



वर्गीय आवश्यकताओं के लिए मानक

टीईसी 20010:2010

(पूर्व सं. टीईसी/जीआर/डब्ल्यूएस/सिम-003/02 जनवरी 2010)

STANDARD FOR GENERIC REQUIREMENTS

TEC 20010:2010

(Earlier No. TEC/GR/WS/SIM-003/02.JANUARY 2010)

यूनिवर्सल सब्सक्राइबर आइडेंटिटी मॉड्यूल (यूएसआईएम)

Universal Subscriber Identity Module (USIM)



ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुरशीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHID LAL BHAWAN, JANPATH, NEW DELHI-110001, INDIA

www.tec.gov.in

© टीईसी, 2023

©TEC, 2023

इस सर्वाधिकार सुरक्षित प्रकाशन का कोई भी हिस्सा, दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली की लिखित स्वीकृति के बिना, किसी भी रूप में या किसी भी प्रकार से जैसे - [इलेक्ट्रॉनिक](#), मैकेनिकल, [फोटोकॉपी](#), रिकॉर्डिंग, स्कैनिंग आदि रूप में प्रेषित, संग्रहीत या पुनरुत्पादित न किया जाए।

All rights reserved and no part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form and by any means - electronic, mechanical, photocopying, recording, scanning or otherwise, without written permission from the Telecommunication Engineering Centre, New Delhi.

Release: Jan., 2010

Price: Free of Cost

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This generic requirement relates to the UICC based Universal Subscriber Identity Module application, called 'USIM' complying to 3GPP Technical Specifications (Release 5) for use in Mobile Equipment (ME) in 3G Telecom Networks. The document covers briefly the role of USIM, its components, functions, physical characteristics, transmission protocols, application and file structure and security features.

HISTORY SHEET

Sl. No.	Standard/Document No.	Title	Remarks
1.	GR/SIM-003/01.APR 05	Universal Subscriber Identity Module (USIM)	First Issue: April 2005
2.	GR/WS/SIM-003/02.JAN 2010	Universal Subscriber Identity Module (USIM)	Second Issue: January 2010
3.	TEC 20010:2010	Standard for Generic Requirements for a Universal Subscriber Identity Module (USIM)	Includes revised Numbering Scheme

Note:

1. The documents have been renumbered as per revised numbering scheme, kindly refer the Mapping-Listing Table pertaining to old and revised document number available on TEC website www.tec.gov.in/. In case of further clarification, please contact at email ID adgdoc.tec@gov.in

2. Inside the documents, General Requirements may be read as Standard for General Requirements, Interface Requirements as Standard for Interface Requirements, Several Requirements as Standard for General Requirements and Test Schedule & Test Procedure (TSTP) as TEC Test Guide.

CONTENTS

1.	Chapter -1 : Introduction	1
2.	Chapter -2 : Functional Requirements of USIM	2-5
3.	Chapter -3 : Technical Requirements	6-12
4	Chapter -4: Guidelines to the Purchaser	13
	Abbreviations	14

References

- [1] 3GPP TS 33.103 (2001): 3G Security Integration Guidelines (Release 4, latest version).
- [2] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".
- [3] ISO/IEC 7811-1 (1995): "Identification cards - recording technique Part- 1: Embossing".
- [4] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique Part- 3: Location of embossed characters on ID-1 cards".
- [5] ISO 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts, Part- 1: Physical characteristics".
- [6] ISO 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts, Part- 2: Dimensions and locations of the contacts".
- [7] ISO/IEC 7816-3 (1989): "Identification cards - Integrated circuit(s) cards with contacts, Part-3: Electronic signals and transmission protocols".
- [8] 3GPP TS 35.206 (2003): 3GPP Technical specifications for GSM-MILENAGE ALGORITHM (Release 5, latest version).
- [9] 3GPP TS 33.102 (2002): 3GPP Technical specifications for 3G security (Release 5, latest version).
- [10] ISO 7816-4 (1997) "Inter Industry command for Interchange".
- [11] 3GPP TS 31.101 (2000): 3GPP Technical specifications for UICC-Physical and Logical Characteristics (Release 1999 with latest updates).
- [12] 3GPP TS 31.102 (2004): 3GPP Technical specifications for USIM applications (Release 5, latest version).
- [13] Public Key Cryptography Standard (2004).
- [14] 3GPP TS 31.111(2004): 3GPP Technical specifications for USIM Applications Toolkit (Release 5, latest version).
- [15] 3GPP TS 33.102 (2002): 3GPP Technical specifications for 3G security (Release 5, latest version).

