SPECIFICATION FOR 4G USIMs

No. : BSNL/Specification/USIM- 001/06 April 2017

BHARAT SANCHAR NIGAM LIMITED
(A Government of India Enterprise),
Bharat Sanchar Bhawan, Janpath,
Website: www.bsnl.co.in
NEW DELHI – 110 001, **INDIA**

Contents

CHAPTER-1

1 Introduction

This document relates to the LTE Universal Subscriber Identity Module (USIM) application based on UICC platform, complying with 3GPP Technical Specifications (Release 8 or above) for use in 3G or VoLTE Mobile Equipment (ME) in UMTS Telecom Networksas well as offers secure access to voice, basic data such as SMS and a host of operator value added services (VAS) and applications. The document covers briefly the role of USIM, its components, functions, physical characteristics, transmission protocols, application and file structure and security features.

2 Description

In UMTS network, a Mobile Equipment (ME) 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 4G subscriber is issued a LTE USIM by the operator, which can be seen as the subscriber's "key" to the network. The LTE USIM is inserted into the mobile terminal and the customer goes through a secure process in order to log onto the network.

The LTE USIM shall be used with a 2G, 3G and VoLTE handset. LTE USIM shall be compatible to work in 4G networks with backward compatibility to work in 3G and 2G network. It shall allow the subscriber to carry with him all the special services, features and the telephone numbers.

3 Functional/Operational Requirements

3.1 Components

3.1.1 Hardware Components

The USIM has CPU, ROM, RAM, and Non Volatile Memory (NVM)or may have Digital signature co-processor as integrated hardware components. Each of these components has a specific role to play.

3.1.2 Central Processing Unit (CPU)

The CPU is the "intelligence" of the chip and performs all the data processing and mathematical calculations and takes all the decisions required by the USIM.

3.1.3 Read Only Memory (ROM) /Flash memory

The ROM shall have a sufficient memory to store the operating system which is the set of commands that USIM understands. It shall include the 3G 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.

In such case of flash, the area reserved for operating system shall have the same behavior as ROM (Write once read many)

3.1.4 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 card.

3.1.5 Non Volatile Memory (NVM)

The Non Volatile Memory stores all of the application data such as the Operator specific parameters (e.g. IMSI) and the subscriber data (e.g. Abbreviated Dialing Nos.). This information is retained even after the power is turned off and can be modified or erased using silicon specific procedure.

3.1.6 Digital signature co-processor (Optional)

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

3.2 Software Components

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

3.2.1 Operating System

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

3.2.2 USIM Applications

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

3.2.3 USIM Tool Kit Applications

The USIM shall provide a platform, as per 3GPP TS 31.111 for USIM Tool Kit Applications (USAT) and 3GPP TS 31.133 forIP Multimedia Services Identity Module (ISIM) Application Programming Interface (API) for launching value added interactive services like Mobile banking, Tele-ticketing, over the air modifications etc. as defined by the operator. Any VAS application shall be as per the requirement

3.3 Functions of USIM Card

The LTE USIM shall be capable to perform the following functions within the 4G application:

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

The LTE 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.

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

3.3.1 Local access control

In the Local access control the identity of the cardholder being an authorized user is achieved through a PIN1 (Personal Identity Number) checking procedure without transmission on the radio interface. The subscriber presents to the LTE USIM (via the handset) a four to eight digit No. which is known only to the subscriber. The LTE 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.

3.3.2 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 4G network that it is valid for use. It shall be as per the procedure defined in 3GPP TS 33.102 and 3GPP TS 31.103.

3.3.3 Customization

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

- International Mobile Subscriber Identity (IMSI)
- IMS private user identity (IMPI)
- Home Network Domain Name (Domain)
- IMS public user identity (IMPU)
- P-CSCF Address (P-CSCF)
- 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)

3.3.4 Service Personalization

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

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

3.3.5 Network Branding and Advertising

For the purpose of advertising and network branding of 4G Mobile Network Operator (MNO); it shall be possible to print artwork containing MNO logo and other network related information on LTE-USIM card with high precision and quality. It shall be possible to accommodate any change in the artwork design in the subsequent batch of LTE-USIM cards.

