Document No: MSG: 02

Version: 1.0

July 22, 2022

MOBILE SECURITY GUIDELINES

(MSG)

सत्यमेव जयते

Government of India
Ministry of Electronics and Information Technology
(MeitY)
New Delhi – 110 003

Metadata of Mobile Security Guidelines (MSG)

SR.No	Data elements	Values
1.	**Title**	Mobile Security Guidelines (MSG)
2.	**Title Alternative**	Security Guidelines for Mobile Device, Mobile Communication and Mobile Services
3.	**Document Identifier** *(To be allocated at the time of release of final document)*	MSG: 02
4.	**Document Version, month, year of release** *(To be allocated at the time of release of final document)*	Version: 1.0 for Public Review.
5.	**Present Status** (Draft/Released/Withdrawn)	Draft
6.	**Publisher**	Ministry of Electronics and Information Technology (MeitY), Government of India (GoI), New Delhi
7.	**Date of Publishing for Public Comments**	20/07/2022
8.	**Type of Standard Document** *(Policy/Technical Specification/Best Practice/Guideline/Process)*	Guideline
9.	**Enforcement Category** *(Mandatory/Recommended)*	Mandatory
10.	**Creator** *(An entity primarily responsible for making the resource)*	Working Group on Mobile Device Security (WG-MDS), Chairman Prof. V. N. Sastry & Co-ordinated by C-DAC & STQC under aegis of MeitY
11.	**Contributors** *(An entity responsible*	Working Group Members, Experts, Closed Group Advisors and others.

SR.No	Data elements	Values
	for making contributions to the resource)	
12.	**Brief Description**	The purpose of the Mobile Security Guidelines (MSG) is to achieve Mobile Security Goals of Confidentiality, Integrity, Availability, Authentication, Authorization, Non-repudiation, Access Control, Traceability, Accountability, Trust and Reliability by the various entities involved in the mobile service ecosystem such as mobile device manufacturer, mobile application developer, mobile network operator, mobile service provider, security testing organization and mobile phone user. MSG is based on the principles of Holistic approach, Futuristic challenges, Usable environment, Comparable strategies and Measurable levels, thereby extending the scope and supplementing the Mobile Device Security Standards. Mobile Security Threats, Mobile Security Vulnerabilities and Mobile Security Control Measures are presented under following three categories (i) Mobile Device Security, (ii) Mobile Communication Security and (iii) Mobile Services Security. Guidelines on Mobile Security Testing and Mobile Application Vetting Process are given to strengthen the Mobile Security Assessment. Guidelines on Security Levels for entities and technology components are given. The adoption of the prescribed guidelines with checklists provided for each category of entities would ultimately ensure enrichment of mobile user's experience towards secure and trustworthy mobile services with privacy protection.
13.	**Target Audience** *(Who would be referring/using the document)*	● (M) Manufacturers of Mobile Phone Device, its Hardware Components, Peripheral Equipment and Interfaces. ● (D) Developers of Mobile Software Services, Functionality, Applications, APIs, Operating System, Browser, micro-services etc. ● (S) Service Providers of Mobile Software Services, Mobile App Stores, Integrators, Government and Non-Government Bodies offering: m-Governance, Mobile Services, Social Media Services and APIs of Mobile Services. ● (N) Network Providers, Mobile Network Operators, Providers of Mobile, Network, Internet,

SR.No	Data elements	Values
		Satellite and Wireless Communication and Wi-Fi Services. ● (R) Regulators, Auditors, Standardization Bodies and Enforcement Agencies. ● (T) Mobile Security Testing and Forensics Organizations/Labs, Quality Assurance and Assessment Bodies ● (A) Academia and Researchers ● (U) Mobile Users and Mobile Subscribers
14.	**Owner of approved Standard/Guidelines**	MeitY GoI, New Delhi, India
15.	**Subject** *(Major Area of Standardization)*	Mobile Security
16.	**Subject. Category** *(Sub Area within major area)*	Mobile Device Security, Mobile Communication Security, Mobile Services Security, Data Privacy, Mobile Security Testing and Mobile Application Vetting
17.	**Coverage. Spatial**	INDIA
18.	**Format**	Word/PDF
19.	**Language** (To be translated in Hindi and other Indian languages later)	English
20.	**Copyrights**	MeitY GoI, New Delhi
21.	**Source** (Reference to the resource from which present resource is derived)	Different resources, as indicated in the Reference list of the document
22.	**Relation** (Related resources)	m-Governance Framework, e-Governance guidelines and Cyber Security by MeitY; Access and Carrier Services by DoT; Mobile Device Security Standard (Dec.2021, LITD) by BIS

DISCLAIMER

This MSG document is informative and advisory in nature and aims to provide guidelines to all mobile ecosystem entities in respect of securing mobile devices and mobile services.

Certain commercial entities, technology, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by C-DAC, STQC and MeitY GoI.

While every care has been taken to ensure that the contents of this document are accurate and up to date, the readers are advised to exercise discretion and verify the precise current provisions of law and other applicable instructions from the original sources. It represents practices as on the date of issue of this document, which are subject to change without notice.

The document enlists guidelines around basic security controls and is not prescriptive in nature. The readers are responsible for making their own independent assessment of the information in this document.

MeitY and/or it's associated/attached offices and organizations retain the right to make changes to this document at any time, without notice. Further, MeitY and/or its associated/attached offices and organizations makes no warranty for the use of this document and assumes no responsibility for any errors which may appear in the document, nor does it make a commitment to update the information contained herein.

In no event shall C-DAC, STQC and MeitY GoI be liable for any compensations whatsoever (including, without restriction, damages for loss of profits, business interruption, loss of information) arising out of the use of or inability to use this document.

Preface

Mobile Security Guidelines (MSG) are prescribed for various entities such as mobile device manufacturer, mobile application developer, mobile network operator, mobile service provider, mobile security testing organization and mobile phone user, so as to ensure the achievement of mobile security goals and protect the data privacy of mobile users. The target of various mobile ecosystem entities is to achieve confidentiality, integrity, availability, authentication, authorization, non-repudiation, access control, traceability, accountability, trust and reliability, termed as mobile security goals.

Although various National and International Standards/Guidelines on different mobile security aspects for specific entities are available, this report on MSG is unique as a single source, comprehensively covered, principles based, uniformly understandable, clearly explained, technically sound, openly available, focused knowledge resource document covering mobile security risks, threats, vulnerabilities and mobile security control measures. Due to very large subscriber base of smart phone device users in India, their growing dependency on mobile services and rising mobile security challenges, they need to be aware of the potential mobile device security threats and corresponding safety measures, which are provided here as a checklist to follow.

Mobile Security is categorized under Mobile Device Security, Mobile Communication Security and Mobile Services Security. Security levels of various entities and of various technology components of the mobile ecosystem are prescribed here. Identification of the present security level of an entity or a component helps to measure the gap and improve towards higher security levels.

MSG supplements the Mobile Device Security Standard (MDSS, Parts 1 to 4) given by the Bureau of Indian Standards (BIS, Dec.2021) and covers Mobile Security Testing, Mobile App Vetting process as well as mobile forensics. Each entity needs to specifically look into the checklist of mobile security control measures specified as per its role and responsibility. Adoption of the prescribed MSG would not only elevate the culture of involvement and accountability of all entities towards ensuring mobile security but also help in building trustworthy and secure mobile services ecosystem in Digital India.

For any queries, feedback and/or suggestions on MSG document, one may please send email as per the details provided in Annexure 0.

Prof. V N Sastry
Chairman
22/07/2022

Executive Summary

Very large subscriber base of mobile phone users is accelerating the growth of Digital India in terms of modern mobile communication infrastructure and efficient mobile services in all spheres across the country connected with the borderless digital world. Mobile application-based services in every domain including education, health and social media have become integral part of daily life of Mobile Users of all age groups and genders. The exposure risk of Mobile Phone Users gives rise to security threats of sensitive information loss and misuse of personal data by adversaries. Therefore, privacy and personal data protection of mobile user are of utmost importance. Mobile services ecosystem has various entities such as mobile device manufacturers, mobile network operators, mobile service providers, mobile app developers, government bodies providing mobile governance services, mobile security testing organizations, facilitators and mobile users. Every one of them are responsible for assuring mobile services to the mobile user in a safe, secure and reliable manner by fulfilling security goals.

In chapter-1, basic concepts, terminology, mobile security risks, threats and vulnerabilities, mobile security goals to be achieved, security levels of mobile ecosystem entities and technology components, mobile security control measures and privacy protection, principles followed in the development of the guidelines, target audience etc. are given. Threat actors may be adversaries, attackers, hackers, intruders, interceptors, impersonators, eavesdropper, malware, spyware, virus etc. Mobile Device Security Vulnerabilities are weaknesses, gaps or loopholes in protective systems, mechanisms or interfaces. Adversaries intend to identify the vulnerabilities of Mobile Ecosystem and exploit them to gain unauthorized entry and access into user's Mobile Device to do malicious activities. Identification of the mobile security vulnerabilities is necessary to plug and insulate them from threat actors or adversaries.

Mobile Security Control Measures are counter measures to prevent mobile security threats from adversaries and to stop exploitation of mobile security vulnerabilities. They help in the mitigation of mobile security risks. Mobile Security Control measures are of three categories (a) Policy based Measures, (b) Technology based Measures and (c) User Oriented Measures. Technology oriented Mobile Security Control Measures are classified under (i) Mobile Device Security, (ii) Mobile Communication Security and (iii) Mobile Services Security. Security Levels of entities and technology components are defined. The Security Levels of (i) Entities are categorized as green, orange and blue level, (ii) mobile users are categorized as beginner, normal user and expert level and (iii) Technology Components such as mobile device, mobile applications, Mobile OS, Mobile SIM are categorized as Low Risk, Medium Risk and High-Risk level.

In chapter-2, Mobile Device based Security Threats, Vulnerabilities and Control measures are given specific to Mobile Hardware, Firmware, Mobile OS, & Pre-installed Apps. Mobile devices store a significant amount of sensitive data, which can be compromised due to vulnerabilities in the insecurely designed mobile device, leading to breach of device integrity & data security; the mobile devices always-on connectivity allows unauthorized parties to access data and portable form-factor devices, making them susceptible to theft and misplacement leading to

misuse. Mobile Device security capability framework is given which has five layers namely, the hardware at the bottom layer, operating system (OS) above it, peripheral interface involved with OS and hardware, application software layer on top, and the user data protection layer involved with hardware, OS and application software. As Mobile Operating System and Subscriber Identity Module (SIM) are significant, so their security threats, vulnerabilities and control measures are presented in separate sections. SIM is a gateway for mobile device connected world and a potential target by adversaries to steal mobile user identity and commit frauds, so it needs to be properly protected.

In chapter-3, Mobile Communication and Network-based Security Risks, Threats, Vulnerabilities and Control Measures are presented. In general, mobile devices are constantly connected to the internet. The end-users might use untrusted public networks, which may enable malicious parties to access and intercept transmitted data through rogue access points there by the Wi-Fi sniffing; eavesdropping; skimming; and sophisticated Man-in-the-Middle (MitM) attacks are likely. Mobile Communication based Vulnerabilities such as weak transport level security, rogue Wi-Fi devices, untrusted Bluetooth devices, misuse of specific electromagnetic waveforms of mobile antennas to spoof and inject commands via the audio interface need to be identified in the deployed environment. Short range and long range mobile communication channels including satellite communication and 5G are presented here.

In chapter-4, Mobile Service based Security threats, Vulnerabilities and control measures are presented. Malicious apps, mobile malware and APIs can steal sensitive data and collect user data. In addition, mobile malware can be used to mount targeted attacks against mobile device users. Smartphones are susceptible to worms, viruses, trojans and spyware similar to computers. Mobile Service based Vulnerabilities such as security vulnerabilities present in old versions of mobile web browser, operating system, applications, APIs and mobile interfaces, unencrypted data storages are to be identified. Proper steps must be taken to fix or control them such as regular updating of Apps to fix vulnerabilities.

In chapter-5, mobile device security testing and mobile device forensics along with requirements and operating procedures of assessment are given. They would be beneficial to the mobile device security testing organizations and labs. The administrative structure of these testing organizations is given to strengthen them with appropriate skills required and bring uniformity. The mobile device security testing is to be done at three levels (i) hardware level, (ii) software level and (iii) firmware level, under static and dynamic testing environments. The guidelines provided are generic, Operating System (OS) agnostic and cover the security requirements at Hardware, OS & Application layers. MSG supplements the Mobile Device Security Standard (MDSS, Parts 1 to 4) given by BIS in Dec 2021 and covers Mobile Security Testing, Mobile App Vetting process as well as mobile forensics.

In chapter-6, checklist of security control measures for various entities are presented. Each entity needs to specifically fulfill the checklist of mobile security control measures specified as per its role and responsibility. Mobile Device empowers mobile users and provides various features for their personal & business purposes. However, mobile users often indulge in risky behaviours primarily due to lack of awareness that could compromise business data. The risky behaviours of end users include Jail breaking/rooting devices to bypass security controls; using un-approved cloud-based apps to share and sync data; using un-approved productivity apps that maintain copies of corporate data; using malicious apps from un-approved app-stores; and exposing business data with malicious intent. MSG provides Checklist for User awareness on Mobile Device Security Controls to safeguard Mobile Users. User Levels are specified so as to help them identify their present level of security awareness and understand mobile security measures to follow.

The central objective of MSG is to ensure privacy, protect sensitive data and provide security of transactions of every mobile device user, by following the mobile security control measures prescribed for various stakeholders involved in the mobile service ecosystem. Adoption of the prescribed MSG would not only elevate the culture of involvement and accountability of all entities towards mobile security but help in building trustworthy and secure mobile services ecosystem in India.

Acknowledgement

MeitY GoI, has constituted the Working Group on Mobile Device Security (WG-MDS) in Feb 2021, chaired by Prof. V.N. Sastry with Technical members from Government, STQC, C-DAC, Industry, Academia and coordinated by C-DAC. It had a dozens of meetings. Following is the list of main contributors in the development of Mobile Security Guidelines (MSG).

1	Prof. V. N. Sastry, Professor & Head of the Mobile and Social Media Banking Lab, IDRBT, Hyderabad	Chairman
2	Ms. Lakshmi Easwari, Director, C-DAC, Hyderabad	Member
3	Mr. A.K. Upadhyaya, Scientist 'F', STQC, New Delhi	Member
4	Dr. Ferdous Ahmed Barbhuiya, Associate Professor (CSE) and Associate Dean (R&D), IIIT Guwahati	Member
5	Dr. Sandeep Kumar, Associate Professor, Computer Science and Engineering Department, IIT Roorkee	Member
6	Prof. Monit Kapoor, Professor and Dean- CSE, Chitkara University, Chandigarh	Member
7	Dr. Deepak Kshirsagar, Assistant Professor, College of Engineering Pune (COEP), Pune	Member
8	Dr. Vinosh Babu James, Technical Standards Director (Assoc.), Qualcomm Standards & Industry Organizations	Member
9	Mr. Pranav Singh, Consultant, Standard and Specification, Global R&D, IDEMIA	Member
10	Mr. Krishna Sirohi, Founder & President, i2TB Research Foundation	Member
11	Mr. Angaj Bhandari, Managing Director - India and South Asia, M/s Fime India	Member
12	Mr. Bappa Mondal, Technical Team Lead, Samsung India Electronics Pvt. Ltd.	Member
13	Mr. Kapil Kant Kamal, Joint Director, C-DAC, Mumbai	Member
14	Mr. Mahesh Patil, Associate Director, C-DAC Hyderabad	Co-opted Member
15	Mr. M Krishna, Assistant Director, Central Forensic Science Laboratory, Hyderabad	Co-opted Member
16	Ms. A. Suganya, Sr. Scientist, Hardware Security Research Group, SETS, Chennai	Co-opted Member
17	Dr. Reshmi T. R. , Scientist, Cryptology and Quantum Cryptography Group, SETS (For 5G Security), Chennai	Co-opted Member
18	Ms. Pallavi Dhanvijay, Joint Director, C-DAC, Pune	Member Convener

The Working Group is thankful to Ms. Kavita Bhatia (MeitY), Mr. Inder Pal Singh Sethi (NIC), Mr. Suresh Chandra (STQC), Dr. Santosh Kumar Pandey (MeitY), Mr. Karimullah Shaik (C-DAC), Ms. Lenali Singh (C-DAC), Prof. D. Janakiram (IDRBT), Ms. Swati Arora (C-DAC), Dr. Gaurav Raina (IIT-Madras), Mr. Saket Modi (Safe Security) for their advice, valuable comments and support.

Table of Contents

List of Tables

List of Figures

1. Introduction

In this chapter, (i) concepts necessary to understand the Mobile Security Guidelines (MSG), (ii) Mobile Ecosystem Entities, Technology components and their Security Levels, (iii) Mobile Security Risks, Threats and Vulnerabilities, (iv) Mobile Security Goals to be achieved, (v) Mobile Users Data and Privacy Protection, (vi) Mobile Security Control Measures, (vii) Principles followed in the development of the Guidelines, (viii) Purpose and Scope of the MSG, (ix) Target Audience for MSG, (x) Abbreviations used, which may be referred in Annexure A (xi) Important Terms defined, which may be referred in Annexure B are given.

1.1 Mobile Device, Mobile Subscriber and Mobile User

(A) A Mobile Device (MD) is identified by its unique International Mobile Equipment Identity (IMEI) number given by its Original Equipment Manufacturer (OEM). Mobile Subscriber (MS) is identified by the International Mobile Subscriber Identity (IMSI) number of the Subscriber Identity Module (SIM) or Universal SIM (USIM) application used in UICC or in embedded UICC, issued to him/her by the Mobile Network Operator (MNO), Internet Service Provider (ISP) or OEM provider. A Mobile User (MU) is an authorized Mobile Subscriber (MS) using a Mobile Device (MD) linked with the registered SIM/USIM. Mobile Subscriber's registered name is displayed when a call is received by any mobile user. For definitions, see Annexure B.

(B) Mobile Device (MD) Features: Mobile device consists of a set of components of the mobile technology stack covering Mobile Device Hardware (Processor, Storage, Execution environment); Mobile Firmware; Mobile Operating System; and Pre- installed (Bundled) Apps. Designed for mobility, MD is compact in size for holding in palm, battery-powered, and lightweight. Most mobile devices have a basic set of comparable features and capabilities. Both feature phones and smartphones support voice, text messaging, and a set of basic Personal Information Management (PIM) type applications including phonebook and calendar facilities. Smartphones add Personal Computer (PC)-like capability for running a wide variety of general and special-purpose applications. Smartphones have popular operating systems such as Android, iOS, Windows Mobile, RIMs BlackBerry OS, Symbian OS, WebOS or etc. Unlike the more limited kernels in feature phones, these operating systems are multi-tasking and full featured, designed specifically to match the capabilities of high-end mobile devices. Many smartphone operating system manufacturers offer a Software Development Kit (SDK) (e.g. the Android1 or iOS2 SDKs). Smartphones contain NAND and RAM memory, support higher data transfer rate, greater storage density and better security features. To facilitate the limitations of space on mobile device mainboards and the demand for higher density storage space (i.e., 2 GB to 256 GB or higher capacity) the new Embedded Multimedia Cards (eMMC) style chips are present in many smartphones.