Universal Subscriber Identity Module (USIM)

(GR No. GR/WS/SIM-003/02 JAN.2010)

Chapter -1

Introduction

1.0 Scope

This generic requirement relates to the UICC based Universal Subscriber Identity Module application, called 'USIM' complying to 3GPP Technical Specifications (Release 5) for use in Mobile Equipment (ME) in 3G Telecom Networks. The document covers briefly the role of USIM, its components, functions, physical characteristics, transmission protocols, application and file structure and security features.

1.1 Role of USIM

In UMTS/ 3G network, a Mobile Station (MS) is split into two parts, one containing the hardware and software specific to the radio interface and the other containing the subscriber specific data. This later part is called USIM. A UMTS Subscriber Identity module is a smart card, which holds all the information required to identify a particular subscription to a mobile service.

Each 3G subscriber is issued a USIM by the operator, which can be seen as the subscriber's "key" to the network. The USIM is inserted into the mobile terminal and the customer goes through a secure process in order to log onto the network.

The USIM shall be used with a 3G / GSM handset. USIM shall be compatible to work in 3G network with backward compatibility to work in 2G network. It shall allow the subscriber to carry with him all the special services, features and the telephone numbers.

USIM shall be a full sized smart card, with perforation to facilitate cutting to a format called "Plug in SIM".

Chapter -2

Functional Requirements of USIM

2.1 Components

2.1.1 Hardware Components

The USIM has CPU, ROM/Flash, RAM, EEPROM and Digital signature co-processor as integrated hardware components. Each of these components has a specific role to play.

2.1.1.1 Central Processing Unit (CPU)

The CPU is the “intelligence” of the chip and performs all the mathematical calculations and takes all the decisions required by the USIM.

2.1.1.2 Read Only Memory (ROM) / Flash Memory

The ROM/ Flash shall have a sufficient memory to store the operating system which is the set of commands that USIM understands. It shall include the GSM –‘Milenage’ algorithms as per 3GPP TS 35.206. The contents of the ROM shall be created as part of the silicon manufacturing process. They shall be permanent and it shall not be possible to change them.

2.1.1.3 Random Access Memory (RAM)

The RAM is an area of volatile memory and its contents are lost each time the power is turned off. It is used to store temporary system flags, to buffer incoming data and as a scratch pad for calculations. The memory of RAM shall be sufficient enough for the execution of application and basic functionality as per the ISO / 3GPP Limits and shall be at least 5KB for 128 KB USIM card and 8KB for 256 KB USIM

2.1.1.4 Electrically Erasable Programmable ROM (EEPROM) / Flash Memory

The EEPROM/ Flash memory stores all of the application data such as the Operator specific parameters (e.g. IMSI) and the subscriber data (e.g. Abbreviated Dialling Nos.). This information is retained even after the power is turned off and can be modified or erased using specific electrical signals.

The USIM shall be programmable for the features like Global Phone book (for 2G ME), Public Phone book (for 3G ME), Short Message Service (SMS), Fixed Dialling Number (FDN) etc. Optionally, USIM shall support dynamic memory management. The memory of the SIM cards shall be available in the option of 128/256 KB. Storing of browser either in ROM or in EEPROM for accessing USIM based applications shall not affect the memory required for application usage viz. 128/256KB.

The Global/ Public Phone book shall be able to store data in the fields viz. short name, additional number, E-mail ID and grouping information for phone book entries.

The Public Phone book capacity shall be minimum 500 and 1000 for 128 KB and 256 KB USIM respectively. The capacity of Global Phone book shall be as per GSM specifications.

2.1.1.5 Digital signature co-processor

The USIM shall have a digital co-processor, to enable Digital Signatures and Public Key Cryptography. The Cryptographic Engine shall support 1024 bit keys.