3.3.6 Support for 'Bearer Independent Protocol '

USIM shall be able to support 'Bearer Independent Protocol' as per ETSI TS 102 223

4 Technical Requirements

4.1 Physical characteristics

4.1.1 USIM Form factors

USIM shall support one of the following form factors:

- 2FF Plug-in UICC
- 3FF Micro UICC
- 4FF Nano UICC

1) 2FF Plug-in UICC:

   The Plug-in UICC shall have a width of 25 mm, a height of 15 mm, and thickness 00.76 mm same as ID-1 UICC and a feature for orientation.

2) 3FF Mini UICC

   The Mini UICC shall have a width of 15 mm, a height of 12 mm, and thickness of 00.76 mm same as ID-1 UICC and a feature of orientation

3) 4FF Nano UICC

   The 4FF shall have a width of 12.3 mm ± 0.1 mm and a height of 8,8 mm ± 0,1 mm, with a thickness range of 0.67 mm + 0.03 mm/-0.07 mm.

All of the above form factors shall comply with ETSI TS 102 221 V11.1.0

4.1.2 USIM card body material (requirements have detailed as below)

The card body shall be made of any material fulfilling the following requirements as defined in ISO-7810

- Bending stiffness
- Flammability
- Toxicity
- Resistance to chemicals
- Light
- Durability
- Peel strength
- Adhesion or blocking

Note: The parameters (1) Bending stiffness and (7) Peel strength above shall not be applicable for half card and quarter card.

In addition to the above card body shall be compliant the following

1) The standard temperature range for storage and full operational use shall be between -25 °C and +85 °C as per ETSI TS 102.221. The structural reliability shall remain in compliance for dimensions and warpage after exposure to the relative humidity of 5 % to 95 % as per ISO 7810.

2) The contact pressure shall be large enough to ensure reliable and continuous contact (e.g. to overcome oxidization and to prevent interruption caused by vibration). 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 shall the contact force exceed 0.5 N per contact.

4.1.3 Electrostatic overload

The card shall not be damaged in normal use by a person charged with static electricity.The performance of the card shall not be degraded by exposure to a static discharge in accordance with the test methods described in ISO/IEC 10373-3.

4.1.4 Supply Voltage

The specifications relating to following as defined in 3GPP TS 31.101 (Rel.8 and above) shall be complied with:

- Class A Operating conditions
- Class B Operating conditions
- Class C Operating condition

USIM shall support at least two consecutive classes as defined in 3GPP TS 31.101, e.g. AB or BC.

4.2 Pin Assignment:

- C1 : Vcc
- C5 : Gnd
- C2 : Reset
- C6 : Vpp
- C3 : Clock
- C7 : I/O
- C4 : RFU
- C8 : RFU

4.2.1 Provision of contacts

ME:Contacting elements in the ME in positions C4 and C8 are optional, and are not used in the GSM application. They shall present high impedance to the LTE-USIM card in the GSM application. If it is determined that the SIM is a multi-application ICC, then these contacts may be used. Contact C6 need not be provided for Plug-in UICC,Mini UICC and Nano UICC.

USIM:Contacts C4 and C8 need not be provided by the USIM, but if they are provided, then they shall not be connected internally in the USIM if the USIM only contains the GSM application. Contact C6 shall not be bonded in the USIM for any function other than supplying Vpp.

4.2.2 Clock

The USIM shall support the clock frequencies as specified in 3GPP TS 31.101 (Rel.8 or above)

4.2.3 Transmission Protocols

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

4.2.4 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, 3GPP TS 31.102 and 3GPP TS 31.103 (Rel.8 and above). The various files in LTE-USIM like Master file, Elementary file and dedicated files are organized in a hierarchical structure (figure-1). These files may be either administrative or application specific.

