Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

embedded UICC (eUICC)

ITSAR Number: ITSAR409022411
ITSAR Name: NCCS/ITSAR/Customer Premises Equipment/SIM/embedded UICC (eUICC)

Date of Release: 28.11.2024 Version: 1.0.0
Date of Enforcement:

MTCTE के तहत जारी:
Issued under MTCTE by:
राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत
National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

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. 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.

Document History

S.no	Title	ITSAR no	Version	Date of release	Remark
1.	Embedded UICC (eUICC)	ITSAR409022411	1.0.0	28.11.2024	First release

Table of Contents

A) Outline

The objective of this document is to present a comprehensive, Country specific security requirements for the embedded (U)ICC/ eSIM for Consumer and M2M solutions as well as Remote SIM Provisioning (RSP) architecture. eUICC is an evolution of traditional physical SIM cards and offer greater flexibility, convenience in mobile telecommunications. The eUICC shall be a discrete tamper resistant component consisting of hardware and software, capable of securely hosting applications as well as confidential and cryptographic data. An eSIM (embedded-SIM) consists of software installed onto an eUICC chip permanently attached to a device with form factor of MFF2. It is a silicon chip that provides a secure vault for storing mobile subscription details into secure & trustful digital format.

RSP is a technology and process used in the mobile telecommunications industry to remotely provision, manage, and update eSIMs (embedded SIMs) over-the-air (OTA). It allows consumers to remotely activate the subscriber identity module (SIM) embedded in a portable device such as a smart phone, smart watch etc., eSIM and RSP architecture as per GSMA specifications SGP.21 Version 3.0, SGP.22 Version 2.5 and SGP.01 Version 4.3 is referred to develop this document.

There are various international standardization bodies/associations working on the security aspects, relevant to the e(U)ICC card. GSMA, ETSI, 3GPP, 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 commences with a brief description of the embedded UICC architecture, its functionalities and Remote SIM Provisioning Architecture and then proceeds to address the common and specific security requirements of Hardware, OS, and elements of eUICC.

B) Scope

The aim of this document is to define security requirements of the embedded UICC (eUICC) /eSIM deployed in consumer and M2M devices. The document targets on the security requirements of eUICC platform, eSIM application, Remote SIM provisioning (RSP) architecture and profile protection. The requirements specified here are binding both on operators and eUICC manufacturers. Target Of Evaluation (TOE) denotes eUICC in this document.

C) Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a 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 – Overview

1.1 Introduction

eSIM is a programmable SIM card, offering remote provisioning. It can be embedded in any type of device for either the consumer or the machine-to-machine (M2M) market. An eSIM is a chip soldered directly onto a device's circuit board during manufacturing, eliminating the need for physical swapping. eUICC is designed for remote SIM provisioning and management, that can host multiple SIM profiles on a single chip. It is not limited to consumer devices and can be used in various applications, including automotive, industrial, and M2M (Machine-to-Machine) devices.

1.2 eUICC Remote SIM Provisioning (RSP) Architecture

eSIM architecture enables over-the-air provisioning of the mobile network operator (MNO) profile without having to replace the physical SIM, e.g., eUICC itself.

The eSIM technology involves an embedded SIM or eUICC set directly into a device, offering the same level of security as traditional physical SIM to own multiple profiles with additional secure over-the-air update capabilities.

GSMA has established two distinct technical architectures for the use of eUICC within Consumer and M2M devices.

eUICC Remote SIM Provisioning Architecture specifications for consumer and M2M device are as follows:

Sno	eUICC type	Specification
1	M2M eUICC	GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification v4.3
2	Consumer device -LPA in eUICC	GSMA SGP.22 - RSP Technical Specification v2.5
	Consumer device -LPA in device	

1.2.1 Consumer eUICC RSP Architecture

Consumer RSP is a client driven model and is based on the end users managing their own devices and the profiles within them. It specifies the Roles and interfaces associated with the Remote SIM Provisioning and Management of the eUICC for consumer Devices. It comprises

around 4 elements: the Subscription Manager-Data Preparation plus (SM-DP+), Subscription Manager – Discovery Server (SM-DS), Local Profile Assistant (LPA) and eUICC.

A Device compliant with this specification shall implement at least one of the following:
• the LPA in the device (LPAd), or
• the LPA in the eUICC (LPAe)

1.2.1.1 RSP -LPA in the device (LPAd)

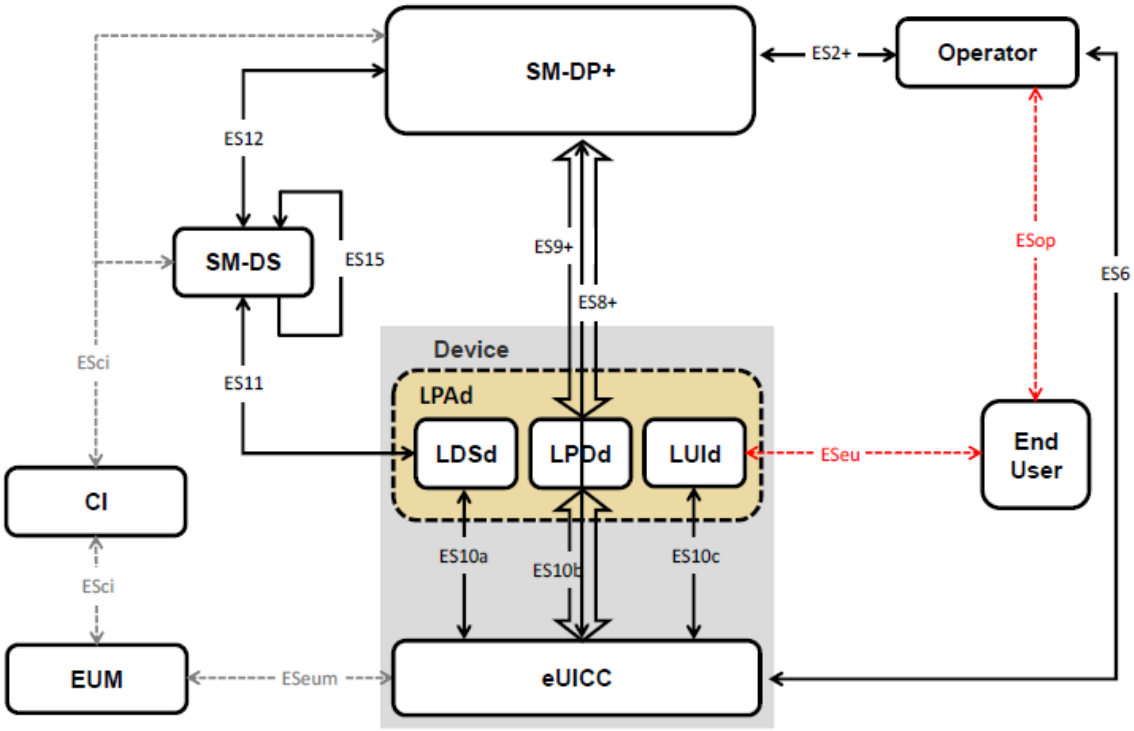

Figure 1. RSP Architecture in Consumer eUICC, LPAd
[Ref: GSMA SGP.22 - RSP Technical Specification v2.5]

Subscription Manager- Data Preparation plus (SM-DP+):

It has the responsibility for the creation, generation, management, download, and the protection of the Profiles, when requested by MNO.

Subscription Manager-Discovery Server (SM-DS):

The SM-DS provides the necessary mechanisms to notify the local discovery service within a device that the SM-DP+ element wants to communicate with it. The element sends an event registration message to the SM-DS for a target consumer device.

Certificate Issuer (CI):

A certificate issuer (CI) is considered a trusted third party, whose responsibility is to authenticate entities (e.g. the eUICC manufacturer, SM-DP+ and SM-DS) and provide digital certificates which enable entities to securely communicate. According to the GSMA, security certification issuers include both cybertrust and digicert.

Local Profile Assistant (LPA):

Local Profile Assistant, is a software component or application that facilitates the management of eSIM profiles on a user's device, such as a smartphone, tablet.

The primary purpose of an LPA is to enable users to download, activate, switch between, and manage eSIM profiles directly on their devices without the need for a physical SIM card or contacting a mobile network operator (MNO).

LPA assists with the download of Profiles and **secures the end user interface** on the device that is used for local control.

It performs mainly the following functions:

Local Discovery Service (LDS) -Retrieving Pending records from SM-DS

Local Profile Download (LPD)-Efficient Download of Bound Profile Package

Local User Interface (LUI)- This function allows the end user to perform Local Profile Management on the Device.

LPAd:

When the LPA is located in the Device, it is called LPAd. The LPAd is a functional element that provides Local Profile Download in the device (LPDd), Local User Interface in the device (LUId), Local Discovery Service in the device (LDSd) features. Figure1 provides the complete description of the consumer Remote SIM Provisioning and Management system, when LPA is in the Device (LPAd).

Interfaces:

The following table provides information about the interfaces within the Consumer device architecture specified in figure1.

Interface	Between		Description
ES2+	Operator	SM-DP+	Used by the Operator to order Profiles for specific eUICC's as well as other administrative functions

ES6	Operator	eUICC	Used by the operator for the management of operator service via OTA services.
ES8+	SM-DP+	eUICC	Provides a secure end-to-end channel between the SM-DP+ and the eUICC for the administration of the ISD-P and the associated Profile during download and installation. It provides Perfect Forward Secrecy.
ES9+	SM-DP+	LPD	used to provide a secure transport between the SM-DP+ and the LPA (LPD) for the delivery of the Bound Profile Package.
ES10a	LDSd	eUICC	Used between the LDSd and the LPA Service to handle a Profile discovery.
ES10b	LPDd	eUICC	Used between the LPDd and the LPA Service to transfer a Bound Profile Package to the eUICC. This interface plays no role in the decryption of Profile Packages.
ES10c	LUId	eUICC	Used between the LUId and the LPA Service for Local profile management by the End User.
ES11	LDS	SM-DS	Used by the LDS to retrieve Event Record for the respective eUICC.
ES12	SM-DP+	SM-DS	Used by the SM-DP+ to issue or remove Event Registrations on the SM-DS.
ES15	SM-DS	SM-DS	used in the case of developments of cascaded SM-DSs to connect those SM-DSs.
Esop	Operator	End User	Business interface between Operator and End User
Eseu	End User	LUI	Interface to initiate local profile management functions.
Eseum	eUICC	EUM	Administration interface between the eUICC vendor (EUM) and the eUICC.
Esci	CI	SM-DP+ SM-DS EUM	This interface used by SM-DP+, SM-DS & EUM to request a certificate and retrieve Certificate revocation status.

1.2.2 M2M eUICC Remote Provisioning Architecture

In this model, M2M uses a server driven (push model) with in charge of provisioning and managing profiles, and is organized around three elements, the subscription manager – data preparation (SM-DP), the subscription manager – secure routing (SM-SR) and the eUICC element.