2.2 Software Components

The software components in USIM include Operating System, USIM Applications, USIM Tool Kit Applications, USIM Browser & its Applications, USIM Browser Plug-ins etc.

2.2.1 Operating System

Operating system is the set of commands that USIM understands. Operating System shall support JAVA Card 2.2 or higher version.

2.2.2 USIM Applications

USIM applications shall be provided as per 3GPP TS 31.102.

2.2.3 USIM Tool Kit Applications

The USIM shall provide a platform, as per 3GPP TS 31.111 for USIM Tool Kit Applications (USAT) for launching value added interactive services like Mobile banking, Tele-ticketing, Over the air modifications etc. as defined by the operator.

2.2.4 USIM Browser and its Applications

Provision shall be made in EEPROM Memory to accommodate Browser Menu and Services. It shall also be possible for the subscriber to use the handset browser as per his option. The USIM card shall provide a browsing mechanism to support the following:

- I. Interpreter for access to Internet Based Applications.
- II. Access to telephony functions from the Menu allowing Setup call, Send SMS, Send USSD, Launch WAP Browser etc.
- III. Support for OTA download of USIM toolkit applications & new plug-ins using SMS.
- IV. Browser should be USIM vendor Independent (i.e. same Browser must run on all SIM cards).
- V. Browser must be able to set-up an operator defined text, which will be displayed while the Browser is waiting for an application to respond.
- VI. Browser Menu Change Management up to 3 levels viz. Main menu, Sub menu, Sub-sub menu.
- VII. Browser must be able to execute a local Script.
- VIII. Dispatch of Terminal Profile.
- IX. Support for Unicode, so as to be able to display Devnagri on the phones that have Hindi/ Vernacular support.
- X. The browser shall be able to navigate through menus stored locally on the USIM as well as on backend application servers.
- XI. Browser should be able to support minimum 20 service sub-titles.
- XII. Browser must be able to permit local storage of subscriber specific confidential information, such as Credit card number, which the Browser can use in transactions in payment type sessions on multiple applications.
- XIII. The Browser must be able to execute scripts based on events such as location update, USIM file Update, etc.
- XIV. Browser must be able to display the text, defined by operator, continuously on screen until user presses a key.
- XV. Provide book marking feature
- XVI. Refresh menu or event list (after OTA update).
- XVII. Support for incremental variable.
- XVIII. Shall inform the user of the progress of the Browser's interaction with the OTA platform during the processing of a Browse request
- XIX. Shall support basic logic to enable development of advanced services that requires basic analysis of inputted data (comparison) and limited arithmetic (to calculate times, or values)

2.2.5 Browser Plug-ins

The Plug-ins are executables, stored on USIM ROM or EEPROM, which enhance the capabilities of browser. Following capabilities shall be supported:

- i) Support for Encryption, Decryption and Signing using Symmetric (DES) keys and Asymmetric Keys (RSA) for Digital Signatures in PKCS11 format shall be provided for USIM card.
- ii) Support for on board generation of a private and public 1024 bit key pair (RSA)
- iii) Dispatch of Cell Global Identity (CGI) as part of the Browser request.

2.3 Functions of USIM Card

The USIM shall be capable to perform the following functions within the 3G application:

- a) Access Control
- b) Customisation
- c) Service Personalisation
- d) Network Branding and Advertising
- e) Support for Bearer Independent Protocol

2.3.1 Access Control to the Network

The USIM application uses 2 PINs for user verification, PIN1 and PIN2. PIN2 is used only in the ADF. The PIN1 and PIN2 are mapped into key references as defined in TS 31.101 [11].

The USIM shall be secure to prevent unauthorised access to the network services involving:

i) Local access control

In the Local access control the identity of the cardholder being an authorised user is achieved through a PIN1 (Personal Identity Number) checking procedure without transmission on the radio interface. The subscriber presents to the USIM (via the handset) a four to eight digit No. which is known only to the subscriber. The USIM shall check the presented value against that, held in its secure memory. If the two are the same then it is assumed that the cardholder is the valid user and handset access is allowed.

ii) Network access control

Once the subscriber has proven his identity to the card, the second access control mechanism takes over. This is where the card proves to the 3G network that it is valid for use. It shall be as per the procedure defined in 3GPP TS 33.102.