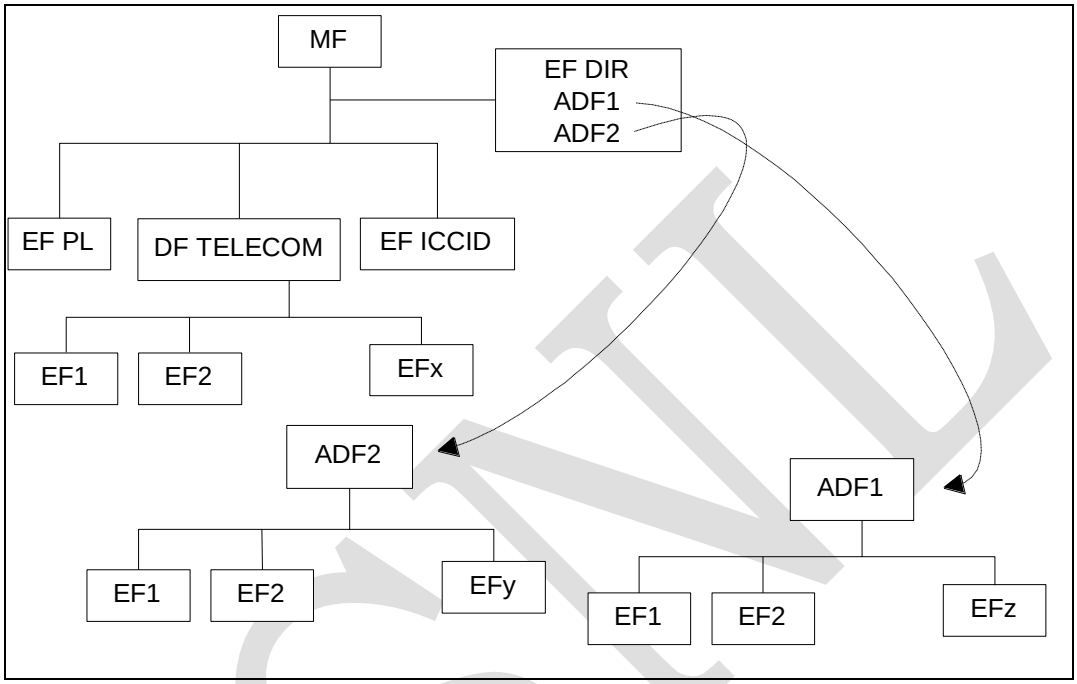

Figure-1

- Master File (MF): This is the unique mandatory file containing access conditions and optionally DFs and/or EFs
- Dedicated File DF (DF1, DF2 ----DFn): 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, ---EFn): Elementary file is one which contains access conditions and data and no other file.

a) 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.

All the important parameter like ICCID, IMSI, IMPI, IMPU, DOMAIN, p-CSCF, PIN, PUK etc. are stored in the EEPROM inside the LTE-USIM in the form of files. The coding and identity of the files shall be as defined in the 3GPP TS 31.102 and 3GPP TS 31.103(Rel.8 and above). Further these files are stored in directories as specified in 31.102 and 3GPP TS 31.103(Rel.8 and above) as follows:

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

- ISIM Directory: In this directory files like IMPI, IMPU, Domain, p-CSCF etc. are stored.
- EAP Directory: In this directory files like EAP-SIM, EAP-AKA are stored.

b) The status of various files in Root directory, GSM directory, Telecom directory, Advance USIM directory, Advance ISIM directory, Advance EAP directory shall be as per 3GPP TS 31.102 and 3GPP TS 31.103 and ETSI TS 102 310 v9.0.0. 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(25 number) – 6F3C
- Cell Broadcast Message Identifier Range (CBMIR)- 6F50
- Enhanced Multilevel Precedence & Preemption(EMLPP) - 6FB5
- Automatic Answer for EMLPP service- 6FB6
- Global Phone Book(250 Entries with two alternate number and one e-Mail Address)

4.3 Card life cycle management

Card life cycle management shall be compliant to Global Platform Specifications version 2.1.1 or higher.

