Indian Telecommunication Security Assurance Requirements (ITSAR)

Pluggable (U)ICC (SIM, USIM and other (U)ICC based applications/applets)

Release Date :

Version : 1.0.0

Enforcement Date :

Security Assurance Standards Facility
National Centre For Communication Security
Department of Telecommunications, Bengaluru-560027

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. Security Assurance Standards (SAS) division of NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Disclaimer: This document purely focusses on the security related technical requirements of Pluggable (U)ICC. The regulations regarding Remote Access and card personalization are not part of this ITSAR.

Document History

Sl. No	ITSAR Reference	Title	Remarks
1			

Contents

A) Overview:

This document defines the security requirements of pluggable 2G/3G/4G (U)ICC based SIM/(U)(I)SIM/applications which are issued to subscriber by licensed telecommunication service provider (TSP) in India. The common public term this as 'SIM'. The (U)ICC is the entity that contains the identity of the subscriber; when placed in a Mobile Equipment (ME)/Terminal, together they become a Mobile Station (MS) or User Equipment (UE), as the case may be, which may then register onto a mobile network. In this document, (U)ICC refers to the secure hardware and the one or more applications running on the (U)ICC platform like SIM, USIM, ISIM and any applets.

As an agent of mobile network operator, (U)ICC provides a mechanism through which subscriber and network can authenticate each other (unilateral authentication in the case of GSM). It can store applications and subscriber related information securely. Portability is the one of the important characteristics of the (U)ICC card.

The objective of this document is to present a comprehensive, Country specific security requirements for the (U)ICC card. There are various International standardization bodies/associations working on the security aspects, relevant to the (U)ICC card. 3GPP, ETSI, GSMA, CC, Global Platform, SIM Alliance(Trusted Connectivity Alliance), ISO/IEC are few among them. The specifications produced by these bodies along with the country specific security requirements are the basis for this document.

This document starts with a brief introduction of (U)ICC platforms and recommends common security requirements of various pluggable (U)ICC platforms, specific security requirements of Hardware, OS & components of (U)SIM, Network security, (U)SIM application related security and the support for special applications that are mandated by Govt of India.

B) Scope:

This document is neutral to removable (U)ICC of various form factors (not embedded -eUICC or eSIM and integrated – iUICC) and applicable to native OS & Java Card platform which are being used in the Indian cellular networks. It also excludes card based NFC. This document does not cover extensively the security requirements at production facility, operator facility and organization's security policy. The requirements specified here are binding both on operators and (U)ICC manufacturers.

C) References:

1. ISO/IEC 7816-4 Inter Industry commands for Interchange.
2. ISO/IEC 7816-8 Security related Inter Industry commands.
3. ISO/IEC 7816-9 Additional inter industry commands and security attributes.
4. 3G TS 21.111, USIM and IC card requirements.
5. 3G TS 22.038, USIM/SIM Application Toolkit. (USAT, SAT)
6. 3G TS 23.048, Security Mechanisms for the (U)SIM Application Toolkit; Stage 2
7. 3G TS 31.101: "UICC - Terminal interface; Physical and logical characteristics".
   3G TS 31.102: "Characteristics of the USIM Application".
8. 3G TS 31.111: "USIM Application Toolkit".
9. 3G TS 31.900, SIM/USIM Internal and External Interworking Aspects.
10. 3GPP TS 42.017 V 4.0.0 Subscriber Identity Modules (Functional Characteristics) R4.
11. 3GPP TS 51.011 Specification of the (SIM – ME) interface.
12. ETSI TS 102.221, Smart cards; UICC–Terminal interface.
13. ETSI TS 102.223, Smart Cards; Card Application Toolkit. (CAT)
14. ETSI TS 102.224 Smart Cards; Security mechanisms for the Card Application Toolkit.
15. ETSI TS 102.225 Smart Cards; Secured packet structure for UICC applications.
16. ETSI TS 102.226, Smart Cards; Remote APDU Structure for UICC based Applications.
17. ETSI TS 102.240, Smart Cards; UICC Application Programming Interface (UICC API)
18. ETSI TS 102.241, UICC API for Java Card.
19. ETSI TS 02.19 Subscriber Identity Module Application Programming Interface.
20. ETSI TS 03.48 GSM 03.48: "Security Mechanisms for the SIM application toolkit".

21. GSM 02.17 Subscriber Identity Module Functional characteristics.
22. GSM 02.48, Security Mechanisms for the SIM Application Toolkit; Stage 1.
23. GSM 03.19: "Subscriber Identify Module Application Programming Interface (SIM API); SIM API for Java Card; Stage 2.
24. GSM 11.11 Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface.
25. GSM 11.14 Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface.
26. Java Card Specifications version 3.0
27. Global Platform Specifications version 2.3.1
28. NIST FIPS 140-2 specification.
29. Generic Requirements No TEC/GR/WS/SIM-001/04 Nov 2015 SIM by TEC, DoT, GoI
30. Generic Requirements No GR/WS/SIM-003/02 Jan 2010 USIM by TEC, DoT, GoI
31. Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0

D) Definitions and Acronyms

D.1 Definitions

1. MTCTE: Mandatory Testing and Certification of Telecom Equipments. Department of Telecommunications, Ministry of Communications (the licensor) has notified “Indian Telegraph (Amendment) Rules” in Gazette of India vide G.S.R. 1131(E) PART XI" on 5th September 2017 which prescribes for Mandatory Testing and Certification of Telecommunication Equipment. Any telegraph which is used or capable of being used with any telegraph established, maintained or worked under the licence granted by the Central Government in accordance with the provisions of section 4 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said Act), shall have to undergo prior mandatory testing and certification in respect of parameters as determined by the telegraph authority from time to time.

2. Original Equipment Manufacturer (OEM): manufacturer of communication and its related products under whose brand, the products are sold or proposed to be sold to operators in the country.

3. Operator/Telecommunication Service Provider: an entity who has been granted with the license to provide telecommunication services in the country

4. ICC: Integrated circuit card. ISO uses the term Integrated Circuit (instead of smart card) to encompasses all those devices when an Integrated circuit is contained within a plastic card. Basically, ICC deployed for 2G application is called SIM.

5. ICCID: The integrated circuit card identification is a unique numeric identifier for the SIM that can be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual account identification number.

6. IMSI: The international mobile subscriber identity is a unique 15-digit number provided to the subscriber. It consists of the MCC, MNC, and MSIN.

7. UICC: Universal Integrated Circuit card. It is a tamper resistant smart card hardware containing file and folder systems which can host more than one network application. SIM,USIM(Universal SIM),ISIM(IMS SIM), TSIM(Tetra SIM) and CSIM/RUIM (Removeable User Identity Module -used for CDMA systems)are referred to as subscription containers of the UICC. The UICC is the physical and logical platform for the USIM. It does at least contain one USIM application and may additionally contain a SIM application. Further to that, the UICC may contain other applications/applets, e.g. for mobile banking or mobile commerce purposes, if these fit with the basic physical and logical characteristics of the UICC.

8. MSISDN: The Mobile Station International Subscriber Directory Number is intended to convey the telephone number assigned to the subscriber for receiving calls on the phone. It has country code +National Destination Code + subscriber number format.

9. Form Factor: The various sizes or forms of card; For removable cases, it can be 1FF,2FF (mini), 3FF(micro) and 4FF(nano).

10. SIM: Subscriber Identity Module. It is the ICC defined for 2G mobile communication (GSM). It has originally been specified as one physical and logical entity, not distinguishing platform and application. In 3G, the SIM may also be an application on the 3G UICC, then of course only represented by its logical characteristics. If the SIM application is active, the UICC is functionally identical to a 2G SIM. The SIM (or SIM application on a UICC) does only accept 2G commands

11. ROM: Read Only Memory is used for storing fixed program of the card. It is persistent nonmutable memory and can’t be written after the card is manufactured.