2.3.2 Customisation

It shall be possible to customise the USIM for the services to be provided by the operator. USIM shall be capable of storing the following minimum inputs for customisation:

- International Mobile Subscriber Identity (IMSI)
- Integrated Circuit Card Identification (ICC id)
- Subscriber Authentication Key (K)
- Personal Identification Number-1 (PIN-1)
- Personal Identification Number-2 (PIN-2)
- PIN Unblocking Key-1 (PUK-1)
- PIN Unblocking Key-2 (PUK-2)
- Service Provider Name (SPN)

2.3.3 Service Personalisation

The USIM shall also act as a portable data storage device, which contains the subscriber related information such as Phone book, SMS and FDN, AoC, SMSC address etc, which can be updated over the air. USIM shall be able to support following:

- Electrical Personalisation: To authenticate the chip, it shall load the customised executable program and initialise the data in the files.
- Geographical card Personalisation: For printing card holder related data on the card body.

2.3.4 Network Branding and Advertising

For the purpose of advertising and network branding of 3G network, it shall be possible to print artwork containing operator's logo and other network related information on USIM card with high precision and quality. It shall be possible to accommodate any change in the artwork design in the subsequent batch of USIM cards.

To facilitate Mobile Advertising, SIM shall support the following

- i) Browser shall be able to setup the idle mode text after reading from a Browser file
- ii) The Browser file shall be over the air updateable
- iii) Shall be able to handle alerts from the phone for events such as
 - o Call Disconnect
 - o Call Connect
 - o Idle Mode Screen
- Upon arrival of such alerts, the Browser shall be able to
 - o Display a text stored in an over the air updateable Browser File
 - o Display a text and a set of Menus
- iv) Populate the handset screen with configurable messages, while the user is waiting for the Browser to send a request to the network
- v) Populate the handset screen with configurable messages, while the user is waiting for the Network to send back information to the Browser for a previously sent request
- vi) Receive Cell Broadcast messages, and send them to the SIM Browser, for the Cell Broadcast message to be displayed as a Browser Menu and/or Text

2.3.5 Support for 'Bearer Independent Protocol '

USIM shall be able to support 'Bearer Independent Protocol' as per 3GPP TS 31.111

Chapter -3

Technical Requirements

3.1 Physical Characteristics

USIM shall support the following physical types:

- ID-1 USIM
- Plug-in USIM

The physical characteristics of both types of USIM shall be in accordance with ISO 7816-1, 2. The following additional requirements shall be applied to ensure proper operation in the 3G environment.

3.1.1 ID-1 USIM

The physical characteristics of the ID-1 UICC shall conform to ISO/IEC 7816-1, 2].

The Terminal shall accept embossed ID-1 UICCs (Universal Integrated Circuit Card). The embossing shall be in accordance with ISO/IEC 7811-1 and ISO/IEC 7811-3. The contacts of the ID-1 UICC shall be located on the front (embossed face, see ISO/IEC 7810 of the card).

a) Provision of contacts

i) Terminal

Contacting elements in the Terminal in positions C4 and C8 are optional, and are not used by a Telecom application complying to the present document. They shall present a high impedance to the UICC. If it is determined that the UICC is a multi-application UICC, then these contacts may be used. Contact C6 need not be provided for Plug-in cards.

ii) UICC

Contacts C4 and C8 need not be provided by the UICC. If provided, they shall not be connected internally in the UICC if the UICC only contains a Telecom application. Contact C6 shall not be bonded in the UICC for any function other than supplying Vpp.

3.1.2 Plug-in USIM

The Plug-in USIM shall have a width of 25 mm, a height of 15 mm, and thickness 0.76 mm same as ID-1 USIM and a feature for orientation.

3.2 USIM card body material

The card body shall be made of Acrylo Butadiene Nitril Styrene (ABS) plastic material / Poly Vinyl Chloride (PVC) and shall be fully compliant to 3GPP TS 31.101, with quality standards stipulated by ISO.