(C) Mobile Device Sections: MD consists of hardware, software and interfaces categorized as: (1) Input Section - key board, touch screen, scrolling, swiping, switch, buttons, microphone/mike, sensors, Bio-metric scanner, camera, video recorder, interface ports as USB, Micro SD card and SIM/USIM/eSIM, NFC Reader etc. (2) Processing & Storage Section - Microprocessor, Memory, fixed and removable Storage, IC Card, Operating System, Service & Library Functions, Application Programming Interfaces etc. (3) Power Section - Battery, Charging, Wiring, Power supply, Voltage controller etc. (4) Communication Section - Transmission and Reception Antennas, Analog and Digital Signal Converters, Modulators, Channel Tuners, Multiplexers, Streamers etc. and (5) Output Section - Visual Screen Monitor, Audio speaker, Status (Position, Time, Signal Strength) indicators, alarm, USB connectors etc.

(D) Mobile Device as Digital Assistant (DA): Mobile Device is not only a personal, mobile, portable device for communication, computation and Sensing but also acts as a gateway for worldwide access of information to the Mobile User (MU). It connects Internet of Thing (IoT) Devices, provides digital services anytime, from anywhere, as well as location based and context based customized services in real time such a map, recommendations and mobile voting. Due to growing number of supported features on MD and increasing dependency of a Mobile User (MU) on it, MD is treated as the identity, companion and digital assistant of a MU.

1.2 Mobile Ecosystem Entities and their Security Levels

(A) Mobile Ecosystem is an interconnected and interdependent system of various entities and components, which altogether create, operate and provide products and services to a mobile user. [Ref: Section 2.23 of MDS Part-1, BIS, Dec 2021]

(B) Entities: Mobile ecosystem has various entities, which are the stakeholders responsible for enabling mobile services in a safe, secure and reliable manner and are accountable to fulfill the mobile security goals prescribed. These entities are broadly classified as : (i) Demand Side Entities: On the demand side of Mobile services are Mobile Users consisting of a large pool of retail segment of citizens, merchants and customers, (ii) Supply Side Entities: On the supply side are those which provide the mobile services such as mobile Governance services by Government, Sectoral service providers such as Health, Education, Home, Energy, Banking and Finance, Agriculture, Transportation, Communication, Entertainment, Social Welfare, Telecom Operators, Social media sites, cloud service providers etc. , and (iii) Facilitation Side Entities : On facilitation side are, Regulators (sectoral regulators such as RBI for Banks, TRAI for Telcos), Standardization Bodies (as BIS, TSDSI, TEC, STQC, MPFI, COAI, IAMAI, C-DAC, IDRBT, NIST, SETS, DSCI, OWASP, ITU, 3GPP), Cloud Service Providers, Service Aggregators, Mobile Device Manufacturers and Hardware Manufacturers (Mobile Device OEM, SIM card, embedded SIM, NFC Device, Network Equipment and Access point manufacturers etc.), Software Developers (Mobile Operating Systems, Mobile Application developers, Mobile browser providers etc.), Sellers and Consultants, Mobile App and Social Media Providers, Government Bodies, NGOs, Academia, R&D organizations/Industries of Mobile Ecosystem etc.

(C) Security Levels of Entities:

(i) All entities of the Mobile Ecosystem, except Mobile User shall be classified under (a) Green Category, if basic security control measures are followed, (b) Orange Category, if basic and foundational security controls are followed and (c) Blue Category, if basic, foundational and advanced security control measures are followed, verified and certified.

(ii) Mobile User Levels: Based upon the awareness of mobile security precautions and knowledge levels of executing mobile security protection steps, a Mobile User and Mobile Subscriber shall be categorized as (a) Beginner, (b) Normal User and (c) Expert.

1.3 Mobile Technology Components and their Security Levels

(A) Technology Components:

Mobile ecosystem has various core and allied components which should fulfill Mobile Security Goals pertaining to their role. These components are (i) Mobile device technology stack, such as the hardware, the operating system, and embedded mobile device components (e.g., baseband radio, sensors, bootloader, isolated execution environments, Subscriber Identity Module [SIM] card or Embedded E-SIM, (ii) Mobile applications, (iii) Networks and Communication interfaces (e.g., cellular, Wi-Fi, Bluetooth, NFC) and services provided by mobile network operators, (iv) Vendor mobile infrastructure, including mobile app stores, sellers, social media providers, updates and backup services provided by the mobile device vendor or cloud services provider, (v) Enterprise mobile services and infrastructure, including Mobile Device Management Software, enterprise mobile app stores, and Mobile Application Management (MAM). [MDS, BIS]

(B) Security Levels of Components:

(i) Mobile Application Levels: Mobile Applications are either pre-installed or downloaded and installed on demand onto a mobile device. It is recommended to follow OWASP MASVS [Ref: MDS, BIS, 2021] for mobile app assessment. Based upon weighted sum of functionality score, Usability score and Security Risk Score, a Mobile Application shall be categorized as (a) Low Risk, (b)Medium Risk and (c) High Risk Application.

(ii) Mobile Device Levels: Mobile Device has two levels of security (i) Level-1: Baseline Security and (ii) Level-2: Comprehensive Security. It is based on the security control requirements fulfilled to achieve security goals. The Level of a Mobile Device reflects the security assurance that it provides and the reliability it guarantees with respect to the use cases and usage supported. It should also be checked the degree to which the Mobile Device fulfils the prescribed goals in MSG. [Ref: MDS, BIS, 2021]

1.4 Mobile Security Risks

(A) A Mobile User (MU) may face various risks or losses due to security lapses on Mobile Device (MD) and its associated Services, for example, loss of sensitive information or personal data due to data leakage, identity theft due to misuse of data etc.

(B) Every unit and component of the mobile device can be a source of threat and target for attack. Hence, the responsibility of protecting the device, securing MU information and preserving privacy lies with mobile ecosystem entities as MD manufacturers, mobile service providers and users. In order to provide efficient and secure mobile services for better User Experience (UE), developers and providers should look into the essential features supported by a MD and its various user interfaces (UI). This includes focusing on the possible risks from mobile phone platforms, channels, applications, browsers, databases, processors, SIM etc. and corresponding protection mechanisms.

(C) Handling the MD of a MU by any unauthorized persons may lead to serious repercussions as MUs often store login credentials of several applications regularly used on their mobile devices for convenience and quick access of those registered sites only by a click or tap. In this manner, unauthorized users can easily access Mobile User’s personal and corporate email accounts, Digi Locker, wallet applications, bank and social media accounts etc. Therefore, MU should take special care to protect the personal MD from being mishandled and misused by others, particularly nearby persons.

(D) Due to a very large subscriber base of Mobile Users in India using smart phones and some still continuing to use feature phones, regular exposure of MU to social media service providers, falling prey to manipulated opinions and becoming victims of fake news, the impact of Mobile Security risks is high. Hence, it is necessary to contain systemic security risks on MU, which is the primary objective of the MSG.

(E) Since several entities such as Mobile Device Manufacturers, Mobile Network Operators, Mobile Service Providers, Mobile App Developers, Government Bodies providing Mobile Governance Services, Mobile Security Testing Organizations, Facilitators and Mobile Users are responsible for ensuring a secure mobile service ecosystem and each of them play a significant role in ensuring Mobile Security Risk minimization. It is essential to develop the culture of proper involvement and accountability of all entities towards reducing Mobile Security Risks and to avoid the blame game.

(F) If a MU is accessing organization data, emails, shared files etc. or data from a mobile Cloud Service provider and the MD is compromised then it poses Security Risks to the Organization and Vice Versa. Such organizations/Mobile Cloud providers should specify the Mobile Device Management (MDM) policy guidelines to the member MU.

(G) If an Adversary gets remote access into the MD, it may encrypt important files in a MD with a decryption key under its possession and create panic to the MU by demanding payment of ransom amount to get back the valuable data to the MU.

(H) MD has built in features to synchronize its data and files such as contact list, updates with external storage or mobile cloud service providers, which has associated risk if mutual authentication is ignored.

(I) If a MD is acting as a hot spot to provide internet connectivity to its connected devices or if MD is connected to a public access device as Wi-Fi Access Point/Modem/Router/Switch or if MD is connected to an Internet of Things (IoT) device or TV or gateway node or if MD is connected to a rogue Base Trans-receiver System (BTS) or g-NodeB (5G Radio Access Node) then it may be subjected to Mobile Security Risks, therefore, care should be taken when connecting MD to unknown network nodes or free untrusted public wireless access nodes or charging points.

(J) High Level Security Risks to MD (Mobile Hardware, Firmware, Mobile OS, & Pre-installed Apps) are grouped into following 4-different categories. The first category is the direct security risks to the mobile device whereas the remaining three categories of risks are indirect & operational security risks to the mobile device, briefly described below: [Section 5.1, MDS, Part-2, BIS, Dec 2021]

(i) Mobile Device based Security Risks (Untrusted Mobile Device): Mobile devices are used by end-users to perform a variety of business-related tasks and store a significant amount of sensitive data. This data can be compromised due to vulnerabilities in the insecurely designed mobile device, leading to breach of device integrity & data security; the mobile devices always-on connectivity allows unauthorized parties to access data and portable form-factor devices, making them susceptible to theft and misplacement leading to misuse.

(ii) Mobile Network-based Security Risks (Untrusted Network): In general, the mobile devices are constantly connected to the internet. The end-users might use untrusted public networks enabling malicious parties to access and intercept transmitted data through rogue access points; the Wi-Fi sniffing; eavesdropping; skimming; and sophisticated Man-in-the-Middle (MitM) attacks.

(iii) Mobile User Behaviour based Security Risks (User Behaviour and Awareness): Mobile Device empowers end-users and provides various features for their personal & business purposes. However, end-users often indulge in risky behaviours primarily due to lack of awareness that could compromise business data. The risky behaviours of end users include Jail breaking/rooting devices to bypass security controls; using un-approved cloud-based apps to share and sync data; Using unapproved productivity apps that maintain copies of corporate data; Using malicious apps from un-approved app-stores; and Exposing business data with malicious intent.

(iv) Malicious Apps & Malware based Security Risks (Untrusted Third Party Applications & malicious Systems): Malicious apps and mobile malware can steal sensitive data and collect user data. In addition, mobile malware can be used to mount targeted attacks against mobile device users. Smartphones and tablets are susceptible to worms, viruses, Trojans and spyware similar to computers.

(K) For the overall security of the mobile device, the security of the mobile device technology stacks as well as the security of the mobile device due to the mobile ecosystem is addressed. In addition to the security requirements, the mobile devices used for personal and enterprise in the different scenarios are defined through security levels.

(L) Risk is caused by threat actors through the exploitation of existing vulnerabilities. Severity is a useful measure of the risk in terms of the degree of impact, which specifies the degree of a potential loss on account of a security threat incident.

1.5 Mobile Security Threats

(A) Mobile Security Threats come from various threat actors to hinder from fulfilling or stopping to attain the security goals. Threat actors may be Adversaries, Attackers, Hackers, Intruders, Interceptors, Impersonators, Eavesdropper, Malware, Spyware, Virus etc. They intend to identify the vulnerabilities or weakness in the protective mechanisms of assets of Mobile Ecosystem and exploit them to gain unauthorized entry and access into user's Mobile Device to do malicious activities.

(B) Mobile Security Threats need to be identified and controlled. They are categorized as (i) Mobile Device based Security Threats, (ii) Mobile Communication based Security Threats and (iii) Mobile Service based Security Threats.

(C) Some mobile apps can illegally be installed in the mobile device without mobile user's knowledge such as spyware and remote screen controller which are capable of taking control of mobile device and engage in the dangerous activity of data theft.

(D) MD is seen as gold mine of personal data that is of interest to hackers. Adding to this, lack of digital literacy and insecure use of mobile devices by Mobile Users are making them more attractive targets for attacks. The form factor of these Mobile devices makes them more prone to physical loss or theft and availability of business/financial/personal data as the same device is used for personal and business-related purposes. Attacker explores the threat attack surface of the mobile device for launching attacks which can be carried out remotely or by malicious insider compromising the MD. For example, Hacker making voice call or sending message with links, posing as an agent or employee of an organization and doing fraudulent transactions with mobile users account.

1.6 Mobile Security Vulnerabilities

(A) Mobile Device Security Vulnerabilities are weakness, gaps or loopholes in protective systems or mechanisms or interfaces, which can be exploited by threat actors to gain unauthorized access to MD. Identification of the mobile security vulnerabilities is necessary to plug and insulate them from threat actors or adversaries.

(B) Mobile Device Security Vulnerabilities are categorized as

(i) Mobile Device based vulnerabilities such as use of a MD without any or with a weak password protection may provide way for an adversary to easily enter into and steal secret information and do identity theft.

(ii) Mobile Communication based Vulnerabilities such as weak transport level security, rogue Wi-Fi devices, untrusted Bluetooth devices, misuse of specific electromagnetic waveforms of mobile antennas to spoof and inject commands via the audio interface.

(iii) Mobile Service based Vulnerabilities such as security vulnerabilities present in old versions of mobile web browser, operating system, applications, APIs and mobile interfaces, unencrypted data storage.

(C) Various security vulnerabilities need to be identified and proper steps must be taken to fix or control them such as regular updating of Apps to fix vulnerabilities that could otherwise be exploited to gain unauthorized access and steal data from MD.

1.7 Mobile Security Goals

Following are the prescribed mobile security goals, to be achieved:

(A) Confidentiality: Ensuring Confidentiality means ensuring the secrecy of information. Confidential data may be for any entity such as a person, mobile phone, organization, Process, Role and Position. Privacy is concerned with a person's private, sensitive and confidential data. Mobile User's critical data such as login credentials, passwords, personal files or photos, transaction information of payment details, location data of MD etc. are to be confidential to the MU and should not be known or disclosed or seen by unauthorized persons. Standard Techniques based on Information Hiding, Coding, Encryption & Decryption are to be used to achieve confidentiality.

(B) Integrity: Ensuring Integrity means maintaining the original data, message or information, accurate and intact without any change, modification, tampering or alteration at stored, transit or transmission state. For example, if a customer sends mobile payment instruction of Rs.50 and Rs.500 is debited from his account, it is integrity violation. Standard Hash Functions and checksums are to be used for integrity check of a file, that is, whether any change in the original file contents has happened or not. Error Correcting codes are useful to check where in the file contents, what type of change has happened. Permission Control, Encryption/Decryption are useful to protect from data modification. Converting a file into portable document format (pdf) is an example of protecting the contents from modification.

(C) Availability: Ensuring Availability means making the services or resources available for access to users from anywhere and anytime without any disruption. Service providers should guarantee service availability and specify the conditions in their Security Policy including eligibility of authorized users, language for better user experience and filter out disruptors or denial of service attackers through periodic monitoring. It is best ensured by rigorously maintaining all hardware bug free, performing hardware repairs immediately when needed and applying System and security upgrades periodically.

(D) Authentication: It is a verification process to check whether a claiming entity is genuine or not, which is done by an authenticating entity before granting permission to access entitled resource to the claiming entity. An authenticating entity X authenticates an entity Y means (i) X has registered the credentials of Y, in registration process, (ii) X verifies the presented credentials of claiming entity Y with pre-stored original credentials of entity Y, (iii) if verification credentials match with original pre-stored credentials, then Y is called an authenticated entity otherwise un-authenticated. It is a binary decision of Yes or No. In Mobile Ecosystem, Mobile User (MU), Mobile Device (MD), Mobile Application (MA) and Mobile Transaction (MT) are to be authenticated. MU shall be verified by at least two of the three factors of authentication: (i) Knowledge factor or "what you know" like PIN, Password, relations, (ii) Possession factor or "what you have" like mobile phone or Card and (iii) Intrinsic factor or "what you are" like biometrics and behavior aspects. Mutual authentication helps to avoid malicious entities such as intruders or impersonators. In case of direct authentication, authenticating entity itself registers and verifies, whereas in indirect authentication, these are done by other entities or third parties, so they should be trustworthy and tracked with proper service level agreements in place. For example, AADHAR based fingerprint verification can be done by UIDAI indirectly for a Banking or Hospital transaction.

(E) Authorization: It means that subsequent to authentication, an authenticated entity is stopped access from using any other resource, which it is not, entitled or authorized to use, for example, a rogue mobile app trying to collect mobile user's data should be stopped. This is achieved by permission control, monitoring state changes, movement of the entity and detecting misbehavior.

(F) Non-repudiation: It means that an entity cannot deny if it has actually done a transaction or genuinely did an action. It ensures that no one should be able to claim that the transaction on his/her behalf was made without their knowledge. Using Public Key Infrastructure (PKI) with digital certificates & digital signatures issued to MU onto a secure element of the MD or

USIM/E-SIM and Mobile Service Providers, non-repudiation is ensured. This is most important for mobile voting in National Elections.

(G) Access Control (AC): It ensures that a genuine entity is not denied access to a privileged service and an unauthorized or impersonating entity is not allowed any access. Access Control Policy should specify which subject (entity) has access or permission to which objects (resources) under what conditions. Proper Access Control Models as Discretionary AC (DAC), Mandatory AC (MAC), Role-Based AC (RBAC), Fine-grained AC etc. Firewalls, Intrusion Detection Systems (IDS), De-materialized Zone (DMZ), Sandboxing and data analytics are used for it.

(H) Traceability: It means that the actual path traversed for the completion of a transaction from source to destination is traceable and is identified as genuine in the supply chain across entities involved. Tracing the source, destination and intermediate nodes of the transaction path traversed in Networks is feasible by locating position, time and status logs as proof of evidence which are maintained by the network or service provider.

(I) Accountability: It means that an entity involved in mobile ecosystem is responsible for the actions that it has performed as per its role, rules of service and prescribed guidelines. Mobile Ecosystem entities are accountable for ensuring Secure Mobile Services. Designated and authorized bodies of the respective regulators of verticals should monitor, do periodic technology audit and verify compliance to security policy and Government regulations.

(J) Trust: It ensures that the participating entity is or publicly evolves to be trustworthy. An Entity's past actions of adherence to rules and positive traits as making less errors, less failures, timely completion, following social order, maintaining ethical practices, complying to rules, gaining good opinion by others etc. count in declaring an entity as trustworthy of Low, Medium or High levels.