12. EEPROM: Electrically Erasable Programmable Read Only Memory can preserve data content when the power is turned off. It is a persistent mutable memory. The content can be modified during normal use of card.

13. Flash memory: It is a sort of EEPROM with smaller cell dimensions, but unlike EEPROM it cannot be erased or written byte-wise. Flash memory can take over the functions of ROM and EEPROM.

14. RAM: Random Access Memory is used as temporary working space for storing and modifying data. It is a non-persistent mutable memory. The information content is not preserved once the power is removed. RAM can be accessed unlimited number of times.

15. Secure Element (SE): It is a microcontroller chip which can store sensitive data and host secure network and other applications. It has the form of SIM/UICC/embedded SIM. It can also include new secure smart platform.

16. Smart card: It is a secure microcontroller which is protected against physical and logical security attacks.
17. USIM: Universal SIM. It is a logical application residing on the UICC. It does only accept 3G commands.
18. Card Issuer: An entity that owns the card and is ultimately responsible for the behavior of the card (operator /telecom service provider).
19. Security Integrated circuit (IC): Security IC comprises of IC hardware and software test functions which are needed during production phase.
20. (U)ICC platform: It includes security IC, card Operating System and related configuration data.
21. Java Card Platform: It is a smart card platform capable of executing Java applets which are written in Java Card language, a sub set of Java language. It consists of three parts 1) Java Card Virtual Machine (JCVM) 2) Java Card Run Time Environment (JCRE) and 3) Java Card API. Optionally, it may include native libraries that support Java card API. JCVM possesses all the knowledge and resources to run Java Bytecodes (Machine independent code generated by a Java compiler and executed by the Java interpreter) in a particular hardware environment. It is implemented in two pieces 1) On-card bytecode interpreter for runtime execution 2) Off-card converter while takes care of other functions such as class loading, linking and bytecode checking. JCRE is responsible for card resource management, network communication, applet execution and on card system & applet security. Java Card API specifies a set of core and extension Java Packages and classes for programming smart card applications and provides classes and interfaces to Java Card Applets.
22. Applets: Applications written for Java card platforms are called as Applets.
23. GlobalPlatform: GlobalPlatform is a non-profit industry association which develop GlobalPlatform's specifications for enabling digital services/applications and devices to be trusted and securely managed throughout their lifecycle i.e technical documentation for deployment and management of multiple applications on smart card.
24. Secured Channel Protocols (SCP): Set of protocols which ensures secured communication between smart card and external world. They allow a smart card and an off-card entity to authenticate each other and establish session keys to protect integrity and confidentiality of communications that follow. Commonly used protocols are: SCP02,03,10,11 and SCP 80,81.
25. Cryptography: The enciphering and deciphering of messages into secret codes by means of various transformations of the plaintext.
26. Cryptanalysis: The process of deriving the plaintext from the ciphertext (breaking a code) without being in possession of the key or the system (code breaking)

27. Key checksum value: In cryptography, a Key Checksum Value is checksum of the key value used to compare keys without knowing their actual values.

28. Application Program Interface: An Application Programming Interface (API) is a set of well-defined methods of communication between software components without any user intervention. It consists of set of instructions and standards to be followed by the participating applications. APIs operate on an agreement of inputs and outputs and are independent of any specific programming language.

29. Native OS/Applications: Native smart card Operating Systems and the applications that run over them are executed in the machine language of the associated target processor. They are usually generated in the C programming language. Native code application is compiled to the instruction set of the smart card's processor rather than to byte code that are interpreted by an interpreter on the smart card.

30. Application ID: data element, which identifies an application in a card. It is defined by ETSI TS 101 220 "Integrated Circuit Cards (ICC); ETSI numbering system for telecommunication; Application providers (AID)"

31. Java Programming Related: 1) Objects: The principal building block of object-oriented programs. Each object is a programming unit consisting of data (variables) and functionality (methods) 2) Class: The Class is a type that defines the implementation of a particular kind of object. A Class definition defines instance and class variables and methods. 3) Method: A Method is a piece of executable code that can be invoked, possibly passing it certain values as arguments. Every Method definition belongs to some class.4) Package: A group of classes. Packages are declared when writing a Java Card program.

32. Toolkit Application Reference (TAR): data element, which identifies an application in the toolkit mechanisms.

33. Global Platform Architecture: It mainly comprises of 1) Security Domain: Security Domains act as the on-card representatives of off-card authorities. They support security services such as key handling, encryption, decryption, digital signature generation and verification for their providers' applications. There are 3 types of Security Domains a) Issuer Security Domain- managed by card issuer b)Supplementary Security Domain-managed by application provider/card issuer/service bureaus c) Controlling authority Security domain-managed by controlling authority, if any 2) Card Manager- As an application on the card that acts as the issuer's agent controls what application can be loaded into the card.

34. Secure messaging: For some applications, it is necessary to cryptographically secure data transmission to the smart card to prevent eavesdropping and manipulation. This sort of security for smart cards is called Secure Messaging. The access to data on (U)SIM shall be through secure messages. It involves either adding a MAC (message authentication code) to each APDU or fully

encrypting each APDU. It is also possible to use send sequence counters (SSCs) for the command and response APDUs to prevent successful playback of previous messages

35. Global Platform Trusted Framework: Trusted Framework provide inter-application communication services between Applications. They are part of or extensions of the card's run-time environment

36. Smart Card Web Server (SCWS): The SCWS technology [SCWS] brings a HTTP Web Server on the (U)SIM card, enabling the end-user to access the (U)SIM contents and applications through a familiar and standardized interface, the web browser of its mobile phone. New services and configuration options can then be brought to the end-user.

37. SIM Profile: The service provider specific credentials, identity, algorithms, parameters and applets stored on the SIM card.

38. **D.2 Acronyms**

2G: Second Generation Technology

3G: Third Generation Technology

3GPP: 3rd Generation Participation Project

4G: Fourth Generation Technology

ADF: Application Dedicated File

ADM Key: Administrator Key

AES: Advanced Encryption Standards

AID: Application Identifier

APDU: Application Protocol Data Unit

CBMID: Cell Broadcast Message Identifier selection for Data Download

CBMIR: Cell Broadcast Message Identifier Range selection

CHV: Cardholder Verification

EF: Elementary File

ETSI: European Telecommunication Standards Institute

GSMA: GSM Association

ICC: Integrated Circuit Card

ISO/IEC: International Standards Organization/International Electrotechnical Commission

MF: Master File

OTA: Over the Air

OS: Operating System

PIN: Personal Identification Number

TPDU: Transfer Protocol Data Unit

E) Conventions

1. Must or shall or required denotes absolute requirement of particular clause of ITSAR.

2. Must not or shall not denotes absolute prohibition of particular clause of ITSAR.

3. Should or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.

4. Should not or not Recommended denotes the opposite meaning of (3) above.

Chapter 1 - Introduction

The (U)ICC is a contact based smart card whose specifications are defined by ISO/IEC 7816. It performs authentication, authorization and ensures secure radio communication with the mobile network. It can be used as a secure data storage for storing subscriber related information; with its tamper resistant hardware, a (U)ICC can protect the data stored on it. It can host variety of applications like banking, government specified, utility related, etc. (U)ICC cards have now emerged as Trust Anchor for the mobile device.