3.3 Physical resistance of USIM

3.3.1 Electrostatic overload

The chips used in USIM shall comply with MIL STD 883C technical specifications and shall accept Class Three electrostatic overload (threshold > 4000 volts).

3.4 Environmental Conditions

The USIM shall be fully compliant with 3GPP TS 31.101 specifications in terms of temperature and humidity resistance. The temperature range for full operational use shall be between -25° C and +70° C with occasional peaks of up to +85° C (not more than 4 hours each time and not over 100 times during the life time of the card).

USIM shall comply with QM-333 for Damp Heat Study State Cycle (55° C at 95% relative humidity).

3.5 Contact pressure

The contact pressure shall be large enough to ensure reliable and continuous contact. The radius of any curvature of the contacting elements shall be greater than or equal to 0.8 mm over the contact area. Under no circumstances, the contact force shall be greater than 0.5 N per contact.

3.6 Electrical Specifications

Electrical specifications shall comply with clause 5 of 3GPP TS 31.101

3.7 Supply Voltage

The USIM shall be capable to operate at 1.8V and 3V. It shall support 1.8V and 3V mobile equipment.

Symbol	Minimum	Maximum	Unit	Class
V _{cc}	4,5	5,5	V	A
V _{cc}	2,7	3,3	V	B
V _{cc}	1,62	1,98	V	C
NOTE: Class A, B and C values are according to ISO/IEC 7816-3 It is possible to support a range of classes. The support shall be consecutive e.g. AB, BC. A combination like AC is not allowed..				

3.8 Clock

The USIM shall support clock rate of 1 to 5 MHz from Mobile Equipment with the restriction of 4MHz shall be the maximum clock speed specified for SIMs for 3V and below..

3.9 Baud Rate

The minimum baud rate for all communication shall be 9600 bps.

3.10 Transmission Protocols

The transmission protocols used to exchange data between ME and USIM shall be as per 3GPP TS 31.101.

3.11 Application and File structure

The application and logical structure of files in USIM and the code associated with them shall be in accordance with 3GPP TS 31.101 and 3GPP TS 31.102. The various files in USIM like Master file, Elementary file and dedicated files are organised in a hierarchical structure (figure-1). These files may be either administrative or application specific.

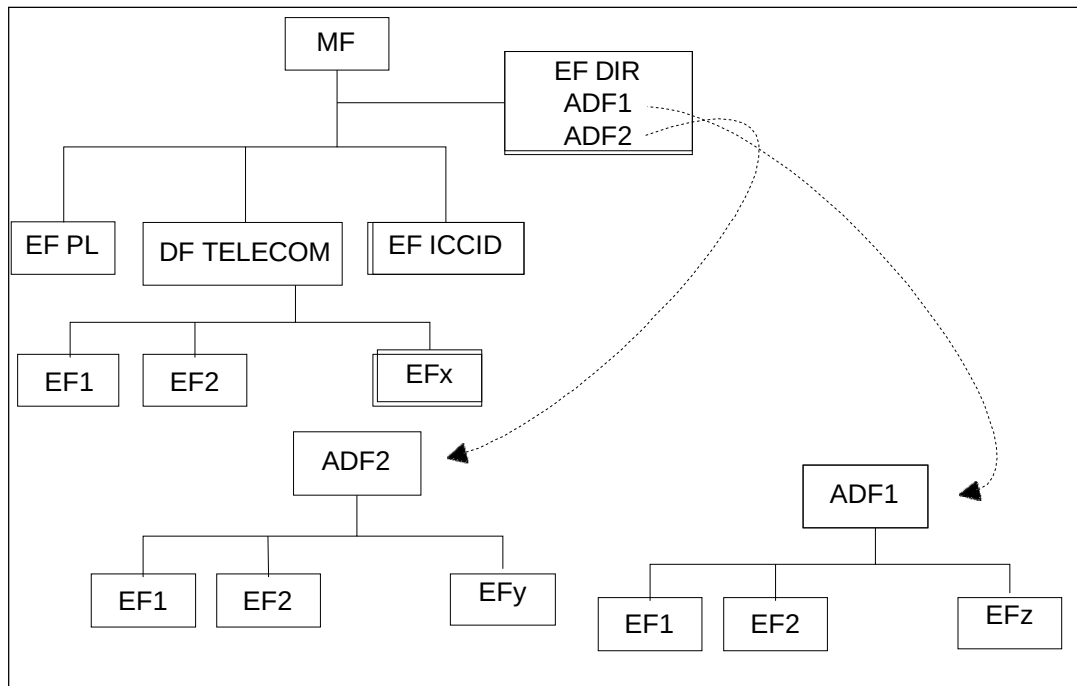


Figure-1

Master File (MF): This is the unique mandatory file containing access conditions and optionally DFs and/or EFs