(K) Reliability: It means that an entity involved in Mobile Ecosystem is reliable provided it is trustworthy. Analysis on the data of an entity's contributions, adherence and violation of rules in free and forced conditions, validation of associations, relations and inheritance may be useful to assess the reliability level of a mobile ecosystem entity. Reliability may be Low, Medium and High Levels.

1.8 Mobile User's Data and Privacy Protection

(A) Data may be of any entity such as a person, mobile phone, organization, Process, Role and Position. Mobile User's Sensitive data such as date of birth, residential address, bank account details, login credentials, passwords, personal files or photos, digital signature, transaction information of payments, AADHAR number, biometric and authentication data, data of current location, places visited and historical events, financial data, health data, ethnic race, caste, political opinions, religious beliefs, genetics, relationships, personal tastes and traits etc. are private to the Mobile User which should not be known, collected or misused by any unauthorized person or entity or organization. Personal data of a Mobile User is to remain private to the mobile user and protected as per the Personal Data Protection (PDP) Act 2019.

(B) People are highly concerned about their privacy and personal data protection. The right to privacy in India is an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the constitution. Privacy of the data of the Mobile User should be protected as per the Government of India regulations and PDP Act 2019.

(C) Privacy is categorized on technical basis as:

(i) Communication privacy (Transmission of data using encryption based on Transport Layer Security-TLS)

(ii) Position privacy (Location privacy since SIM/E-SIM can access mobile user location).

(iii) Path privacy (Intermediate nodes as Routers or Trans-receivers stations, process route information).

(iv) Identity privacy (Personal privacy such as IMEI/ESN/MEID, ICCID, eID, IMSI etc.).

(v) Personal data privacy (Use cryptography techniques for data protection).

(D) No personal data of mobile user shall be processed by any person, except for any specific, clear and lawful purpose. The personal data shall be collected digitally only to the extent that is necessary for the purpose of processing of such personal data. Every person processing personal data of a data principal or mobile user shall process such personal data—(a) in a fair and reasonable manner and ensure the privacy of the data principal or mobile user and (b) for the purpose consented to by the data principal or mobile user which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.

(E) Every data fiduciary or personal data consumer or collector shall give to the data principal or mobile user a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:— (a) the purposes for which the personal data is to be processed; (b) the nature and categories of personal data being collected; (c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable; (d) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; (e) the basis for such processing, and the consequences of the failure to provide such personal data, (f) the source of such collection, if the personal data is not collected from the data principal; (g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable; (h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable; (i) the period for which the personal data shall be retained or where such period is not known, the criteria for determining such period; where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary.

(F) The procedure for grievance redressal and notice shall be clear, concise and easily comprehensible to a reasonable person or mobile user in multiple languages where necessary and practicable.

(G) The data fiduciary shall take necessary steps to ensure that the personal data of mobile user processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed. The data fiduciary shall have regard to whether the personal data—(a) is likely to be used to make a decision about the data principal; (b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or (c) is kept in a form that distinguishes personal data based on facts from personal data of opinions or personal assessments.

(H) Where personal data of mobile user is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement of PDP Act, the data fiduciary shall take reasonable steps to notify such individual or entity of this fact.

(I) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing. The personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any Indian law for the time being in force.

(J) The data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data of mobile user in its possession otherwise such personal data shall be deleted in such manner as specified by PDP Act 2019.

(K) The consent of the data principal or mobile user in respect of processing of any sensitive personal data shall be explicitly obtained— (a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal; (b) in clear terms without recourse to inference from conduct in a context; and (c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing and should be made available when asked by the MU.

(L) If the personal data is to be processed without obtaining consent of Mobile User it should have reasonable purposes as specified by regulations in India.

(M) To safeguards and protect the rights of data principals "sensitive personal data", is to be specified with regard to— (a) the risk of significant harm that may be caused to the data principal or mobile user by the processing of such category of personal data; (b) the expectation of confidentiality attached to such category of personal data; (c) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and (d) the adequacy of protection afforded by ordinary provisions applicable to personal data. What type of additional safeguards or restrictions have been considered for the purposes of repeated, continuous or systematic collection of sensitive personal data of mobile user for profiling of such personal data is to be published.

(N) Enterprises try to protect their information, communication and application infrastructure, causing them to have private mail servers, data storages etc. Data center and respective cloud service infrastructure security must be followed as per the Personal data protection Act 2019. Mobile User's data storage would be situated within geographical region of India only in a secured and protected environment with its management office in India.

(O) Threats on a Mobile Device come from various threat actors or adversaries who are responsible for breach of trust and privacy of MU, so such threat actors, their owners and promoters responsible should be identified, data of their culpable actions to be collected for proper evidence of violations, legal action to be initiated for blacklisting and punishment, so that nobody can dare to do similar harm to others in India.

(P) Mobile User Identification for online mobile services should be done with at least two factors of authentication. Mobile Devices with embedded scanners or plugins satisfying UIDAI guidelines may use AADHAR based user authentication for specific services as e-voting, high value payment transactions, passport and e-filing of Tax etc.

(Q) Use of Public Key Infrastructure with digital certificates & digital signatures issued by the Certifying Authorities of India onto the secure element of the MD or USIM/E-SIM of the Mobile User and Mobile Service Providers would ensure non-repudiation and help in e-Voting, which should be implemented as per IT Act 2000 and 2008. DoT, TRAI and CCA may issue suitable guidelines for PKI implementation on Mobile Devices in India in a phased manner.

(R) SIM/E-SIM manufacturing in India is much needed (One may refer to DoT notification 800-04/2017/As-II on dated 16/04/2021 for personalization of SIM and e-SIM and their IT equipment and data utilized for personalization shall be within India). Since localization of data is necessary as per Indian regulations, and additionally SIM/E-SIM supply chain security including software (OS, Active program in HW, Applications), secure personalization until end customer delivery shall be implemented, Network Configuration, Keys and Data Exchange and data center shall remain localized.

1.9 Mobile Security Control Measures

(A) Mobile Security Control Measures (MSCM) are counter measures to prevent mobile security threats from adversaries and to avoid exploitation of mobile security vulnerabilities. They help in the mitigation of mobile security risks. Different Control-measures of security are being developed and applied to mobile devices, from security in different layers of communication to the dissemination of information securely to end users. There are industry wide best practices which should be observed at all levels, from design to use, through the development of operating systems, software layers, and downloading of mobile apps. Security Controls vary, as all do not act at the same level, and they range from the management of security by the operating system to the user. The Control Measures for mobile services security are classified into three categories:

(B) Policy based Measures:

(i) Mobile Security Threats can be controlled by following:

(ii) Regulatory Guidelines, Organizational Security Policy and Standards of Mobile Security.

(iii) Setting business conditions of transaction limits based on security threat level, such as limiting transaction limit for mobile payment using unencrypted SMS channel as maximum Rs.5000/-.

(iv) Established Social practices as delivering content in native language of a mobile user and use of familiar symbols/codes/identity to avoid mobile user's exposure risk.

(C) Technology Oriented Measures:

For end to end mobile security (i) security goals given in Section 1.7 need to be fulfilled across each layer (Physical, Data Link, Network, Transport, Session, Presentation, Application) of the Open System Interconnection (OSI) Model of communication, (ii) Surveillance of Mobile Network Systems and real time monitoring of communication traffic through Intrusion Detection Systems and Firewalls should be in place and Antivirus solutions with periodic updates need to be deployed, (iii) Secure coding practices need to be followed by developers, (iv) Security Testing of mobile application need to be done and valid certificate of security clearance be obtained from authorized Mobile Security Testing Organization before deployment, (v) Periodic Security audit of entities and systems should be conducted by recognized entities, (vi) mobile operating systems (OS) must establish the protocols for introducing external applications and data without introducing risk through sandboxing, light weight cryptography, fine grained access control etc. (vii) Mobile App Store Owners and

Providers must ensure that their mobile apps for public use in India are compliant to MSG and other mobile security standards such as BIS, OWASP, otherwise it degrades trust.

(D) User Centric Measures:

User Awareness is the main pillar of mobile device security. User's knowledge of security precautions to be taken for mobile device security should be gradually upgraded to a mature level. If users are careful, many attacks on mobile device can be avoided, especially phishing and application permissions on a mobile device. Some useful mobile security control measures that a mobile user should follow are given in Section 6.8.

1.10 Principles

(A) Mobile security concerns are of paramount importance, due to large scale mobile users, growing mobile security threats and dependency on multiple entities of mobile ecosystem. Several steps have been taken by the Government by bringing their various services on digital media as e-Governance and Digital India initiatives. Mobile Governance and Digital India initiatives focus on providing all government services onto the mobile phone for its citizens and residents. The development of MSG is based upon five basic principles:

(i) **Holistic:** It should follow holistic approach by including all stakeholders of mobile ecosystem as per their roles and responsibilities.

(ii) **Futuristic:** It should give direction for overcoming not only the present challenges of mobile security threats but to target emerging futuristic mobile security challenges.

(iii) **Usable:** It should not only be simple to understand and convenient for implementation but Usable across all segments of Mobile Users in India.

(iv) **Comparable:** it is to be of comparable level with respect to the various available standards of National and International bodies such as BIS, OWSSP, TSDSI, TRAI, NIST,3GPP on Mobile Security.

(v) **Measurable:** It should define levels of mobile security entities and components to help in identifying their present security level and enabling the path to achieve higher security level.

1.11 Scope

(A) MSG describes the terms and definitions of mobile device technology ecosystem. It defines security goals, roles and responsibilities of stakeholders, security levels and security requirements. It is applicable to each category of stakeholders of the mobile ecosystem as per their roles and responsibilities.

(B) MSG defines Mobile Security Control measures in three categories as (a) Policy Based Measures, (b) Technology Based Measures and (c) User Oriented Measures, in order to mitigate various emerging mobile security threats and security vulnerabilities.

(C) MSG specifies mobile device security testing and mobile device forensics guidelines along with requirements and operating procedures of assessment, which would be beneficial to the mobile device security testing organizations and labs. The mobile device security testing is to be done at three levels (i) hardware level, (ii) software level and (iii) firmware level under static and dynamic testing environments. The guidelines are generic, Operating System (OS) agnostic and covers the security requirements at Hardware, OS & Application layers.

(D) The central objective of MSG is to ensure privacy, protect sensitive data and provide security of transactions of every mobile device user, by following the security controls prescribed for various stakeholders involved in the mobile service ecosystem.

(E) MSG prescribes Technology oriented Mobile Security Control Measures along with checklists for ready reference by Technology Providers with focus on (i) Mobile Device Security, (ii) Mobile Communication Security and (iii) Mobile Service Security.

(F) MSG provides Checklist for User awareness on Mobile Device Security Controls to safeguard Mobile Users. User Levels are specified so as to help them identify their present level of awareness and understanding of Mobile Security Measures.

(G) MSG supplements the MDSS (Parts 1 to 4) given by BIS in Dec.2021 and covers Mobile Security Testing, Mobile App Vetting process as well as mobile forensics. Each entity needs to specifically fulfill the checklist of mobile security control measures specified as per its role and responsibility.

(H) Adoption of the prescribed MSG would not only elevate the culture of involvement and accountability of all entities towards mobile security but help in building trustworthy and secure mobile services ecosystem in India

1.12 Target Audience

The following entities represented by the notations for each entity group are the target audience of the MSG:

(A) M : Manufacturers of Mobile Phone Device, its Hardware Components, Peripheral Equipment and Interfaces.

(B) D : Developers of Mobile Software Services - Functionality, Applications, APIs, Operating System, Browser, micro-services etc.

(C) S : Service Providers of Mobile Software, Mobile Application providers, Mobile App Stores, Integrators, Government and Non-Government Bodies providing m-Governance and Mobile Services, Social Media Services and APIs of Mobile Services.

(D) N : Network Providers as Mobile Network Operator, Providers of Mobile, Network, Internet, Satellite, Wi-Fi and Wireless Communication Services.

(E) R : Regulatory Bodies as Regulators, Auditors, Standardization Bodies and Enforcement Agencies.

(F) T : Testing agencies as Mobile Security Testing Labs and Forensics Organizations, Quality Assurance, Enforcement and Assessment Bodies.

(G) A : Academia and Researchers

(H) U : Mobile Users and Mobile Subscribers

1.13 Checklist

SR.No	Checklist	Section
1	Entities of Mobile Ecosystem	1.2
2	Security Levels of Entities	1.2(C)
3	Mobile Technology Components	1.3
4	Security Levels of Mobile Technology Components	1.3(B)
5	Mobile Security Risks	1.4
6	Mobile Security Threats	1.5
7	Mobile Security Vulnerabilities	1.6
8	Mobile Security Goals	1.7
9	Data Privacy of Mobile User	1.8
10	Mobile Security Control Measures	1.9
11	Principles of MSG	1.10
12	Target Audience	1.12

2. Mobile Device based Security and Control Measures

(A) In this chapter, Security aspects of Mobile Devices - Hardware, Software and Firmware along with Mobile Device Security Framework are given. Threats, Vulnerabilities and Control Measures of Mobile Device Security with special focus on Mobile Operating System and SIM Card are given.

(B) Mobile Device (MD), its sections and components are explained in Section 1.1. Here mobile device security and potential approaches for mitigating the various security threats and vulnerabilities are given. Mobile Phone Handsets Safety Requirements should be followed (IS 16333, Part-1, 2015 & BIS, reaffirmed 2021)

(C) The mobile device software and hardware should provide essential security services, such as cryptographic services, crypto library, data-at-rest protection, and key storage services to support the secure operation of applications on the device. Additional security features such as security policy enforcement, application mandatory access control, anti-exploitation, user authentication, and software integrity protection are required to be implemented to address the real-time threats.

(D) Mobile devices are subject to the threats of traditional computer systems along with those entailed by their mobile nature. Mobile Device Security Threats are given in Section 1.5. The threats considered in this standard are those of network eavesdropping, network attacks, physical access, malicious or flawed applications, persistent presence, data, biometric impersonation, revocation of biometric credentials, revocation of biometric template etc.

2.1 Mobile Device Security Capability Framework

(A) This security capability framework of the smart mobile device is diagrammatically shown in Figure 1 in the Annexure D having five layers namely, the hardware at the bottom layer, operating system above it, peripheral interface involved with OS and hardware, application software layer on top, and the user data protection layer involved with hardware, OS and application software.

(B) Security objective of hardware: To Ensure the security of Flash and baseband within the mobile communication device at the chip level. To assure that the system programs, device parameters, security data and user data in the chip will not be changed or illegally acquired.

(C) Security objective of operating system: To ensure that it can monitor, protect and prompt accessing of system resources with no presence of execution of a benign/malicious behavior which the user is unaware of, or is not under the control of the user. To assure that its own software upgrading is also under control.

(D) Security objective of peripheral interface: To Ensure that the user can get to fetch usage details using peripheral interface of wireless type and wired type, data have finer control on the connection and have secure data transmission on the peripheral interfaces. To assure to verify that only authentic application/API can access data from peripheral interfaces such as sensors and IoT devices.

(E) Security objective of application layer: To ensure that the mobile device can identify the sources of application software to be installed thereon and can control the sensitive behavior of the application software already installed thereon.

(F) Security objective of user data protection: To guarantee the safe storage of user data, so as to assure that it will not be accessed, acquired or falsified illegally, thus ensuring that it can be recovered in a reliable way through backup.

2.2 Mobile Operating System Security

The Mobile Operating System (OS) should ensure proper security measures at various layers in the stack as mentioned below:

(A) Application-level Security

(i) Protect app and user data: When developing a mobile app, it is not only required to focus on usability and performance but also security measures. A secure mobile app can lead to significant end-user satisfaction and enable trust.

(ii) App-defined and user-granted permissions: Mobile app permissions built upon security features can help mobile device to support the data minimization, control, and transparency goals related to user privacy.

(iii) Application Sandboxing: Isolate user-level applications from each other so as to prevent data leakage between applications.

(iv) Virtual Private Network (VPN): There should be built-in support for VPN clients & VPN apps which in-turn support different profiles such as personal & work. This helps the business-related applications to secure their assets and data on mobile device. This also helps in addressing the privacy related concerns of the mobile users. Even though it is possible for some mobile users to misuse the VPNs to access banned content and hide their identity, use cases of the VPNs outnumber the misuse cases and hence need to be supported by the Mobile operating system with care.

(v) Application Blacklisting/Whitelisting: Blacklist unauthorized apps and Whitelist authorized apps using Device Management Software.

(vi) Application Verification: Ensure that applications being installed on mobile device come from a valid and trusted source. OS-level capability provided by each mobile OS should verify the digital signature of mobile applications.

(vii) Anti-debugging checks, code obfuscation checks, hooking checks, emulator checks etc. need to be done. This makes the mobile application resilient against some of the reverse engineering attacks for binary code protection.

(B) Framework level Security

(i) Protect system resources including the network, camera, GPS etc.: Mobile Applications must ask an explicit permission to use input devices (system resources) such as camera, GPS and microphone. For a third-party mobile application to access these devices, it must first be explicitly provided access permission by the mobile user through the use of Mobile OS Permissions.

(ii) Managing keys and enforcing security at system level should be done.

(iii) Secure Containers: Multi-user framework can be used to securely separate work and personal profiles on a single, unified interface.

(iv) Device Resource Management: Ability to enable/disable device peripherals. Carrying out automatic, regular device integrity and compliance checks. Using device management software, need to be done.

(v) Remote Wipe: If a mobile device is lost, data and personal information can be misused. Even if it is locked, adversaries pay money to get it unlocked. So, remote wipe facility is advisable to be enabled on the Mobile Device.

(C) Kernel level Security

Boot level security: Bootloader is an important component in a mobile device whose security and integrity directly affects the system wide security of the device. So, check for bootloader vulnerabilities and re-evaluate.

(i) System and Operating System/Kernel level security: Enable robust security at the kernel/OS level by leveraging the security features in the underlying kernel, such as Address Space Layout Randomization (ASLR), containerization, Mandatory Access Control etc.

(ii) Secure Inter Process Communication (IPC): On a mobile device, applications and system processes need to communicate among themselves so as to exchange relevant data. In Android, IPC is provided using binder mechanism and it allows verifying the source of the application connecting to the right destination which could be another application or core system functionality.

(iii) Secure Device Drivers: Mobile Operating System locks down the processes which have access to vendor-specific device drivers. Look into the security impact due to modifications in device drivers.

(iv) Device Encryption: Full disk encryption has become a common feature that provides confidentiality to mobile device as well as user data. In the recent mobile operating systems, there also exist per file encryption mechanism which further enhances the security of data. Ensure that hackers do not get this privilege otherwise it may be misused for ransomware attack.