A) Hardware components of (U)ICC

Like any other computer system, (U)ICC as a smart card has the following hardware components

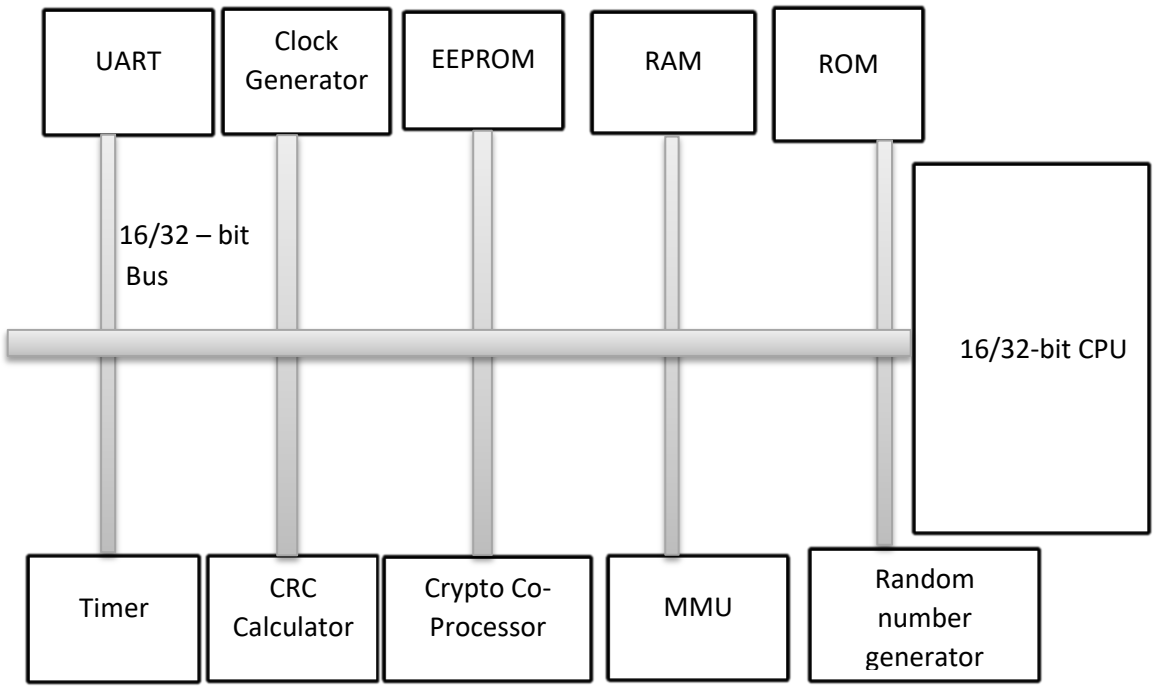


Fig 1. Hardware Components of (U)ICC

- CPU: It can be 8/16/32 bit microprocessor and is responsible for main processing functions.
- Memory: There are three types of memory

    - RAM: It is the working memory meant for holding temporary data. It is a volatile memory.

- EEPROM: It is the chip's nonvolatile memory where hierarchical file system exists. The applications, phone books, browser menu, plug-ins, OS patches, settings are stored in EEPROM.

- ROM is a Read Only memory that stores the OS, algorithms related to user authentication& data encryption and may also contain some diagnostic/testing functions

    - ROM shall be burnt during chip manufacturing process and EEPROM is programmed/loaded during card Personalization Phase. If flash memory is used, the memory allocated for OS and other ROM functions shall be burnt during chip manufacturing phase or at Production Facility and shall not be modifiable after the issuance of card to the subscriber.

SIM cards can have supplementary hardware like

- Crypto Co processor: A dedicated processor for executing the cryptographic algorithms. This can fasten the process and enhance the performance of the (U)ICC.
- True Random number generator (RNG) generates those unpredictable random numbers which are used in cryptographic algorithms.
- CRC Calculator: It generates CRC codes which can be used to secure data or program by means of error detection capability. (to provide data integrity)
- Universal Asynchronous Receiver Transmitter (UART) hardware is used to enhance the data transmission rate between (U)ICC and external world and the Internal clock multiplication unit minimizes the Java run time and speeds up the crypto calculations.
- Direct Memory Access (DMA) makes it possible to copy or exchange data between two or more memory areas at high speeds and offloads the CPU.
- Memory Management Unit (MMU): Such a unit monitors the memory boundaries of the current application program while it is running. This ensures the forming of barriers for each of the applications and the applications cannot access forbidden memory areas. (The access rights of the application to the memories can be controlled with the memory management unit (MMU))
- NFC: Near Field Communication (NFC) is contactless interface towards other NFC enabled readers and tags.

B) Software/Firmware components of (U)ICC:

B.1 Operating System(OS)

(U)ICC OS has very small amount of program code and is vendor specific. Unlike other common OS, this OS does not have provision for user interface, multitasking and access to external memory. It can process internal data securely and output the calculated result to a terminal for further processing.

The Operating System can either be native (proprietary, vendor specific) or interpreter based. Native Operating System and the applications are usually written in the C programming language. Most interpreter-based Operating Systems are also written in C, but the application programs are written in an interpreted programming language such as Java and such systems are called Java Card System or Java Card Platform.

Few important tasks of (U)ICC OS are listed below,

1) Transfer data to and from (U)ICC card
2) Protecting the access to data
3) Control the execution of commands
4) Manage files and memory
5) Manage and execute cryptographic algorithms
6) Managing and executing the program code.

B.2 Application software

Since (U)ICC is a portable, tamper resistant and trusted element, it can be used to host secure applications ranging from mobile banking to information services. Initially, (U)ICC was considered as a means for authentication. The feasibility of using (U)ICC for Value Added Services was realized with the introduction of SIM (Application) Toolkit (STK), a construction Kit which enabled the development of supplementary services. The SIM Application Toolkit enables the SIM to directly access functions of the mobile station, such as driving the display, polling the keypad, sending short messages and other functions needed in connection with a value-added service. It contains set of commands and reversed the master slave relationship that exists between Mobile Equipment and SIM, thus enabling the SIM to proactively send commands to Mobile Equipment. SIM tool kit applications took the form of simple menus (STK menu). STK menu allowed the subscriber to send messages to avail the services like stock quote, news, balance enquiry, money transfer, call forwarding etc. The SAT (SIM Application Toolkit) applications were originally based on proprietary APIs, but along with the introduction of the Java Card, it is possible to provide better interoperability of the applications.

As an alternative to static SIM toolkit applications with a fixed pre-installed menu, operators opt for dynamic SIM toolkit, where the menus and user dialogs are generated on the fly based on information provided by a central server. SIM-browsers or micro browsers (consumes small amount memory and processing power) residing on the SIM provide this functionality, with their ability to interpret byte