Dedicated File DF (DF1, DF2 --- DF_n) : A dedicated file (DF) allows for functional grouping of files. It can be parent of DFs and/or EFs. DFs are referenced by file identifiers.

An application DF (ADF) is a particular DF that contains all the DFs and EFs of an application.

Elementary File EF (EF1, EF2,---EF_n) : Elementary file is one which contains access conditions and data and no other file.

3.11.1 The file ID shall be assigned at the time of creation of the file concerned. No two files under the same parent shall have same ID.

3.11.2 All the important parameter like ICCID, IMSI, PIN, PUK etc. are stored in the EEPROM inside the USIM in the form of files. The coding and identity of the files shall be as defined in the 3GPP TS 31.102. Further these files are stored in directories as specified in 31.102 as follows:

- **ROOT Directory:** In this directory ICCID, PL and DIR elementary files are stored.
- **GSM Directory:** In this directory files like Kc, Kc GPRS, CPBCCH etc. are stored.
- **Telecom Directory:** Files like Phonebook, FDN, E-mail etc. are stored in this directory.

3.11.3 The status of various files in Root directory, GSM directory and Telecom directory shall be as per 3GPP TS 31.102. In addition, the provision of following files shall be mandatory:

- Cell Broadcast Message Identifier Selection (CBMI) – 6F45
- Cell Broadcast Message Identifier for Data download – 6F48
- GPRS Location Information – 6F53 EF_{LOCIGPRS}
- GPRS Ciphering Key – EF_{KCGPRS}

- Short Message Status – 6F43
- Short Message Parameter – 6F42
- Short Messages – 6F3C
- Cell Broadcast Message Identifier Range (CBMIR)- 6F50
- Enhanced Multilevel Precedence & Preemption(EMLPP) - 6FB5
- Automatic Answer for EMLPP service- 6FB6

3.11.4 . The following standard GSM files shall be configured as OTA updateable:

- Abbreviated Dialing Numbers, ADN
- Fixed Dialing Numbers, FDN
- Service Dialing Numbers, SDN
- MSISDN
- Service Provider Name, SPN
- Extension files, EXTn
- Barred Dialing Number, BDN
- Short message service Parameter, SMSP
- Language Preference, LP
- Location Information, LOCI
- PLMN Selector, PLMNsel
- HPLMN search period, HPLMN
- SIM Services Table, SST
- Accumulated Call Meter, ACM
- ACM maximum value , ACMmax
- Price per Unit and Currency Table, PUCT
- Group Identifier Level 1 and 2, GID1 and GID2
- CBMI Selection, CBMI
- Cell Broadcast Message Identifier for Data Download, CBMID
- Cell Broadcast Message Identifier Range selection, CBMIR
- Access Control Class, ACC
- Forbidden PLMN, FPLMN
- Emergency Call Codes, ECC
- GPRS Location Information, GPRSLOCI
- Operator controlled PLMN Selector with Access Technology, OPLMNwAcT
- HPLMN Selector with access technology, HPLMNwAcT
- Last Used Access Technology, RPLMNwAcT
- Higher Priority PLMN search period, HPPLMN
- Image Instance Data Files, IIDF
- Image , IMG

Other than the above, such files as required by the SIM Browser, shall also be Over the Air updateable.

3.12 Security Features

USIM shall be provided with adequate security features to protect data and authenticity for their entire life. The security features shall be in conformity with 3GPP TS 33.102, TS 33.103 & 3GPP TS 35.206 and shall ensure the following:

- authentication of the USIM to the network;
- authentication of the network to the USIM;
- authentication of the user to the USIM;
- data confidentiality over the radio interface;

- file access conditions;
- conversion functions to derive GSM parameters.