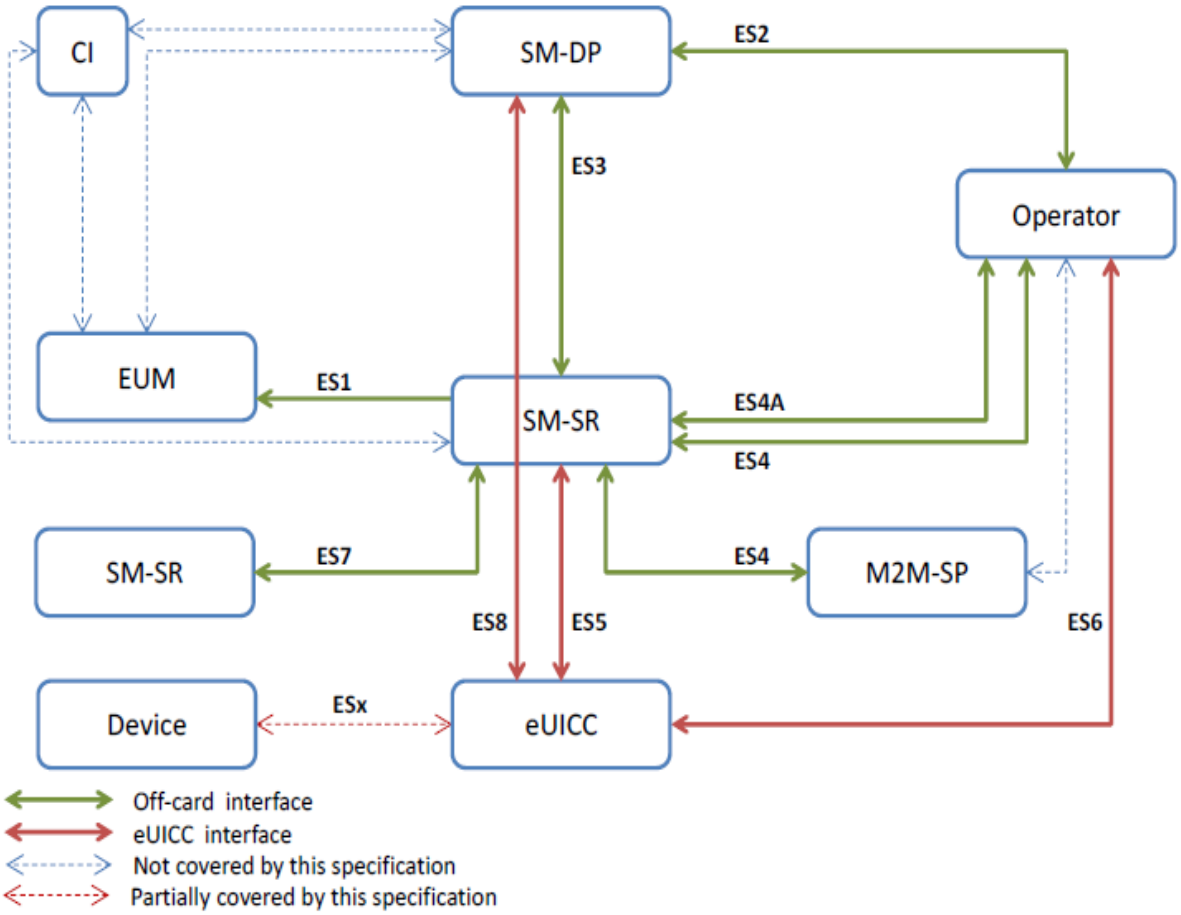

Figure 2. Remote Provisioning Architecture for M2M eUICC

[Ref : GSMA SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical specification V4.3]

Subscription Manager Data Preparation (SM-DP)

SM-DP acts on behalf of the MNO and is responsible for the preparation, storage, and protection of MNO profiles, while also downloading and installing profiles onto the eUICC. It also performs the functionality of downloading and installing the profiles onto the eUICC through SM-SR.

Additionally, it is responsible for managing profile enabling and deletion requests from the eUICC through the SM-SR.

Subscription Manager Secure Routing (SM-SR)

The SM-SR is responsible for securing the link between the SM-DP and the eUICC for the delivery of MNO profiles. It manages different functions such as enabling, disabling, and

deleting the different profiles on the eUICC. A key characteristic is that for the M2M device authentication with the SM-SR uses PSK (pre-shared key cryptography) and only allows a single SM-SR to communicate with the eUICC. The SM-SR holds a database of all the eUICC under its control and the key sets used to manage them. A group of deployed eUICC are managed by a single SM-SR. The SM-SR acts as a gateway between the SM-DP and the eUICC.

eUICC Manufacturer (EUM):
M2M device manufacturers can select any certified eUICC and can purchase directly from the eUICC manufacturer (EUM). EUM registers the eUICC at a designated SM-SR. After registration with SM-SR, it is ready for profile download and can be shipped to the M2M device manufacturer.

Interfaces:
The following table provides information about the interfaces within the M2M device architecture

Interface	Description
ES1	Interface between the EUM and the SM-SR that allows the registration of an eUICC with in the SM-SR
ES2	Interface between the MNO and the SM-DP that allows managing a Profile and to trigger Profile loading.
ES3	Interface between the SM-DP and the SM-SR that allows managing a Profile and to trigger Profile loading.
ES4	Interface between the MNO and the SM-SR that allows enabling, disabling, and deleting Profiles.
ES5	Interface between the SM-SR and the eUICC that allows OTA communication.
ES6	Interface between the MNO and the eUICC that allows managing the content of the MNO's Profile.
ES7	Interface between two SM-SR that allows managing the SM-SR change process.
ES8	Interface between the SM-DP and the eUICC that allows downloading of a Profile within the eUICC.

1.3 Schematic representation of eUICC Card architecture:

This section describes the internal high-level architecture of the eUICC in which profiles are provisioned based on the security framework defined in the Global Platform Card Specification.

M2M DEVICE:
Profiles are contained within security domains (SD) on the eUICC.

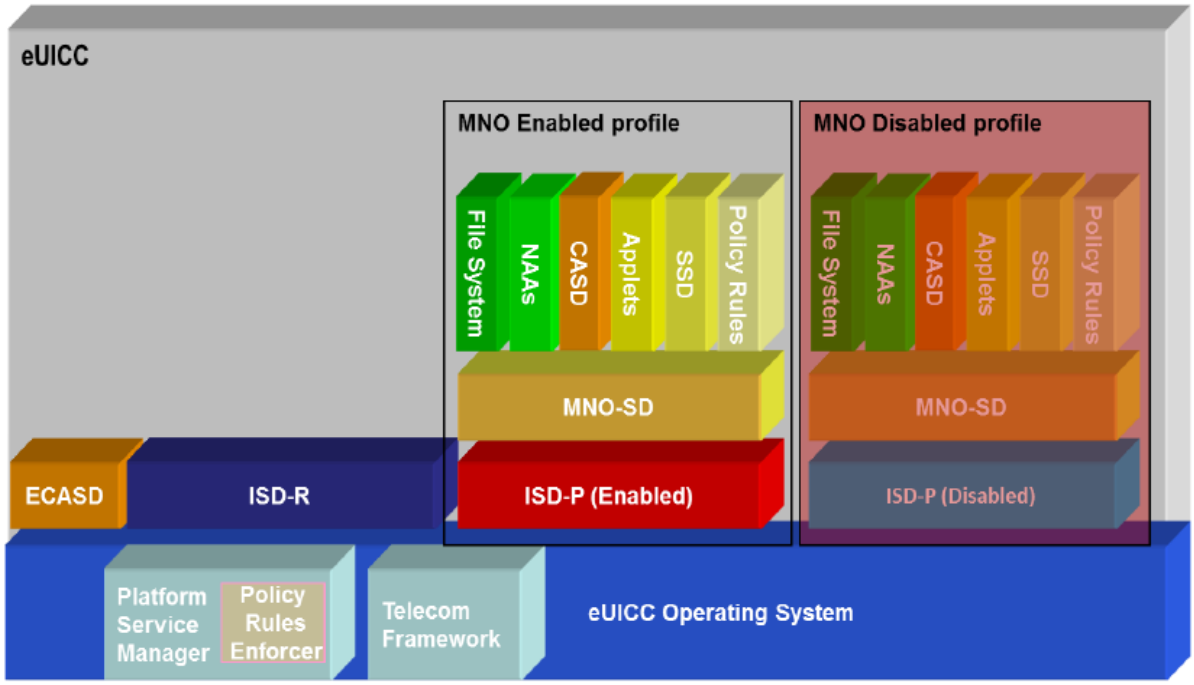

Figure 3: Schematic representation of the eUICC in M2M Device
[Ref: GSMA SGP.01 Embedded SIM Remote Provisioning Architecture Version 4.3]

Operating system (OS) contains the basic platform features, e.g. support of the features defined in the Global Platform Card Specification.

eUICC Certificate Authority Security Domain (ECASD):

- Contains a non-modifiable eUICC private key, the associated Certificate, the CI's root public keys and the EUM keyset for key/certificate renewal;
- It is associated to the ISD-R, which provides the underlying secure OTA channel;
- It is created within an eUICC at time of manufacturing;
- It Cannot be deleted or disabled after delivery;
- It is configured by the EUM at pre-issuance;

Issuer Security Domain-Root (ISD-R)

It is the on-card representative of the SM-SR that executes the Platform Management commands (such as ISD-P creation and deletion, Profile enabling and disabling, policy enforcement function, transport function).

An ISD-R shall:

a. be created within an eUICC at time of manufacturing;
b. be associated to an SM-SR;

c. not be deleted or disabled;
d. provides a secure OTA channel using Platform Management Credentials (SCP80 or SCP81) to the SM-SR;
e. implement a key establishment protocol for the support of the change of SM-SR;
f. Offers wrapping and unwrapping service of the transport part during Profile download;
g. be able to create new ISD-Ps with the required cumulative granted memory (CGM)
h. not be able to create any SD except an ISD-P;
i. executes Platform Management functions in accordance to the Policy Rules;
j. not be able to perform any operation inside an ISD-P.

Issuer Security Domain-Profile (ISD-P)

It is the on-card representative of the Operator, or SM-DP if delegated by the Operator.
An ISD-P shall:

a. be a separate and independent entity on the eUICC;
b. contain a Profile including MNO-SD, Connectivity Parameters, file system, NAAs and Policy Rules;
c. contain a state machine related to creating, enabling, and disabling the Profile;
d. contain keys for Profile management for the loading and installation phase;
e. Implement a key establishment protocol to generate a keyset for the personalization of the ISD-P;
f. be able to receive and decrypt, load, and install the Profile created by the SM-DP;
g. be able to set its own state to disabled once the Profile is installed;
h. provide SCP03 capabilities to secure its communication with the SM-DP;
i. The SM-DP performs the Profile Management functions (eUICC Eligibility Verification Function, Profile Download and Installation Function, Policy Rules Update Function, Profile Lifecycle Management Authorization Function) on the ISD-P during the load and install phase.
j. be able to contain a CASD. This CASD is optional within the Profile and provides services only to security domains of the Profile and only when the Profile is in Enabled state.
k. Once the Profile is installed in its ISD-P on the eUICC, the Profile and ISD-P shall be in union and thereafter it is the state of the ISD-P that is managed.

MNO-SD

It is the on-card representative of the Operator.
An MNO-SD shall:

a. Be associated to itself;

b. Contain the Operator OTA Keys;
c. Provide a secure OTA channel (SCP80 or SCP81);
d. Have the capability to host Supplementary Security Domains.
e. The MNO-SD is managed by an Operator OTA Platform once the Profile is enabled.

CONSUMER DEVICE:

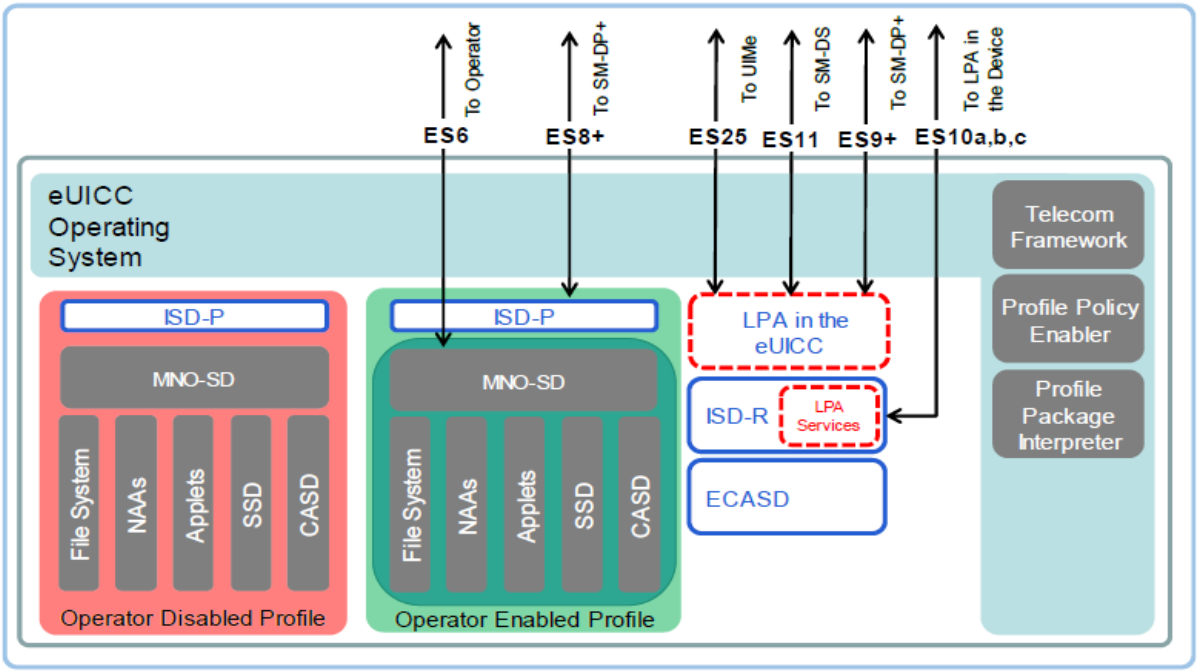

Figure 4: Schematic representation of the eUICC in Consumer Device
[Ref: GSMA SGP.21 RSP Architecture Version 3.0]

Embedded UICC Controlling Authority Security Domain (ECASD):

The ECASD is responsible for the secure storage of credentials needed to support the required security domains on the eUICC.

There shall only be one ECASD on an eUICC. The ECASD shall be installed and personalized by the EUM during the eUICC manufacturing as described in Global Platform Card Specification.