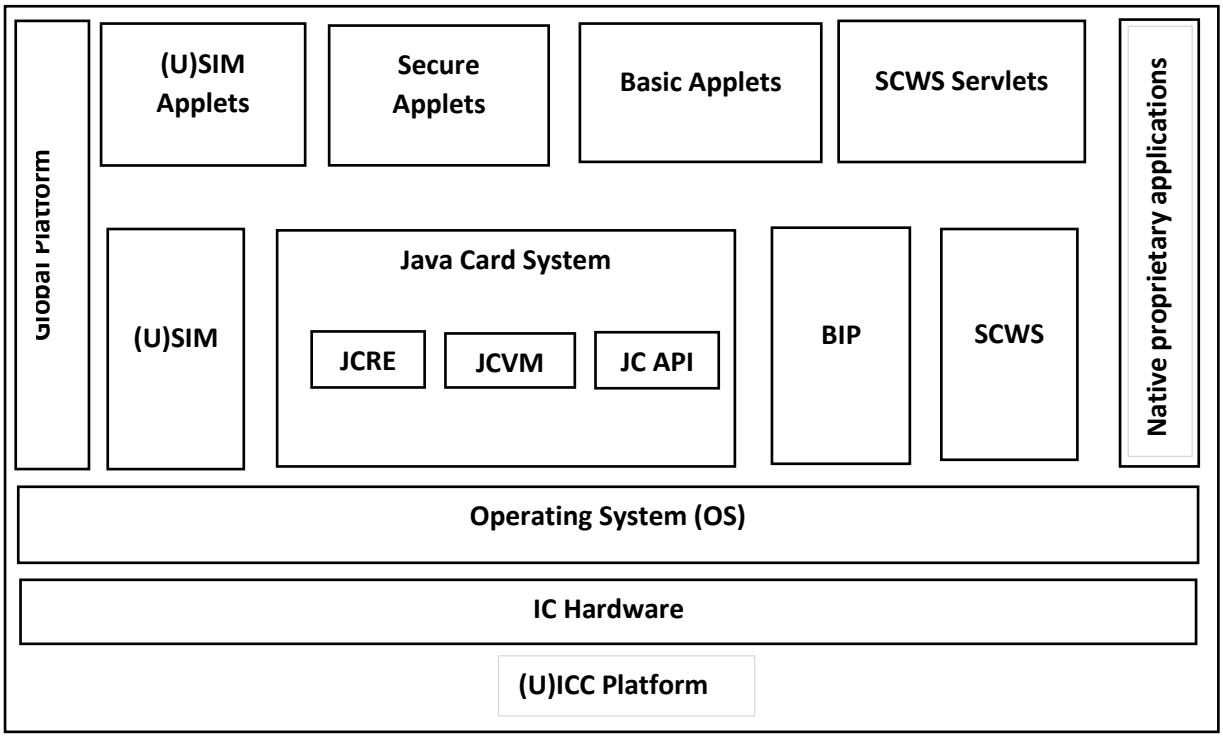
codes. It can be considered as an extension of SIM OS and can interpret WML dialect to access WML application.

In order to make (U)ICC to communicate in HTML, Smart Card Web Server (SCWS) concept was introduced. The Smart Card Web Server consists of an HTTP server embedded in the (U)ICC card which aids (U)ICC card to act as a Web server by hosting web-based application or http content. The SCWS enables the local web browser running in the handheld to communicate with the (U)ICC, offering a nice, interoperable and dynamic interface in comparison to the STK interface. The SCWS can target both static pages stored on the card but also applications, as long as they are registered in the SCWS.

B.3 Platforms of (U)ICC:

There are two broad platforms of (U)ICC namely Native card and Java card.

Architecture diagram of these platforms are as below,



B.3.1 Native OS and Java card Platform of (U)ICC:

(U)ICC can have native OS and may contain native applications. Native smart card Operating Systems and the applications that run over them are executed in the machine language of the associated target processor. They are usually generated in the C programming language. Native code application is compiled to the instruction set of the smart card's processor. This "native" vendor specific OS prohibited the portability of (U)ICC applications. The popularity of Java Programming language facilitated the introduction and subsequent implementation of Java Card specifications in SIMs. Java card as a platform loaded on (U)ICC OS provided the feasibility of multi-application SIM cards. Java Card Platform is capable of executing

Java applets (Java based SIM applications) which are written in Java Card language, a sub set of Java language. Java Card platform consists of three parts 1) Java Card Virtual Machine (JCVM) 2) Java Card Run Time Environment (JCRE) and 3) Java Card API. Optionally, it may include native libraries that support Java card API. JCVM possesses all the knowledge and resources to run Java Bytecodes (Machine independent code generated by a Java compiler and executed by the Java interpreter.) in a particular hardware environment. It is implemented in two pieces 1) On-card bytecode interpreter for runtime execution 2) Off-card converter while takes care of other functions such as class loading, linking and bytecode checking. JCRE is responsible for card resource management, network communication, applet execution and on card system & applet security. Java Card API specifies a set of core and extension Java Packages and classes for programming smart card applications and provides classes and interfaces to Java Card Applets. The Java card architecture includes Java card virtual machine, Java card API, Java card run time environment.

B.3.2 Java Card supporting Global Platform:

The deployment of multiple applications on (U)ICC necessitated a standard for the platform so as to ensure secure and interoperable applications environment. These standards are developed by Global Platform, a non-profit industry association. Its objective is to standardize certain aspects of the technology so that interoperability, availability and security of multi-application smart card technology is enhanced. Global Platform architecture mainly comprises of 1) Security Domain: Security Domains act as the on-card representatives of off-card authorities. They support security services such as key handling, encryption, decryption, digital signature generation and verification for their providers' applications. There are 3 types of Security Domains a) Issuer Security Domain- managed by card issuer b)Supplementary Security Domain-managed by application provider/card issuer/service bureaus c) Controlling authority Security domain-managed by controlling authority, if any 2) Card Manager- As an application on the card that acts as the issuer's agent controls what application can be loaded into the card.

Chapter 2 - Common Security Requirements

This section describes the common security requirements for pluggable (U)ICC platform.

Section 1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement

The protocols used for the (U)ICC (Local and Remote) management shall support authentication mechanisms. If TLS1.2 is used it should be patched up to date**.**

Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” shall only be used for(U)ICC management and maintenance.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

(U)ICC management traffic shall be protected strictly using Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

For Integrity protection of management traffic , The support of digital signature may not be required.

For Integrity protection of management traffic ,cryptographic checksum is permitted only with AES CMAC with min 128 bits key size

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.4]

2.1.3 User Authentication – Local/Remote

Requirement:

The various user accounts (other than system /admin accounts) on a system shall be protected from misuse. To this end, at least one authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user in closed environment

Authentication attributes include
- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

Minimum two of the above Authentication attributes shall be mandatorily combined to protect user accounts ((other than system /admin accounts) in open .environment (internet)

For remote access management traffic , for integrity protection CRC verifying mechanism is not permitted only Hash or MAC (CC) are permitted

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.1]

Section 2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication as mentioned in Security requirement - 2.1.3 shall be prevented.

This requirement shall also be applied to accounts that are only used for communication between systems.

2.2.2 Protection against brute force and dictionary attacks

Requirement:
A protection against brute force and dictionary attacks that hinder AUTHENTICATION ATTRIBUTE guessing shall be implemented.
Brute force and dictionary attacks aim to use automated guessing to ascertain AUTHENTICATION ATTRIBUTE for user and machine accounts.

(i) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.3 Enforce Strong Password /PIN

Requirement:

(a) The configuration setting shall be such that a (U)ICC shall only accept passwords/PINs that comply with the following criteria:
(i)Absolute minimum length of 4 characters. It shall not be possible setting this absolute minimum length to a lower value by configuration.
(ii) It can be decimal or hexadecimal.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3]

2.2.4 PIN Changes

Requirement: It should be possible to change PIN after correct presentation of old PIN.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.2]

2.2.5 Removal of predefined or default authentication attributes

Requirement:

PIN1 has to be unique to each customer.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 5.2.3.4.2.3]

Section 3: Software Security

2.3.1 Secure Update/Upgrade

Requirement:
Secure Update:
(U)ICC's application updates shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

Software update integrity shall be verified strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.
Secure Upgrade:
(i) (U)ICC Software package integrity shall be validated in the installation and upgrade stages strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

(ii) Tampered software shall not be executed or installed if integrity check fails.

(iii) (U)ICC's software upgrades shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR version 1.0.0" only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Source code security assurance

Requirement:

a) Vendor should follow best security practices including secure coding for software development and should be augmented with designated TSTL source code review duly supported by furnishing the Software Test Document (STD) generated while developing the (U)ICC.
b) Also, Vendor shall submit the undertaking as below:
(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the (U)ICC Software, which includes vendor developed code, third party software and open source code libraries used/embedded in the (U)ICC.
(ii)The (U)ICC software is free from all known security vulnerabilities, security weaknesses listed in the CVE and CWE databases as on the date of product release. Critical/severe, medium and high vulnerabilities based on CVSS (latest CWE database) for software weakness need to be patched during product release. For Low level vulnerabilities which are found during testing, vendor shall have remediation plan and patch them at the earliest.
(iii) The binaries for (U)ICC and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

2.3.3 Known Malware and backdoor Check

Requirement:

Vendor shall submit an undertaking stating that (U)ICC is free from all known malware and backdoors as on the date of product and shall submit their internal Malware Test Document (MTD) of the P-GW to the designated TSTL.

