

Ministry of Communications
Department of Telecommunications
(Access Services Cell)
Sanchar Bhawan, 20, Ashoka Road, New Delhi

No.: 800-04/2017/AS.II

Dated: 16.07.2021


To,

1. All CMTS/UASL/UL (having Access Service Authorization) Licensees
2. SIM Manufacturers supplying SIMs to the Telecom Service Providers

Subject: Standard Operating Procedure (SOP) for Personalisation of SIM cards.

Vide instructions no. 800-04/2017/AS.II dated 19.08.2019, it has been mandated that Personalization of SIM cards provided to the subscribers for accessing the mobile network of Licensed Telecom Service Providers shall be mandatorily done within India w.e.f 01.03.2020.

2. In this regard, the Standard Operating Procedure (SOP) to be followed by the Licensed Telecom Service Providers and SIM Manufacturers for personalization of SIM cards is enclosed as **Annexure**.


(Suresh Kumar)
ADG (AS-II)
011-23310215

Enclosure: A/a

Copy to:-

1. Director General Telecom, DoT HQ
2. DDG(SA), DoT HQ

**DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA**

**Standard Operating Procedure
for
SIM Personalization
(Version 1.0)**

Contents

1. Introduction	2
2. Purpose of SOP	2
3. Stakeholders	3
4. SIM Production Lifecycle	4
5. Personalization Process	6
6. Security Controls	7
7. Incident Management	14
8. Glossary	15

1. Introduction

A Subscriber Identity Module or Subscriber Identification Module (SIM), widely known as a SIM card, is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number, OTA key and other keys which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store applications, contact information etc. on many SIM cards depending upon the card storage capacity.

With the introduction of smartphones and need of smaller SIM cards for Smart Phones, the traditional mini-SIM was redesigned into the micro-SIM, and later it was redesigned again into the Nano-SIM standard of today. Further with the growth of IOT and M2M, embedded SIM cards (eSIM) are developed which are soldered in device enabling itself with Remote Provisioning feature.

Form Factor of SIM:

SIM is usually categorized on the basis of following form factors (FFs):

- Pluggable form factors such as 1FF,2FF (Mini SIM), 3FF (Micro), and 4FF (Nano)
- Embedded/ soldered form factors such as MFF1/ MFF2.
- eSIM (Embedded SIM) with Remote profile management)

As per DoT order no. 800-04/2017/AS.II dated 19.08.19, it has been decided that Personalisation of SIM cards, provided to the subscribers for accessing the mobile network of Licensed Telecom Service Providers, shall be mandatorily done within India w.e.f 01.03.2020.

2. Purpose of SOP

- a) To ensure that directive issued by the DOT (AS) is converted into actionable points by virtue of Standard Operating Procedure (SOPs) to which various stakeholders adhere to uniformly.
- b) To outline a clear procedure for formulating auditable steps for security implementation surrounding the SIM personalization and related data exchange and its management, with in the country.
- c) To ensure that all stakeholders have a clear understanding about the required minimum control mechanism for SIM personalization in India.

This document covers the Standard Operating Procedure to be adopted during personalisation of SIM card not having the capability of remote lifecycle management i.e. all SIM except eSIM provided to the subscribers for accessing the mobile network of Licensed Telecom Service Providers.

3. Stakeholders

The SOPs is applicable to all concerned dealing with various functions/ roles for Secure Personalization of SIM. The stakeholders are as follows.

1. Department of Telecommunications (DOT) and Telecommunication Engineering Center (TEC) for policy framework and its notification related to the SIM personalization in India.
2. Field Units (LSAs) of DoT for auditing the licensed MNO and SIM manufacturers as per SOP.
3. Licensed Mobile Network Operators (MNO), who is responsible for SIM sourcing for their subscribers, providing relevant profiles application to SIM manufacturers and storing the keys transferred by SIM manufacturers.
4. SIM manufactures registered in India having their SIM personalisation related system development and Personalization Centre.