3.13 Authentication and Key agreement procedure

The authentication mechanism and cipher & integrity key generation which are invoked by the network shall be as per 3GPP TS 33.102.

The mechanism achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the Authentication centre (AuC) in the user's Home Environment (HE). In addition, the USIM and the HE keep track of counters Sequence Number (SQN_{MS}) and SQN_{HE} respectively to support network authentication. SQN_{HE} is a counter in the HLR/AuC, individual for each user and SQN_{MS} denotes the highest sequence number the USIM has ever accepted.

When the SN (Serving Network)/VLR initiates an authentication and key agreement, it selects the next authentication vector and sends the parameters RAND (Random Challenge) and AUTN (authentication token) to the user. Each authentication token consists of the following components: a sequence number SQN, an Authentication Management Field (AMF) and a message authentication code MAC (Message Authentication Code) over the RAND, SQN and AMF.

The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the SN/VLR. The SN/VLR compares the received RES with XRES. If they match the SN/VLR considers the authentication and key agreement exchange to be successfully completed. The USIM also computes CK and IK. The established keys CK and IK will be used by the ME to perform ciphering and integrity functions.

A permanent secret key K is used in this procedure. This key K has a length of 128 bits and is stored within the USIM for use in the algorithms. Also more than one secret key K can be stored in the USIM. The active key to be used by the algorithms is signalled within the AMF field in the AUTN.

The card security shall be based on two types of authentication

- Passive Authentication
- Active Authentication

3.13.1 Passive Authentication

The USIM shall support seven passive authentication passwords, which consist of two user's secret code called PINs & three Administrative Secret Codes (ADM). User secret codes shall have their own unblocking secret codes called PUK (PIN unblocking key) as per 3GPP/GSM standards. Passwords shall be initialised at the USIM vendor's personalisation centre according to operator's needs. Access conditions, which define type of authentication conditions, required to access various files use passive authentication.

3.13.2 Active Authentication

It shall provide total transparent means for verification that both the card and the network have the same secret key. There shall be two types of active authentication:

- Internal authentication which verify the genuineness of the card registered in the network.
- External authentication ensures that an application has the right of access to certain highly sensitive files.

3.14 Transportation password generation

The transport of output files (which contains K, IMSI, ICC-id etc.) from USIM vendor to operator shall be protected by transport keys, as finalised mutually between the operator & the USIM vendor.

3.15 Network Security

The USIM shall provide features required for authenticating itself to the 3G network and generating the keys used to cipher the calls. These features shall comprise of certain keys and algorithms as per the procedure at 2.3.1 (ii)

3.15.1 Algorithms and processes

USIM shall support GSM – ‘Milenage’ algorithms as per 3GPP TS 35.206. The procedure for authentication shall be as per 3GPP 33.102.

3.16 Additional security features

Additional security features that shall be available in the USIM are described below:

- Additional Elementary files (EF) created inside the card shall be managed as per 3GPP31.102 recommendations. As security policy depends on 3G operator needs, three states shall be made available for accessing data from the external world:
 - Under no condition
 - Under secret code control (PIN code, or administrative secret code)
 - Never (EF locked)
- Unique serial number (ICCID) to avoid card cloning.
- “Inhibition systems” to prevent any power value out of range of the specification: Clock frequency, power supply value.
- Manufacturing diversified secret code to be presented before any EEPROM allocation.
- Read/Update access to EEPROM 100% controlled by ROM software and issuer application.

3.17 Application Security Keys

The following additional 8 bit DES Symmetric keys and 1024 bit Asymmetric Key generated as random key shall be provided both on 128 and 256 KB USIM.

- 4 ADM Keys
- 16 Application keys
- 2 OTA keys (KIC & KID)
-

An additional private 1024 bit Asymmetric Key generated as random key shall be provided on each of the USIM card; For cards using strong encryption (1024 bit RSA) the key pair should be generated by the On-board key generation plug-in. The private key should after generation be stored safely and should never be readable. The public key should be available for upload using a wml call to the plug-in.