Section 4: Security requirements related to hardening

2.4.1 No unused functions

Requirement:

Unused functions i.e the software and/or hardware functions which are not needed for operation or functionality of the (U)ICC shall not be present in the (U)ICC's software and/or hardware.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:

Vendor to ensure that the (U)ICC shall not contain software and/or hardware components that are no longer supported by Vendor or its 3rd Parties including the open source communities, such as components that have reached end-of-life or end-of-support.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.5]

2.4.3 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the (U)ICC shall not be present.

[Reference: TSDSI STD T1.3GPP 33.117 -14.2.0 V.1.0.0. Section 4.3.2.3]

2.4.4 Unnecessary Services Removal

Requirement:

(U)ICC shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]

2.4.5 Restricted reachability of services

Requirement:

The (U)ICC shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers.

2.4.6 Avoidance of Unspecified Wireless Access

Requirement:

An undertaking shall be given as follows: "The (U)ICC does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement:
The security event log shall be access controlled using file access conditions such that only privilege users including the administrator have access to read the log files but not allowed to delete the log files.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:
The (U)ICC shall log all important Security events with unique System Reference details as given in the Table below.
(U)ICC shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event Types	Description	Event data to be logged
Financial transaction(if hosted in (U)ICC/(U)SIM)	Events related to financial transaction	Transaction reference
		Event details
		Outcome of event (Success or failure)
		Time stamp (date and time)

2.5.3 Secure Log Export

If financial application is hosted on (U)ICC/(U)SIM, secure log export mechanism shall comply with the relevant standards such as that of EMVco

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:
Vendor shall submit to TSTL, the list of the connected entities with (U)ICC and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration and detailed procedure of establishing the communication with each entity.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the (U)ICC (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

Vendor shall also submit cryptographic module implementation testing document and the test results to designated TSTL for scrutiny.

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithms embedded in the crypto module of (U)ICC are implemented in compliance with respective FIPS standards (for the specific crypto algorithm.)
Vendor shall also submit cryptographic algorithm implementation testing document and the test results to designated TSTL for scrutiny.

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

When (U)ICC is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear to users and administrators.

Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.2]

2.6.5. Protecting data and information in storage

Requirement:

For sensitive data in storage (persistent or temporary), read access rights shall be restricted. Files of (U)ICC system that are needed for the functionality shall be protected against manipulation.

In addition, the following rules apply for:

(i)Systems that need access to identification and authentication data in the clear/readable form e.g. in order to perform an activity/operation, such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
(ii)Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0”.

(iii)Stored files: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

Note : Storing of IMSI in encrypted form is exempted as per global standards

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

(U)ICC shall not create a copy of data in use and/or data in transit.

Protective measures should exist against use of available system functions / software residing in (U)ICC to create copy of data for illegal transmission. The software functions, components in the (U)ICC for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

Section 7: Network Services

2.7.1: Traffic Separation

Requirement:

(U)ICC shall support physical and/or logical separation of management traffic and control plane traffic.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.5.1].

Section 8: Vulnerability Testing Requirements

2.8.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of (U)ICC are reasonably robust when receiving unexpected input.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.4]

2.8.2 Vulnerability Scanning

Requirement:
It shall be ensured that there is no known vulnerabilities exist in the (U)ICC.
The purpose of vulnerability scanning is to ensure that there no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the (U)ICC that can be detected by means of automatic testing

tools. The test for this requirement can be verified by using a suitable Vulnerability scanning tool.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

Section 9: Operating System

2.9.1 Growing Content Handling

Requirements:

Growing or dynamic content on shall not influence system functions. A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop (U)ICC from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.1]

2.9.2 Authenticated Privilege Escalation only

Requirement:

(U)ICC shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.2.1]

2.9.3 OS Hardening

Requirement:

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in (U)ICC

Kernel based network functions not needed for the operation of the (U)ICC shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.2]

2.9.4 Protection from buffer overflows

Requirement:

(U)ICC shall support mechanisms for buffer overflow protection.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.5]

2.9.5 File-system Authorization privileges

Requirement:

(U)ICC shall be designed to ensure that only users that are authorized to modify files,
data, directories or file systems have the necessary privileges to do so.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.7]

Section 10: Web Servers

This entire section of the security requirements is applicable if the (U)ICC supports web management interface.

2.10.1 HTTPS

Requirement:

The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.1]

2.10.2 Webserver logging

Requirement:

Access to the (U)ICC webserver (for both successful as well as failed attempts) shall be logged by (U)ICC.
The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.2.1]

2.10.3 HTTPS input validation

Requirement:

The (U)ICC shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
(U)ICC shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]

2.10.4 No system privileges

Requirement:

No (U)ICC web server processes shall run with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

2.10.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for (U)ICC operation shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3]

2.10.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for (U)ICC operation.
In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.4]

2.10.7 No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:

If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.5]

2.10.8 No CGI or other scripting for uploads

Requirement:

If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.6]

2.10.9 No execution of system commands with SSI

Requirement:

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.7]

2.10.10 Access rights for web server configuration

Requirement:

Access rights for (U)ICC web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]

2.10.11 No default content

Requirement:

Default content that is provided with the standard installation of the (U)ICC web server shall be removed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9]

2.10.12 No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.10]

2.10.13 Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the (U)ICC web server and the modules/add-ons used.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.11]

2.10.14 Web server information in error pages

Requirement:

User-defined error pages and Error messages shall not include version information and other internal information about the (U)ICC web server and the modules/add-ons used.
Default error pages of the (U)ICC web server shall be replaced by error pages defined by the vendor.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.12]

2.10.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for (U)ICC operation shall be deleted.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]

2.10.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the (U)ICC web server's document directory.
In particular, the (U)ICC web server shall not be able to access files which are not meant to be delivered.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]

2.10.17 Execute rights exclusive for CGI/Scripting directory

Requirement:

If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]

Section 11: Other Security requirements

2.11.1 No PIN Recovery

Requirement:

No provision shall exist for (U)ICC PIN(s) recovery.

2.11.2 Software Integrity Check – Boot

Requirement:

(U)ICC shall support the possibility to verify software image integrity at boot time, detecting, for example, software image tampering and/or unauthorized software image updates. (C)RC integrity check mechanism is not permitted.

2.11.3 Unused Physical and Logical Interfaces Disabling

Requirement:

(U)ICC shall support the mechanism to verify both the physical and logical interfaces exist in the product.

Physical and logical accessible Interfaces which are not under use shall be disabled

---

2.11.4 Security Algorithm Modification

Requirement:

It shall not be possible to modify security algorithms supported by (U)ICC.

Chapter 3 - Security requirements of (U)ICC Platform

The attack scenarios for ICs and smartcard software include physical manipulation and probing, malfunction attacks, inherent and forced leakage attacks, abuse of test features, attacks on the implementation of cryptographic functionality implemented in hardware, software or in a combination of both, cryptographic attacks or software attacks

3.1 ICCID shall uniquely identify the (U)ICC.

3.2 The (U)ICC hardware shall provide protection against the operations such as out-of-range – voltage/temperature/frequency, active shield etc

3.3 (U)ICC hardware shall maintain the integrity and confidentiality of the contents stored in its memories and correctly execute the software residing on it.

3.4 (U)ICC hardware shall be resistant to physical attacks that are directed to get access or modify IC. In a case where, by extracting internal signal with the tools, attackers can get access to secret data.

3.5 (U)ICC hardware shall be resistant to perturbation attacks that alter the normal behavior of an IC in order to create a vulnerability and thereby weakening the crypto operations.