5 Security Features

LTE 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, 3GPP TS 33.103 & 3GPPTS 35.206 and shall ensure the following:

- authentication of the LTE USIM to the network;
- authentication of the network to the LTE USIM;
- authentication of the user to the LTE USIM;
- data confidentiality over the radio interface;
- file access conditions;
- Conversion functions to derive GSM parameters.

5.1 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 and 3GPP TS 33.103.

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 LTE-USIM and the Authentication center (AuC) in the user's Home Environment (HE). In addition, the LTE-USIM and the HE keep track of counters Sequence Number (SQNMS) and SQNHE respectively to support network authentication. SQNHE is a counter in the HLR/AuC/IMS, individual for each user and SQNMS 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 LTE-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 directory and ISIM directory 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 signaled within the AMF field in the AUTN.

The card security shall be based on two types of authentication

- Passive Authentication
- Active Authentication

5.1.1 Passive Authentication

The USIM shall support seven passive authentication passwords, which consist of 'two user's secret codes' 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 initialized at the USIM vendor's personalization Centre according to operator's needs. Access conditions, which define type of authentication conditions, required to access various files, use passive authentication.

5.1.2 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 authentications which verify the genuineness of the card registered in the network.
- External authentication which uses relevant data of an application on SIM for verification by an external server for example PIN verification for m-banking application and authentication by OTA server etc.

5.1.3 Transportation password generation

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

5.1.4 Network Security

The LTE-USIM shall provide features required for authenticating itself to the 4G network and generating the keys used to cipher the calls. These features shall comprise of certain keys and algorithms as per the procedure at Clause 5.1

5.1.5 Algorithms and processes

LTE-USIM shall support 'Milenage' algorithms in 4G,3G and 2G mode as per 3GPP TS 35.206. The procedure for authentication shall be as per 3GPP TS 33.102 and 3GPP TS 33.103.

5.1.6 GSM conversion Function

To gain GSM access, the LTE-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.

5.1.7 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 3GPP TS 31.102 and 3GPP TS 31.103 recommendations. As security policy depends on 4G 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 (ICC-ID) 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 NVM allocation.
- Read/Update access to NVM controlled by Operating System and issuer application.

5.1.8 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 LTE-USIM.

- 3 ADM Keys
- 8 Application keys
- 2 OTA keys (KIC & KID)

The Asymmetric private key in PKCS 15 format and the URL (Uniform Resource Locator) for the Public Key Certificate must be stored securely on the LTE-USIM card, while the corresponding Public Key shall be stored on the Public repository and URL shall point to the Public Key.

5.2 EPS network Authentication

For authenticating with LTE network the UISM shall include the LTE specific files as specified in the Release 8 of the 3GPP 31.102 specification. The USIM files system supports:

- EMM parameters storage,
- EPS Location Information

The recommendation is to use a Release 8 USIM to store EPS security context instead of ME storage. UICC keeps security context, allows fast reconnection to LTE network and avoid regular or systematic key derivation. The TS 31.102 Release 8 and TS 33.401 specifications describe a new set of files dedicated for LTE authentication.

LTE Authentication with a LTE USIM

i. The N°85 service in USIM service table shall be enabled to indicate the support to E-UTRAN security context.

ii. The ADF USIM shall contain EF EPSNSC.

iii. The EF EPSLOCI file shall be supported.

iv. EPS AKA authentication shall be supported as defined in 3GPP TS33.401.

v. The card shall support the security algorithms to be executed shall use the keys derived from the key (KASME) generated using EPS-AKA. The lifetimes of the generated keys are defined in 3GPP TS 33.402.

6 Government of India Application frame work

6.1 Java Application

USIM shall reserve minimum 32K of Non Volatile Memory (NVM) space that will be used for uploading Government specific applications like; Disaster management system, social welfare system for health and safety etc.

6.2 Cell Broadcast Services

The UICC based ISIM shall have capability for card configuration for files SST, CBMID & CBMIR as per 3GPP TS 51.011. The configuration details shall be provided as part of personalization profile or shall be done via OTA. These configurations are mandatory in order to receive cell broadcast messages by UICC based ISIM.

Memory required for this application shall be part of the allocated memory as mentioned in Clause 6.1.