(v) Trusted Execution Environment (TEE): Modern System-On-Chips (SoCs) which are used in the mobile devices, have hardware features to enable and use TEE. This mechanism provides two separate execution environments commonly called as secure and normal world. The secure world is tightly coupled to access security peripherals including the secure memory, which ensures that crucial data and I/O devices are accessed through a sandboxed mechanism.

(vi) Secure Key Management: Key storage is important for security of data and storing and accessing it from the mobile device such as Secure Element (SE) or Hardware Security Module (HSM) provides an assurance of secure access to these cryptographic keys. The keys stored in SE and HSM require authentication for accessing it and hence make it suitable for restricting access to it, assuring that it is used only by benign components of the system. Keystores are preferred to be protected using hardware level security like TEE.

(vii) Firmware update: implementation of digitally signed firmware, which is the next level of security that restricts the attacker to load rogue Firmware.

(D) Secure Software Development Life Cycle (Secure SDLC):

During the development, implementation and release of the updates to the existing Mobile OS/application/APIs version or newer version, OEMs must comply with the Secure SDLC with procedural aspects:

(i) Design aspects: (a) Ensure to have rich and configurable security model and design using Unified Modelling Language (UML), (b) Do Security review of all the features of the platform, (c) Incorporate widely accepted security components and controls

(ii) Penetration testing and code review: Identify weaknesses and possible vulnerabilities well before major releases and fix them before the release.

(iii) Incident response: Comprehensive security response process should be in place.

(iv) Monthly security update: Frequent update cycles should be in place.

2.3 SIM Security

(A) Subscriber Identity Module (SIM) resides on an Integrated Chip (IC) Card or Smart Card or Universal Integrated Circuit Card (UICC) popularly known as SIM Card, which is issued by an authorized Mobile Network Operator for providing Cellular Mobile Communication Services to its registered Mobile User. SIM Card after plugged in its slot or embedded in a mobile device and personalization is done then it becomes the virtual identity of the registered Mobile User for all-important transactions from the mobile phone device. SIM is a potential target by adversaries to steal mobile user identity and commit frauds, as it is a gateway for mobile device connected world, so it should be protected.

(B) SIMs are of three types (Figure 2) (1) Pluggable SIM, which depending upon the size and form factors (FF), are categorized as Mini (2FF), Micro (3FF), and Nano (4FF) SIM. These are pluggable on IC/UICC platform, detachable from mobile phone and used for communicating with devices under GSM/3GPP network (As shown in Figure 3), (ii) Embedded SIM (eSIM) with soldered form factors of M2M Communication, supports GSMA M2M and Consumer devices communication with remote profile management and product lifecycle using GSMA SGP.02 and GSMA SGP.21 respectively (As shown in Figure 4). In a mobile device where SIM is soldered with static multiple profiles and connectivity, managed with IMSI swap using 3GPP OTA is referred here as eUICC, (iii) Soldered SIM (sSIM) is the GSMA eSIM of next generation for M2M and consumer business providing unique GSMA infrastructure for remote profile management and profile activation.

(C) The life cycle of the SIM form factors is based on their production and personalization. SIM manufacturers personalize the cards OS Loading, Network Profile, Static Application, Security Domain and respective keys etc. in the factory. Whereas for SIMs under GSMA specification, OS, Bootstrap Profile and eSIM Certificates are personalized in GSMA SAS certified factory and in next step OEM manufacturer shoulders the eSIM in the OEM board by getting GSMA eSIM from eSIM manufacturer.

(D) SIM/eSIM Threats:

(i) Any kind of internally left malware in SIM/eSIM, unrecognized/customized functionality or unknown application coupled with Operating System is a threat.

(ii) Remote management functionality and remotely managed unwanted applications or applets may also cause a threat for an unsecure SIM Operating System.

(iii) The data on the SIM/eSIM as well as the data with the connected digital systems that the device is able to access, such as : (a) Subscriber Identity or Identity in other form or purpose, (b) Authentication data to access network, (c) Algorithm and security keys and other keys used in end-to end security, (d) Encryption of commands send to SIM/eSIM or to the devices to control/read/update information, (e) Input sources data that could be used to attack a device, (f) Remote services to target SIM/eSIM, (g) Using some lab Devices used to target for side channel attack and read voltage variation to observe algorithm activity and pattern, (g) Environment Data in the physical presence of an adversary or when the mobile device as used outside of normal conditions are likely to be compromised to secure SIM.

(E) SIM Security Control Measures:

Securing SIM/eSIM is one of the basic steps to protect all kinds of SIM/eSIM known frauds. SIM/eSIM software in the form of Operating System, Applications and Network Profile need to be protected. For identifying SIM/eSIM and its respective contents as well as SIM/eSIM security and its requirement for implementation see Annexure F.

Following are important for SIM/eSIM/Soldered SIM security:

(i) SIM OS development, its functional Testing, validation and security implementation along with its security testing are to be done in a secured and certified protected environment.

(ii) SIM OS software security with implementation of protection profile is to be carried out as defined in Common Criteria or GSMA specifications.

(iii) Securitize the SIM/eSIM assets by ensuring Side Channel Attack (SPA) and Differential Power Analysis (DPA).

(iv) SIM OS delivery from its secure development area to mass production (SIM Personalization Centre) is to be done in a secure way.

(v) Secure personalization Centre for SIM and protected personalization process (As per the DoT order no. 800-04/2017/AS II dated 19.08.19, personalization of SIM card provided to the subscribers for accessing the mobile network, shall be mandatorily done within India w.e.f 01.03.2020) and this guideline extended for eSIM for the SIM category i.e. GSMA eSIM and eUICC is to be followed.

(vi) Data Security is required for a data centre, for data generation area in SIM production, for MNO (Network management, Data preparation Infrastructure), during data in transit and data in rest. Self-destroying process after achieving its retention time is necessary.

(vii) Supply Chain Security is required for component used in Product development and order process. Active programming code that resides in supply chain component, may be a threat. Its security/quality check process for Hardware and software should be done.

(viii) Standardized Security process for data sharing to customers. Physical and logical security is to be followed.

(F) Software and Data security:

Since SIM/GSMA eSIM manufacturing technology and high capability is available in India, it is advantageous from security perspective and as per IT security acts requirement to have data localization. Hence SIM, operating system development, Personalization, Network Configuration including IT equipment, Keys, Data centre and Data Exchange are to be localized. Further GSMA eSIM, GSMA Remote Service provisioning, IT infrastructure for M2M and consumer devices including Over the Air (OTA) service IT infrastructure also shall be localised. India M2M business need to promote to adopt domestic manufactured GSMA eSIM and advanced versions for connected mobile world security.

(G) Certification bodies for SIM:

(i) In SIM/eSIM development and manufacturing infrastructure, following entities in the Annexure G need to address for their security concerns, recommended security and their recommended certificate bodies. GSMA eSIM operational security challenges are observed as per below business case scenarios.

(a) Imported GSMA eSIM is in Imported Device (OEM) and its Remote Personalization is done from Foreign Land. - *A serious challenging scenario*

(b) Imported GSMA eSIM is in Imported Device (OEM) and its Remote Personalization is done from Local Land. - Moderate challenge. Machine manufacturer has to follow supply chain security for active programming codes.

(c) Imported GSMA eSIM is in Local Device (OEM) and its Remote Personalization is done from Foreign Land - A serious challenging Scenario.

(d) Imported GSMA eSIM is in Local Device (OEM) and its Remote Personalization is done from Local Land - A Minor Challenging Scenario

(e) Local GSMA eSIM is in imported Device (OEM) and its Remote Personalization is done from Foreign Land - A serious challenging Scenario.

(f) Local GSMA eSIM is in Imported Device (OEM) with Remote Personalization is done from Local Land (India) - A Minor Challenging Scenario

(g) Local GSMA eSIM is in Local Device (OEM) with Remote Personalization is done from Foreign Land - A serious challenging Scenario.

(h) Local GSMA eSIM is in Local Device (OEM) with Remote personalization is done from Local Land (India) —No Challenge and so it is most preferable**.**

(ii) Un-secure Operating system poses security threat. it is recommended to develop OS in a standardized secured protected area, having well-defined security process to transfer it to the Personalization Centre. In addition, in case of eSIM transfer to OEM assembling house standardized supply chain security is mandatory. OS security has no control if eSIM is developed in foreign land only and relies on GSMA or Common Criteria Protection Profile (PP).

(a) Challenges in supply chain security for local eSIM and foreign eSIM.

(b) Data security and privacy for local eSIM Managed from Foreign land.

(c) Challenges on multiple personalized of APNs (no validation rules to check how many APN's are configured).

(d) Challenge to OEM for eSIM integration and configuration, Multi-cloud Authentication, adaptable attestation, secure peripherals.

(iii) Algorithms and Secrete Keys: Standardized algorithms, under control of the SIM operating system, are responsible for encryption and decryption of data using the relevant keys stored in SIM, location only and only if known by Operating system. The ordering party or SIM issuer should use standard algorithms.

(iv) SIM Applications: Application personalization in SIM, is for specific business needs, and depends upon the requirement of the application provider. Application development shall be in a protected secure environment. It can be personalized either in the factory (Personalization Centre) or shall be deployed remotely using OTA services directly in the field after verification.

(v) SIM/eSIM assets description and their Owner need to understand the security levels and threat intensity. Please refer Annexure H

(H) SIM/eSIM Personalization Process

(i) SIM personalization is a highly complex process, it requires quality process and continuous inspection to produce the quality delivery. For quality process the organization shall be highly secure and protected like Common Criteria certification for R&D (OS development and security testing centre) with ISO 9000, ISO 27001, TEVCCS from STQC including GSMA SAS shall be mandatory for SIM/eSIM development and for manufacturing process for SIM/eSIM/USIM/M2M suppliers.

(ii) SIM manufacturer should handover SIM in secure way to MNO and it should be verified and acknowledged. For Embedded SIM. Data generation is the part of MNO using SM-DP and SM-DP+ server. Figure 6 shows the complete SIM/eSIM product lifecycle including risk area.

(iii) Identified Risk Area in SIM (Pluggable, eUICC and non GSMA RSP) Card production and operation. As picturized in Figure 6, the identified risk area and their concerned security challenges are:

(a) Intermediate value Risk Area: Intermediate risk value area needs secure communication and is very much related with the supply chain components, such as Silicon, Module, plastic body and M2M form factor (DFN-8/SON-8, DFN-6 as per ETSI TS 102.671) shown in Figure 6 in grey colors. Also the Input file provided by MNO/TSP and Module delivery and Plastic body embedding aspects.

(b) High value Risk Area: High Value Risk Areas not only require secure communication, but the concerned area shall also be protected with standard physical and logical security as shown in Figure 6 in red. It should focus on (i) SIM/eSIM Development, (ii) SIM Production (Factory) with Data Generation and data centre for SIM/eSIM, eSIM/M2M form factor processing, Secure personalization and Supply chain Security, (iii) R&D on OS Development, Application Development, SIM profile Development, OS functional testing and validation, Security implementation (Securitizing process) and testing, (iv) OEM (For Embedded SIM (eUICC/GSMA eSIM) business case)-Equipment manufacturer shouldered the ordered embedded SIM (eUICC/GSMA eSIM) and Deliver OEM to the desired use case manufacturer (Car, Phone, cellular IoT device etc. (v) MNO/TSP - SIM provider and 3GPP Network operator for 2G/3G/4G/5G and beyond Services, GSMA eSIM Profile download and subscription management, GSMA eSIM activator and Network Profile activator and eSIM/M2M service provider having GSMA RSP infrastructure (SM-DP, SM-DP+, SM-SR, SM-DS, LPA).

(I) SIM/eSIM OS Development and Application Security

(i) OS development for targeted chips is a tedious and complicated task. The software development organizations design their OS in such a way that it could be used for a long time until any major change comes in chip technology or in software development tools. Weak design of OS could be vulnerable and can be easily targeted for unauthorized access for OS assets, below shall be implemented to face such challenges.

(ii) OS and application shall be developed in Indian geography. Physical location of development centers must be aloof from the outside world and premises shall have standardized physical and logical security following Intellectual property level protected environment. Secure Bootloader shall be implemented. Securitizing the Assets of SIM/eSIM is the most important activity for the development of OS. The OS development team has to securitize the Algorithm, keys from third party access even from Side Channel Attack (SCA), Differential Power Analysis (DPA). Implementation of standardized Protection Profile from common criteria community or from GSMA shall be implemented as standard security. Digitally signed firmware and OS update shall be implemented

(J) Authentication layer is the core component of the SIM/eSIM secure framework and the purpose is to provide and verify identity. The mechanism to store and present identity information is the key factor of security. SIM Identity ICCID (Integrated Circuit Card Identity) and eSIM Identity eID are to be secure. Secure encrypted IMSI using SUCI (Subscription Concealed

Identifier) implementation by MNO to prevent IMSI and subscriber privacy by any attack. Cellular device Identity IMEI/ESN/MEID (International Mobile Equipment Identity for 3GPP network/Electronic Serial Number for CDMA 2000 Network/Mobile Equipment Identifier for CDMA 2000 Network). These are supply chain identity and open to everyone are much vulnerable. In the age of hybrid networks and massive cellular IoT. It is mostly targeted by the attacker to steal the Identity.

(K) It is recommended to have virtual Identity known to only the network host and device, it also helps to lock the device with SIM/eSIM. Follow the recommended process to create virtual Identity using ITU x.509 certificate using PKI infrastructure. This Virtual Identity integrated with certificate issued by a certification authority shall be used to identify the device and then further process for authentication and even end-to-end encryption. Virtual Identity and certificate-based authentication can be used for *Service Layer Security* (see section 4.3) to secure Endpoint devices or nodes. This should be recommended for cloud service secure authentication.

(L) SIM can be used as Root of Trust device, where identification, authentication and authorization are needed. See Figure 8 Implementation of OPEN Mobile API (Global Platform Technology specification v3.3) (Please see Section 4.2(F)) in mobile devices, shall be mandatory for secure operation for banking, Identity, healthcare and telecom use cases.

(M) It is recommended that 3GPP network Infrastructure and GSMA RSP infrastructure shall be established in India in tune with TSDSI standards.

(N) Application Level Security

(i) In the SIM/eSIM domain, critical components of Application logic are implemented and distributed to a number of Endpoints, Gateways and Servers. Many distributed computing software components require client-side modules to communicate with servers. This would facilitate application developers to harness the centralized security, compute and storage, which has been a major driver of the emergence of cloud computing. Follow strictly the Registration Procedures.

(ii) Registration and Identification of the M2M Service Provider and M2M Application Service Provider by a Registration Authority. Registration and Identification of the Common Platform Layer and the Application Layer Instances. Registration and Identification of the End Point Devices. (Custodian/OEM/SIM/eSIM). Use 32k NVM reserve for Govt Use cases as recommended in ITSAR UICC.

2.4 Mobile Device Software

(A) Platforms

(i) Android and iOS are at the top in Mobile Operating System Market Share Worldwide. Many of the mobile device manufacturers have customized variants of Android. Most of the mitigations steps against platform/kernel level attacks require protection features to be enabled and harnessed at various levels such as:

(a) Underlying hardware security features in Trusted Execution Environment.

(b) Keeping platform software/kernel up to date by employing latest patches.

(c) Enabling kernel level features such containers, Address Space Layout Randomization etc.

(d) Enabling build time features such as stack canaries, no execution (NX) permissions on data memory etc.

(ii) Mobile OS Security is separately given in Section 2.2 as it requires special attention.

(B) Mobile Browser

(i) See Section 4.1

(C) Device Database

Due to increase in usage of mobile devices, the percentage of personal/business data stored on the devices has increased rapidly. These data are commonly stored as files, database, shared preferences, external storage and keystore. So, the mobile devices need to provide mechanisms for the developers to securely store the user's sensitive data on the devices such as the encryption methodologies of file encryption or full disk encryption (FDE).

(D) Library functions

An increasing number of developers are incorporating third-party native libraries in their applications for code reuse and other purposes. These libraries can access the complete process address space and can share all the permissions which the user has given to the applications. Hence, it is highly recommended for the developers to give proper emphasis in assessing the security of these third-party libraries before being used as part of the application development.

(E) Application Program Interfaces (API)

Mobile applications commonly use APIs to interact with back-end services and information. So, it is important to prevent the API calls from tampering. It is advised to use proper cryptographic mechanisms to ensure the confidentiality & the mutual authentication of both client & server before any communication through APIs happen.

2.5 Mobile Device Hardware

(A) Processors

Processors should provide a secure environment in which confidential data in the device can be protected. Processors also should employ a physical shield to guard against physical attacks. Additionally, processors should provide constant scrambling and encryption of secret data. It should also have mechanisms to prevent side-channel assaults and can identify improper voltage or temperature changes.

(B) Trusted Execution Environment

Trusted Execution Environment (TEE) ensures data protection even if the mobile operating system is compromised. Every Mobile device does not have TEE. Applications of national importance may possess sensitive data of the users such as the Aadhaar information, PAN related information etc. which needs to be protected from compromise with isolated environments such as TEE.

(C) SD Card:

When sensitive data is not properly safeguarded as part of the app storage, it becomes vulnerable. The application may be able to save data in different locations, such as on the device or on an external SD card. The often-used mechanisms on the mobile platform to store the data are File based Storage, Shared Preference, Internal Storage, External Storage, SQLite Databases, and Realm Databases. Security of sensitive data on mobile device storage can be enhanced by adhering to the below guidelines

(i) Usage of secure storage API calls with respect to mobile platform.

(ii) Inducing cryptography mechanisms to enhance the security of sensitive data.

(iii) Store app-specific data within the internal app storage instead of external storage.

(iv) Usage of Hardware-backed Keystore is preferable to enhance the security of sensitive data stored on-device storage.

(v) Full Disk Encryption or File-based Encryption techniques must be incorporated at the OS level to achieve overall storage security.

(D) SIM Card: SIM Security is separately given is Section 2.3 as it requires special attention.

(E) Sensors:

Modern mobile devices incorporate a number of sensors which include accelerometers, touch, magnetometers, gyroscopes, cameras, fingerprint, microphone, location etc. Regarding the various classifications of the sensor refer: Annexure D (Categories of sensors)

(F) Storage:

Modern mobile devices support multiple storage devices such as the internal, external SD Card and more recently by connecting the flash storage through the USB. Since the external storage is formatted with FAT file system and the kernel on the mobile device support have permission model enforced on natively supported file systems such as EXT3/4, JFFS2 etc. all the information stored on these devices is accessible to any application. The internal storage and hardware assisted secure storage are recommended mechanisms to store crucial data. Also, many platforms provide Full Disk Encryption (FDE), per file separate encryption keys etc. as the protection mechanisms, which may be used.