3.6 (U)ICC hardware shall be resistant to Side Channel Attacks (Timing/Power/Electromagnetic Analysis). In a case where, by analyzing the emitted EM radiation from IC, by using timing differences and power consumption by electronic components, attacker can get access to secret keys.

Operating System(OS) : The perspective of Secure OS is tied to the chip hardware. The possibility of Trap door, Trojan Horse and any other vulnerabilities shall be completely excluded in the card OS program code. OS shall be crash proof, reliable, secure and robust.

The following security requirements aim to ensure that the Operating System software/firmware are appropriately set by reducing their surface of vulnerability,

3.7 The OS shall manage memory, allocation of program memory (ROM and EEPROM), data memory (usually EEPROM) and working storage (RAM) to applications.

3.8 The OS shall provide sufficient interfaces to interpreter for accessing file management, cryptographic algorithms and other applications of the card.

3.9 OS shall feature a configurable access control mechanism that provides the options when creating the services.

3.10 OS shall grant file access privileges and monitor compliance with access rule reference file.

3.11 OS shall enforce access policy on subjects (Users/administrator), objects (files) and operations (Authentication, Read, Update, Activate, Deactivate, Increase, Invalidate, Rehabilitate and Reset).

3.12 OS shall allow the subject to perform any operation on the object only if it is listed in the object's Access Control List (ACL).

3.13 Storage of user data and its access control**-** OS shall protect the integrity and confidentiality of user data stored (PIN/CHV, Phonebook, SMS list, location information etc.,) and shall ensure that only authenticated entities with sufficient access control rights can access the restricted files and services. There shall be a mechanism to check for integrity errors of data.

3.14 Execution environment**:** The Operating System shall provide a secure execution environment based on the secure operation of CPU (e.g. well-known instructions, no hidden or unspecified code) that controls the execution flow, detects and reacts to potential security violations. The Operating System shall ensure that patches installed before delivering, if any, cannot be bypassed.

3.15 Memory management**:** The Operating System shall manage the persistent and volatile memories of the product according to the capacities of the underlying (U)ICC so as to control access to sensitive content protected by the Operating System. Operating System memory management services may include memory allocation/deallocation, access control, integrity checks, enciphering (on-the-fly) etc. The Operating System shall ensure that no residual information is available from memories, for instance, cleaning persistent memory upon allocation and deallocation and wiping of volatile memory upon sensitive operations.

3.16 I/O management**:** The Operating System shall manage Input/Output interfaces together with the IC platform. Any kind of external interface is allowed (contact, contactless, USB, etc.). The Operating System shall provide the same security level whatever the communication mode is. The Operating System shall handle all communication requests and shall be able to decide whether to accept or deny them. The (U)ICC platform shall prevent leakage of data through the I/O buffers by ensuring that only genuine request can output data via the I/O interfaces. The Operating System shall control I/O buffers in order to prevent data leakage.

3.17 Life cycle management**:** The Operating System shall manage its life cycle and shall provide a secure transition mechanism between states in particular, the mechanism shall prevent re-entering irreversible states. The Operating

System shall prevent abuse of functionalities that are available only at certain states in the Operating System life cycle.

3.18 Key management: The Operating System shall provide secure generation, destruction, replacement and storage of cryptographic keys according to the FIPS 140-2 specification. This holds good if any financial applications are hosted in (U)ICC/(U)SIM.

3.19 Cryptographic operations**:** The Operating System shall provide a secure implementation of all the cryptographic operations used by the OS itself (e.g. for memory encryption) and/or by the integrated application (e.g. for signature or communication protocols). These operations may correspond to cryptographic primitives (e.g. DES, SHA) or to complex functions (e.g. signature generation).

3.20 Atomic operations**:** The Operating System shall provide means of performing atomic operations, for instance, writing or erasing of individual or multiple memory locations. The Operating System shall guarantee that atomic operations are either performed completely or have no effect in case of interruption i.e., In case of abruptions, OS shall be able to restore original state of data.

3.21 Separation mechanism**:** The Operating System shall implement a separation mechanism between itself and the Application Layer that runs on top of it, e.g. separate execution domains and memory contexts for the Operating System and the Application Layer.

3.22 OS shall ensure that an application cannot access memory locations outside its allocated space as part of application management.

3.23 Services to the Application Layer**:** The Operating System provides security services to the Application Layer through the Operating System API, which may consist, for instance, of:

- API for cryptographic operations
- API for key management
- API for atomic transaction
- API for RNG.

The above security services rely on security features of the Operating System configuration. For instance, if the Operating System provides a key management API to the Application Layer, this means that the key management feature shall manage Application Layer keys also.

3.24 The program code shall be downloaded and executed only after passing suitable security checks.

(U)ICC assets and attack scenarios

Assets are security-relevant elements to be directly protected by the (U)ICC. They are divided into following two groups.

- Direct Assets: Authentication Keys, User& ADM PINS, OTA Keys, ICCID, IMSI, Operator Constants, XORing constants, application data, application code.
- Indirect Assets: Maximum Counter values, File system access, PIN management, Network Access algorithms and Remote file and applet management.

(U)ICC shall be **resistant** to the following attacks on assets,

3.25 Exploitation of Test Features: The attack path aims to enter the IC test mode to provide a basis for further attacks. The attacker is able to read out the content of the nonvolatile memory.

3.26 Retrieving keys with Fault Analysis: Attacker tries to obtain a secret by comparing a calculation without an error and calculations that do have an error. Fault Analysis can break cryptographic key systems, allowing to retrieve algorithmic keys.

3.27 Attacks on Operating System/Software: Attacker make attempts to discover software error/bugs to create vulnerabilities. Attacker may install Trapdoor or Trojan horse which can be exploited to their advantage.

3.28 Attacks on Random Number Generator is made to predict the output of RNG.

3.29 Attacks on Protocols used (one such example is attacks involving OTA server): Attacker makes an attempt to exploit the inherent vulnerabilities in the protocol.

3.30 Attacks on Java card Platform: This logical attack consists in executing ill-formed applications, i.e. malicious applications that are made of illegal sequences of byte-code instructions or that do not have valid byte-code parameters.

3.31 Attacks in a multi-application environment: In a multi-application platform, application isolation is achieved by combination of physical and logical measures. This Application isolation is target of attacks to reach application data (including keys) and code.

The (U)ICC platform shall provide the following main security functionality:

3.32 The (U)ICC platform shall provide protection against the memory aging.

3.33 (U)ICC platform shall support a mechanism for management of security functionality data like PINs, Cryptographic Keys and counters.

3.34 (U)ICC shall have a secure communication with its terminal and shall support secure messaging service.

3.35 Random numbers which are required for cryptographic operations shall be generated in a secure manner. The Random Number Generation shall be conformant to the quality requirements of the NIST scheme.

3.36 Deficiency of Random Numbers**:** Random Numbers generated shall be unpredictable and shall have sufficient entropy.

3.37 Transaction Data Logging: (U)ICC shall store the logs related to financial transactions which are readable after successful verification of PIN. The personal data which are no longer necessary shall be deleted immediately. This holds good if any financial applications are hosted in (U)ICC/(U)SIM.

3.38 (U)ICC shall support the mechanism for specifying the level of protection explicitly by the user/administrator for each asset.

3.39 (U)ICC shall have a mechanism to authenticate to users for accessing the data stored internally.

3.40 (U)ICC shall have security measures that can protect the stored data (as given below) from unauthorised disclosure.

- Application Provider Security Domains cryptographic keys
- Controlling Authority Security Domains cryptographic keys
- cryptographic keys Issuer Security Domain cryptographic keys
- Verification Authority Security Domain cryptographic keys
- Private data of the (U)SIM application

3.41 (U)ICC shall have security measures that can protect the stored data (as given below) from unauthorised modification and destruction.