The ECASD shall contain the following:

- eUICC private keys for creating signatures.
- Associated Certificates for eUICC Authentication.
- The Certificate Issuers' (CI) root public keys for verifying SM-DP+ and SM-DS Certificates.
- eUICC Manufacturers' (EUMs) keyset for key/Certificate renewal.

Additionally, the ECASD shall provide security functions used during key establishment and eUICC Authentication.

Issuer Security Domain-Root (ISD-R)

The ISD-R is responsible for the creation of new ISD-Ps and the lifecycle management of all ISD-Ps.

Issuer Security Domain-Profile (ISD-P)

The ISD-P is a secure container (security domain) for the hosting of a Profile. The ISD-P is used for Profile download and installation in collaboration with the Profile Package interpreter for the decoding/interpretation of the received Bound Profile Package.
The ISD-P is the on-card representative of the SM-DP+.

Mobile Network Operator-Security Domain (MNO-SD)

The MNO-SD is the on-card representative of the Operator which issued the Profile. It contains the Operator's Over-The-Air (OTA) Keys and provides a secure OTA channel.

Profile Policy Enabler

The eUICC Operating System (OS) service which offers Profile Policy Rules validation and enforcement.

Telecom Framework

The telecom framework is an operating system service that provides standardized network authentication algorithms to the NAAs hosted in the ISD-Ps. Furthermore, it offers the capability to configure the algorithms with the necessary parameters.

Profile Package Interpreter

The Profile Package interpreter is an eUICC operating system service that translates the Profile Package data into an installed Profile using the specific internal format of the target eUICC.

Local Profile Assistant (LPA)Services

The role provides necessary access to the services and data required by the LPA functions. These services include:

a. Provide the address of the Root SM-DS and (if configured) the Default SM-DP+
b. Transfer Bound Profile Package from the LPAd to the ISD-P
c. Provides information regarding the installed Profiles and their Profile Metadata.
d. Provides Local Profile Management.
e. Supports Remote Profile Management operations

f. Provides functions for the LPA to authenticate and interact with the SM-DS.
g. Ensures access to the EID is restricted to only the LPA.

1.4 eUICC Security Platform Architecture for M2M:

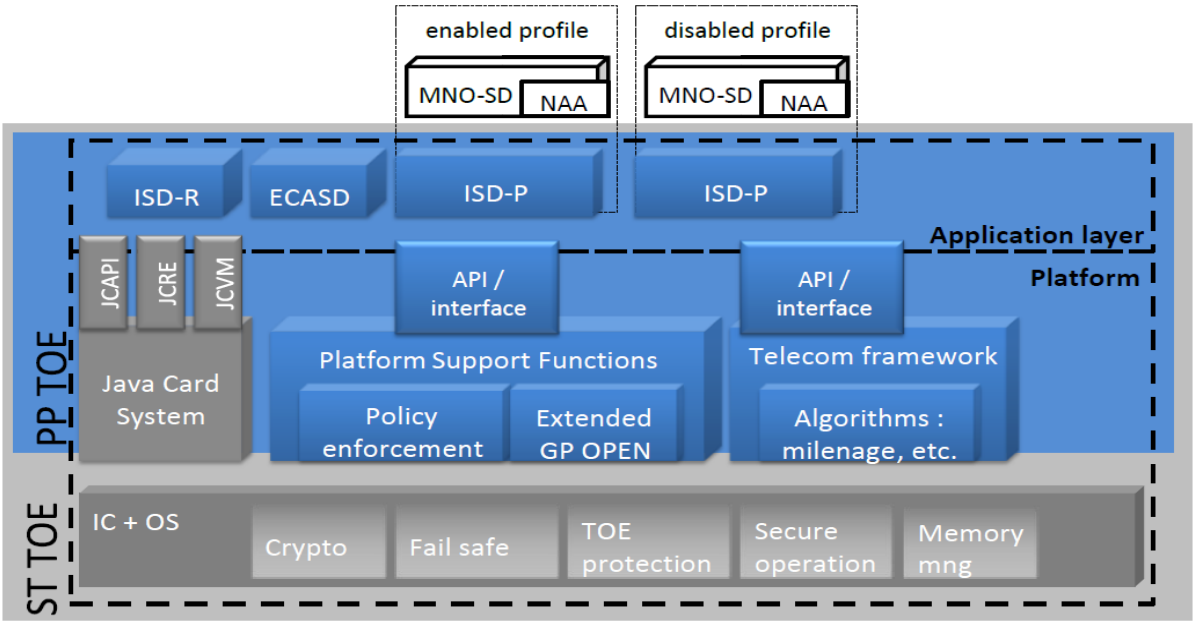

Figure5: Security Architecture of eUICC based on [PP0084]
[Ref: GSMA SGP.05 Embedded UICC Protection Profile]

Application Layer:

The goal of Application layer is to implement the eUICC functionalities which rely on the notion of a Profile. A Profile is the combination of a file structure, data and applications to be provisioned onto, or present on, a eUICC. Each Profile, combined with the functionality of the eUICC, behaves basically as a SIM card. A eUICC may contain more than one Profile, but only one profile is activated at a time. Each Profile is controlled by a unique ISD-P; consequently, only one ISD-P is enabled at a time on the eUICC.
A Profile can have several forms:

- A Provisioning Profile: The Profile contains Network Authentication Parameters. When installed on a eUICC, it enables access to communication network(s), only to provide transport capability for eUICC management and Profile management between the eUICC and an SM-SR.
- An Operational Profile: A Profile containing Network Authentication Parameters as well as MNO's applications and 3rd party applications.

- A Test Profile: A Profile that is used to provide connectivity to test equipment and cannot be used to connect to any MNO.

Platform Layer:

The Platform layer capabilities include:

- The **Platform Support Functions (PSF),** which are responsible for the administration of the eUICC.
- **Extended Global Platform OPEN functions** (**Extended GP OPEN)**, which extend the capabilities of a GP OPEN and Trusted Framework and must at least provide:
    a. API for SDs
    b. APDU dispatching to SDs
    c. SDs selection
    d. eUICC content management, which typically includes loading, installation, enabling, disabling, deletion of SDs.
    e. Trusted communications between SDs
- **Policy Enforcement functions**, which are in-charge of the verification and application of Policy Rules within the Profile (POL1) during Platform Management activities.
- **Telecom Framework**, which includes algorithms used by Network Access Applications (NAA) to access mobile networks. The NAAs are part of the Profiles, but the algorithms, as part of the Telecom Framework, are provisioned onto the eUICC during manufacturing.

Java Card System:

Java Card Platform can execute 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)** 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.
2. **Java Card Runtime Environment (JCRE)** is responsible for card resource management, network communication, applet execution and on card system & applet security.
3. **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.

Integrated Circuit (IC) or Chip:

The secure IC which is a hardware Device composed of a processing unit, memories, security components and I/O interfaces. It shall implement security features to ensure:

- The confidentiality and the integrity of information processed and flowing through the Device.
- The resistance of the secure IC to externals attacks such as physical tampering, environmental stress or any other attacks that could compromise the sensitive assets stored or flowing through it.
- The IC security features are required to be certified, either according to [PP0035] or according to [PP0084].

Embedded software (ES)

The eUICC relies on an Embedded Software (ES) loaded into the secure IC and which manages the features and resources provided by the chip. It is, generally divided into two levels:

1) Low level:

Drivers related to the I/O, RAM, ROM, EEPROM, Flash memory if any, and any other hardware component present on the secure IC,

2) High Level:

Protocols and handlers to manage I/O, memory and file manager, cryptographic services and any other high-level services provided by the OS.

Runtime Environment:

The Runtime Environment is responsible for providing an interface to all applications that ensures that the runtime environment security mechanisms cannot be bypassed, deactivated, corrupted or otherwise circumvented, for performing secure memory management to ensure that Isolation between security domains via an application firewall and provides applications with cryptographic means to protect their communications.

Chapter 2 – Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Management protocols mutual authentication

Requirement:

The protocols used for the eUICC (Local and Remote) management shall support mutual authentication mechanisms.

Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for eUICC management and maintenance.

[Reference: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0 Section 4.2.3.4.4.1]

2.1.2 Management traffic protection

Requirement:

eUICC management traffic shall be protected strictly using secure cryptographic controls prescribed in of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. 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 username, enables unambiguous authentication and identification of the authorized user.

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 for protecting user accounts (other than system /admin accounts) from misuse.

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

[Reference: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.4.2.1]

Section 2.2: Authentication Attribute Management

2.2.1 Authentication policy

Requirement:

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes shall be prevented.
This requirement shall also be applied to accounts that are used only 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 in eUICC.
Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.

Various measures or a combination of the following measures must be taken to prevent this:

a) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
b) 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.
c)Using an authentication attribute blacklist to prevent vulnerable passwords.

In-order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by eUICC. An exception to this requirement is machine accounts.

[Reference: TSDSI STD T1.3GPP 33.117-V17.1.0, Section 4.2.3.4.3.3]

2.2.3 Enforce strong password /PIN

Requirement:

The configuration setting shall be such that an eUICC 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 shall only be decimal or hexadecimal.
iii. PIN must be unique to each customer.

[Reference: a) TSDSI STD T1.3GPP 33.117-V17.1.0, Section 4.2.3.4.3.1,
b) 3GPP TS 51.011 V4.15.0, Section 9.3]

2.2.4 PIN changes

Requirement:

It should be possible to change PIN after presentation of correct old PIN.

[Reference: TSDSI STD T1.3GPP 33.117-V17.1.0 Section 4.2.3.4.3.2]

2.2.5 Management data protection

Requirement:

The data of Platform Support Function (PSF) linked to TOE Security Functionality (TSF) code shall be protected from unauthorized modification.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.2.2
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 3.1.2.2]

Section 2.3: Software Security

2.3.1 Secure update

Requirement:

a) eUICC Software package integrity shall be validated in the installation and update stage via cryptographic means, e.g. digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
b) Tampered software shall not be executed or installed if integrity check fails.

c) A security mechanism is required to guarantee that only authorized entities can initiate and perform the software update.

[Reference: TSDSI STD T1.3GPP 33.117-V17.1.0 Section 4.2.3.3.5]

2.3.2 Secure upgrade

Requirement:

a) eUICC Software package integrity shall be validated in the installation and upgrade stage via cryptographic means, e.g. digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
b) Tampered software shall not be executed or installed if integrity check fails.
c) A security mechanism is required to guarantee that only authorized entities can initiate and perform the software upgrade.

[Reference: TSDSI STD T1.3GPP 33.117-V 17.1.0 Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD) generated while developing the eUICC.

b) Also, OEM 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 eUICC Software, which includes OEM developed code, third party software and opensource code libraries used/embedded in the eUICC.
(ii) The eUICC software shall be free from CWE top 25, OWASP top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.
(iii) The binaries for eUICC and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

[Reference a) https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
b) https://owasp.org/www-project-top-ten/
c) https://owasp.org/www-project-api-security/]

2.3.4 Known malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that eUICC is free from all known malware and backdoors as on the date of offer of eUICC to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the eUICC to the designated TSTL.

2.3.5 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the eUICC shall not be present/configured.
OEM shall provide the list of software that are necessary for eUICC operation.
In addition, OEM shall furnish an undertaking as "eUICC does not contain Software that is not used in the functionality of eUICC."

[Reference: TSDSI STD T1.3GPP 33.117 V17.1.0, Section 4.3.2.3]

2.3.6 Unnecessary services removal

Requirement:

eUICC 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- V17.1.0, Section 4.3.2.1]

2.3.7 Restricted reachability of services

Requirement:

The eUICC shall restrict the reachability of services only to the interfaces meant for the legitimate communication peers.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, Section 4.3.2.2]

2.3.8 Self testing

Requirement:

The eUICC must perform self-tests during initial start-up, at the request of the authorized user and after power-on. The eUICC shall enter secure state if self-test fails or attacks are detected.

[Reference: Common Criteria Protection Profile Cryptographic Service Provider BSI-CC-PP-0104-2019, section-4.1 O.TSF]

Section 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:
Unused functions i.e., the software and hardware functions which are not needed for operation or functionality of the eUICC shall not be present in the eUICC.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:

OEM to ensure that the eUICC shall not contain software and hardware components that are no longer supported by them or their 3rd Parties including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be given by OEM.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0Section 4.3.2.5]

2.4.3 Avoidance of unspecified mode of Access

Requirement:

eUICC shall not contain any access mechanism which is unspecified or not declared.
An undertaking shall be given by the OEM as follows:
"The eUICC does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel."