2.6 Mobile Device Firmware

(A) The mobile device firmware includes various components including the kernel, device drivers, platform software, runtime libraries, virtual machines and so on. The core firmware interacts with various components such as I/O ports, displays and external servers/cloud infrastructure to get updates on various components.

(B) Input/Output Interfaces and Ports:

Many of the OEMs do not have in-depth expertise in system level firmware components and rely on the ODMs to provide security of I/O interface and ports access, using device drivers. It is required to have security of device drivers also to be evaluated before shipping the firmware. This includes I/O ports that control the baseband peripherals, specialized interfaces such as NFC, and the important ports where sensors are connected.

(C) User Interface Stack:

User interfaces are very important in mobile devices as users interact with the sensitive applications using these interfaces. Users generally use them to provide confidential and personal information such username, password, PIN etc. which can be disclosed if the firmware components are compromised. There have been attacks where the malicious UI widgets are super imposed on benign UI screens to capture user personal information and misuse it. Many modern processors provide secure world executions and capture of input and output data from user with special hardware access which can be harnessed to provide security on User Interface Stack.

(D) IoT Interfaces:

With the evolution of IoT, many devices get connected to Mobile Devices for sensing, monitoring and controlling operations. These devices use wireless technologies such as Wi-Fi, Bluetooth, NFC etc. for communication. The communication/protocol stack for such devices are implemented inside the firmware of the device. There have been number of attacks on these protocols stacks especially from the perspective of lack of authentication before data exchange, exposure of data due to lack of confidentiality features in implementation of protocols etc. Also there exists firmware components that update the firmware on the IoT devices with Mobile as the gateway, which makes it vulnerable to disclosure of firmware updates, and also get access to hard coded keys if any used in the firmware/or to connect to device.

2.7 Checklist

SR.No	Checklist	Section
1	App Sandboxing	2.2(A)(iii)
2	VPN Security	2.2(A)(iv)
3	System Peripheral Security	2.1(D)
4	Secure Containers	2.2(B)(iii)
5	Secure IPC	2.2(C)(ii)
6	Device Encryption	2.2(C)(iv)
7	TEE	2.2(C)(v)
8	Secure Key Management	2.2(C)(vi)
9	Device Drivers Security	2.2(C)(iii)
10	SIM Security	2.3
11	Browser Security	2.4(B)
12	Security of Libraries	2.4(D)
13	Firmware Security	2.6

3. Mobile Communication based Security and Control Measures

(A) In this chapter, Mobile communication security of short range and long-range communication channels, various standards of wireless communication and mobile communication channels, evolution of 1G to 5G and beyond with security features, session management in secure manner, control measures of mobile communication security are presented.

(B) The emergence of long-range radio technologies allows wireless communication over kilometers. There is lot of academic and industrial attention in this specific area of developments. These devices use unlicensed industrial, Scientific and Medical (ISM) radio bands, Global System for Mobile communication (GSM) frequency bands etc. which are different. Many new services are also offered like an operator. The frequency bands of ISM radio frequency bands are designated and defined by the ITU Radio Regulations.

(C) The actual performance provided by the wireless communication technologies differ on several metrics such as range, data rate, energy consumption, delay etc. These metrics are dependent on deployment frequencies, modulations etc. and in the same environment setting these different signals will behave differently. The important metrics are the following: (i) range, is the maximal distance of communication, (ii) data rate is the speed of the communication and (iii) energy consumption is dependent on the other metrics.

3.1 Mobile Communication Security

(A) The data transmission communication path of a mobile device for availing any service from service providers is diagrammatically shown in Figure 7

(B) The wireless data transmission path from a mobile device takes through access network, radio network and core network of Mobile Network Operator, has some intermediate components such as access point, wireless router, satellite antenna, cellular base station, firewall, enterprise gateway, service providers servers etc.(Figure 7) If the mobile device uses data from cellular networks, the Extended Authentication Protocol for Authentication and Key Agreement (EAP-AKA) is used. The Wi-Fi access router uses different authentication methods based on the organization or enterprise network policies.

(C) Ensure security across all seven layers of the Open System Interconnection (OSI) Model, namely, Physical, Data Link, Network, Transport, Session, Presentation and Application or TCP/IP Model and between every pair of intermediate devices in the entire path of Communication from source device to end device and vice versa. Multiple Operators involved in the end to end communication should follow the latest standard domestic guidelines issued by TRAI, TSDSI and DoT. Other relevant International Standards issued by ITU, 3GPP, IMT, ETSI, NIST, IEEE, OWASP are to be followed.

(D) The Radio Communication range of a Mobile Phone is of Short Range and Long Range types. Among short range (a) up to 0,1 Meters, (b) up to 1 meter, (c) up to 10 meters, (iv) up to 100 meters and among long range (i) up to 1 Kilometer, (ii) up to 5 Kilometers, (iii) up to 10 KMs, (iv) up to 25 KMs, (v) beyond 25 KMs. Depending upon the operational environment as private or public, with line of sight or omni directional communication feasibility on the mobile device the spectrum frequency ranges vary and accordingly the security specifications and standards exist.

(E) Communications security involves defense against the interception of communication transmissions. Communications security includes crypto security [i.e., encryption or decryption], transmission security, emission security [i.e., intercept and analysis of emanations from equipment] and physical security.

(i) Issues in Communications security:

(a) The protection of communications lines of IT systems, such as a central computer and remote terminals is called Line Security. Line security is effective over lines an organization controls, generally the use of cryptographic security defeats wiretapping.

(b) The procedures for secure communication give minimal advantage to an adversary to intercept data communications from IT systems, telephones, radio, and other systems.

(c) TEMPEST is the code word for the Science of eliminating undesired signal data emanations used by the National Security Agency. Shielding is one strategy to reduce data emanations.

(d) Technical security, also called technical surveillance countermeasures, provides defense against the interception of data communications from microphones, transmitters, or wiretaps.

(ii) The mobile devices normally use the frequency below 6 GHz range of Radio Access Networks with use of spread spectrum technologies and strong encryption methods.

(iii) The use of directional antenna controls the signal spreads but can be theoretically intercepted. High sensitive receiver or a high-gain receiver antenna are generally used by hackers for eaves dropping the signals need to be deleted. The target reachability of any target can be changed or altered using amplifiers and high-gain transmit antennas.

(F) Wi-Fi offloading is a technique that allows mobile users to make and receive calls or texts over Wi-Fi. The handover to a Wi-Fi network is seamless and remains unaware to the mobile users. In Wi-Fi offloading the majority of cellular data users are actually using a nearby Wi-Fi hotspot for much of the time without knowing it and that means they are vulnerable to Wi-Fi hacks. The major risks identified in Wi-Fi communication are:

(i) Rogue Access Point (AP): Unauthorized APs that allow attackers to bypass perimeter security.

(ii) Rogue Client: Victim devices that have connected to malicious APs and may be infected with malware payloads which would be spread onto the other devices in secure networks.

(iii) Neighbour AP: Client devices on private networks that connect to nearby neighbour SSIDs and risk accidentally connecting to malicious APs.

(iv) Ad-Hoc Connections: Sharing files client to client (Airdrop for example) through mobile app is convenient, but anything shared this way, including infected files, will bypass security controls.

(v) Evil Twin AP: An AP set up by a hacker to mimic the SSID of a legitimate AP to intercept the victim's connection without them ever noticing.

(vi) Misconfigured AP: Access Points on the networks that do not comply with minimum security standards such as encryption settings are called misconfigured AP which paves way for attacks in network.

3.2 Mobile Communication Standards

(A) The collection of all cellular towers, wireless access points, antennas, network cabling, power, ports, hardware, and software are associated with the deployment of a mobile wireless communication network. The evolving and latest standards of ITU, IMT, 3GPP, ETSI, TSDSI, IEEE, NIST, LORA, NFC Forum, Global Platform are for specific aspects of mobile and wireless communication that need to be followed. Mobile Device may connect with other wireless devices in its neighborhood, so the following standards are to be carefully looked into.

(B) Wired Equivalent Privacy (WEP):

(C) WEP is the security protocol for wireless networks defined in the IEEE 802.11b standard. The use of WEP is proved to be insufficient to ensure privacy if used alone without other mechanisms for data encryption.

(D) Wi-Fi Protected Access (WPA):

(E) WPA is a Wi-Fi standard, designed to improve the security features of WEP understanding, its failures and shortcomings. The extensible authentication protocol (EAP), PEAP – MSChapV2. PittNet, Wi-Fi etc. utilize the WPA protocol.

(F) IEEE 802.1x:

The IEEE 802.1x is for port-based network access control (PNAC) on wired and wireless access points. 802.1X defines authentication controls for any user or device trying to access a

LAN or WLAN. NAC—A proven networking concept that identifies users and devices by controlling access to the network. It supports a maximum connection rate of 54 Mbps throughput in the 5GHz band. This standard has backward compatibility with 802.11b/g and requires special wireless adapters.

(G) IEEE 802.11a:

The IEEE 802.11a standard applies to wireless local area networks and supports a maximum connection rate of 54 Mbps throughput in the 5GHz band. This specification is not backwardly compatible with 802.11b/g and requires special wireless adapters.

(H) IEEE 802.11b:

The IEEE 802.11b applies to wireless local area networks and supports a maximum connect rate of 11 Mbps with fall back to 5.5, 2, and 1 Mbps in the 2.4GHz ISM band. This standard was ratified in 1999.

(I) IEEE 802.11g:

It is an extension to the 802.11 standard that allows for a maximum connect rate of 54 Mbps while maintaining compatibility with the 802.11b standard in the 2.4GHz band This specification is compatible and complementary to the 802.11b standard.

(J) IEEE 802.11i:

This extension provides for improved encryption methods and for the integration of the IEEE 802.1x authentication protocol as well as advanced encryption mechanisms such as AES (Advanced Encryption Standard), for an optional, fully compliant implementation of 802.11i.

(K) IEEE 802.11n:

This IEEE standard uses multiple transmitter and receiver antennas (also known as multiple-input and multiple-output, or MIMO) to allow for increased data throughput and range.

3.3 Short Range Mobile Device Communication Channels

Some popularly used standards on mobile device are:

(A) Wireless Fidelity (Wi-Fi)

The IEEE 802.11b (802.11 High Rate) standard protocol called Wi-Fi is an extension to 802.11 and provides 11 Mbps transmission in the 2.4 GHz band. The use of Wi-Fi, the latest Wireless radio technologies has enabled inter-device communications.

(i) Wi-Fi CERTIFIED WPA3™: WPA3™ is used for Wi-Fi security and provides a cutting-edge for security. The widespread success and adoption of Wi-Fi CERTIFIED WPA2 and WPA3 adds new features to simplify Wi-Fi security to enable more robust authentication with increased cryptographic strength for highly sensitive data markets and maintain resiliency of mission critical networks. The WPA3 networks:

(a) Use the best and most recent security methods.

(b) Do not allow outdated legacy protocols.

(c) Mandatorily require usage of Protected Management Frames (PMF).

(ii) WPA3-Personal: It is used for better protection to individual users by providing more robust recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-Shared Key (PSK) in WPA2-Personal. The features of WPA3 include:

(a) Natural password selection: Allows users to choose passwords of their choice.

(b) Ease of use: The enhanced protections with no change in the way users connect to a network.

(c) Forward secrecy: Protects data traffic even if a password is compromised after the data was transmitted.

(iii) WPA3-Enterprise: WPA3-Enterprise standard offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data:

(a) Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)

(b) Key derivation and confirmation: (HMAC-SHA384) a 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm.

(c) Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) Key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using 384-bit or higher bit elliptic curves are to be used.

(d) Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) or with higher bits to be used.

(B) Near Field Communication (NFC):

It is a standard of the NFC Forum for communication between two nearby electronic devices. NFC operates in a frequency range centered on 13.56 MHz and offers a data transmission rate of up to 424 kbit/s within a distance of approximately 10 centimeters. Recent Smartphones mostly support NFC features.

(i) Secure Element: The Secure Element (SE) is a protected execution environment for NFC applications. The good analogy is the contactless payment chip card. The SE can take many forms:

(a) A UICC that runs the SIM and USIM applications on the smart phone.

(b) An embedded smart card chip.

(c) A smart micro SD card.

(ii) Security measures for NFC devices and applications include:

(a) An on/off switch for Device NFC: to prevent unrecognized use of NFC functionality.

(b) NFC functionality is automatically turned off when the phone is asleep/off.

(c) Data encryption: to prevent unauthorized access to confidential data during NFC transmission.

(d) Stronger authentication methods by adopting stronger passwords, fingers biometric scans, etc. so that it is not used by unauthorized users.

(e) NFC tag lock for prevention of overwriting.

(f) Usage of digital signatures on NFC tags to guarantee the authenticity and integrity of tag's data.

(g) For avoiding the tracking of NFC device users when the NFC application allows anonymous transactions by using dynamic identifiers.

(C) Radio-Frequency Identification (RFID):

It uses electromagnetic fields to automatically identify and track tags attached to objects. A RFID tag is an electronic digital tag that trades information with a RFID reader by means of radio-waves. Most RFID tags consist of at least two primary parts. The very first is an antenna that receives radiofrequency (RF) waves. The second is an integrated circuit (IC) that process and store data as well as to modulate and demodulate radio waves transmitted/received by the antenna. A RFID tag is also referred to as a RFID chip. RFID systems can function in Low Frequency (LF), High Frequency (HF) or Ultra High Frequency (UHF). The three main challenges in adoption of RFID are (1) The concerns of security, (2) the problems surrounding the privacy of the data captured and (3) The characteristics associated with the physical nature of RFID.

(i) RFID Security Issues: The issues associated with RFID Security, also known as Intrusion Detection, refers to the discovery of foreign attacks upon the system usually utilising the tags that hinder the overall integrity of the data.

(a) Eavesdropping: Setting up an additional tag reader to record tag data.

(b) Unauthorized Tag Cloning: Copying tag data to additional tag to gain the similar privileges as original.

(c) Man-in-the-Middle (MIM) Attack: When an external tag object pretends to be either a tag or is a reader between actual tags and other readers.

(d) Unauthorized Tag Disabling: When an external reader disables a tag inappropriately thereby not allowing it to remain usable again.

(ii) RFID Privacy Issues: Within the context of an RFID-enabled facility, the concept of privacy issue is to unknowingly release critical information thereby deriving specific knowledge or may be tracking meaningless data. In the past, several methodologies are proposed to ensure maximum privacy of an individual, including the common approach like Encrypting/Rewriting and Hiding/Blocking Tags.

(iii) Categorizing RFID issues: The methods adopted for solving RFID issues are of three categories:

(a) Physical Approaches in which methods attempt to correct RFID anomalies by resting the environment around the scanners,

(b) Middleware Approaches where algorithms are correcting the anomalies at the time of capturing

(c) Deferred Approaches which attempt to correct RFID data at the time of storage in the Database are: (i) If there is increased likelihood that the missed objects will be found then Use Middleware or Deferred Solutions, (ii) If duplicate anomalies are generated when all tags are read then specific Software for the application can be used which can account for generated anomalies so that correction filter can be deployed on the edge itself, (iii) If additional cost or effort is required for user while purchasing extra tags, equipment or need more time to move the objects then there is no solution to this as Physical Approaches inherently demand additional labour for the user to correct the mistakes as opposed to Middleware or Deferred Approaches.

(D) Bluetooth (BT):

Bluetooth is a wireless technology standard that was invented by Ericsson in 1994. It is based on the IEEE 802.15.1 standard and is managed by the Bluetooth Special Interest Group (SIG). A Bluetooth Personal Area Network (PAN) is also called a piconet (very small network) that typically has a range of 10 meters. Wireless communication between a mobile phone and a remote headset. Wireless communication between a mobile phone and a Bluetooth car stereo system. Wireless communication with PC input and output devices, like mouse, keyboard and printer. GPS receivers, medical equipment, barcode scanners, and traffic control devices use Bluetooth. Bluetooth Extended (BLE) is the extended standard of BT.

(E) QR Code:

Quick Response (QR) Code is popularly used by mobile phones to scan the machine readable content. It is used in merchant payments. Bharat QR Code standard is to be used in India.

3.4 Long Range Mobile Device Communication Channels

(A) The long-range radio technologies of ISM radio band and GSM frequency band allows wireless communication over kilometers. The actual performance provided by the wireless communication technologies differ on several metrics such as range, data rate, energy consumption, delay etc. These metrics are dependent on deployment frequencies, modulations etc. and in the same environment setting these different signals will behave differently.

(B) Satellite Communication Service

(i) Satellite transmission resembles the operations of a line-of-sight microwave in which one of the stations is a satellite orbiting the earth in a geocentric or heliocentric way in low, medium or high altitude. A mobile phone having satellite antenna can access it. It is also useful in hilly and terrain areas where laying of conventional cellular infrastructure is costly and difficult to monitor. Since Drones are getting used which have either satellite connectivity and controlled by Mobile Phone or directly connected to mobile phone, the communication security is to be properly implemented.

(ii) Navigation System: The satellites have great role in the navigation services. Satellite Navigation is based on a global network of satellites which helps in locating the position by transmitting radio signals. The most familiar is the satellite navigation using Global Positioning System (GPS) satellites developed and operated by the United States. There are also other similar services such as GLONASS developed and operated by the Russian Federation, Galileo developed and operated by the European Union, BeiDou developed and operated by China and NavIC or Indian Regional Navigation Satellite System developed and operated by Indian Space Research Organization (ISRO), India. All these satellite navigation service providers follow the recommended practices guided by International Civil Aviation Organization (ICAO) Standards to support use of these constellations for aviation.

(iii) Global positioning system (GPS): GPS formally known as the Navstar Global Positioning System was developed for the military purposes in 1980 by US Department of Defense (DoD). GPS is still operated and maintained by DoD with the guidance of National Space-Based Positioning, Navigation and Timing (PNT) Executive Committee (EXCOM). It is a satellite navigation system that uses satellite signals to locate the position on earth. The 2D positioning of the device based on the longitude or latitude is identified accurately in around 3 to 15 meters distance. This technology works in all conditions and generally uses many satellites' signals for location identification. The accuracy of locating the device using this technology depends on the antenna quality, signals received and the spread of signals by the satellites in the sky. This technology is proven to be successful in many navigation and timing applications. As the GPS accessible equipment's are generally small and inexpensive, GPS is being used in a wide variety of applications across the globe.

(iv) Indian Regional Navigation Satellite System (IRNSS) or NavIC: IRNSS is an independent regional navigation satellite system being developed by India which can provide accurate position information service in India and in around 1500 kms around from its boundary. There are two types of services provided by NavIC to the general public and authorized users namely, Standard Positioning Service (SPS) and Restricted Service (RS). The navigation services of IRNSS provides position accuracy of better than 20 meters in the primary service area. If any foreign government or private player offers Satellite based Mobile Services or hybrid services with terrestrial communication in India, clearance should be obtained from GoI and MSG is to be strictly followed to protect the privacy of domestic mobile users.