4. SIM Production Lifecycle: The brief of process of SIM personalisation is explained in figure 1. However, the security measures and procedures to be adopted during the SIM personalisation process are elaborated in Section-6 of this document.

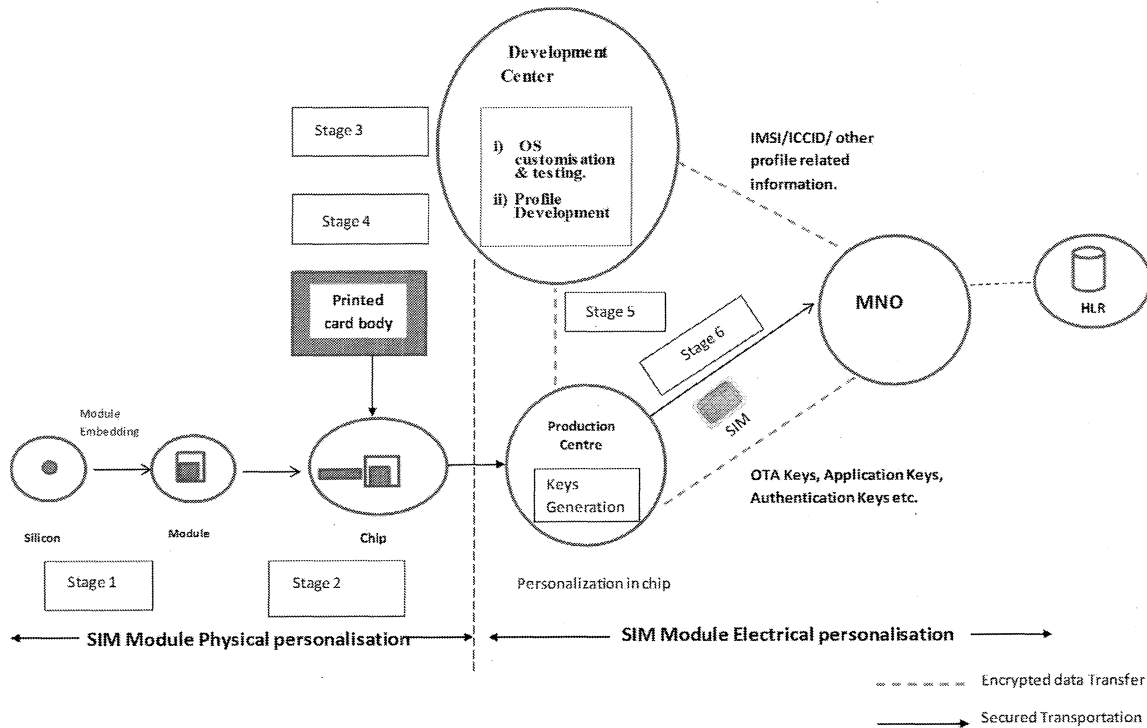


Figure 1

SIM lifecycle comprise of taking the printed card body, development of IC by milling and embedding the IC into the printed card and subsequently personalization or loading of operating systems, IMSI, OTA Keys, application keys and all keys into the chipset. The product lifecycle of SIM are as follows:

i. Stage 1: Development, Manufacturing, Testing and Packaging of ICs

This is the first stage of SIM development. The IC is designed, processed and embedded in plastic body.

ii. Stage 2: SIM Product finishing process

After Stage-1, the external finishing and external colour and visual finishing are done and SIM hardware is ready for software based personalisation.

iii. Stage 3: Development of SIM OS software

Development of operating system is done at Development centre of SIM manufacturer. In this stage, the SIM pre-personalisation activities start with the

development/customisation of Operating System (OS) of the SIM. The SIM operating system is responsible to manage all execution/process in SIM.

The key functions of the SIM Operating System, which are common across all SIM, products include:

- Management of interfaces between the card and the outside world, primarily in terms of the interchange protocol.
- Management of the files and data held in memory.
- Access control to information and functions (for example, select file, read, write, and update data).
- Management of card security and the cryptographic algorithm procedures.
- Maintaining reliability, particularly in terms of data consistency, sequence interrupts, and recovering from an error.