- The code of the (U)SIM application on the card.
- The code of the Global Platform framework on the card
- The data of the card management environment, like for instance, the identifiers, the privileges, life cycle states, the memory resource quotas of applets and security domains.
- Application Provider Security Domains cryptographic keys
- Controlling Authority Security Domains cryptographic keys
- Issuer Security Domain cryptographic keys
- Verification Authority Security Domain cryptographic keys
- Private data of the (U)SIM application
- The code of the Smart Card Web Server (SCWS) on the card.
- The secret data (PINs, passwords, runtime credentials) used by the SCWS server to authenticate the User before providing access to web pages controlled by access rights.

3.42 (U)ICC shall provide protection from unauthorised disclosure of the user data that is sent or received through any communication channel.

Chapter 4 – Specific Security requirements of (U)SIM

(U)SIM shall support following specific features,

4.1 If (U)SIM is removed from ME/UE, the services shall terminate immediately.

4.2 Network Authentication

(U)SIM shall be able to authenticate with the network. This can be unilateral authentication for 2G and mutual authentication for 3G and 4G. Upon successful authentication, all the ensuing communication shall be encrypted.

4.2.1 Network Authentication /Network Access: The operator shall use strong algorithms for authentication, data confidentiality and integrity protection which could withstand all forms of known attacks. The use of deprecated algorithm shall be strictly avoided. Denial of Service attacks which attempts to down grade the service from 4G to 2G/3G can be mitigated by implementing strong algorithms in 2G/3G systems. Ciphering should always be enabled in 2G network.

The table below lists the algorithms that shall be used in Indian mobile network.

Sl No	Security property	GSM	GPRS	3G-UMTS	4G-LTE
1	Authentication	Comp 128-3 or GSM Milenage	Comp 128-3 or GSM Milenage	Milenage or Tuak	Milenage or Tuak
2	Encryption	A5/3 or A5/4	GEA3 or GEA4	UEA1-Kasumi or UEA2-Snow 3G	EEA1 Snow 3G or EEA2 AES 128 or above
3	Integrity Protection	-	-	UIA1-Kasumi or UIA2 Snow 3G	EIA1 Snow 3G or EIA2 AES 128 or above

4.2.2 Default algorithmic parameters shall not be used. (for e.g default MILENAGE offset values(available in ETSI spec) shall not be used).

4.3. Over the Air (OTA) Communication

OTA communication enables the operator to establish a direct connection with the (U)ICC/(U)SIM post issuance to the customer. This can be used by operator to

manage the existing application/files and deploying new application/services through Remote File Management and Remote Applet Management.

The communication between OTA server and (U)ICC /(U)SIM is secured with cryptographic algorithms.

The security features to be supported and the algorithms that shall be used for the information exchange between OTA server and (U)ICC/(U)SIM are tabulated below.

Sl No	Name	Security mechanism
1	Message authentication	Cryptographic Checksum(also called as Message Authentication Code-MAC) or a Digital Signature
2	Message integrity	Cryptographic Checksum(also called as MAC)
3	Message confidentiality	Message ciphering/encryption
4	Replay protection	Counter
5	Proof of receipt	Status code packed into response message

4.3.1 Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” shall only be used for secured channel protocols, both for data integrity and transport security.

4.3.2 The (U)ICC /(U)SIM shall support 15 nos Ciphering(KIC) secret keys & 15 nos of Cryptographic Checksum and Digital Signature(KID) secret keys. The key lengths for KIC and KID shall be 128 bits or more for AES.

4.3.3 These 15 key sets of KIC & KID shall be stored securely in USIM and OTA server(s).

4.4 End User Authentication: The user shall be able authenticate successfully with the (U)SIM as a protection against the use of stolen card.

a) The (U)SIM shall support means to authenticate the user which be performed by the verification of a numeric PIN of four (4) to eight (8) decimal digits.

b) User authentication should be enabled when the (U)SIM is first inserted into the ME/UE (Optional Requirements)

c) (U)ICC should prompt the user to change the PIN after initial correct PIN presentation. (Optional Requirements)

Following correct PIN presentation, the ME may perform functions and actions on (U)SIM data.

d) 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 (U)ICC has been removed, the USIM has been deselected or the ME has been switched off.

e) Once a PIN is blocked, further PIN verifications shall be denied. The (U)SIM shall support a mechanism for unblocking a blocked PIN. Unblocking of a PIN is performed by using the relevant PIN Unblocking Key.

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

g) 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 (U)ICC has been removed, the (U)SIM has been deselected or the ME has been switched off. Unblocking of a blocked PIN shall not be possible.

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

4.5 File Access Condition: The (U)SIM contains hierarchical file system which is programmed in EEPROM. The root file is called as Master File (MF). Under MF, there are Directory Files (DF) which are meant for directories. Subordinate to DF are the Elementary Files (EF) which contain the actual data. Files can be of administrative or application specific.

Every file in SIM card is associated with set of rules called as Access Control List which allows access condition of READ, UPDATE, INVALIDATE, REHABLITATE, INCREASE, DEACTIVATE and ACTIVATE. The condition levels are

Always- Free file access and command can be executed

Never-File access is prohibited and the command can never be executed

PIN1: File access is allowed with the presentation of valid PIN1 and command can be executed. PIN1 is used by subscriber.

PIN2: File access is allowed with the presentation of valid PIN2 and command can be executed.

ADM: set by administrative authority and is equivalent to super user. Min 10 ADM PINs shall be possible.

Secret Codes: In 3G mode, 16 application PINs shall be supported (8 global and 8 local pins- which can be used within an ADF). Further upto, 10 administrative PINs can be defined. A replacement PIN, called Universal PIN, may also exist. In 2G case, CHV1 and CHV2 shall be supported. Additionally, 11 admin PINs can also be defined.

4.6 Application Level Security

(U)ICC/(U)SIM application development environment includes both 1) Native STK based (vendor specific, written in assembly language or C and 2) Java Card based

(Applets). The native applications can be banking, location services and information services. Java Card based environment ensures portability of applications. Each application shall be uniquely identified by AID.

4.6.1 Application Security Keys: (U)ICC/(U)SIM shall generate symmetric and asymmetric application security keys. These application security keys shall comply to Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0"

4.6.2 Native STK based applications:

4.6.2.1 The applications developed to work in native OS shall be loaded securely and shall be tested exhaustively for the absence of any malware.

4.6.2.2 The security of the native OS application lies in the hands of the Operating System and hence OS shall be hardened.

4.6.2.3 Any changes in an application, must be sent as software patches and stored in EEPROM.

4.6.2.4 If the applications share card data, they must trust one another or be tested exhaustively together

4.6.3 Java Card Based: Java Card platform shall counter the unauthorized disclosure or modification of the code and data (keys, PINs, biometric templates, etc) of applications and platform. The Java Card System shall provide strong and secure application installation mechanism, firewall mechanism, dedicated API for security services.

4.6.3.1 The bytecode checker, shall ensure that no application uses resources outside its range.

4.6.3.2 Application security shall include mutual authentication, data integrity and data confidentiality.

4.6.3.3 The applications/applets shall only be installed in (U)ICC after the verification of the digital signature. The converted applets (known as the CAP file) shall be signed as a package by the issuer using a AES secret key, and the card shall check this signature (using the same key) when the CAP file is loaded.

4.6.3.4 Java card system Code/Data/Application shall be protected against unauthorized disclosure and modification.

4.6.3.5 Application bytecode and Java card system byte code must be protected against unauthorized execution.

4.6.3.6 Cryptographic keys owned by applets shall be protected from unauthorized disclosure and modification. Similarly, end user's PIN shall be protected from unauthorized disclosure and modification.