(C) Cellular Communication Generations and Services

(i) Cellular communication (CC) is the most popular way to connect people together for real-time communication and data transmission. CC systems have an enormous number of users, and large amounts of data, including user- and system-oriented data, are generated in CC systems every day.

(ii) The globally accepted standard is Global system for mobile communication (GSM) is used for digital cellular communication and CDMA, which is operating at 900 MHz frequency. GSM uses various cryptographic algorithms for security such as A5/1 and A5/2 stream ciphers are ensuring over-the-air voice privacy. The A5/1 was first developed and stronger algorithm used in Europe and the United States; A5/2 is a weaker algorithm and is used in few countries across the world is to be upgraded.

(iii) Over 200 countries use GSM which has narrowband time division multiple access (TDMA) technology. The basic three frequencies in which GSM standard works are as follows:

(a) 900 MHz: It was used by the original GSM system.

(b) 1800 MHz: It was used to support the growing number of subscribers.

(c) 1900 MHz: It is mainly used in the US.

(iv) The wireless communication can provide high quality, reliable communication just like wired communication (optical fiber) and each new generation of services is a better solution in that direction. The analog to digital conversion is said to be the major transition part in the evolution of initial generations:

(a) 1G - First Generation: The 1G was introduced in 1987 by Telecom and used analog systems for its first cellular mobile phone network. The phones in this generation had generally poor battery life and voice quality also bad. These were introduced in the 1980s and continued until being replaced by 2G digital telecommunications. The maximum speed of 1G is 2.4 Kbps. The first generation (1G) cellular systems uses analog systems which introduced wireless communication (only voice telephony) but with larger handsets.

(b) 2G - Second Generation: The concept of Carrier Division Multiple Access (CDMA) and GSM was brought in this generation. The small data services like SMS and MMS was also introduced. 2G capabilities are achieved by allowing multiple users on a single channel via multiplexing. The 2G Cellular phones are used for data along with voice. The advances from 1G to 2G introduced many services that we use today, such as SMS, internal roaming, conference calls, call hold and billing based on services e.g. charges based on long distance calls and real time billing. The maximum speed of 2G cellular networks with General Packet Radio Service (GPRS) is 50 Kbps and similarly with Enhanced Data Rates for GSM Evolution (EDGE) is 1Kbps. In second generation (2G) standards such as GSM and CDMA One, the digital technology came in. The introduction of digital technology made the cell phones and network infrastructure cheaper enabling better network service levels and high end phones.

(c) 3G - Third Generation: The Universal Mobile Telecommunications System called UMTS as its core network architecture - This network combines aspects of the 2G network with some new technology and protocols to deliver a significantly faster data rate. Based on a set of standards used for mobile devices and mobile telecommunications use services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union. One of the requirements set by IMT-2000 was that speed should be at least 200Kbps to call it as 3G service.

(d) 4G - Fourth Generation: The MIMO (Multiple Input Multiple Output) and OFDM (Orthogonal Frequency Division Multiplexing) technology are the key players to make these services possible. LTE (Long Term Evolution) is a series of upgrades to existing UMTS technology and is Telstra's existing 1800MHz frequency band. The 4G network assures speed of 1000Mbps or 1Gbps when the device is stationary or walking, 300ms to less than 100ms is the latency expected and hence significantly reduces congestion. The fractional parts: 4.5G and 4.9G are marking the transition of LTE in different stages (in the stage called LTE-Advanced Pro) and by implementing more MIMO and D2D in IMT 2020 is the requirement for the 5G networks.

(e) 5G - Fifth Generation: The development of 5G standard by 3GPP is almost completed and many countries have started adopting the technology. In India 5G is getting rolled out in 2022 for public service. The 5G network is seen as the improvement on 4G. It promises to mobile users, higher data rates, more connection density, very low latency, among other improvements. The major features of 5G include device-to-device communication, better battery consumption, IoT connectivity, edge computing, and improved overall wireless coverage. The max speed of 5G is over 35 times faster than 4G. The key technologies Massive MIMO, Millimeter Wave Mobile Communications etc. are key players in 5G. Release 18 by 3GPP is the latest update in 2022.

(f) Beyond 5G – Sixth Generation (6G): The standardization work for 6G is in progress by TSDSI and 3GPP. Its standard on 6G Security is recommended to be followed in near future.

(D) Ad-Hoc Drone/Mobile Vehicular Communication Service:

The Vehicular Ad-hoc Networks (VANETs) application prototypes are now started their implementations for accident detection, driver assistance at road intersections and in traffic management. The safety of autonomous vehicles where road safety is the major concern is ensured with the inter-vehicle communication (IVC) and vehicle to road communication (VRC) Good. The introduction of flying ad-hoc networks has opened many opportunities and value-added services. The FANET inherit many features from the predecessor's mobile ad hoc networks (MANETs) and with vehicular ad hoc networks (VANETs).

(E) Data Service

(i) Short Message Service (SMS): It is a text messaging service component of most telephone, Internet, and mobile device systems. It is unencrypted message so app based encryption may be used to secure the SMS text.

(ii) Unstructured Supplementary Service Data (USSD): It is sometimes referred to as "quick codes" or "feature codes", is a communication protocol used by GSM cellular telephones to communicate with the mobile network operator's computers. USSD can be used for WAP browsing, prepaid call-back service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network. USSD messages are up to 182 alphanumeric characters long. USSD dealing codes are operator specific or PAN India based, for example, *123# for balance enquiry for an MNO and *99# for Mobile Payments across all MNOs in India.

(a) Unlike short message service (SMS) messages, USSD messages create a real-time connection during a USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS. When a user sends a message to the phone company network, it is received by a computer dedicated to USSD. The computer's response is sent back to the phone, generally in a basic format that can easily be seen on the phone display.

(b) Messages sent over USSD are not defined by any standardization body, so each network operator can implement whatever is most suitable for its customers. USSD can be used to provide independent calling services such as a call back service (to reduce phone charges while roaming), enhance mobile marketing capabilities or interactive data services.

(c) USSD is commonly used by prepaid GSM cellular phones to query the available balance. Here is no store-and-forward capability, as is typical of other short-message protocols like SMS. In other words, an SMSC is not present in the processing path.

(F) Voice Service:

The Internet Protocol (IP) telephony otherwise called as Voice over Internet Protocol (VoIP) is a solution that has group of technologies for voice delivery and multimedia sessions over IP networks, such as the Internet. The IP-based voice is over broadband or IP networks, whereas the VoIP virtual lines need associated telephone lines and are identified using a VoIP grade services. The evolution of voice and communication services for packet switched networks, LTE, Wi-Fi and 5G is the starting point of VoLTE.

(G) Multimedia Service:

The two or more media components such as voice, data, video, and image, combined in a single session delivered between two or more parties is called as multimedia services. It is classified as interactive or distribution services where the interaction of user defines the behavior of interactive services and broadcast-based services are defined as Distribution Services. Streaming content delivery as You Tube videos, Live Programmes through TV and Social Media sites, Live Classroom Web Meetings etc. are happening through the Mobile Phone. It should be ensured that the providers of digital content and the content itself is trustworthy and if found to be malicious, action should be quick to stop their services in India.

(H) GPRS: The packet oriented mobile data standard on the 2G and 3G cellular communication network's global system for mobile communications (GSM) is called General Packet Radio Service (GPRS). Third Generation Partnership Project (3GPP) maintains GPRS and is billed as per their usage in contrast to circuit switching data. The GPRS provides data rates of 56–114

Kbit/s in 2Gn.

3.5 Session Management

(A) Session management refers to the process of securely handling multiple requests to a web-based application or service from a single user or entity. Websites and browsers use HTTP to communicate, and a session is a series of HTTP requests and transactions initiated by the same user. Broken authentication and session management is consistently one of the OWASP Top 10 Web Application Security Risks, and a vulnerability that developers must continually guard against.

(B) Session management is used to facilitate secure interactions between a user and some service or application and applies to a sequence of requests and responses associated with that particular user.

(C) Session tokens serve to identify a user's session within the HTTP traffic being exchanged between the application and all of its users. HTTP traffic on its own is stateless, meaning each request is processed independently, even if they are related to the same session.

(D) Session fixation can also take place if the properties of a session token allow an attacker to fixate the token of the user once authenticated; it can then also be used to hijack the session.

(E) There are many aspects to enforcing proper session management; all best practices should be implemented for mitigating potential compromise. Refrain from sending sensitive traffic and tokens over an unencrypted channel (HTTP).

(F) New session tokens should be generated at every stage of a session; as soon as a user visits the application, when they provide correct credentials, and when a user logs out of their account.

(G) Session tokens should be reasonably long, unpredictable, and unique. These properties can help to ensure that an attacker cannot guess or get the token through brute force attack.

(H) When the Mobile User is travelling in a vehicle, train, ship, flight etc. the handoff in horizontal, terrestrial and vertical directions should be compatible as per the 3GPP standards of speed limits, which is 500 KM/Hour in 5G.

3.6 Checklist

SR.No	Checklist	Section
1	Mobile Communication Security	3.1
2	Mobile Communication Standards	3.2
3	Wi-Fi Security	3.33.3(A)
4	NFC Security	3.33.3(B)

SR.No	Checklist	Section
5	RFID Security	3.33.3(C)
6	Bluetooth Security	3.33.3(D)
7	NAVIC Satellite GPS	3.4(B)(iv)
8	5G and Beyond Security	3.4(C)(iv)(e)
9	QR Code	3.33.3(E)
10	Drone Security	3.4(D)
11	SMS	3.4(E)(i)
12	USSD	3.4(E)(ii)
13	Voice Service	3.4(F)
14	Multimedia Service	3.4(G)
15	Session Management	3.5

4. Mobile Service based Security and Control Measures

In this chapter, Security aspects of Mobile Services obtained through mobile browser, mobile applications and mobile cloud are presented. Light weight cryptography techniques and quantum safe cryptography techniques are prescribed for secure mobile services. Adoption of best practices of Secure Coding for Developers is prescribed.

4.1 Mobile Browser Security

(A) Mobile browser of a mobile device is an application service which helps to connect it to a website or web server for browsing, interacting, fetching pages, downloading and displaying multimedia web content to mobile user in user preferred language. Mobile browsers are to be regularly up gradated not only in terms of growing functionality but performance and security point of view as well. They need to efficiently manage the various multimedia objects efficiently in a mobile small screen, such as social networking and Internet music, video, Video channels and TV channels in a fully secure manner.

(B) Mobile Browser Security Challenges:

(i) Weak Operating system - that cannot check and identify the malware may allow it to run as a background process can cause the reading/modifying the browser memory space in privileged mode.

(ii) Man-in-the-Middle (MitM) Attacks - Browser components may be hacked using man- in-the middle attack

(iii) Weak Browser plugin can cause misbehaviour of browser and even could be hacked.

(iv) Weak cryptography of Browser may impact the network communications and could be intercepted outside by the attacker using best performing advance machine.

(v) Advanced Jailbreaking and Rooting Techniques.

(C) Cookie Security:

A cookie is a piece of software code that an internet web site sends to mobile browser to 99provide access information at that site. A cookie is stored as a simple text file on the mobile device by a website’s server and only that server will be able to retrieve or read the contents of that cookie. Cookies let one to navigate between pages efficiently as they store mobile user preferences to improve user experience of a website. If the cookies show abnormal behavior in terms of their functionality and security in the following categories then the website originating such cookies may be blacklisted from public use in India.

(i) Analytics cookies – They register the mobile device information to keep track of browsing patterns when user visits the website.

(ii) Service cookies – They remember user registration and their login details such as login details, payment cards profile, settings preferences, and keeping track of the pages visited.

(iii) Non-persistent cookies – They are known as Per-session cookies which provide seamless navigation. These are only available at the time of active browsing session and should not record the data permanently.

(D) Security Precautions from Mobile Browser Cookies

(i) Cookie services and their policy must be read carefully by the Mobile User while surfing and accessing any web page. Most of the threats are targeting via analytics cookies, it is recommended to block the third-party cookies for safe surfing.

(ii) Carefully set the Privacy setting in the browser.

(iii) Download browser from safe source such as Mobile application stores (Google play, Apple stores and Microsoft) and keep it updated.

(iv) Always use mobile phone recommended security and keep it updated.

(v) Be warned using unsafe link such as malicious Link, Phishing link and compromised link.

(vi) Several mobile security attacks happen through exploited mobile web browsers. To ensure the security, the browsers should implement: (a) delete all the traces of history as soon as mobile user closes the browser or exits the website in a session, (b) block third-party scripts and Ads, (c) do not allow trackers to keep user data, (iv) use a secure VPN, (v) mobile user should constantly update the mobile browser app and its secured APIs.

4.2 Mobile Cloud Services Security

(A) Mobile Users get various services such as mobile apps, software, data backup, authentication, crowd sourcing, public Wi-Fi service, block chain service etc. from cloud service providers. Based on frequently usage and experiences of cloud services, mobile cloud computing security is a major issue. Few major security challenges in mobile cloud computing are described and classified as below:

(B) Data Privacy and Security Challenges in Mobile Cloud Computing:

(i) Violation of privacy rights and Risk of data theft.

(ii) Various physical security challenges.

(iii) Encryption and decryption keys management.

(iv) Virtual Machines and its concerning Security and auditing issues.

(v) Lack of standard for data integrity and its assurance.

(vi) Lack of quality Services due to the different vendors for different requests.

(C) Security of Mobile Users Data in Cloud

(i) Protection of data on the mobile cloud from any attack is to be ensured. If the Cloud service providers are providing the services worldwide then for Mobile Users in India, they shall be needed to establish the cloud service mobile user data in servers located within India for data privacy and security including Database Security Management.

(ii) Focusing on mobile device security majorly contains two specific challenges, one is about end user data protection, either from cloud or from the device. Second is jailbreaking of device, every mobile phone has a particular operating system and specific restrictions are installed through the mobile manufacturer. Jailbreaking the mobile phone can bypass those restrictions and allow more customization but it opens up more security vulnerabilities. So, Jailbreaking should be avoided.

(iii) Protect mobile devices from Jailbreaking; Disable programming interface and make it harder for an attacker to obtain the firmware to update the device and tamper its identity including Operating System and Software Assets. Digitally signed firmware is to be implemented to restrict the attacker to load rogue Firmware.

(iv) Protection of data on the cloud from any attack: This is needed to focus. These clouds are providing the services worldwide from other than countryside location where the user exist. Therefore, that shall be needed to establish the cloud service within India geographical region for user data and their data privacy and establish the cloud services and servers with their security including Database Security Management.

(D) Cloud Service architecture and Delivery Models Issue:

(i) Structured query language related, application programming interface security challenges concerning to Platform as a Service (PaaS) model security.

(ii) Data security management, web application vulnerability and scanning challenges concerning to Software a Service (SaaS) model security.

(iii) Communication security, transport layer security, server configuration challenges concerning to Infrastructure as a Service (IaaS) model security

(E) Mobile Cloud Infrastructure challenges:

(i) Weak cloud infrastructure and its concern security.

(ii) Weak encryption algorithm implementation.

(iii) Weak X509 certificate and its implementation.

(iv) Unknown cloud provider with known challenges.

(F) Mobile Cloud Security

(i) Registration of cloud services shall be in India, Data centre and respective infrastructure must be followed as per the data protection laws and policy of India. It would be situated under geographical region in India in a secured and protected environment.

(ii) Certificate based authentication.

(iii) Cloud connectivity shall be based on X509 certificated. Cloud infrastructure shall have connectivity with Certificate Issuer of India (http://cca.gov.in). The device connected to cloud shall be authenticated based on issued certificate from India as in Figure 8.

(iv) The certificate shall be stored in secure element (UICC/eUICC/eSIM). The diagram in Figure 8 is explaining the concept

(v) OPEN Mobile API shall be mandatory in mobile devices/terminals for secure authentication and more security.

(vi) Virtual device Identity shall be Implemented to avoid supply chain ID, which is known and transparent and specifically targeted to get the access of devices. Please see Section 2.3(K) for the details.

(vii) Strong implementation of X509 certification for authentication service.

(G) OPEN Mobile API in Mobile Devices/Terminals:

For security concerns and Trusted services, it is recommended to be mandatorily to use Standard Open mobile API for the mobile vendors producing the connected devices in India. This can prevent the fraud related to Identity Theft and even SIM Swap fraud in financial services and OTP fraud.

(H) Secure Element or SIM (UICC/eUICC/eSIM) is a security enabler as a hardware security token should be used to communicate mobile terminals using Open Mobile API defined by Trusted Connectivity alliance and using specifications from Global Platform. This enables the enhanced security to the mobile devices to enable SIM or secure element for below secure use cases.

(i) Secure NFC services.

(ii) Vital in M2M & IoT where human intervention is very limited or absent.

(iii) The secure token issuer for TLS & secured application interfaces.

(iv) May also facilitate MNOs as a load balancer in case of seamless offloading to Wi-Fi through GBA/EAP with identity tokens.

(v) New guidelines on payment - avoiding card on file and new card Token-based transactions in payment. And mobile valet.

(vi) Ticketing services and public transport.

(vii) ID services and Access control.

(viii) Loyalty Services.

(ix) Security Features of the Block chain on a Secure Element, SIM (UICC/eUICC/eSIM).

4.3 Mobile Applications Security

(A) Mobile App or m-application services have become part of Mobile User's daily life. These are making our daily life easy and bringing transparency in system for any type of transaction, thereby enabling boundary less digital transactions across world. However, due to rouge Apps mobile users are becoming vulnerable for targeted attacks and frauds.

(B) Application Development:

Application development world brings innovations and promotes new Ideas for business and start-ups. Since unverified mobile applications or services could steal personal data from Mobile Device, it is important to register the App Developer as a legal entity in India with security certified premises and product, if the application is being targeted for the Indian Mobile Users. In Case of generic App target for global customer, user has to additionally agree with App store and App terms and condition on their risk.

(C) Pre-Installed Application:

Many mobile device manufactures provide some applications integrated with their Mobile Operating system; these applications are available as default applications with mobile phone. Some applications are automatically installed during mobile update with FOTA without the consent of mobile user. This is recommended that, Mobile phone manufactures shall provide basic applications which are helpful to mobile user for basic Calling, Messaging and basic multimedia operations depending on mobile phone type.

(D) On Demand Installed:

Mobile apps on demand by the mobile user should be installed from secured App store. The security of mobile application should be the responsibility of App store to do security test and put for public use. Registered user in app cloud can download the mobile Apps without any hesitation once with the notion that app store has taken care of security clearance before it is made available for use.