The operating system should also have the capability of supporting the standard algorithm as these are responsible for processing, encryption and decryption of data using the relevant keys stored in SIM.

iv. Stage 4: SIM Personalization

After development of operating system in pre-personalisation Stage-3, the next step is loading of operating system into the SIM. The MNO sends its profiles data including IMSI/ICCID, details of application to SIM Manufacturers production house in encrypted form. After receiving this information, manufacturer generates profiles and keys. This is most important stage of SIM personalisation wherein all important data like IMSI/ICCID and security keys such as authentication keys, OTA keys, Application keys, PINs/PUKs and all network related profiles, as provided by operator, are securely generated for secure injection into the chip. Subsequently the module is sent to production house securely.

v. Stage 5: Transfer to Production Center:

In this stage, the profiles, keys and third party applications are securely injected on the CHIP. The designed SIM as per requirement of MNO are securely sent for storage in warehouse for further delivery to MNO.

vi. Stage 6: Delivery of SIM to the MNO

The SIM is securely transferred to Licensed MNO for its end usage. All the keys are securely transferred to MNO for secure loading into HLR.

5. Personalization Process

Personalization is mainly the process of transferring the electrical information onto the card module. Personalisation process inter-alia include development/customisation and loading of OS into the Chipset, development and loading of Applications into the chipset, sourcing of required details from Licensed Telecom Operator, transfer and loading of Keys into the Chipset. The procedure for SIM personalisation lifecycle is given below:

i). Development & Integration of Operating System:

The SIM operating system inter-alia has the functionality for encryption and decryption of keys. All standardised algorithm which are used for encryption and decryption of keys has to be supported by SIM operating system as it is responsible to process the encryption and decryption of data using the relevant keys stored in SIM.

Although the development of operating system is part of pre-personalisation process, but considering its importance, it should be developed in protected environment preferably within the country having defined Security process. In case OS development is done for global customers outside India, its integration with MNO profile and security testing and loading into chipset has to be done within geographical boundaries of the country following security requirements given in Section 6.2.

ii). Installation of Operating System on SIM hardware:

After integration of operating System with customer specific parameters, the security tested OS is ported into the chip. This shall be done by SIM Card manufacturer within secured environment in the facility located in India.

iii). Generation and transfer of keys:

The operator should send IMSI/ICCID, application and other related information to the SIM manufacturer premises in encrypted manner over secure channel(s) using PGP or other advanced Cryptographic techniques. The SIM manufacturer generates applications keys and other keys on the basis of inputs received from MNO in an encrypted manner. All the details such as IMSI/ICCID, Algorithms, keys (Ki, OTA keys, Bank keys, Application keys, PINs/PUKs) or any operator specific information shall be transferred to production house through secure protocol like SFTP preferably using VPN and should be handled in line with Security Accreditation Scheme (SAS) for UICC Production issued by GSMA. Now the Operator profile, OTA keys, 3G/4G keys, application keys are loaded into Chip module i.e SIM card.

iv). Transfer of SIM:

Subsequently the fully loaded SIM card is transferred securely to the MNO. All the Keys and other related information is encrypted and transferred to operator as an encrypted file for further loading in MNO's system for making them ready for activation.

v). Storage of keys at MNO's database i.e. HLR:

The encrypted keys as securely transferred by SIM manufacturer should be stored in HLR in encrypted form by MNOs nodal officer responsible for SIM personalisation/loading in MNO's system.

6. Security Controls

The MNO and SIM personalisation agency should prepare an organization security policy elaborating the organization setup, roles and responsibilities for Security Management covering the SIM personalisation lifecycle. The security policy should be well documented along with the responsibility matrix for managing the security setup along with incidents. Proper access controls and authentication mechanisms, roles, escalation matrix, incident management procedure etc. should also be specified in the policy.