4.6.3.7 It should be possible to prevent applet impersonation which aims to gain illegal access to resources.

4.6.3.8 DoS attack by consuming resources of card shall be prevented.

4.6.3.9 Each applet shall be prevented from accessing the contents or behavior of objects owned by other applets.

4.6.3.10 For runtime checking, Java Card shall use a software firewall mechanism that explicitly links each object with the applet thereby preventing access to those objects by other applets unless a “shareable interface” is explicitly provided.

4.6.3.11 Application Sandboxing**:** (U)ICC shall provide for Application Sandboxing feature so that the system assigns a unique user ID (UID) to each application and runs it in its own process. By default, apps can't interact with each other and have limited access to the OS. If app A tries to do something malicious, such as accessing application B's data, it shall be prevented from doing so.

4.6.3.12 If there is a security breach, it should be possible to lock the card.

4.6.3.13 Off card communications shall be through secure channel defined by Secure Channel Protocols.

4.6.3.14 Before loading the key to the card, the key check value shall be verified.

4.6.3.15 If native methods are declared by Java card, they shall be subjected to security check.

4.7 **Compliance to Government guidelines and requirements**:

Compliance to THE INFORMATION TECHNOLOGY ACT, 2000 and Banking applications shall meet IDRBT/RBI guidelines

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

4.7.2 For Mobile banking transactions, the (U)ICC /(U)SIM card shall comply to “Mobile Banking transactions in India-Operative Guidelines for Banks”, as amended from time to time.

4.7.3 Govt applications:

(U)SIM shall reserve minimum 32K of Non Volatile Memory (NVM) space for installing Government notified application like disaster management, social welfare, health , safety ,Aadhaar, Driving License, Access to welfare schemes etc

Cell Broadcast Services: The SIM shall have capability for card configuration for files SST, CBMID and CBMIR. 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 SIM. Memory required for this application shall be part of the 32 K allocated memory.

(U)ICC/(U)SIM 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.

(U)ICC/ (U)SIM shall support special SSD (Supplementary Security Domain) for Government of India compliant to Global Platform Specifications version 2.1.1 or higher. This security domain shall be manageable by Govt of India.

4.7.4 Emergency Helpline Number 112 has to be burnt into SIM.

4.7.5 A UE/ME shall have the capability to store one or more 'ICE (In case of Emergency) information' on the (U)ICC which enables first responders to contact victim's emergency contacts.

4.8 Global Platform Specification:

Global Platform specification-based card shall support

Application security: Applications should 1) Expose only data and resources that are necessary for proper application functionality 2) Perform internal security measures required by the Application Provider 3) An Application can use the cryptographic services of its associated Security Domain 4) Applications can access the Secure Messaging services of their associated Security Domain only. 5) Off card application shall use crypto algorithms and keys for digitally signing the data and signature verification. 6) Backend systems shall ensure secure Operating Systems, system security policies, and audit procedures

Data: Card runtime environment shall provide hardware neutral API for applications as well as a secure storage and execution space for applications to ensure that each application's code and data can remain separate and secure from other applications on the card. It shall be ensured that runtime environment security mechanisms cannot be bypassed, deactivated, corrupted, or otherwise circumvented.

Secure memory management shall be resorted to ensure that 1) Each application's code and data (including transient session data) as well as the runtime environment itself and its data (including transient session data) is protected from unauthorized access from within the card. 2)When more than one logical channel is supported, each concurrently selected Application's code and data (including transient session data) as well as the runtime environment itself and its data (including transient session data) is protected from unauthorized access from within the card 3) The previous content of the memory is not accessible when that memory is reused 4) The memory recovery process is secure and consistent in case of a loss of power

Each trusted framework present on the card shall 1) Check the application access rules of the inter-acting Applications according to their respective privileges 2) Enforce the Trusted Framework security rules for inter-application communication, 3) Ensure that incoming messages are properly routed unaltered to their intended destinations 4) Ensure that any response messages are properly returned unaltered (except for any cryptographic protection) to the original receiver of the incoming message

The security and integrity of the card's components viz runtime environment, security domains, applications shall be ensured through data integrity, resource availability, confidentiality and authentication security mechanism. The other procedural means of protection, such as code testing and verification, physical security, and secure key handling shall be implemented.

The governmental restrictions upon cryptography shall be strictly adhered.

Secure Communication: Global Platform card shall offer the following security services associated with messages and defined within a Secure Channel Protocol (SCP)

-The Entity authentication – In which the card or the off-card entity proves its authenticity to the other entity through a cryptographic exchange.

-Integrity and authentication – In which the receiving entity (the card or off-card entity) ensures that the data being received from the sending entity (respectively the off-card entity or card) actually came from an authenticated entity in the correct sequence and has not been altered.

- Confidentiality – In which data being transmitted from the sending entity (the off-card entity or card) to the receiving entity (respectively the card or off-card entity) is not viewable by an unauthenticated entity Authentication of the off-card entity combined with the card Life Cycle State allows the card to assume its environment and/or context.

Secured channel protocols shall be used for the communication between the card and the off-card entity. Each entity shall mutually authenticate and establish session keys to protect the integrity and confidentiality of communication.

Chapter 5 - Security at Operator and Production Facility

5.1 Operator facility:

5.1.1 The operator shall maintain Card Management System that can store the entire details of a (U)ICC /(U)SIM card's life cycle.
5.1.2 The operator shall have secure key management system which shall be part of operator's information security policy. Key management techniques determine how keys are generated, stored, transmitted and refreshed.

5.1.3 The data exchange between (U)ICC/(U)SIM vendor and operator shall be encrypted, preferably with AES 128. The transport key(s) shall be generated by operator and shall be securely disseminated to the (U)ICC/(U)SIM, AuC and OTA platform suppliers(s) in a secure way.

5.1.4 Support of upto to 256 key sets to ensure the ability to utilize unique key sets between the (U)ICC/(U)SIM providers and between (U)ICC/(U)SIM order batches shall be made available. The operator should document procedures to define and securely retain the key values.

5.1.5 Different SIM transport keys shall be used with each SIM card vendor. A range of transport keys shall be used with each SIM card vendor. Transport keys shall not be shared across multiple SIM card vendors

5.1.6 Application management system that takes care of entire life cycle of an application shall be put in place by operator. Application management systems are used to manage card applications.

5.1.7 Post-issuance application downloads: No application shall be loaded in the card, without verifying the authenticity of the application.

5.1.8 The operator shall allow SIM OTA messages only from whitelisted sources.

5.1.9 Operator's Organizational security policy shall include (U)ICC/(U)SIM related risk assessment.

5.1.10 To the extent possible, the operator shall weed out the (U)ICC/(U)SIM cards which pose significant security risk. This may be done in a phased manner.

5.1.11 (U)ICC/(U)SIM used for testing (e-g for roaming, charging) shall be properly accounted and kept under safe custody.

5.2 Production facility

5.2.1 The hardware test features must be documented and destroyed after use.

5.2.2 The Test functions which get access to secret keys and data or undocumented feature shall be removed.

5.2.3 No debugging commands/functions must be left in the hard/soft masks.

5.2.4 During production phase, (U)ICC /(U)SIM vendor shall ensure that no malware like Trojan Horse, trap door and Backdoor are installed in the (U)ICC/ (U) SIM. Thorough testing shall be performed and there should be multiple layers of control for ensuring this.

5.2.5 Risk analysis shall be carried out by (U)ICC/ (U)SIM vendor.

5.2.6 Personalization is the one of the key processes during the (U)ICC production stage. Personalization shall be carried out only in India.

APPENDIX

List of Undertakings/Submission

1. Source Code Security Assurance (against test case 2.3.2)
2. Known Malware and backdoor Check (against test case 2.3.3)
3. Avoidance of Unspecified Wireless Access (against test case 2.4.6)
4. Cryptographic Based Secure Communication (against test case 2.6.1)
5. Cryptographic Module Security Assurance (against test case2.6.2)
6. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)