Section 2.5: 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 privileged 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- V17.1.0 Section 4.2.3.6.3]

2.5.2 Audit event generation

Requirement:

The eUICC/eSIM shall log all important security events with unique system reference details as given in the Table below.
eUICC/eSIM must record, in 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 eUICC)	Events related to financial transaction	Transaction reference
		Event details
		Outcome of event (Success or failure)
		Time stamp (date and time)

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0 Section 4.2.3.6.1]

2.5.3 Secure log export

Requirement:

"Secure Log export shall comply with the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls only"

Section 2.6: Data Protection

2.6.1 Cryptographic based secure communication

Requirement:

eUICC shall communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

OEM shall submit to TSTL, the list of the connected entities with eUICC 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 eUICC (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.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the eUICC (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."

[Reference: a) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.
b) ENISA Recommendation "Standardization in support of the cybersecurity certification," Dec 2019]

2.6.3 Cryptographic algorithms implementation security assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of eUICC shall comply with the respective latest FIPS standards (for the specific crypto algorithm).

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithms implemented inside the Crypto module of eUICC is in compliance with the respective latest FIPS standards (for the specific crypto algorithm embedded inside the eUICC)."

2.6.4 Protecting data and information– confidential system internal data

Requirement:

a) When eUICC 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.

b) Access to maintenance mode shall be restricted only to authorized privileged user.

[Reference: TSDSI STD T1.3GPP 33.117-V 17.1.0 section 4.2.3.2.2]

2.6.5 Protecting data and information in storage

Requirement:

a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of eUICC system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with appropriate non-repudiation controls.

b) 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 (e.g., user passwords) in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

iii) Stored files in the eUICC: Shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0 section 4.2.3.2.3]

2.6.6 Protection against copy of data

Requirement:

a) Without authentication & authorization and except for specified purposes, eUICC shall not create a copy of data in use or data in transit.

b) Protective measures should exist against use of available system functions / software residing in eUICC to create copy of data for illegal transmission.

2.6.7 Protection of user data

2.6.7.1 Protection of keys

Requirement:

Cryptographic keys are owned by the Security Domains of MNO, ISD-R, and ISD-P. eUICC shall have security measures that protect all the cryptographic keys (as given below) from unauthorized disclosure, modification, and destruction.

- 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

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.1.1
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section:3.1.1.1]

2.6.7.2 Secure profile data

Requirement:

Confidential sensitive data of the applications mainly the following must be protected from unauthorized disclosure and modification:

a) PROFILE_NAA_PARAMS: Parameters used for network authentication, including keys.
b) PROFILE_IDENTITY: The International Mobile Subscriber Identity (IMSI) is the user credential when authenticating on a MNO's network via an authentication algorithm.
c) PROFILE_POL1: Data describing the Policy Control Functions in a profile.
d) PROFILE_USER_CODES: Optional activation code and hash of the optional confirmation code.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.1.2
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 3.1.1.2]

2.6.7.3 Secure profile code of MNO-SD

Requirement:

Profile applications, including first and second level applications (e.g., MNO-SD, CASD, SSD), along with the associated file system, must be safeguarded against unauthorized modifications to ensure their integrity and security.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.1.3
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 3.1.1.3]

2.6.8 Protection of TSF code

Requirement:

The TSF Code (TOE Security Functionality code) distinguishes between ISD-R, ISD-Ps and ECASD and platform codes. All these assets must be protected from unauthorized disclosure and modification.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.2.1
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0 section 3.1.2.1]

2.6.9 Data confidentiality

Requirement:

a) The eUICC must prevent unauthorised disclosure of sensitive data including SECRETS, eUICC_PRIVKEY, SK. EUICC.ECDSA and secret keys from keysets such as MNO_KEYS, ISD-R_KEYS, ISD-P_KEYS, PROFILE_NAA_PARAMS during storage and manipulation.
b) Platform Support Functions and the telecom framework must ensure the confidentiality of this data, while applications are required to utilize the protection mechanisms provided by the runtime environment.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:4.1.4, O. DATA-CONFIDENTIALITY
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.4, O. DATA-CONFIDENTIALITY]

2.6.10 Data integrity

Requirement:

a) The eUICC shall avoid unauthorised modification of the following data when managed or manipulated:
    1. Identity management data
        i. eUICC_PRIVKEY;

ii. eUICC_CERT;
iii. CI_ROOT_PUBKEY;
iv. EID
v. SECRETS;
vi. SK. EUICC.ECDSA,
vii. CERT.EUICC. ECDSA,
viii. PK.CI.ECDSA,
ix. CERT.EUM.ECDSA,
x. CRLs.

2. The following keysets:
   i. MNO_Keys,
   ii. ISDR_KEYS,
   iii. ISDP_KEYS
3. Profile data
   i. PROFILE_NAA_PARAMS,
   ii. PROFILE_IDENTITY
   iii. PROFILE_POLICY_RULES,
   iv. PROFILE_USER_CODES.
4. Management data:
   i. PLATFORM_DATA,
   ii. DEVICE_INFO,
   iii. PLATFORM_RAT.

b) Platform Support Functions and the telecom framework must ensure the integrity of the sensitive data they process, while applications are required to utilize the integrity protection mechanisms offered by the runtime environment.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:4.1.4, O. DATA-INTEGRITY2.

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.4, O. DATA-INTEGRITY]

Section 2.7: Network Services

2.7.1: Traffic separation

Requirement:

eUICC shall support logical separation of management traffic and control plane traffic.

[Reference: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0, section 4.3.5.1].

Section 2.8: Vulnerability Testing Requirements

2.8.1 Robustness against unexpected input:

Requirement:

OEM shall submit an undertaking that the externally reachable services of eUICC are reasonably robust when receiving unexpected input.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0 section 4.4.4]

2.8.2 Vulnerability scanning

Requirement:

It shall be ensured that no known vulnerabilities exist in the eUICC. This requirement shall be verified by using a suitable vulnerability scanning tool.
The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide remediation plan.

Sl No	CVSS Score	Severity	Remediation
1	9.0 – 10.0	Critical	To be patched immediately
2	7.0 – 8.9	High	To be patched within a month
3	4.0 – 6.9	Medium	To be patched within three months
4	0.1 – 3.9	Low	To be patched within a year

Zero-day Vulnerability shall be remediated immediately or as soon as possible.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.4.3]

Section 2.9: Operating System

2.9.1 Growing content handling

Requirement:

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

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, Section 4.2.4.1.1.1]

2.9.2 Authenticated privilege escalation only

Requirement:

eUICC 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- V17.1.0, section 4.2.4.1.2.1]

2.9.3 OS hardening

Requirement:

a) Appropriate OS hardening procedures including security measures required to ensure the OS security and miniaturization etc. shall be implemented in eUICC.
b) Network functions not needed for the operation of the eUICC shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0 section - 4.3.3.1.2]

2.9.4 Protection from buffer overflows

Requirement:

eUICC shall support mechanisms for buffer overflow protection

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section - 4.3.3.1.5]

2.9.5 File-system authorization privileges

Requirement:
eUICC shall be designed to ensure that only authorized users shall have the necessary privileges to modify files, data, directories, or file systems.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section - 4.3.2.7]

Section 2.10 Secure Identity Management

Identity management data is used to guarantee the authenticity of actor's identities such as EID, eUICC cert, CI's root certificate (self-signed), EUM's certificates, SM-DP, SM-SR, MNO, SM-DP+, shared secrets, used to generate credentials.

2.10.1 Protection of eUICC private key

Requirement:

The eUICC private key is used by the eUICC for its identity which is stored in ECASD. It shall be protected from unauthorized disclosure and modification.

[Ref: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.2.3, D.eUICC_PRIVKEY

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 3.1.2.3, D.SK. EUICC.ECDSA]

2.10.2 Protection of eUICC certificate

Requirement:

A certificate issued by the EUM (eUICC Manufacturer) shall be protected from unauthorized modification.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1 section: 3.1.2.3, D. eUICC_CERT.

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 3.1.2.3, D. CERT.EUICC. ECDSA]

2.10.3 Protection of CI_ROOT_PUBKEY

Requirement:

The CI's root public key is used to verify the certification chain of eUICC. It shall be protected from unauthorized modification.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.2.3, D.CI_ROOT_PUBKEY

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 3.1.2.3, D. PK.CI.ECDSA]

2.10.4 Protection of eID

Requirement:

The eID (eUICC-ID) uniquely identifies the eUICC. This identifier is set by the eUICC manufacturer stored in ECASD. In consumer device EID is used as a key by SM-DP+ and SM-DS and in M2M device it is used as a key by SM-SRs to identify eUICCs in its databases. eID shall be protected from unauthorized modification.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.2.3, D.EID. b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 3.1.2.3, D.EID]

2.10.5 Protection of shared secrets

Requirement:

The shared secrets used to protect the profile download shall be protected from unauthorized disclosure and modification.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:3.1.2.3, D. SECRETS
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section: 3.1.2.3, D. SECRETS]

Section 2.11: Web Servers

This entire section of the security requirements is applicable if the eUICC supports web management interface.

2.11.1 HTTPS

Requirement:

The communication between eUICC web client and eUICC web server shall be protected strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.2.5.1]

2.11.2 Webserver logging

Requirement:

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

a) Access timestamp
b) Source (IP address)
c) Account (if known)

d) Attempted login name (if the associated account does not exist)
e) Relevant fields in http request. The URL should be included whenever possible.
f) Status code of web server response

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:

The eUICC shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
eUICC 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- V17.1.0, section 4.2.5.4]

2.11.4 No system privileges

Requirement:

No eUICC web server processes shall run with system privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for eUICC operation shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for eUICC operation.
In particular, Common Gateway Interface (CGI) or other scripting components, Server Side Includes (SSI), and Web based Distributed Authoring and Versioning (WebDAV) shall be deactivated if they are not required.

Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.4]

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

Requirement:

If CGI 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- V17.1.0, section 4.3.4.5]

2.11.8 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- V17.1.0, section 4.3.4.6]

2.11.9 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- V17.1.0, section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:

Access rights for eUICC web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the eUICC web server shall be removed.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.9]

2.11.12 No directory listings

Requirement:

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

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

Requirement:

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

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.11]

2.11.14 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 eUICC web server and the modules/add-ons used. . Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the eUICC web server shall be replaced by error pages defined by the OEM.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for eUICC operation shall be deleted e.g., php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g., via links or in virtual directories) reside in the eUICC web server's document directory.
In particular, the eUICC web server shall not be able to access files which are not meant to be delivered.

[Reference: TSDSI STD T1.3GPP 33.117- V17.1.0, section 4.3.4.14]

2.11.17 HTTP user sessions

Requirement:

To protect user sessions, eUICC web server shall support the following session ID and session cookie requirements:

a) the session id shall uniquely identify the user and distinguish the session from all other active sessions.
b) the session id shall be unpredictable.
c) the session id shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
d) in addition to the session idle timeout, euicc web server shall automatically terminate sessions after a configurable maximum lifetime. this maximum lifetime defines the maximum session span. when the maximum lifetime expires, the session shall be closed, the session id shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. the default value for this maximum lifetime shall be set to 8 hours.
e) session id's shall be regenerated for each new session (e.g., each time a user logs in).
f) the session id shall not be reused or renewed in subsequent sessions.
g) eUICC shall not use persistent cookies to manage sessions but only session cookies. this means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.
h) where session cookies are used the attribute 'httponly' shall be set to true.
i) where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
j) where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
k) eUICC shall not accept session identifiers from GET/POST variables.
l) eUICC shall be configured to only accept server generated session ID's.

[Reference: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.3]

Section 2.12: Other Security requirements

2.12.1 No PIN recovery

Requirement:

No provision shall exist for eUICC PIN(s) recovery.

2.12.2 Software integrity check – boot

Requirement:

eUICC shall verify software image integrity at boot time, typically using a standard cryptographic hash as prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

2.12.3 Unused physical and logical interfaces disabling

Requirement:
eUICC shall support the mechanism to verify both the physical and logical interfaces existing in the product.
Physical and logical accessible Interfaces which are not under use shall be disabled.

2.12.4 Security algorithm modification

Requirement:

It shall not be possible to modify security algorithms supported by eUICC.

2.12.5 Secure random number generation

Requirement:

Random numbers which are required for cryptographic operations shall be generated in a secure manner. The Random Number Generation shall be conformant to the Cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

2.12.6 IMSI security

Requirement:

The Subscription Concealed Identifier, called SUCI, is a privacy preserving identifier containing the concealed SUPI.
For SUPIs containing IMSI, the UE shall construct the SUCI with the following data fields:

a) The SUPI Type as defined in TS 23.003 identifies the type of the SUPI concealed in the SUCI.
b) The Home Network Identifier is set to the MCC and MNC of the IMSI as specified in TS 23.003.
c) The permanent user identity (IMSI) of a user to whom services are delivered cannot be eavesdropped on the radio access link.