The adequate security controls should be maintained during entire lifecycle of SIM personalisation including Physical Security, Data Security in rest, transit and during destruction. The IT system and physical environment used for SIM personalisation shall be separate and isolated. UICC Personalisation centre has to be accredited under the Security Accreditation Scheme (SAS) of GSMA for UICC Production. If Personalisation centre is not accredited with GSMA SAS, the same should comply to GSMA SAS guidelines and it will be audited by a team specified by DoT to assess the compliance with GSMA SAS guidelines. The broad security guidelines to be adopted are given in following sections.

6.1. Physical Security:

The manufacturer premises are mainly divided into two broad areas comprising of Development centre and Production centre. Physical security controls are required at all areas(s) where any work related to SIM personalisation is carried out. Broad guidelines for physical security are given below.

- i. A clear site perimeter and boundary must be identified for all areas.
- ii. Map each area and define physical security protection standards for each area on sensitivity basis.

- iii. The access to the Factory Perimeter represents the exterior ring where a first identification of people demanding access to factory buildings takes place. It is protected by a wall and fence with access via a Security Gate. Visitor management should be as per SAS guidelines
- iv. The production & Warehouse shall be located in a high security zone where access is via turnstile (one by one entry). The access shall be restricted only to authorized personnel. Security Guard should carry out the frisking of all employees. A nodal officer should be designated who can allow the access of authorized person in this area. A record of all visitors shall be logged with date and time of entry and exit.
- v. Access control with CCTV monitoring should be present at each nodal entry/exit points into the building and its different sensitive areas.
- vi. The most sensitive area is data room, personalisation room, data storage and data destruction room. Mechanisms to handle any unidentified, attempted or unauthorised access should be implemented and all entry and exit should be recorded. No personal electronic devices like mobile, USB disks /storage disk etc. shall be allowed in this area.
- vii. Regular and periodic auditing should be done for any authorised or unauthorised activity within the areas by the security and internal audit team.
- viii. Clear access control mechanism for entry in sensitive area should be defined and implemented using identity cards and biometric authentication. The access activity should also be logged, monitored and maintained regularly. The access to sensitive areas should only be on need basis.
- ix. Integrated security systems are to be installed to ensure integrity and security of sensitive assets & information. The main physical security systems include access control system, CCTV & anti intrusion system.
- x. Time and date of the CCTV system is synchronized with access control and finally to NTP (Network Time Protocol) server.
- xi. Access Control, CCTV & Intrusion alarm are monitored 24 x 7 by Security officer, security assistant and security guard present in Security Control Room.
- xii. Procedures for the monitoring of any alarm with reaction rules are to be in place. In cases of obvious evidence of serious occurrence (e.g. Panic Alarm & Fire alarm) police, Local Fire Station, security agency head office (if required) and Organization Management must be informed immediately.

6.2. Operating System Security:

The SIM operating system is very important part and carries all the algorithms required for encryption and decryption of keys. The Operating system should preferably be developed within India and should be tested in secured environment by security testing team which is different from development team. Security testing will be as per the requirements specified in Indian Telecom Security Assurance Requirements (ITSAR), as and when released.

6.3. Data Security:

Data Security is key component of Security Management in SIM personalisation process. Data Security comprises of Security of data during its motion or transit, in use and in rest including final disposal by secure destruction.

6.3.1 Security of Data in motion and in use:

Data in motion involves transfer of keys operator profile, application information, algorithm or any relevant data etc. between MNO and SIM manufacturer either through network or physical media. It also includes transfer of data within MNOs premises (from creation of SIM personalisation related data to be sent to the SIM personalisation agency till loading of keys in the system) and movement of data in the SIM manufacturer premises during SIM personalisation lifecycle. Therefore, effective security controls should be implemented during the all stages at MNO premises and at SIM manufacturer's premises. Following are the important security controls to be implemented while data is in motion:

- i. Data exchange with internal and external stakeholder should be done in encrypted form atleast through SFTP and secure VPN with TLS certificate from both sides.
- ii. Adequate access control mechanism should be maintained at each stage of movement of data.
- iii. Direct access to the data should be avoided without check and balance mechanism. All administrative access to data should be done where explicitly authorised by using Biometric or any other equivalent authentication mechanism.
- iv. Roles and responsibilities of authorised person for data access at each node whether at production house or R&D centre should be well defined on the organization's Security policy.