(E) Apps for Pre-installed and on-Demands

(i) Mobile phone security shall not allow to download unregistered and non-verified third-party Apps in mobile phone.

(ii) Developer mode option should only be available on engineering sample phones only. Engineering sample phones shall be made available based on special request to the phone manufacturer.

(iii) No Pre-Install Application shall be installed without end-user consent, even if, when very first-time phone is being configured. User consent is also applicable (installing apps) while pushing FOTA update in phone e.g. for security or new OS patched by Mobile manufacturer.

(iv) App store should be registered in India, as a legal entity with appointment of nodal officer and grievance management facility.

(v) This would be the App store responsibility to check the security and venerability of App and verify the legal credentials of App developer with his App practice statements.

(vi) App Store has to follow IT act 2000 and all its latest amendments for ensuring security and privacy of mobile users.

4.4 Cryptography – Light weight and Quantum Safe Methods

(A) Cryptography plays important role in securing the user's data - even more so in a mobile environment, where attackers having physical access to the user's device is a likely scenario. Cryptography Techniques such as encryption/decryption, signature generation, symmetric key generation, hash etc. should be foolproof with security certified APIs. This section provides an outline of cryptographic concepts and best practices relevant to mobile devices and apps. These best practices are independent of the mobile operating system.

(i) Cryptography Key Length: Even the most secure encryption algorithm becomes vulnerable to brute-force attacks when that algorithm uses an insufficient key size. Cryptography key length fulfils accepted industry standards

(ii) Symmetric Encryption with Hard-Coded Cryptographic Keys The security of symmetric encryption and keyed hashes (Message Authentication Codes (MACs) depends on the secrecy of the key. Secret keys must be stored in secure device storage whenever symmetric cryptography is used in mobile apps. Secret keys must not be stored in the same place as the encrypted data.

(iii) Weak Key Generation Functions: Ensure that passwords aren't directly passed into an encryption function. Instead, the user-supplied password should be passed into a Key Derivation Function (KDF) to create a cryptographic key. Choose an appropriate iteration count when using password derivation functions.

(iv) Weak Random Number Generators: It is fundamentally impossible to produce truly random numbers on any deterministic device. Pseudo-random number generators (RNG) compensate for this by producing a stream of pseudo-random numbers. Cryptographically secure RNGs generate random numbers that pass statistical randomness tests and are resilient against prediction attacks (e.g. it is statistically infeasible to predict the next number produced). Mobile devices should offer standard implementations of RNG algorithms that produce numbers with sufficient artificial randomness.

(v) Custom Implementations of Cryptography: Using proprietary cryptographic functions for mobile devices may be avoided as the functions are not validated properly. Instead, publicly known standard security algorithms that are widely regarded can be used. Mobile operating systems offer standard cryptographic APIs that implement those algorithms. At all implementations of cryptography, the following procedures must be ensured:

(a) Round keys (like intermediary/derived keys in AES/DES/Rijndael) are properly removed from memory after consumption to prevent cache memory timing side channel attack.

(b) The inner state of a cipher should be removed from memory as soon as possible.

(vi) Weak Block Cipher Mode of operation: Cipher Block Chaining (CBC) mode is recommended instead of Electronic Code Book (ECB). This ensures that each encrypted block is unique and randomized even if blocks contain the same information. When storing encrypted data, it is recommended to use a block mode that also protects the integrity of the stored data, such as Galois/Counter Mode (GCM). The latter has the additional benefit that the algorithm is mandatory for each TLS v1.2 implementations, and thus is available on all modern platforms. NIST guidelines on block mode selection and ECC may be referred for details.

(vii) Predictable Initialization Vector: CBC, OFB, CFB, PCBC modes of operation require an initialization vector (IV) as an initial input to the cipher. The IV doesn't have to be kept secret, but it shouldn't be predictable. Make sure that IVs are generated using a cryptographically secure random number generator. For more information on IVs, see Crypto Fail's initialization vectors article.

(viii) Protecting Keys in Memory: When memory dumping is part of the threat model, then keys can be accessed the moment they are actively used. Memory dumping either requires root-access (e.g. a rooted device or jailbroken device) or it requires a patched application with Frida. Therefore, it is best to consider the following, if keys are still needed at the device:

(a) Make sure that all cryptographic actions and the keys itself remain in the Trusted Execution Environment (e.g. use Android Keystore) or Secure Enclave (e.g. use the Keychain and when signing, use ECDHE).

(b) Always zero out keys before the memory is released, whether using native code or not. This means overwrites the memory structure (e.g. nullify the array) and know that most of the Immutable types in Android (such as Big Integer and String) stay in the heap.

(ix) Protecting keys in Transport: When keys need to be transported from one device to another, or from the app to a backend, make sure that proper key protection is in place, by means of a transport key pair or another mechanism. Often, keys are shared with obfuscation methods which can be easily reversed. Instead, make sure asymmetric cryptography or wrapping keys are used.

(x) Side Channel Attack Resistance: Implementation of cryptography functions must resist the side channel attack such as cache memory timing attack, power and EM analysis attack. Evaluation style testing (Test Vector Leakage Assessment) is used to evaluate the side channel leakage in cryptography implementation.

(xi) Cryptographic policy: When high-risk applications are created, it can often be a good practice to have a cryptographic policy, based on frameworks such as NIST Recommendation for Key Management. When basic errors are found in the application of cryptography, it can be a good starting point for setting up lessons learned/cryptographic key management policy.

4.5 Secure Coding Practices

(A) Mobile application development security vulnerabilities are similar to web applications, from the perspective that are exposed on the Internet. Mobile applications that are installed in user devices are entry points to the device network.

(B) Building Security in Mobile App development

To improve Android apps security and overall performance follow Googles guidelines for application development. Use the best practices of development environment.

(C) Reviewing source code

Source code review can detect a broad range of security issues, including those mentioned in this document. Android strongly encourages both manual and automated source code review.

(D) Ensure the security at the backend service, the platform service and APIs

Almost every mobile application interacts with a backend server by using web services or protocols. If the applications are implemented with using backend services, platform services, APIs, and if they are not hardened, it gives an opportunity to mobile attackers to steal the sensitive information on the mobile device when sending data to the backend service.

(E) Use implicit intents and non-exported content providers

An implicit intent interaction allows users to send sensitive information from one app to another app that they trust.

(F) Apply signature-based permissions

If data is shared between two apps it can be controlled by using *signature-based* permissions. These permissions don't require any confirmation from the user. If both apps are signed with the same signing key then those apps can share the data including sensitive information.

(G) Use the network security measures in the implementation

(i) Use SSL while communication.

(ii) Modify or add a network security configuration file.

(iii) If the application is implemented by using new or customized CAs, a developer can declare the network's security settings in a configuration file. This implementation allows creating the configuration without modifying an app’s source code.

(H) Ensure that runtime code is interpreted correctly

If the runtime interpretation of code is not handled properly then there is a chance for the attacker to get the sensitive data from the user’s device. It can lead to the injection of infected code leading to memory leakage, surveillance and spyware.

(I) Verify the device and application integrity

Modified devices (rooted or flashed with customized OS images) and/or applications undermine the security and privacy controls implemented in the mobile application. If a mobile application is modified, then the applications cannot be trusted and the behaviour also can change completely.

(J) Provide the right & relevant permissions.

(K) Share data securely across apps.

(L) When sharing data, implement it by using content providers. Do not use the "file://" URIs anywhere in the source code.

(M) Store data safely

(i) Store only non-sensitive data in the cache file.

(ii) Use Shared Preferences in private mode.

(N) Secure the application from client-side injections.

(O) Update all app dependencies.

(P) Handle the biometric sensors and secure hardware properly.

4.6 Checklist

SR.No	Checklist	Section
1	Mobile Browser Security	4.1
2	Cookie security	4.1(C)
3	Mobile Cloud Service Security	4.2
4	Secure Element	4.2 (H)
5	Mobile Application Security	4.3
6	Light Weight Cryptography	4.4
7	Secure Coding Practices	4.5

5. Mobile Device Security Testing, App Vetting and Device Forensics

Mobile Security Testing is necessary to gain the confidence that the mobile device, Firmware, OS, mobile communication and mobile apps within the mobile device are able to counter the various threats and vulnerabilities highlighted in MSG. An organization needs to test/assess/vet the mobile device security. There are various mobile security testing standards available which are followed by the industry. Further an organization is required to define its security requirements and set up an organizational structure to take up the task of assessing/vetting the security of the device and associated software. Another aspect i.e. Mobile forensics is also important to collect/recover evidence from Mobile Device in case of a cyber-crime. Finally, Cryptanalysis is an important aspect and its implementation must be assessed for security assurance. These mobile security aspects are given in the subsequent sections of this chapter.

5.1 Standards

Some standards listed below contain provisions as part of MSG, which are subject to revision, and parties to agreement based on this standard are encouraged applying the latest versions of the standards listed as follows:

(i) Mobile Device Security Standard (Part-1 to 4), BIS, Dec 2021

(ii) OWASP Top 10 Mobile Security Risks

(iii) OWASP MASVS, Version 1.1

(iv) CIS Benchmarks (Android and iOS)

(v) SANS Mobile Device Checklist

(vi) NIST SP 800- 163r1 (2019): Vetting the Security of Mobile Applications

5.2 Security Requirement Specification

(A) An organization is required to define the security requirements for mobile device technology stack that needs to be complied before approval for its usage by the organization or its customer/public. The following security requirements should be fulfilled by organizations.

(B) General Security Requirements

General security requirements define the characteristics of a mobile device technology stack that should or should not be present in order to ensure the mobile security. These requirements are considered “general” since they can be applied across all mobile devices and tailored to meet the security needs and risk tolerance of an organization. General app security requirements may be derived from a number of available standards, best practices, and resources including those specified by BIS, NIST, NIAP, OWASP, CIS and SANS.

(C) Organization-specific security requirements

Organization-specific security requirements define the policies, regulations and guidance that an organization must follow to ensure the security posture of the organization. Examples include banning social media apps from installation on the organization’s mobile devices and restricting installation the security posture of mobile apps. Such factors can be derived by considering the criteria as shown in Table below. of apps developed by specific vendors. Organizations shall install Mobile Device Management (MDM) policy on mobile devices for enterprise use and can control access and authentication/authorization. To help develop organization-specific or sector specific security requirements, it is helpful to identify non-vulnerability related factors that can impact.

Criterion	Description
Policies	● Security ● Privacy ● Social Media ● Applicable regulations ● Usage
Ownership	● developer ● developer’s organization, ● developer’s reputation,
Data Sensitivity	● Data at rest ● Data in transit.
OS	Type of OS used and their hardening related requirements
Firmware	OTA updation and Integrity check
Documentation	Device, testing, OS and App related documentation

Table 1:Organization-specific security requirements

5.3 Administrative Structure for Security Testing and Vetting

(A) An organization or Security Testing Lab undertaking the mobile device security testing and app vetting needs to have following category of personnel: Administrator, Test Engineer, Test Managers, Quality Assurance (QA) Manager/QA Engineer. Typically, a Testing/vetting organization should have 1 administrator, 1 Test Manager, 1 QA Manager, at least 2 Test Engineers and 2 QA Engineers and some Lab Technicians.

(B) Administrator: Administrator will receive the mobile device or mobile app along with documentation for vetting from OEM/OEM representative/mobile app developer/service provider. The job will be assigned to the test manager/engineer. then test engineers will take up the activity of mobile device security vetting using dynamic testing tools, static testing tools, documentation review, witnessing the test/demonstration by OEM/mobile app developer/service provider and prepare a draft report.

(C) Test Manager/Test Engineer: The test manager will coordinate the test engineer's activity and review the report generated by the test engineer. After review, if everything is fine, it will be sent to QA professional for approval or sent back to the test engineer for rework. Otherwise, it will be forwarded to QA professional for approval.

(D) Quality Assurance Manager/QA Engineer: The QA person will perform the quality checks with respect to the standards and methodology followed and tools used and provided to release the report. If there is clarification required from the testing team, the report will be sent back to the test manager. The test manager upon the receipt of satisfactory clarification from the testing team (test manager/test Engineer), the report will be approved by QA. After approval, the QA will send a report to the administrator to release. Then finally, the administrator releases the report.

5.4 Mobile Forensics Methodology and Tools

(A) Mobile forensics is an emerging field under digital forensics, which is generally handled by cyber forensic community and investigating agencies. Mobile forensics deals with scientifically extracting and analysis of the evidential data stored in the internal memory of the mobile device. It presents a challenging problem to the cyber forensic experts due to its fast/continuous technology development and upgradation of its security features at regular intervals.

(B) Today's smartphones have become the new fingerprints of evidence as it contains all kinds of heterogeneous data generated by the various types of applications, software and hardware embedded in the mobile device. Proper Categorizing/Correlation of the data with reference to the incident type will provides a lead to the investigating agencies in solving the cases. The vital information that could be extracted from the mobile devices are

(i) Call logs (Incoming, outgoing, missed call history)

(ii) Contacts List

(iii) Text messages,

(iv) Images, videos, and audio (voice records) files

(v) Internet browsing history, content, cookies, search history, analytics information

(vi) To-do lists, notes, calendar entries, ringtones

(vii) Documents, spreadsheets, presentation files, PDFs and other user-created data

(viii) Passwords, passcodes, swipe codes, user account credentials depending upon the type of extraction

(ix) Historical geolocation data, cell phone tower related location data, Wi-Fi connection info

(x) List of installed apps and their Data

(xi) System files, usage logs, error messages

(xii) Deleted data from all of the above depending on the type of extraction.

(C) Using forensic tools and manual exploration we may use the following for the extraction of data:

(i) Manual Extraction

(ii) Logical Extraction

(iii) Hex Dump

(iv) JTAG

(v) Chip-Off

(vi) Micro Read

(D) Forensic tools designed to acquire the data from the internal memory of the mobile phones and SIM cards in a forensically sound manner by way of providing the hash values for the data acquired. An informative list of Forensic tools for mobile devices is given in Annexure K.

5.5 Cryptanalysis

Cryptographic controls are very important regarding the protection of mobile security.

(A) For Device level and Communication level security the following Cryptographic Security controls are required to be assessed by the testing organization:

Security Characteristics	Security Controls Requirements	Inputs Required	Assessment & Evaluation Checkpoints
Data Protection	Protected Storage (Device Encryption)	It is required to test what type of encryption is used by device and its details along with certification, if any	Testing team is required to check what type of encryption is used by the device and whether it is adequate and certified as per FIPS 140-2, ISO/IEC 19790 :2006 Test Engineer has to verify that the data in storage on device is actually encrypted – manufacturer to demonstrate. OEM is required to provide the certification, documentation and demonstration.
	Protected Communications (VPN - Virtual Private Network)	Details of protecting information	Check the cryptographic controls used. Verify that the same has been implemented & it is effective - manufacturer to demonstrate.
	Data Protection in Process (Encrypted Memory)	Details of encrypted memory used in the device	Check mechanism used for encrypted memory. Verify that the same has been implemented & it is effective – Manufacturer to demonstrate.

Table 2:Device Level Cryptographic Security controls

(B) Application Level: The mobile application vetting is required to be done against the OWASP MASVS. The following three requirements are pertaining to Cryptanalysis.

(i) V2 Data storage and privacy requirement

(ii) V3 Cryptography requirement

(iii) V5 Network communication requirement

OEM will be required to provide the certification, documentation and demonstration. Further, Static testing (code review) will be required to verify the implementation of crypto control.

5.6 Static Testing

The testing team is required to carry out code review for verifying the implementation of security controls and detection of vulnerabilities. Static Testing can be done manually where test engineer can independently review the source code or OEM may provide walkthrough. There are many automated tools available for static testing. The testing team may first use the authentic automated tools to detect the vulnerabilities followed by manual code review/walkthrough.

5.7 Dynamic Testing

This is a black box testing technique in which the mobile application is executed using automated tools and vulnerabilities are detected. The dynamic testing can be done manually also by using proxy tools for different set of inputs. Proper care is to be taken if production servers of an organization are connected for dynamic testing instead of lab or simulated environment.

5.8 Testing Tools

There are some proprietary and large number of open-source tools available for doing static and dynamic testing. The informative list of testing tools is given in the Annexure J.

5.9 Mobile Device Security Vetting-Approach & Methodology

The assessment and evaluation of the security requirements are described below. Assessment can be done using automated tool testing, manual testing, code review (manual and automated), demonstration and verification of documentation.

(A) Assessment & Evaluation - Inputs Required

The following documentation shall be provided by the device manufacturer:

(i) Device details (providing Make, Model, Serial Number, operating system, Mobile Pre- installed Applications, Location of manufacturing, etc.) submitted for assessment and evaluation.

(ii) Mobile device detailed specifications with capabilities & features.

(iii) Factory set mobile device with default configuration for India along with configuration settings details

(iv) Security Architecture document covering security design details.

(v) Security Policies and Practices used for the mobile device.

(vi) Implementation details of the security controls identified in Table 2

(vii) Details of components used with part numbers along with sources of supply.

(viii) Internal test reports of the mobile device.

(ix) Third party Test/Audit Reports and Certifications obtained for the mobile device.

(x) Any other document(s) that will provide more insight over the implementation of security.

(B) It is expected that the security documentation will specify the implementations required by the Standard. Documentation can be provided in three ways. First option is to provide full comprehensive document explaining the controls completely. Second option is to provide the limited documentation sufficient to provide confidence to the Evaluator regarding the implementation. Third option is to visit the vendor/developer/manufacturer's premises and show the documents pertaining to the controls so that the team of Evaluators gains confidence in the implementation of security controls.

(C) If a mobile device submitted for evaluation comprises of the hardware that has been part of an already certified device of the same mobile device manufacturer and the certification is still valid then assessment of hardware may not be required. In this case, only OS and preinstalled mobile apps need to be assessed.

(D) Mobile Operating System Security Requirements Verification (Device & Communication level):

A new mobile device comes with operating system having default configuration setting. In order to make it secure, the default operating system setting needs to be configured with secure settings before use. The security of the mobile operating system shall be verified by checking its configuration settings using a checklist with focus on security configuration issues that are unique to the mobile platform. The checklist shall be based on the following security principles:

(i) Data at Rest & Data in Transit protection

(ii) Access Control

(iii) Application updates

(iv) Integrity violation checking

(v) Security updates

(vi) Verified boot mechanism

(E) A checklist covering above security principles or following checklists may be used:

(i) Mobile Device Security Standard of BIS, Dec.2021

(ii) SANS checklist,

(iii) CIS checklist for Android

(iv) CIS checklist for iOS

5.10 Guidelines for Mobile Security Testing

(A) Mobile Device Level Security

Any device security implementation can be addressed based on the Confidentiality, integrity and availability model. For achieving these goals the hardware-based security foundations in the SoC are extremely important. Such security aspects involve features like secure boot, storage security and key provisioning and hardware crypto.