[Reference: a) 3GPP TS 33.501 V18.5.0, Section-6.12.2;
b) 3GPP TS 23.003 V18.5.0, Section- 2.2A
c) ETSI TS 133 102 V14.1.0 (2017-03), section-5]

Chapter 3 - Security Requirements of eUICC Platform

Section 3.1: Hardware (HW)

3.1.1 Protection of hardware

Requirement:

a) The eUICC hardware shall provide protection against the operations such as out of range – voltage/temperature/frequency, active shield etc.,
b) eUICC hardware shall maintain the integrity and confidentiality of the contents stored in its memories and correctly execute the software residing on it.
c) eUICC 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.
d) eUICC hardware shall be resistant to perturbation attacks that alter the normal behavior of an IC.
e) eUICC 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.
f) eID (eUICC ID) shall uniquely identify the eUICC.

Section 3.2: Operating System (OS)

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

3.2.1 eUICC OS update

Requirement:

An eUICC should support a secure mechanism for OS updates in the field.
a) In M2M device: in case an eUICC OS update happens, the EUM shall ensure that:

i) The resulting eUICC shall maintain, at least, the same level of security compliance than the previous eUICC.
ii) The eUICC Information Set (EIS) property 'updatedPlatformVersion' and 'remainingMemory' are updated.

b) In consumer device, "the process and mechanisms used to perform an eUICC OS Update in respect of consumer device may be Device manufacturer and EUM implementation-specific but shall be secured"

[Reference: GSMA SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification, V4.4, Section-2.2.6 and GSMA SGP.22 RSP Technical Specification, V3.0.1 section 2.4.13]

3.2.2 Secure and robust OS

Requirement:

The possibility of trap door, trojan horse and any other vulnerabilities shall be completely excluded in the card OS program code.

3.2.3 OS access control

Requirement:

a) OS shall feature a configurable access control mechanism that provides the options when creating the services.
b) OS shall grant file access privileges and monitor compliance with access rule reference file.
c) OS shall enforce access policy on subjects (users/administrator), objects (files) and operations (authentication, read, update, activate, deactivate, increase, invalidate, rehabilitate, and reset).
d) 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).
e) 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.

3.2.4 Secure execution environment

Requirement:

a) 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).
b) The program code shall be downloaded and executed only after passing suitable security checks.

3.2.5 Life cycle management of OS

Requirement:

Life cycle management of OS shall include:
a) Secure transition mechanism between states, such mechanism shall prevent the OS entering irreversible states.
b) The operating system shall prevent misuse of functionalities that are available only at certain states in the operating system life cycle.

3.2.6 Key management

Requirement:

The operating system shall provide secure generation, destruction, replacement, and storage of cryptographic keys according to the FIPS 140-2 or later standards.

3.2.7 Cryptographic operations

Requirement:

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 via cryptographic means using secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

3.2.8 Application management

Requirement:

a) OS shall ensure that an application cannot access memory locations outside its allocated space as part of application management.
b) The operating system shall provide security services to the application layer through:
    - API for cryptographic operations

- API for key management
- API for atomic transaction
- API for Random Number Generator (RNG).

Section 3.3: Protection from Attacks

3.3.1 Attack resistance

Requirement:

eUICC shall **be resistant** to the following attacks on the direct and indirect assets:

a) Exploitation of Test Features
b) Retrieving keys with Fault Analysis.
c) Attacks on Operating System/Software
d) Attacks on Random Number Generator.
e) Attacks on Protocols used (e.g., attacks involving OTA server).
f) Attacks on Java card Platform.
g) Attacks in a multi-application environment.

The direct and indirect assets include:

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

3.3.2 Prevention of memory exhaustion

Requirement:

Memory exhaustion is a type of denial-of-service attack and shall be prevented as follows:

a) On-card mechanisms shall manage the ISD-P creation in order to avoid attacks focusing on depleting the memory resources of the card.
b) Once an ISD-P is created, the mechanism shall automatically delete the ISD-P if the awaited process of the 'Download Profile' is not received in the proper time frame. This action should also send a notification to the SM-SR.

[Reference: ENISA, Embedded sim ecosystem, security risks and measures, March 2023, Section 5.4, SM6]

3.3.3 Protection against under-sizing memory attack

Requirement:

An under-sizing memory attack by the SM-SR prevents MNOs and SM-DPs from installing profiles on an eUICC. To avoid this,

a) eUICC's mutable characteristics such as 'remaining Memory' shall be protected to prevent under sizing memory attack.
b) eUICC shall sign the values to be sent to the SM-SR during an 'AuditEIS' function, using its private key including specific timestamp.

[Reference: ENISA, Embedded sim ecosystem, security risks and measures, March 2023, Section 5.4, SM7]

3.3.4 Inflated profile attack protection

Requirement:

Profile upper bound size shall be defined to minimize the inflated profile attacks. When making a 'Download Profile' request, the SM-DP and the SM-SR shall check the size of the profile to be safely created with this maximum size, thus mitigating malicious actions of profiles that exhaust the remaining memory.

[Reference: ENISA, Embedded Sim Ecosystem, Security Risks and Measures, March 2023, section 5.4, SM8]

3.3.5 Profile locking

Requirement:

To prevent profile abuse by opportunistic MNOs:

a) An upper bound of the locking period (e.g. 12 months) must be defined and a mechanism shall exist to automatically unlock the eUICC once the specified time frame expires.
b) A counter (to a specific value, e.g. >1) shall be set to permit profile locking only for a specific number of times during the lifetime of the eUICC.

[Reference: ENISA, Embedded sim ecosystem, security risks and measures, March 2023, section 5.4, SM9]

Section 3.4: Platform Security

3.4.1 Authentication of platform support functions

Requirement:

The platform shall guarantee that only the ISD-R or the service providers (SM-DP, MNO) owning a security domain with the appropriate privilege can manage the applications on the card associated with its security domain.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:4.1.1, O.PSF

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.1, O.PPE-PPI]

3.4.2 eUICC integrity- domain rights

Requirement:

a) The eUICC shall ensure that unauthorized actors shall not get access or change personalized MNO-SD keys. Modification of this security domain keyset is restricted to its corresponding owner (SM-SR, SM-DP, MNO OTA Platform).
b) eUICC shall ensure that only the legitimate owner of each security domain can access or change its confidential or integrity-sensitive data.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:4.1.1, O. eUICC-DOMAIN-RIGHTS

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.1, O. eUICC-DOMAIN-RIGHTS]

3.4.3 Secure communication channels

Requirement:

The eUICC must maintain secure SCP 80/81 communication channels between SM-SR and ISD-R (in M2M devices), between SM-DP and ISD-P (in M2M devices), between SM-DP+ and ISD-R (in consumer devices) and between MNO-SD and MNO OTA platform, ensuring all communications are safeguarded against unauthorized disclosure, modification, and replay.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1 section:4.1.1, O. SECURE-CHANNELS

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.1, O. SECURE-CHANNELS]

3.4.4 Secure operation

Requirement:

The PSF (Platform Support Function) of M2M device, PPE (Profile Policy Enabler) and PPI (Profile Package Interpreter) of consumer device and telecom framework belonging to eUICC shall ensure the correct operation of their security functions.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1 section:4.1.3, O. OPERATE

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.3, O. OPERATE]

3.4.5 Secure API

Requirement:

The platform code belonging to eUICC shall provide an API to:

a) provide atomic transaction to its services, and
b) control the access to its services. The eUICC must prevent the unauthorised use of commands.

[Ref: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:4.1.3, O. API
b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.3, O. API]

3.4.6 Internal secure channels

Requirement:

The eUICC shall ensure that the communication shared secrets transmitted from the ECASD to the ISD-R or ISD-P are protected from unauthorized disclosure or modification.
This protection mechanism shall rely on the communication protection measures provided by the runtime environment.

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:4.1.1, O. INTERNAL-SECURE-CHANNELS

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.1.1, O. INTERNAL-SECURE-CHANNELS]

3.4.7 Memory aging

Requirement:

The eUICC platform shall provide protection against the memory aging.

3.4.8 Secure runtime environment

Requirement:

The runtime environment shall provide secure means for card management activities, including:

a) load of a package file
b) installation of a package file
c) extradition of a package file or an application
d) personalization of an application or a security domain
e) deletion of a package file or an application
f) privileges update of an application or a security domain
g) access to an application outside of its expected availability

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:4.2.2, OE.RE.PSF

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section 4.2.2, OE.RE.PPE-PPI]

3.4.9 Preservation of secure state during failure

Requirement:

The eUICC shall preserve a secure state when the following types of failures occur:

a) failure of creation of a new ISD-P by ISD-R
b) failure of installation of a profile by ISD-R.
c) failure that leads to a potential security violation during:
    i. installation of a profile
    ii. PPR and RAT enforcement (in Consumer device)
    iii. POL1 enforcement (in M2M device)
    iv. Network authentication

[Reference: a) GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section: FPT_FLS.1.1/Platform_Services, FPT_FLS.1.1.

b) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section: FPT_FLS.1.1/Platform_Services, FPT_FLS.1.1.]

Section 3.5: Application-Level Security

3.5.1 Application security keys

Requirement:

eUICC shall generate application security keys as prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

3.5.2 STK based application

Requirement:

a) The applications developed to work in OS shall be loaded securely and shall be tested exhaustively for the absence of any malware.
b) To incorporate any change in an application, it must be possible to delete the existing application securely and download new application in a secured domain.

3.5.3 Java card based

3.5.3.1 Java card platform

Requirement:

a) Java card platform shall counter the unauthorized disclosure or modification of the code and data (keys, PINs, biometric templates, etc) of applications and platform.
b) The java card system shall provide strong and secure application installation mechanism, firewall mechanism, dedicated API for security services.

3.5.3.2 Protection of applications/applets

Requirement:

a) The applications/applets shall be installed in eUICC only after the verification of the digital signature. The converted applets (known as the CAP file) must be signed as a package by the issuer using an AES secret key, and the card shall check this signature (using the same key) when the CAP file is loaded.
b) Cryptographic keys owned by applets as well as end user's PIN shall be protected from unauthorized disclosure and modification.
c) Each applet shall be prevented from accessing the contents or behaviour of objects owned by other applets.
d) Applet impersonation shall be prevented.

3.5.3.3 Protection of system code

Requirement:

a) Java card system code/data/application shall be protected against unauthorized disclosure, modification, and execution.
b) The bytecode checker, shall ensure that no application uses resources outside its range.

3.5.3.4 Attack prevention mechanism

Requirement:

eUICC shall have protection mechanisms against application-level (resources of card) Denial of Service (DoS) attacks.

3.5.3.5 Application sandboxing

Requirement:

eUICC must provide a robust application sandboxing feature to enhance security. This feature ensures the implementation of a unique user ID (UID) for each application, facilitating the execution of applications in isolated processes.

[Reference: ETSI TS 101 220 V17.1.0, smart cards]

3.5.3.6 Protection of card

Requirement:

a) In case of security breach, it shall be possible to lock the card.
b) Before loading the key to the card, the key check value shall be verified.
c) If native methods are declared by Java card, they shall be protected through security check.

Chapter 4 – Specific Security Requirements

Section 4.1: Specific Security Requirements of eUICC in M2M device use cases

4.1.1 Network Authentication

4.1.1.1 Network access authentication

Requirement:

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.

The table below lists the algorithms that must be used for network access authentication.

Sl No	Security property	GSM	GPRS	3G-UMTS	4G-LTE	5G
1	Authentication	Comp 128-3 or GSM Milenage	Comp 128-3 or GSM Milenage	Milenage orTuak	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	AES 128 or above
3	Integrity Protection	-	-	UIA1-Kasumi or UIA2 Snow 3G	EIA1 Snow 3G or EIA2 AES 128 or above	AES 128 or above

4.1.1.2 No default algorithmic parameters

Requirement:

Default algorithmic parameters shall not be used. (for e.g., default MILENAGE offset values shall not be used).

4.1.2 Over the Air (OTA) Communication

4.1.2.1 Secure OTA communication

Requirement:

a) The communication between OTA server and eUICC shall be secured with cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
b) The communication over eUICC interfaces, ES5 (the Platform Management commands) and ES6 (the OTA Platform commands) shall be protected by either a SCP80 or SCP81 secure channel. The ES8 (The Profile Management commands) interface shall be protected by a SCP03 secure channel.

[Reference: GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, version 4.3, section:2.3]

4.1.2.2 OTA communication on ES5 (between SM-SR and eUICC)

Requirement:

In eUICC remote provisioning and management system, the OTA communication is exclusively handled by the SM-SR. The SM-SR shall use SMS and HTTPS for remote OTA communication with the eUICC.

- The eUICC shall support SMS and HTTPS
- The SM-SR shall support SMS and HTTPS

[Reference: GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, version 4.3, section:2.4.1]

4.1.2.3 SMS protocol (SCP 80)

Requirement:

- The eUICC shall support the sending of secure packet over SMS as defined in 3GPP TS 31.115.
- The eUICC shall support RAM (Remote Application Management) over SMS.
- The SMS (MT or MO) shall make use of a Cryptographic Checksum (CC) with a length of 64 bits using AES CMAC mode, ciphering using AES in CBC mode with key length 128 bits or more.