UICC based ISIM shall have an application to process and display the received cell broadcast message. The application shall have capability to permanently enable one or more CB channel for Govt. Broadcast messages as per instructions of Govt. of India from time to time.

6.3 Supplementary Secure Domain

USIM shall support special SSD (Supplementary Secure Domain) for Government of India compliant to Global Platform Specifications of SIM Alliance Forum version 2.1.1 or higher.

7. OTA capabilities of LTE-USIM

LTE will multiply the range of services offered to end users and will therefore also increase the number of applications on the UICC that require OTA administration.

LTE introduces an all-IP environment suitable for OTA exchanges for administration between the UICC and Server which can be done through HTTP (as it is described in Global Platform 2.2 Amendment B: “Remote Application Management over HTTP”). Each card acts as an HTTP client and the OTA platform as an HTTP server.

The OTA over HTTPS process starts by sending a PUSH SMS embedding the OTA server connection data. This information is needed by the UICC to open a BIP channel and then a TCP/IP connection with the OTA.

LTE provides a high potential of OTA applications in line with the new expectations of subscribers:

1. Automatic and immediate access to LTE voice and multimedia services (ISIM personalization with end user public identities)
2. Access (IMS subscription) and
3. Traffic preferences and Remote applet and file management
4. Remote applet and file management
   - The UICC shall support ETSI TS 102 225 and ETSI TS 102 226 Release 9.

- The UICC shall support OTA exchanges for administration between the UICC and Server through HTTP. The UICC shall act as a HTTP client and the OTA platform as an HTTP server.
- The UICC shall support Bearer Independent Protocol (BIP) for OTA as per ETSI TS 102 223.
- The UICC shall support GP_2.2 AMD B over HTTP v 1.1.1
- The UICC must support the AES algorithm for OTA security
- SMS and HTTP security must be with SPI 0x16 for all applications
- MSL defined for applets shall be mapped to security used for the HTTP session
- KIC, KID and all other security keys shall protected on the card

8. GENERIC BOOTSTRAPPING ARCHITECTURE (GBA)

Generic Bootstrapping Architecture (GBA) benefits users by authenticating them across several services by utilizing their valid user identity. This valid identity shall be also located in the Home Location Register (HLR) or a Home Subscriber Server (HSS), both in the MNO's infrastructure. In this way, operators can benefit by acting as an identity or authorization verifier to service providers over the internet or over IMS.

The user authentication is achieved by AKA authentication, i.e. a shared secret between the smart card inside the mobile phone and the HLR/HSS, by making a network component challenge to the SIM card and verifying that the answer is identical to the one expected by the HLR/HSS.

9. Extended Authentication Protocol (EAP)

EAP (Extensible Authentication Protocol) is a framework for transporting authentication protocols suitable for identifying mobile subscribers over IP networks (ADSL and Wi-Fi).

The peer is composed of several components:

- The UICC EAP Framework provides information to the terminal about the existing UICC applications that provide UICC EAP clients.
- A UICC application provides one or more UICC EAP clients.
- A UICC EAP client implements one specific EAP method.

The LTE USIM shall have configuration to support EAP. Following standards may be referred for the implementation of EAP;

The ETSI TS 102 310 v9.0.0 specifications document defines additional features that shall be provided by the UICC to support EAP authentication capabilities.

The UICC shall provide support for different EAP methods, ensuring interoperability between the UICC and any terminal, independent of their respective manufacturers.

EAP AKA shall be implemented according to 3GPPTS 33.234.

CHAPTER-2

Information for the procurer of product

Annexure for Guidelines to the BSNL CO/BSNL field units.

1) Option for Digital Signature Co-processor in 128/256 KB LTE-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.
2) Clause 3.2.3 – The requirement of VAS application/s shall be specified by the tendering authority at the time of procurement.
3) Clause 5.1.8 Application Security Keys: Purchaser can specify the actual requirement of security keys at the time of procurement.

ABBREVIATIONS

Abbreviation	*Expanded Form*
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
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
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	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 the document ========