3.18 GSM conversion Function

To gain GSM access, the USIM shall be able to provide the conversion functions c2 and c3 required to derive GSM parameters (SRES, cipher key Kc) from available 3G parameters.

3.19 Anti tear mechanism

Card shall have anti tear mechanism to prevent USIM data damage during accidental voltage cut- off (battery failures, battery pull - out without switch - off etc.)

3.20 OTA capabilities of USIM

USIM shall provide an Over the Air downloading mechanism for Remote File Management and Remote Applet Management compliant to 3GPP TS 23.048.

3.21 : Compliance to THE INFORMATION TECHNOLOGY ACT, 2000 and RBI guidelines:

a. The SIM card shall comply to the “IT Act 2000” in respect to asymmetric crypto system (system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature) , Secure electronic record , Secure digital signature and other relevant clauses.

b. For Mobile banking transactions, the SIM card shall comply to “Mobile Banking transactions in India - Operative Guidelines for Banks” Oct 2008, as amended from time to time

Chapter 4

Guidelines to the Purchaser.

- 4.1 Option for Digital Signature Co-processor in 128/256 KB USIM to be decided at the time of procurement as the extra hardware involves appreciable cost. In addition, software license shall be required from the certifying authority.
- 4.2 Clause 2.1.1, 2.1.1.2, 2.1.1.4: The tendering authority may decide the requirement of ROM or Flash Memory at the time of purchase depending upon the suitability and availability of the product.
- 4.3 Clause 2.1.1.4 EEPROM: Phonebook capacity of 500/1000 to be defined at the time of actual procurement subject to availability of handset supporting the same.
- 4.4 Clause 2.2.4 USIM browser & its applications: Purchaser to ensure the compatibility of browser in USIM & 3G OTA platform at the time of actual procurement. 'USAT' browser defined by 3GPP has not been widely implemented, therefore, commercial availability of the browser shall be ensured.
- 4.5 Clause 3.17 Application Security Keys: Purchaser can specify the actual requirement of security keys at the time of procurement.

Abbreviations

ABS	Acrylo Butadiene Nitryl Styrene
ACM	Accumulated Call Meter
ADF	Application Dedicated File
ADN	Abbreviated Dialling Number
ADM	Access condition to an EF which is under the control of the authority which creates this file
AMF	Authentication Management Field
AoC	Advice of charge
AuC	Authentication Centre
AUTN	Authentication Token
CBMI	Cell Broadcast Message Identifier Selection
CBMIR	Cell Broadcast Message Identifier Range
CGI	Cell Global Identity
CK	Ciphering Key
CPBCCH	Compact Packet BCCH
DES	Digital Encryption Standard.
DF	Dedicated File
EEPROM	Electrically Erasable Programmable ROM
EF	Elementary File
EMLPP	Enhanced Multilevel Precedence & Pre-emption
ETSI	European Telecommunications Standards Institute
FDN	Fixed Dialling Number
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HE	Home Environment
HLR	Home Location Register
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ID	Identifier
IEC	International Electro-technical Commission
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
ISO	International organisation for standardization
Kc	Cryptographic key; used by the cipher A5
Ki	Subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, cipher key generator, A8
MAC	Message Authentication Code
ME	Mobile Equipment
MF	Master File
MS	Mobile Station
MSISDN	Mobile Subscriber ISDN number
OTA	Over The Air
PIN	Personal Identification Number
PL	Preferential Language
PLMN	Public Land Mobile Network
PKCS	Public Key Cryptography Standard

PUK	PIN Unblocking Key
PVC	Poly Vinyl Chloride
RAM	Random Access Memory
RAND	A Random challenge issued by the network
RES	Response
ROM	Read Only Memory
SMS	Short Message Service
SMSC	Short Message Service Centre
SN	Serving Network
SPN	Service Provider Name
SRES	Signed Response calculated by a USIM
SQN	Sequential Number
UNBLOCK- - CHV1/2	Value to unblock Card Holder Verification1/2
UICC	Universal Integrated Chip Card
URL	Uniform Resource Locator
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
VLR	Visited Location Register
WAP	Wireless Application Protocol
XRES	Expected Response

- End of document-