- v. The application(s) and hardware platform used for processing SIM personalisation data should be free from any security vulnerabilities.

6.3.2 Security of Data in rest:

Data at rest includes storage of all keys and operator specific details required for SIM personalisation and physical inventory of SIM loaded with data either at MNO location or SIM personalisation manufacturer's location. SIM inventory after personalisation and prior to delivery to MNO are to be stored either in secured area with limited access rights or in the secure vault depending on risk and the requirements of the concerned MNO. The secure vault is equipped with Access control gate with limited rights & physical defender door with double keys. The security controls to be adopted during data Storage are as follows:

- i. All physical equipment associated with key management activity, such as physical keys and SIMs are stored securely. There are two ways to store keys:
 - Within a secure cryptographic device (HSM) with FIPS-140 or equivalent certification
 - Keys under another key encryption or any other equivalent encryption mechanism.

Each Key Custodian has to conduct and document a key inventory control once in a quarter in the presence of a member of security department as documented in security policy. In case of any change of key custodian the transfer of responsibility to next custodian will be documented. Detail procedure of key management is covered in further sections.

- ii. All the Keys which are stored in SIM personalisation software and data server should be encrypted with at least AES-256 or above encryption algorithms.
- iii. The work station and server carrying the keys or related data should be secured and only one nodal officer along with alternate nodal officer can access the System with dual factor authentication with biometric as one of the factor.

6.3.3 Secure Disposal/Destruction of Data:

After the completion of personalisation process and successful transfer of keys and related data to Mobile Network Operator Nodal officer, all keys and operator specific data should be destroyed securely by the SIM personalisation agency within time limit specified by MNO.

6.4. Key Management:

An organisation level well documented operating procedure for secure key management should be implemented under the security policy of the organisation. One of the main principles in key management process is the dual control mechanism which must be ensured by stakeholder organizations with clear definition of different roles and their responsibilities. Following are some of the key roles which may be made part of key management process:

- a. Key Manager
- b. Key custodians
- c. Technical System Administrator,
- d. Security officer

a. Key Manager

Key manager takes over the role of implementation of key management in the organization. He prepares key generation procedures. Key Manager is responsible to plan the procedures for generation, storage and handling of keys. Key Manager is responsible for ensuring that all key management activity is carried out in accordance with these procedures and fully documented. Key Manager is responsible for all activities related to key management including training of various roles, monitoring implementation.

b. Key Custodian

Key Custodians is responsible for their respective key parts. Key custodians is trained on his role and responsibilities and operating procedure and have to sign a statement acknowledging their responsibilities for safeguarding key components or other keying materials entrusted to them. The reporting structure of Key Custodian should avoid conflict of roles. They must not be temporary staff. Each Key Custodian has to conduct and document a key inventory control at least once in a quarter in the presence of a member of security department.

c. Technical System Administrator (TSA):

Technical system administrator is responsible for regulation and control of systems used in SIM Personalisation process. The TSA shall be responsible for implementation of security control for security of data in rest, in motion and in use during the SIM personalisation lifecycle till transfer of keys and related data to MNO and final destruction/disposal of data.

d. Security Officer:

The security officer is part of CISO team who will be responsible for enforcement of security controls in respective organisations i.e. MNO and SIM personalisation agency. CISO team shall conduct at least quarterly internal security audit and provide feedback for corrective actions/improvements as per security policies of respective organisations.

e: Key Lifecycle Management: The key lifecycle management activities shall be performed within geographical boundaries of India.

