-000150	005		F	Partial AID selection requirements	3.2.0	3.3.0
2001-03	TP-11	-	-			Issued as version 4.0.0 in order to create a complete set of specifications for release 4. The contents of version 4.0.0 are identical to the contents of version 3.3.0	3.3.0	4.0.0
2002-06	TP-16	-	-			Issued as version 5.0.0 in order to create a complete set of specifications for release 5. The contents of version 5.0.0 are identical to the contents of version 4.0.0	4.0.0	5.0.0
2002-09	TP-17	TP-020208	009		A	Clarification on the use of the USIM and the SIM	5.0.0	5.1.0
2004-03	TP-23	TP-040023	010		C	Update with respect to the third form factor and removal of an unused reference	5.1.0	6.0.0
2004-06	TP-24	TP-040100	011		D	Release 6 alignment	6.0.0	6.1.0
2005-06	CT-28	CP-050136	015		A	ISO/IEC 7816-Series Revision	6.1.0	6.2.0
2006-05	CT-32	CP-060349	0017	1	F	Review of TS 21.111, USIM and IC Card Requirements	6.2.0	6.3.0
2006-09	CT-33	action item	-		-	MCC to raise spec to Rel-7	6.3.0	7.0.0
2007-03	CT-35	CP-070070	0019	2	B	Requirements for the Enhanced USIM phonebook	7.0.0	8.0.0
2007-10						Editorial correction to cover page	8.0.0	8.0.1
2007-12	CT-38	CP-070839	0020	2	B	Completion of the requirements for the Enhanced USIM phonebook Renaming of the feature to Contact Manager. Contact Manager moved to a dedicated section	8.0.1	8.1.0

History

Document history		
V8.0.1	January 2008	Publication
V8.1.0	January 2008	Publication