[Reference: 1. GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, version 4.3, section:2.4.3
2. 3GPP TS 31.115 V18.0.0, "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications"]

4.1.2.4 HTTPS protocol (SCP 81)

Requirement:

The eUICC shall support HTTPS Transport Layer Security (TLS) protocol v1.2 as defined in Global Platform Amendment B and shall support at least one of the following pre-shared key cipher suites

- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_CBC_SHA256

The Pre-Shared Keys (PSK) shall have an entropy of at least 128 bits.

[Reference: GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, version 4.3, section:2.4.4]

4.1.2.5 TLS session management

Requirement:

ISD-R and SM-SR shall support neither TLS session resumption (RFC 4507 or RFC 5077) nor several parallel TLS sessions.

[Reference: GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, version 4.3, section:2.4.4.1.3]

4.1.3 Communication on ES8 (between SM-DP and eUICC)

Requirement:

a) The ES8 interface is between the SM-DP and its ISD-P and goes through the SM-SR and rely on SCP 03. Hence, the eUICC shall support the Secure Channel Protocol 03 (SCP03) as defined in latest Global Platform Card Specification Amendment D.
b) AES session keys shall be generated every time a secure channel is initiated and are used in the mutual authentication process. These keys shall comply with Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, version 4.3, section:2.5]

4.1.4 Identification and authentication

Requirement:
The eUICC must

- identify the remote user SM-SR by its smsr-id and authenticate using CERT.SR.ECDSA.

- identify the remote user SM-DP by its smdp-id and authenticate using CERT.DP.ECDSA
- identify the remote user MNO-OTA by its mno-id and authenticate MNO-OTA via SCP80/81 using the keyset loaded in the MNO profile.
- identify the on-card user MNO-SD by its Application identifier (AID) and bind MNO-SD to the ISD-P of the corresponding MNO profile.

[Reference: GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1, section:6.1.2]

Section 4.2: Specific Security Requirements of eUICC in Consumer device use cases

4.2.1 Remote secure communication

The Remote SIM Provisioning (RSP) ecosystem relies on remote secure communication to achieve function execution requests and data exchanges. Any of the remote secure communication defined for RSP shall follow the rules hereunder.

4.2.1.1 Mutual authentication

Requirement:

- The server (the entity providing the function, e.g. SM-DP+) shall be authenticated first by the client (the entity requesting the function). Authentication shall include the verification of a valid server certificate.
- The client shall be authenticated by the server in a second step. In case the client is the eUICC, authentication shall include the verification of a valid eUICC and EUM certificate. Client authentication does not apply to the LPA.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:2.6.2]

4.2.1.2 Authorization

Requirement:

Based on authentication, the server shall always check that the requesting client is authorized before delivering the requested function execution.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:2.6.2]

4.2.1.3 Data privacy

Requirement:

- The eUICC, as a client, shall not reveal any private data to an unauthenticated server.
- The eUICC, as a client, shall not generate any signed material before having authenticated the Server.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:2.6.2]

4.2.2 Public Key Infrastructure (PKI)

Requirement:

Remote SIM Provisioning (RSP) ecosystem shall be based on a Public Key Infrastructure (PKI). Certificates must be used for authentication of the belonging entity via signature created with associated private key.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:2.6.3]

4.2.3 Protocol for profile protection and eUICC binding

Requirement:

- The Profile shall be protected by security mechanisms which are based on SCP11a as specified by the Global Platform Card Specification Amendment F latest version.
- The ISD-R shall not persistently store any SM-DP+ public key.
- Establishment of the session keys shall use only the shared secret generated from the one-time key pairs.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:2.6.4]

4.2.4 Key length and hashing functions

Requirement:

Key length and hashing functions shall comply with Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:2.6.5]

4.2.5 TLS cipher suites

Requirement:

RSP servers (e.g. SM-DP+) shall support the Transport Layer Security (TLS) protocol v1.2 and above. RSP servers shall use the cipher suites as prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:2.6.6]

4.2.6 OTA Communication

4.2.6.1 Communication on ES6 (between operator/service provider and eUICC)

Requirement:

The ES6 is the interface between the operator/service provider's OTA Platform and an enabled profile in eUICC. ES6 functions must use secure channel protocol (SCP 80/81) for communication between operator and MNO-SD of the enabled profile.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:5.4]

4.2.6.2 Communication on ES8+ (between SM-DP+ and eUICC)

Requirement:
The ES8+ is an interface defined between the profile package binding function of the SMDP+ and the eUICC. A secure channel shall be established between the profile package binding function of the SM-DP+ and the eUICC by:

a) mutual authentication of the eUICC and the SM-DP+ using SK.DPauth.ECDSA /CERT.DPauth.ECDSA and SK.EUICC.ECDSA/CERT.EUICC.ECDSA.
b) session keys agreement based on exchanged one-time public keys of both parties during mutual authentication.
c) session keys shall comply with Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

The data exchanged after channel establishment must be secured using SCP03t.

[Reference: GSMA SGP.22 RSP Technical Specification, version 2.5, section:5.5]

4.2.6.3 Protection of LPA interfaces

Requirement:

LPA shall ensure that the interfaces ES10a, ES10b and ES10c are trusted paths to the LPAd (LPA in the device).
The device-specific security implementation shall:

a. Verify the integrity of the LPAd and authorize it to be used.
b. Provide access to the trusted LUId user interface only for the authorized LPAd.

c. Provide access to the ISD-R of the eUICC only for the authorized LPAd.
d. Restrict access to the LPAd to only those applications and services that are provided by the OEM to enable the services and functions of the LPAd.
e. Protect the LPAd and the data it handles from unauthorized access and modification. Such data includes, but is not limited to, the EID, activation code, confirmation code, end user credentials, profile metadata, profile download and notification payloads, and event records.

[Reference: a) GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Section-4.3.1.4.
b) GSMA SGP.22 - RSP Technical Specification v2.5, section- C.3]

4.2.6.4 Communication on ESeu (between End User and LUI)

Requirement:

ESeu is the interface between the end user and the LUI. All local profile management operations of the LPA shall be explicitly initiated or authorized by the end user or device owner. The ESeu interface shall support the following requirements:

i. The LPA shall protect profile metadata from unauthorized access.
ii. The LPA shall provide a trusted link from the end user to the eUICC through the LUI.
iii. The communication between the end user interface of the primary device and the LUI of the companion device shall be protected (confidentiality, integrity, and authentication).

[Reference: GSMA SGP.21 - RSP Architecture v3.0, Section- 4.2.3, 4.11.3]

4.2.7 Identification and authentication

Requirement:

The eUICC must

- identify the remote user SM-DPplus by its sm-dp+ id and authenticate using CERT.DPauth. ECDSA.
- identify the remote user MNO-OTA by its mno-id and authenticate MNO-OTA via SCP80/81 using the keyset loaded in the MNO profile.
- identify the on-card user MNO-SD by its Application Identifier (AID).

[Reference: GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0, section: 6.2.1]

4.2.8 LPA integrity

Requirement:

LPA integrity within the eUICC must be maintained through robust security mechanisms such as secure boot, platform signing to ensure trust and protection against compromise.

[Reference: GSMA SGP.21 - RSP Architecture v3.0, section Annex G]

4.2.9 End user authentication

Requirement:

a. eUICC shall authenticate the user with a numeric pin of 4 to 8 decimal digits. Only upon entry of correct pin Mobile Equipment (ME) shall perform further actions.
b. The PIN shall be blocked and ME shall neither have access to the protected data nor shall be able to perform any action in the following cases:
    i. upon three consecutive entries of incorrect PIN
    ii. if the ME has been switched off.
c. Once PIN is blocked, further PIN verifications shall be denied.
d. eUICC shall have PIN unblock mechanism. A blocked PIN shall be unblocked by using PIN unblocking key. Unblocking key shall be at least of 8 decimal digits.
e. PIN change must be allowed only upon the entry of current PIN or unblock PIN.
f. User shall not be able to modify the unblock PIN. An indication shall be given to the user if an incorrect unblock PIN is entered. The unblock PIN shall be blocked in the following cases:
    i. upon ten consecutive entries of incorrect PIN
    ii. if the ME has been switched off.
g. It shall not be possible to read PINs or unblock PINs.

[Reference: 3GPP TS 51.011 V4.15.0, Section 9.3]

4.2.10 eUICC remote management of files and application

4.2.10.1 eUICC shared file system RFM

Requirement:

a) eUICC Shared File System Remote File Management (RFM) shall have access only to the Master File (MF) and all Dedicated Files (DF) and Elementary Files (EF) that are located under the MF.
b) No ADF (Application Data File) shall access the UICC Shared File System RFM.

[Reference: 1. 3GPP TS 31.116 v17.0.0 Release 17, section-5.3,
2. ETSI TS 102 226 V18.0.0, section-7.2]

4.2.10.2 RFM implementation over HTTPS

Requirement:

When using remote Application Protocol Data Unit (APDU) to perform RFM over HTTPS, the RFM/HTTP communication must occur over a secure and latest version of TLS.

[Reference: 1. 3GPP TS 31.116 v17.0.0 Release 17, section-5,
2. ETSI TS 102 226 V18.0.0, section-7.4, annex B]

4.2.10.3 Remote Application Management (RAM)

Requirement:

a) The Minimum-Security Level of a RAM application shall be validated via cryptographic means, e.g. digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
b) RAM Application shall support all features and functionality as below:
    - Application installation,
    - Application removal,
    - Application locking/unlocking,
    - Application information retrieval shall be compliant to the latest Global Platform Card Specification

[Reference: 1. 3GPP TS 31.116 v17.0.0 Release 17, section-6,
2. ETSI TS 102 226 V18.0.0, section-8.0, 8.1]

Annexure-I

Definitions

1) **Actor:** Physical entity (person, company, or organization) that can assume a Role in the functional architecture. It is possible for an Actor to assume multiple Roles in the same functional architecture.
2) **Assets:** Assets are security-relevant elements to be directly protected by the TOE. They are divided into two groups. The first one contains the data created by and for the user (User data) and the second one includes the data created by and for the TOE (TSF data).
3) **Application IDentifier (AID**): Data element, which identifies an application in a card
4) **Application Protocol Data Unit (APDU):** Standard communication messaging protocol between a card accepting device and a smart card.
5) **Application Program Interface:** An Application Programming Interface (API) is a set of well-defined methods of communication between software components without any user intervention
6) **Application Firewall:** This term is used to describe the functions of the eUICC Runtime Environment that restrict the capability of applications to access or modify data belonging to other applications. The Java Card System Firewall is an example of such Application Firewall.
7) **AuditEIS:** It is a function that allows the Operator to retrieve the up-to-date information for the Operator's Profiles. This function allows the SM-DP, requesting on behalf of an Operator, to retrieve up to date EIS information. At the end of the successful execution of this function, the SM-SR SHALL update its EIS database upon the basis of this information.
8) **Card Application Toolkit (CAT):** Set of applications and related procedures that may be used during a card session.
9) **CERT.EUICC. ECDSA:** Certificates issued by the EUM for a specific, individual, eUICC. Certificates contain public keys (PK. EUICC.ECDSA) and are stored in ECASD. This certificate can be verified using the EUM Certificate.
10) **CI_ROOT_PUBKEY:** The CI's root public key is used to verify the certification chain of eUICC and remote actors. It is stored in ECASD.
11) **Controlling Authority Security Domain (CASD):** security domain providing cryptographic functions, as specified in Global Platform Card Specification Amendment A.
12) **Consumer solution:** for the 'direct to consumer' channel, this solution is required where the end user (or consumer) has direct choice of the operator supplying

connectivity. Consumer solutions require a high degree of end user interaction, with the principle that the end user is familiar with operating the end user interface and actively choosing their network connectivity provider. The Consumer solution also targets enterprises who use devices targeted to the consumer market.