(i) Key Generation

All key generation shall take place within secured environment and stored as per requirements specified in Section 6.3.2. The Key manager shall verify that there is no physical key logger linked between a key board and Key management PC. The key length must be chosen according the relevant security standards and/or according security best practices.

(ii) Key Import & export:

Keys may be imported or exported in open form (two or three parts) or in enciphered form (encrypted by a transport or key encryption key). The equipment (Hardware Security Module) for the key management should be placed in a locked rack which is located in the Dual access controlled server room within the SIM personalization high security area.

The HSM rack is accessible only under dual control. One key is under the responsibility of the key manager and the other key is under the responsibility of the HSM Administrator. All of this activity should be recorded as per key management procedure.

(iii) Key Distribution/key Exchange

The Key distribution should be done in encrypted manner and one master key or Private key should be made available to decrypt keys at the destination. Only authorized Key custodians have access to their Key Components at any point of Key distribution process. Master key, Private keys are not exportable from the HSM system in open form.

All key components distributed through an electronic channel of communication would be encrypted under a transport key.

The Key components will be stored in tamper-evident environment with a two-part Key Transfer form attached to each component. Second part would be digitally signed by

recipient after verifying the integrity of the key component and acknowledged to the key issuer.

Upon receipt of a key component, Key Custodian inspects and ensures that no one has tampered with the key component package. If there are any signs of tampering, the key would be regarded as compromised and the key compromise procedures will be followed.

(iv) Key Storage:

All physical equipment associated with key management activity, such as physical keys and SIMs are stored securely. Each key custodian group shall have a dedicated secure locker to store their secrets. All physical keys/PIN to the locker have to be handed to the key custodian, thus assuring that no other party can access the locker.

(v) Key Validation

Key Check Value should be checked after the successful loading of the keys during key ceremony.

(vi) Key Backup

Backup of the master keys of the same security strength as for operational keys should be done in the production process.

(vii) Key Compromise

If there are any indications of a key compromise (e.g. broken TEE, circulation in clear form, etc.) the key must not be used anymore and respectively imported into the system. The nodal officer must be informed and the circumstances of the incident must be investigated and report of incidents should be created and maintained in a well-documented manner. All parties sharing the key have to be informed immediately.

A report must be written including analyses of the concerned keys. The Key database is to be updated. All parties sharing the key will be informed immediately.

(viii) Key Destruction at Server

A key destruction takes place in dual control always. All keys stored within the HSM can be destroyed at the end of its life if defined, as once keys are destroyed and same cannot be rebuild. All components, backups and copies of the keys would be destroyed.

If a key that resides inside Cryptographic device cannot be destroyed, then the device itself will be destroyed in a manner to ensure that no residual trace of the key remains.

The record of Destruction Key is signed by a witness other than the security manager, key manager or custodian. The record of Destruction Key is kept indefinitely.

6.5. Auditing and logging:

- i. The complete log history of each key (physical or encryption) should be logged.
- ii. All the operations or activity in system should be logged and be recorded in audit file.
- iii. All the transfers should also be logged at the STFP server with restricted access.
- iv. Logs should be maintained for 1 year and should be regularly analysed for any malicious activity.

7. Incident Management

The organization policy should contain well documented process as per SAS guidelines for handling incidents.

8. Glossary

AES-Advance Encryption Standard

CISO-Chief Information Security Officer

HSM- Hardware Security Module

FF-Form Factor

ICCID-Integrated Circuit Card ID

IMSI-International Mobile Subscriber Identity

ITSAR- Indian Telecom Security Assurance Requirements

MNO- Mobile Network Operator

OTA-Over the Air

OS-Operating System

PIN-Personal Identification Number

PUK-Personal Unblocking Key

SIM-Subscriber Identity Module

SFTP-Secure File Transfer Protocol

TEE- Trusted Execution Environment

VPN-Virtual Private Network

MFF1- M2M Form Factor 1

MFF2- M2M Form Factor 2

eSIM- Embedded SIM