13) **Companion Device:** A Device that relies on the capabilities of a Primary Device for the purpose of Remote SIM Provisioning.
14) **Certified Revocation List (CRL):** The optional certificate revocation lists (extract) stored in the eUICC.
15) **Cryptography:** The enciphering and deciphering of messages into secret codes by means of various transformations of the plaintext.
16) **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)
17) **Device: In Consumer device-** User equipment used in conjunction with an eUICC to connect to a mobile network. E.g. a tablet, wearable, smartphone, or handset.
    In M2M device- Equipment into which an Embedded UICC and a communication module are inserted during assembly. Examples include Utility meter, car, and camera.
18) **DEVICE_INFO:** This asset includes the security-sensitive elements of Device Information data, such as the device type allocation code (TAC) or the device capabilities (ex. support for updating of certificate revocation lists (CRLs)), that is provided to the eUICC by the LPAd.
19) **Dedicated File (DF):** file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files
20) **Disabled (Profile):** The state of a Profile where all files and applications (for example NAA) present in the Profile are not selectable over the eUICC Terminal interface.
21) **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.
22) **EID:** The EID (eUICC-ID) uniquely identifies the eUICC. This identifier is set by the eUICC manufacturer and does not change during operational life of the eUICC. It is stored in ECASD.
23) **Embedded UICC Controlling Authority Security Domain (ECASD):** It is responsible for the secure storage of credentials needed to support the required security domains on the eUICC.
24) **Elementary File (EF):** file containing access conditions and data and no other files.
25) **Emergency Profile:** An Operational Profile with a Profile Attribute allocated, indicating that this Profile is an Emergency Profile. An Emergency Profile provides the capability to make/receive Emergency Calls.
26) **Enabled (Profile):** The state of a Profile when its files and/or applications (for example, NAA) are selectable over the UICC-Terminal interface.

27) **End User:** The person using the Device.
28) **End User Data:** Information that pertains to the identity of an End User e.g. personal details, name, address, biometric characteristics, assigned identification numbers, etc.
29) **eSIM:** eSIM is the top-level generic descriptor applied to the Devices and eUICCs that support Remote SIM Provisioning.
30) **ES6**: The interface used by the Operator to manage the content of their Profile.
31) **ES8+:** Provides a secure end-to-end channel between the SM-DP+ and the eUICC for the administration of the ISD-P and the associated Profile during download and installation.
32) **eUICC:** A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the Device, and enables the secure changing of Profiles.
33) **eUICC_PRIVKEY:** The eUICC private key is used by the eUICC to prove its identity and generate shared secrets with remote actors. It is stored in ECASD.
34) **eUICC Certificate (eUICC- CERT):** A certificate issued by the EUM for a specific eUICC. This certificate can be verified using the EUM Certificate. It is stored in ECASD.
35) **EUM (eUICC Manufacturer):** Supplier of the eUICCs and resident software (for example firmware and operating system).
36) **EUM Certificate:** A certificate issued to a GSMA accredited EUM which can be used to verify eUICC Certificates. This certificate can be verified using the Root Certificate.
37) **eUICC Memory Reset:** An action that returns the eUICC to a state equivalent to a factory state.
38) **eUICC OS Update:** A mechanism to correct existing features on an eUICC by the original OS Manufacturer when the eUICC is in the field.
39) **Event:** A Profile download which is set by an SM-DP+ on behalf of an Operator, to be processed by a specific eUICC.
40) **Event Record:** The set of information stored on the SM-DS for a specific Event, via the Event Registration procedure. This information consists of either: the Event-ID, EID, and SM-DP+ address or the Event-ID, EID, and SM-DS address.
41) **Event Registration:** A process notifying the SM-DS on the availability of information on either a specific SM-DP+ or a specific SM-DS for a specific eUICC.
42) **Fallback (or Fall-back):** The Fall-back Mechanism shall be activated in case of loss of network connectivity by the current Enabled Profile. The eUICC shall disable the current Enabled Profile and enable the Profile with Fall-back Attribute set. Only one Profile can have the Fall-back attribute set.
43) **File:** directory or an organized set of bytes or records in the SIM
44) **First level application:** selectable application that is indicated in EF_{DIR} under the MF. (e.g. eSIM application)
45) **Form Factor:** The various sizes or forms of card; For removable cases, it can be 1FF,2FF (mini), 3FF (micro) and 4FF (nano). For embedded SIM, Form Factor is MFF2.

46) **Global Platform:** Global Platform is a non-profit industry association which develop Global Platform'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.
47) **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.
48) **Hash of the optional Confirmation Code (Hashed Confirmation Code)**: End User may use to confirm a Profile Download and Installation via the Local User Interface (LUId).
49) **Home PLMN:** This is a PLMN where the MCC and MNC of the PLMN identity match the MCC and MNC of the IMSI.
50) **Issuer Identifier Number:** The first 8 digits of the EID.
51) **Issuer Security Domain (ISD):** A security domain on the UICC as defined by [Global Platform Card Specification]. This Protection Profile defines an ISD called ISD-P for the SMDP, and an ISD called ISD-R for the SM-SR.
52) **ISDP_KEYS:** This Profile Management keyset is used by SM-DP to perform Profile Management functions via its on-card representative (ISD-P).
53) **ISDR_KEYS:** This Platform Management keyset is used by SM-SR to perform Platform Management functions, via its on-card representative (ISD-R).
54) **IMSI:** The international mobile subscriber identity is a unique 15-digit number provided to the subscriber. It consists of the MCC, MNC, and MSIN.
55) **Integrated Circuit Card IDentifier (ICCID):** Unique number to identify a Profile in a eUICC.
56) **Integrated circuit card (ICC)** 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.
57) **Integrated circuit (IC):** Security IC comprises of IC hardware and software test functions which are needed during production phase.
58) **Integrated eUICC:** An eUICC implemented on a Tamper Resistant Element (TRE) that is integrated into a System-on-Chip (SoC), optionally making use of remote volatile/non-volatile memory.
59) **Local Profile Assistant:** A functional element in the Device or in the eUICC that provides the Local Profile Download (LPD), Local Discovery Services (LDS) and Local User Interface (LUI) features.
60) **Local Profile Management:** Local Profile Management are operations that are locally initiated on the End User (ESeu) interface.
61) **Local Profile Management Operation:** Local Profile Management Operations include enable Profile, disable Profile, delete Profile, query Profile Metadata, eUICC Memory

Reset, eUICC Test Memory Reset, set/edit Nickname, add Profile and edit default SM-DP+ address.

62) **Logical Interface:** In case of MEP: logical connection between an endpoint in the Device and an Enabled Profile or another logical secure element.
63) **LPA Proxy:** A component of the Device used as a proxy between an Operator authorized platform and the corresponding Profile to manage the Profile's content.
64) **Master File (MF):** unique mandatory file containing access conditions and optionally DFs and/or EFs.
65) **Machine to Machine (communication):** communication between remotely deployed devices with specific responsibilities and requiring little or no human intervention, which are all connected to an application server via the mobile network data communications
66) **Mobile Network Operator Security Domain (MNO-SD):** Security domain part of the Profile, owned by the Operator, providing the Secured Channel to the Operator's OTA Platform. It is used to manage the content of a Profile once the Profile is enabled.
67) **M2M solution:** for the 'business to business to consumer' channels, this solution serves the needs of business-to-business customers, specifically in the Internet of Things (IoT) market.
68) **M2M Service Provider (M2M SP):** A Service Provider relying on an Operator providing the Profiles on the eUICC.
69) **MFF (M2M Form Factor):** new form factor dedicated to M2M applications.
70) **M2M UICC:** UICC with specific properties for use in M2M environments, this includes existing form factors and the new form factors MFF1 and MFF2.
71) **MNO_KEYS:** Keys used by MNO OTA Platform to request management operations from the ISD-P. The keys are loaded during provisioning and stored under the control of the MNO SD.
72) **Modem:** component in the terminal that provides interfaces to the mobile network, to the UICC and to a Connected Entity
73) **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.
74) **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.
75) **Network Access Application (NAA):** Application residing in a Profile providing authorization to access a network.

76) **Operator/Telecommunication Service Provider:** An entity who has been granted with the license to provide telecommunication services in the country.
77) **Operator Credentials:** A set of credentials owned by the Operator, including Network Access Credentials, OTA Keys for Remote File/Application management, and authentication algorithm parameters
78) **Operational Profile:** A Profile that allows connectivity to a commercial mobile network.
79) **Optional Activation Code:** End User may use to initiate a Profile Download and Installation via the Local User Interface (LUId).
80) **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.
81) **OTA Keys:** The credentials included in the Profile, used in conjunction with OTA Platforms.
82) **OTA Platform:** An Operator platform for remote management of UICCs and the content of Enabled Operator Profiles on eUICCs.
83) **PK.CI.ECDSA:** The CI's public key (PK.CI.ECDSA) used to verify the certification chain of eUICC and remote actors. It is stored in ECASD.
84) **PLATFORM_DATA:** The data of the platform environment, like the identifiers and privileges including SM-DS OID, MNO OID and SM-DP+ OID and the eUICC life-cycle state of the ISD-P security domain.
85) **Platform Management:** A set of functions related to the, enabling, disabling and deletion of a Profile and the transport of Profile Management functions to an eUICC. Platform Management actions are protected by Platform Management Credentials shared between the SM-SR and the ISD-R. Platform Management does not affect the contents of a Profile.
86) **PLATFORM_RAT:** Data describing the Rules Authorization Table (RAT) of the eUICC. These rules are initialized at eUICC manufacturing time or during the initial device setup provided that there is no installed operational profile. The OEM or EUM is responsible for setting the content of the RAT. RAT is stored in the eUICC.
87) **Policy:** Principles reflected in a set of rules that governs the behavior of eUICC and/or entities involved in the remote management of the eUICC.
88) **Policy Rule:** Defines the atomic action of a Policy and the conditions under which it is executed.
89) **Primary Device:** A Device that can be used to provide some capabilities to a Companion Device for the purpose of Remote SIM Provisioning.
90) **Profile:** Combination of a file structure, data, and applications to be provisioned onto, or present on, an eUICC and which allows, when enabled, the access to a specific mobile network infrastructure.

91) **PROFILE_IDENTITY:** The International Mobile Subscriber Identity is the user credential when authenticating on a MNO's network via an authentication algorithm. The IMSI is a representation of the subscriber's identity and will be used by the MNO as an index for the subscriber in its HLR. Each IMSI is stored under the control of the ISD-P during provisioning.
92) **Profile Management:** A set of functions related to the downloading, installation, and content update of a Profile in a dedicated ISD-P on the eUICC. Download and installation are protected by Profile Management Credentials shared between the SM-DP and the ISD-P (in M2M), between SM-DP+ and the ISD-P (in Consumer).
93) **Profile Policy Enabler (PPE)**: It ensures Enforcement of the PPRs of a Profile. It verifies that a Profile containing PPRs is authorized by the RAT.
94) **Profile Package Interpreter (PPI):** Profile Package Interpreter, an eUICC Operating System service that translates the Profile Package data (as defined in SIMalliance eUICC Profile Package Specification) into an installed Profile using the specific internal format of the target eUICC.
95) **Profile Policy Management:** A policy control system that allows the Service Provider to implement, manage and enforce its subscription terms and conditions associated with the installed Profile.
96) **PROFILE_POLICY_RULES(PPR):** Data describing the profile policy rules (PPRs) of a profile. These rules are loaded during provisioning and stored under the control of the ISD-P. They are managed by the MNO OTA Platform.
97) **Provisioning Profile:** A combination of Operator data and applications to be provisioned on an eUICC for the purposes of providing connectivity to a mobile network solely for the purpose of the provisioning of Profiles on the eUICC.
98) **PROFILE_NAA_PARAMS:** Parameters used for network authentication, including keys.
99) **PROFILE_USER_CODES:** It consists of the optional Activation Code and hash of the optional Confirmation Code (Hashed Confirmation Code).
100) **Rules Authorization Table (RAT):** These rules are initialized at eUICC manufacturing time or during the initial device setup provided that there is no installed operational profile. The OEM or EUM is responsible for setting the content of the RAT. RAT is stored in the eUICC.
101) **Remote SIM Provisioning (RSP):** The downloading, installing, enabling, disabling, and deleting of a Profile on an eUICC.
102) **Remote Profile Management (RPM):** Profile Management operations performed by a managing SM-DP+ at the request of the Profile Owner.
103) **RSP Server:** Either an SM-DS or SM-DP+.
104) **Second level application:** Application which can only be activated during the session of a first level application. NOTE: A second level application may have an AID. This AID is not to be stored in EF(DIR) unless it is also a first level application

105) **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.

106) **Secure Channel:** A secure channel is a trusted channel which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms.

107) **Secured data:** data field containing the secured application message and possibly padding octets.

108) **Secured packet:** information flow on top of which the level of required security has been applied.

109) **SECRETS:** It includes the one-time keys of eUICC, SM-DP+, session keys (S-ENC and S-MAC) and the initial MAC chaining value. And shared secret used to protect the profile download and to protect the new SM-SR credentials during a handover.

110) **SK. EUICC.ECDSA:** The eUICC private keys, stored in ECASD, used by the eUICC to prove its identity, and generate shared secrets with remote actors.

111) **Smart card:** It is a secure microcontroller which is protected against physical and logical security attacks.

112) **SM-DP+ OID:** Identifier of the SM-DP+ that is globally unique and is included as part of the SM-DP+ Certificate.

113) **SM-DS OID:** Identifier of the SM-DS that is globally unique and is included as part of the SM-DS Certificate.

114) **Subscriber:** An entity (associated with one or more users) that is engaged in a Subscription with a Telecommunication Service Provider. The Subscriber is allowed to subscribe and unsubscribe to services, to register a user or a list of users authorized to use those services, and to set the limits relative to the use that associated users make of those services.

115) **Subscription:** Describes the commercial relationship between the Subscriber and the Telecommunication Service Provider.

116) **SUbscription concealed Identifier (SUCI):** A one-time use subscription identifier, called the SUbscription Concealed Identifier (SUCI), which contains the Scheme-Output, and additional non-concealed information needed for home network routing and protection scheme usage.

117) **Subscription Permanent Identifier (SUPI):** The SUPI is a globally unique 5G Subscription Permanent Identifier allocated to each subscriber in the 5G System. It may indicate an IMSI, a Network Specific Identifier (NSI), a Global Line Identifier (GLI) or a Global Cable Identifier (GCI).

118) **Tamper Resistant Element (TRE):** A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data.

119) **Target Of Evaluation (TOE):** The TOE is physically defined as a device consisting of hardware, firmware, and software. The TOE may be implemented as security integrated circuit platform for application, dedicated system on chip core or security integrated circuit.

120) **Telecom Framework:** A set of service(s) and/or application(s) of the TOE supporting the NAA by providing network authentication algorithms.

121) **Transport layer:** layer responsible for transporting Secured Packets through the network

122) **Trusted Link:** According to NIST SP 800-53r5, a mechanism by which an end user (through an input Device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the end user or the security functions of the information system and cannot be imitated by untrusted software.

123) **UICC:** smart card that conforms to the specification written and maintained by the ETSI Smart Card Platform project.

124) **UICC application session:** execution of a sequence of commands internal to the UICC that can result in the performance of one or several proactive UICC sessions.

Annexure-II

Acronyms

3GPP	-	Third Generation Partnership Project
ADF	-	Application Dedicated File
ADM Key	-	Administrator Key
AES	-	Advanced Encryption Standards
AID	-	Application Identifier
APDU	-	Application Protocol Data Unit
API	-	Application Programming Interface
CAT_TP	-	Card Application Toolkit Transport Protocol
CERT	-	Certificate
CASD	-	Controlling Authority Security Domain
CBC	-	Cipher Block Chaining
CC	-	Cryptographic Checksum
CERT.EUICC. ECDSA	-	Certificate of the eUICC for its Public ECDSA key
CERT.EUM.ECDSA	-	Certificate of the EUM for its Public ECDSA key
CERT.DPauth.ECDSA	-	Certificate of the SM-DP+ for its Public ECDSA key used for SM-DP+ authentication.
CERT.SR.ECDSA	-	Certificate of the SM-SR for its Public ECDSA key
CERT.DP.ECDSA	-	Certificate of the SM-DP for its Public ECDSA key
CI	-	Certificate Issuer
CIN	-	Card Image Number / Card Identification Number
CHV	-	Card Holder Verification (PIN)
CMAC	-	Cipher-based Message Authentication Code
CRL	-	Certificates Revocation List
CSP	-	Communication Service Providers
DH	-	Diffie-Hellman
DF	-	Dedicated file
DNS	-	Domain Name System
ECC	-	Elliptic Curve Cryptography
ECASD	-	eUICC Certificate Authority Security Domain
ECDSA	-	Elliptic Curve cryptography Digital Signature Algorithm
ECKA	-	Elliptic Curve Key Agreement algorithm
eID	-	eUICC-ID
EIS	-	eUICC Information Set
EPS	-	Evolved Packet System
ESIN	-	EUM Specific Identification Number
eSIM	-	Embedded Subscriber Identity Module
ETSI	-	European Telecommunications Standards Institute
EUM	-	eUICC Manufacturer

eUICC	-	Embedded Universal Integrated Circuit Card
GP	-	Global Platform
GPCS	-	Global Platform Card Specification
GSMA	-	GSM Association
GSMA CI	-	GSMA Certificate Issuer
HLR	-	Home Location Register
HR	-	High Resolution
HTTP	-	Hypertext Transfer Protocol
ICCID	-	Integrated Circuit Card ID
IMS	-	IP Multimedia Subsystem
IMEI	-	International Mobile Equipment Identity
IMSI	-	International Mobile Subscriber Identity
ISD	-	Issuer Security Domain
ISD-P	-	Issuer Security Domain Profile
ISD-R	-	Issuer Security Domain Root
ISO	-	International Standards Organization
ITU	-	International Telecoms Union
JCAPI	-	Java Card API
JCRE	-	Java Card Runtime Environment
JCS	-	Java Card System
JCVM	-	Java Card Virtual Machine
LDS	-	Local Discovery Service
LPA	-	Local Profile Assistant
LPAd	-	Local Profile Assistant when LPA is in the Device
LPAe	-	Local Profile Assistant when LPA is in the eUICC
LPD	-	Local Profile Download
LPR	-	LPA Proxy
LTE	-	Long Term Evolution
LUI	-	Local User Interface
MAC	-	Message Authentication Code
MCC	-	Mobile Country Code
ME	-	Mobile Equipment
MF	-	Master File
M2M	-	Machine to machine
MNO	-	Mobile Network Operator
MNO-OID	-	Mobile Network Operator- Object Identifier
MNO-SD	-	Mobile Network Operator - Security Domain
MNC	-	Mobile Network Code
MO	-	Mobile Originated
MT	-	Mobile Terminated
MSISDN	-	Mobile Subscriber International Subscriber Directory Number

MSP	-	Mobile Service Provider
NAA	-	Network Access Application
OID	-	Object Identifier
OS	-	Operating System
OTA	-	Over The Air
PIN/PIN2	-	Personal Identification Number/ Personal Identification Number 2 (obsolete terms for CHV1 and CHV2, respectively)
PKI	-	Public Key Infrastructure
PK.CI.ECDSA	-	Public Key of the CI
PK.EUICC.ECDSA	-	Public Key of the eUICC
PLMN	-	Public Land Mobile Network
POL1	-	Policy Rules within the Profile
PP	-	Protection Profile
PPK	-	Profile Protection Key (random keys per profile)
PSF	-	Platform Support Functions
PPI	-	Profile Package Interpreter
PPR	-	Profile Policy Rule
PPAR	-	Profile Policy Authorization Rule
PUK	-	PIN Unblocking Key
QR Code	-	Quick Response Code
RAM	-	Remote Applet Management
RAT	-	Rules Authorization Table
RoT	-	Root of Trust
RE	-	Runtime Environment
RFM	-	Remote File Management
RPM	-	Remote Profile Management
RSA	-	Rivest / Shamir / Adleman asymmetric algorithm
RSP	-	Remote SIM Provisioning
SAS	-	Security Accreditation Scheme
SAS-SM	-	Security Accreditation Scheme for Subscription Management
SAS-UP	-	Security Accreditation Scheme for UICC production
SCP	-	Secure Channel Protocol
SD	-	Security Domain
ShS	-	Shared Secret
SIM	-	Subscriber Identity Module
SK.EUICC.ECDSA	-	Private key of the eUICC for creating signatures
SK.DPauth.ECDSA	-	Private Key of the of SM-DP+ for creating signatures for SM-DP+ authentication.
SM	-	Subscription Manager
SMS	-	Short Message/Messaging Service
SM-DP	-	Subscription Manager Data Preparation
SM-SR	-	Subscription Manager Secure Routing

SM-DP+	-	Subscription Manager - Data Preparation plus
SM-DS	-	Subscription Manager - Discovery Service
S-ENC	-	Session Key for message Encryption/Decryption
S-MAC	-	Session Key for message MAC generation/verification
SoC	-	System-on-Chip
SSD	-	Supplementary Secure Domain
STK	-	Sim Tool Kit
SUCI	-	Subscription Concealed Identifier
SUPI	-	Subscription Permanent Identifier
TAR	-	Toolkit Application Reference
TLS	-	Transport Layer Security
TLV	-	Tag-Length-Value
TRE	-	Tamper Resistant Element
TS	-	Technical Specification
TOE	-	Target Of Evaluation
TSF	-	TOE Security Functionality
	-	User Interface
UICC	-	Universal Integrated Circuit Card
UIMe	-	User Interface Module for LPAe
URL	-	Uniform Resource Locator
USIM	-	Universal Subscriber Identity Module

Annexure-III

List of Submissions

List of Undertakings to be furnished by the OEM for eSIM Security testing submissions.

1. Source code security assurances (against testcase 2.3.3)
2. Know malware and backdoor check (against testcase 2.3.4)
3. No unused software (against testcase 2.3.5)
4. No unsupported components (against testcase 2.4.2)
5. Avoidance of unspecified mode of access (against testcase 2.4.3)
6. Cryptographic based secure communication (against testcase 2.6.1)
7. Cryptographic module security assurance (against testcase 2.6.2)
8. Cryptographic algorithms implementation security assurance (against testcase 2.6.3)
9. Robustness against unexpected input (against testcase 2.8.1)

Annexure-IV

References

1. TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0, “Catalogue of general security assurance requirements”.
2. 3GPP TS 51.011 V4.15.0, “Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface”.
3. 3GPP TS 31.115 V18.0.0, “Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications”.
4. 3GPP TS 31.116 V17.0.0, “3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Remote APDU Structure for (U)SIM Toolkit applications”.
5. 3GPP TS 33.501 V18.5.0, “Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system”.
6. 3GPP TS 23.003 V18.5.0, “Technical Specification Group Core Network and Terminals Numbering, addressing and identification.”
7. 3GPP TS 24.008 V18.5.0, “Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3.”
8. 3GPP TS 31.102 V18.4.0, “Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application.”
9. GSM Association GSMA SGP.05 - Embedded UICC Protection Profile, version 4.1
10. GSM Association GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile, Version 1.0
11. GSM Association GSMA SGP.22 - RSP Technical Specification, Version 2.5
12. GSMA SGP.22 RSP Technical Specification, V3.0.1
13. GSM Association GSMA SGP.01- Embedded SIM Remote Provisioning Architecture, Version 4.3.
14. GSM Association GSMA SGP.21, RSP Architecture, Version 3.0
15. GSM Association GSMA SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 4.3.
16. GSMA eSIM Whitepaper, The what and how of Remote SIM Provisioning, March 2018.
17. GSMA, eUICC Security Assurance Scheme (eSA) scheme.
18. GSMA, SAS Standard for Subscription Manager (SAS-SM) Roles, Version 3.2
19. GSMA, Security Accreditation Scheme for UICC Production (SAS-UP)– Standard, Version 9.2.
20. Common Criteria Protection Profile, Cryptographic Service Provider, BSI-CC-PP-0104-2019.
21. ENISA Embedded Sim Ecosystem, Security Risks and Measures, March 2023.

22. ENISA Recommendation “Standardization in support of the cybersecurity certification,” Dec 2019.
23. ETSI TS 101 220 V17.1.0, “Smart Cards; ETSI numbering system for telecommunication application providers”.
24. ETSI TS 102 221 UICC-Terminal interface; Physical and logical characteristics, Version 15.0.0.
25. ETSI TS 102.223, Smart Cards; Card Application Toolkit. (CAT)
26. ETSI TS 102.224 Smart Cards; Security mechanisms for the Card Application Toolkit.
27. ETSI TS 102 225 Secured packet structure for UICC based applications, Version 18.0.0.
28. ETSI TS 102 226 Remote APDU structure for UICC based applications, Version 18.0.0.
29. ETSI TS 102.240, Smart Cards; UICC Application Programming Interface (UICC API)
30. ETSI TS 102.241, UICC API for Java Card.
31. ETSI TS 131 048 V5.1.0, “Security mechanisms for the (U)SIM application toolkit” (3GPP TS 31.048 version 5.1.0, Release 5).
32. ETSI TS 133 102 V14.1.0, “Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture”.
33. ETSI TS 102 671, Smart Cards; Machine to Machine UICC; Physical and logical characteristics, Version 16.0.0.
34. Global Platform Technology, Card Specification, Version 2.3.1, GPC_SPE_034.
35. Global Platform Technology, Remote Application Management over HTTP Card Specification v2.3 – Amendment B, GPC_SPE_011.
36. Global Platform Technology, Secure Channel Protocol '03' Card Specification v2.3 – Amendment D, GPC_SPE_014.
37. Secure Channel Protocol '11', Card Specification v2.3 – Amendment F, GPC_SPE_093.
38. Security Guidelines for UICC Profiles, Version 1.0, GSM Association.
39. Global Platform Technology, Secure Channel Protocol '03', Card Specification v2.3 – Amendment D, Version 1.1.2, GPC_SPE_014.
40. Global Platform Card, Secure Channel Protocol '11', Card Specification v2.2 – Amendment F, Version 1.0, GPC_SPE_093.