(i) Secure boot

(a) Secure boot is defined as a boot sequence in which each software image to be executed is authenticated by software that was previously verified. It guarantees the integrity of the device.

(b) One Time Programmable (OTP) Fuse

(i) To protect the mobile device from hacking and tampering, a feature called One Time Programmable (OTP) fuse is implemented in the SoC. Other uses of the OTP fuse include anti-rollback. Secure debug fuses are used to disable the debug capability on commercial phones to prevent invasive debug and unauthorized code tracing and sniffing attacks. (As shown in Figure 9)

(ii) Encryption: Depending on the applications the SoCs need to provide the Encryption mechanisms. The encryption can be for full disk or File-based encryption.

(a) Key material may be bound to the secure hardware (e.g., Trusted Execution Environment (TEE), Secure Element (SE) of the device. When this feature is enabled for a key, its key material is never exposed outside of secure hardware. (As Shown in Figure 10)

(B) Mobile Communication Level Security

Evaluation of the identified security controls are to be taken up by the Testing organization. The vetting process may use the following techniques/combination of techniques:

(i) Document Verification

(ii) Design walkthrough

(iii) Code Review (Automated, Manual)

(iv) Code Walkthrough

(v) Dynamic Testing (Automated, Manual)

(C) Mobile Application-Level Security

(i) All critical applications of national importance need to be certified by the Government. It is important to have mechanisms such that all critical applications of national importance must undergo common certifying authority. Implementation of common certifying authority will help in multiple ways in reducing the

(a) Fake applications to genuine Government applications

(b) Enhances the capability to the user to filter apps based on common signature

(c) Special certificates issued by the government will help in creating a special badge for the government applications

(ii) The agent specific to the Indian context may be installed for verifying the authenticity of applications installed on the device.

(iii) The government authorized agent must be tightly coupled with all OEMs. The tight integration of agents will help in distinguishing the genuine Government application from total installed applications on the device [See in Figure *11*].

(iv) Applications of national importance need to be installed and executed in a trusted environment on the mobile device

(v) Security of stock applications need to be assessed thoroughly before being installed on the mobile devices

(vi) Secure update and OTA

Software updates play an important role in overall Mobile Device Security. Mobile devices can receive and install over-the-air (OTA) updates to system and application software. It is always good practice to have every OEM adhere to

(a) Review based analysis of the product (i.e. apps, platform)

(b) Comprehensive security response process

(c) Frequent update cycles

(vii) Application-level permissions: Android categorizes permissions into different categories viz. install-time permissions, runtime permissions, and special permissions. (As shown in Figure 12)

The Android Manifest is the main source of information for Application-level permissions, so deep analysis of manifest is essential. The over usage of permissions plays a major role in compromising overall mobile device security.

SR.No	Type of Permission	Description	Requirement/Utility	Whether these permissions are actually utilized
1	ACCESS NETWORK STATE	Allow applications to access information about networks	Used by the App to determine if a user is connected to the internet or not. According, login/playing options are provided on the game launch.	YES

Table 3:Application permissions acknowledgement

When the user requests access to a particular resource, the application should request only the permissions that it needs [As shown in Figure 12]. When developers make a request to access a particular resource, users need to be well informed on the need to access that particular resource as part of the functionality of the application.

(viii) Social Media applications

The following is a list of best practices that users need to follow to keep their personal information safe.

(a) Avoid clicking on malicious/suspicious links or attachments
(b) Use strong and secure passwords
(c) Keep one's identity safe & secure
(d) Backup the data at regular intervals
(e) Keep the Anti-Virus solutions up to date
(f) Keep all operating system and applications up to date
(g) Verify the security of the website is used

5.11 Checklist

SR.No	Checklist	Section
1	Mobile Security Standards	5.1
2	Organization structure of Security Testing Labs	5.3
3	Mobile Forensics	5.4
4	Cryptanalysis	5.5
5	Mobile Security Vetting Process	5.9
6	OTP	5.10(A)(i)(b)

6. Checklist of Guidelines for Various Entities

The prescribed Mobile Security Guidelines (MSG) are for all the entities of the mobile ecosystem because ensuring security is everyone's responsibility like cleanliness for an orderly society. They are prescribed along with brief explanation for clear and overall understanding of the security challenges, threats, vulnerabilities and security control measures in the respective chapters of Mobile based Security control measures, Mobile communication-based security control measures, Mobile services-based control measures, Mobile Security Testing, and App Vetting. The mobile ecosystem entities are of nine broad categories, namely, (1) Manufacturers (M), (2) Developers (D), (3) Service Providers (S), (4) Network Providers (N), (5) Testers (T), (6) Regulators (R), (7) Academic Researchers (A), (8) Mobile Users (U) and (9) Others (O). Here, the checklist of the guidelines to be followed by respective entities are given for quick reference. However, it is advisable for each category of entities to refer to the respective chapters of the MSG for details and adopt the latest standards and guidelines that may be published by the organizations listed in the references given in the MSG.

6.1 Checklist for Manufacturers (M)

The Manufacturers of Mobile Device, Hardware Components, Peripheral Equipment and Interfaces etc. should follow these guidelines:

(A) Identify the security areas to be focused as given in the Mobile Device Features and Sections of Section 1.1.

(B) Adhere to the safety requirements of Mobile Phones during manufacturing. [Ref: IS-16333, Part-1, BIS, 2021]

(C) Assess the Mobile Device Security Level given in Section 1.3.

(D) Identify the Security Risks, Threats and Vulnerabilities of Mobile Device to focus as given in Sections 1.4, 1.5 and 1.6.

(E) Evaluate as to how the various security goals given in Section 1.7 are to be fulfilled through Security by Design of the Mobile Device.

(F) Evaluate how the Mobile Device complies to the Data and Privacy protection requirements of Mobile User as given in Section 1.8.

(G) Follow the Mobile Device based Security and Control measures as given in Chapter 2.

(H) Follow the Mobile Device Security Capability Framework which stipulates the requirements for the security capability of the smart mobile device in its hardware, operating system, peripheral interfaces, application software, and user data protection as given in Section 2.1.

(I) Ensure to satisfy the security measures at various layers in the Mobile Operating System

(OS) stack such as application-level Security to protect app and user data. System and Operating System/Kernel level security, Device Encryption, Trusted Execution Environment (TEE), Secure Key Management, Firmware update etc. as given in the Section 2.2.

(J) As SIM is a potential target of attack, SIM applications are to be personalized in SIM and in the factory in a secure manner. SIM/eSIM security guidelines as given in Section 2.3 are to be followed.

(K) Mobile Device Security attacks from kernel, mobile browser, library functions, API calls etc. have to be strictly mitigated as given in Section 2.4.

(L) Security requirements are broadly classified into two categories (i) General Security Requirements applicable to all mobile devices and (ii) Organization-Specific Security Requirements are specific to the organization's policies, regulations, and guidance. This security aspect is part of the device security of mobile devices. for details see Section 5.2.

(M) Follow Checklist Section 2.7.on security of Technical Components.

6.2 Checklist for Developers (D)

The Developers of Mobile Software Services, Applications, APIs, Operating System, Browser, Functionality etc. should follow these guidelines:

(A) Identify the security areas to be focused as given in the Mobile Device Features and Sections of Section 1.1.

(B) Assess the Security Level of (i) Developer as given in Section 1.2(C)(i) and (ii) Developed Application as given in Section 1.3(B)(i).

(C) Evaluate as to how the various security goals given in Section 1.7 are achieved in the developed Mobile Software and Application.

(D) Ensure the Security of mobile device software in terms of OS, kernel, mobile browser, library functions, APIs used, database, SIM OS, Interfaces etc. as given in Section 2.5.

(E) The Mobile OS and framework should ensure proper security measures at various layers in the stack such as application-level Security to protect app and user data. System and Operating System/Kernel level security, Device Encryption, Trusted Execution Environment (TEE), Secure Key Management, Firmware update etc. as given in Section 2.2. Ensure proper Access Control Model implementation in Mobile OS.

(F) The mobile Browser has various security challenges such as Weak Operating system/plugin, Man-in-the-Middle (MitM) Attacks, Weak cryptography of Browser, Advanced Jailbreaking and Rooting Techniques, which can be seen in Section 4.2.

(G) Mobile Application service has become integral part of daily life to get services as per demand of the mobile user. Ensure that mobile users are not becoming vulnerable to targeted attacks and fraud due to rouge Apps. See Section 4.3.

(H) Follow Mobile Application Security testing and vetting as given in 5.9.

(I) Cryptography plays an important role in securing the mobile user's data. Techniques such as encryption/decryption, signature generation, symmetric key generation, hash etc. should be fool proof with security certified APIs. For energy constrained devices as mobile phones, light weight cryptography protocols are suitable for implementation, which can be seen in NIST standard and Section 4.4

(J) Best Secure coding practices should be followed in mobile application development to protect from vulnerabilities. See Section 4.5.

(K) Security by Design and Secure Software Development Life Cycle (S-SDLC) is the suggested approach, which need to be strictly followed.

(L) Unified Modelling Language (UML) is to be followed for Software and Mobile Applications design and development. The design diagrams are to be presented if required for security testing and certification.

(M) Implement Mobile Cloud Services security as given in Section 4.2.

6.3 Checklist for Service Providers (S)

The Providers of Mobile Software and Services such as Government, Public and Private Organizations providing Mobile Governance Services; Mobile Applications, Social Media Application, Mobile App Stores and APIs of Mobile Services etc. should follow these guidelines:

(A) Check how the various security goals given in Section 1.7 are achieved in the Mobile Software and Applications provided. Trust and Reliability of the provider should not be compromised even if the services are from outsourced organizations.

(B) Ensure that the Security Testing and Vetting of the Mobile Applications or Services have been properly done and they are certified by authorized organizations. Every new version, updates and patches should have security clearance certificate.

(C) For security concerns and Trusted services, it is recommended to use Standard Open mobile API for the mobile vendors producing the connected devices in India. Secure Element or SIM (UICC/eUICC/eSIM) should be used to communicate with mobile terminals using Open Mobile API defined by Trusted Connectivity alliance and using specifications from Global Platform. The details are given in Chapter 5. The chapter also recommends certain methods of storing the data in a secured way using cryptography. Chapter 6 gives the way of verifying the security controls and checking for security compliances.

(D) Use secured keys and PKI for data communication. Various vulnerabilities and the control measures during the data transit using cryptographic techniques are given in Chapter 5.

(E) Ensure that the mobile software and services provided are free from any security vulnerabilities; they are certified as tested and updated periodically. Highest care on Mobile Browser, Mobile Cloud Services, and mobile Applications of Preinstalled Apps and on demand Apps should be taken to ensure they are free from any security vulnerability as given in Chapter 4.

(F) Ensure that the digital certificate of the developer of mobile apps or services is valid and verified as authentic.

(G) Ensure the Security of mobile device software in terms of OS, kernel, mobile browser, library functions, APIs used, database, SIM OS, Interfaces etc. as given in Section 2.5.

(H) Ensure that the mobile services provide better user experience and protect privacy of Mobile user as given in Section 1.8.

(I) Ensure that the APIs and libraries used in the services or mobile applications are security tested and standardized.

(J) Do periodically monitoring and if any services or mobile apps with similar name are found to be provided by other agencies or websites as duplicate or fake apps, then report and lodge compliant.

(K) Ensure maintaining Quality of service (QoS) to the Mobile Users in terms of voice, data, multimedia and real time interactive sessions without compromising on security.

(L) Mobile Cloud Service provider should ensure that the mobile users data storage is in India and privacy norms are compliant to the regulations as given in Section 4.2.

6.4 Checklist for Network Operators (N)

The Mobile Network Operators, Tele Communication and Network providers, Cloud Infrastructure Providers, WIFI Providers, Internet Service Providers and Integrators should follow these guidelines:

(A) This entity is responsible for providing end-to-end security of mobile communication. See Chapter 3, Section 1.5 and 1.6 of Chapter 2, and Chapter 5 for the security vulnerabilities at these layers and the controls to mitigate them.

(B) Follow the security standards of wireless communication and Mobile communication security channels. See Section 3.1.

(C) Mobile device can communicate wirelessly within a short-range using wireless communication modes of NFC, Wi-Fi, RFID and Bluetooth etc. Ensure that no interception or no man in the middle type of attack is possible. See Section 3.2.

(D) The emergence of long-range radio technologies allows wireless communication over kilometers. The use of Wi-Fi, the latest Wireless radio technologies has enabled inter-device communications. The last decade has seen many new wireless technologies and devices. These devices use unlicensed industrial, Scientific and Medical radio bands, Global System for Mobile communication frequency bands etc. See Section 3.3. and ensure efficient communication with security.

(E) Session management refers to the process of securely handling multiple requests to a web-based application or service from a single user or entity. The details are given in Section 3.4.

(F) Mobile cloud computing lets the mobile user store their data remotely and access the applications. The primary security challenges in mobile cloud services described in Section 5.2. are to be properly handled.

(G) Mobile Application service has become integral part of our daily life bringing convenience and transparency in system for any type of transaction. As mobile users are becoming vulnerable to targeted attacks and fraud due to rouge mobile apps, ensure to deploy network and edge intelligence to eliminate them and alerting fraudulent transactions. See the details as given in Section 5.1.

(H) Cryptography plays an important role in securing the user's data - especially in a mobile environment. Techniques such as encryption/decryption, signature generation, symmetric key generation, hash etc. should be foolproof with security certified APIs and standard techniques are used in secure mobile communication.

(I) Follow secure coding practices for mobile communication services an interfaces as given in Section 5.3.

(J) Use WPA3 Standards on edge from where last mile connectivity is provided.

(K) For secure element interface on NFC, adopt ISO/IEC 7816 APDU Smartcard interface.

(L) Implement robust intrusion detection system for unknown devices or cloned SIMs to alert Telecom service providers or MNO.

(M) Having an internet service provider with faulty security can largely create a dent in the data and service delivery. Therefore, it is important to have a secure network.

(N) Check the compliance to the wireless network standard and follow the guidelines and policies established by telecom regulatory bodies given in Section 3.2.

(O) Ensure that requests of HTTPS only are allowed to enforce session security for critical transactions.

(P) The recommended security software, hardware settings, patches, and protocols used to render services in the network should be implemented and used.

(Q) Follow the policies and procedures along with national, state, and local cyber laws pertaining to the security of sensitive and confidential data exchanged in the networks.

(R) The wireless network interface adapters should be installed according to published instructions.

(S) When using wireless network interface adapters support and troubleshoot problems not supported by the provider.

(T) Report the known misuse or abuse of network or associated equipment to the IT Help Desk or TRAI/DoT.

(U) Implement Security Operations Centre (SOC) for Network Security Management. Designate a Certified Information Security Officer (CISO) to lead the SOC.

6.5 Checklist for Security Testers (T)

The Mobile Security Testing Organizations/Labs, Mobile Forensics Organizations, Quality Assurance and Assessment Bodies should follow these guidelines:

(A) Follow the guidelines defined for organization/tester/developers/QA to test/assess/vet mobile device security and various standards suggested.

(B) Cryptanalysis is an important aspect for security assurance. See Section 5 and list of Standards on Mobile security given in Section 5.1.

(C) The security requirements for the mobile device technology stack need to be complied with before approval for its usage by the organization. The organizations should develop (A) General Security Requirements (B) Organization-specific security requirements. The details are given in Section 5.2.

(D) Mobile forensics is important in the case of cybercrime. Follow standard digital forensics methodology. The mobile forensics presents a challenging problem to the cyber forensic experts due to its fast/continuous technology development and upgradation of its security features at regular intervals. Proper Categorizing/Correlation of the data with reference to the incident type will provides a lead to the investigating agencies in solving the cases. Follow the details given in Section 5.4.

(E) Cryptographic Security controls are required to be assessed by the testing organization. The details are given in Section 5.5 (A).

(F) The mobile application vetting is required to be done against the OWASP MASVS. The following three requirements are pertaining to Cryptanalysis. The details are given in Section 5.5 (B).

(G) Get insight of the use of testing tools for mobile security testing. See the informative list of mobile security testing tools as given in the Annexure J.

(H) Follow the Mobile Device Security Vetting -Approach & Methodology as given in Section 5.9.

(I) Follow guidelines for Device Level Security Testing as given in Section 5.10 (A)

(J) Follow guidelines for Communication Level Security as given in Section 5.10 (B)

(K) Cryptographic Security controls are required to be assessed by the testing organization. See the details as given in Section 5.5 (A)

(L) Guidelines for Application level Security given Section 5.10 (C)

(M) Test the security levels of the entities as given Section 1.2 and use the format given in Table of Annexure M to assign levels.

(N) Test the security levels of the technology Components as given Section 1.3 and use the format given in Table of Annexure L to assign levels.

(O) Follow the administrative structure prescribed in Section 5.3

6.6 Checklist for Regulators (R)

The Regulators, Auditors, Standardization Bodies and Enforcement Agencies may follow these guidelines:

(A) Revise various policies and standards available on mobile device security and their compliance.

(B) Revise and enforce the Security aspects of Mobile User Identity and Data Privacy as referred in Section 1.8.

(C) Advice the implementation of Mobile security grievance mechanism to all providers.

(D) Advice Security Key Management as referred in Section 1.8(F).

(E) Ensure that SIM Personalization and implementation is followed as per prescribed standard, which may be seed in Section 2.3.

(F) Mobile OS, Mobile Browser, SIM and Mobile Device are to be certified by competent government body for Mobile Sale and for Public Use in India.

(G) Mobile Security Testing and Forensics process as per prescribed standard.

(H) Periodic reports on mobile security threats reported and challenges faced in India may be compiled and compliance of entities to MSG be analyzed for giving advice.

(I) For location-based information of mobile users, mobile applications may use NAVIC system of India for privacy and data protection.

(J) Monitor if security attacks on networks and mobile devices of mobile users through quantum computers and targeted attacks are happening and if so, take appropriate action.

(K) For non-state actors and adversaries harming mobile users in India, initiate lodging of international compliant in a time bound manner.

6.7 Checklist for Researchers (A)

The Academia and Researchers should follow these guidelines:

(A) Mobile Device (MD) may pose various risks to the Mobile User (MU) such as fear of the MD being lost or stolen, loss due to sensitive information leakage, personal data theft and misuse of critical transaction data of MU from the MD, reputation loss on account of identity theft, social engineering etc. Explore easy ways to enrich mobile users awareness on security.

(B) Explore new techniques to identify threat actors as Adversaries, Attackers, Hackers, Intruders, Interceptors, Impersonators, Malware, Spyware, Virus etc. and their modus operandi. Develop protective mechanisms to insulate them.

(C) Explore how prescribed Mobile Security Goals in Section 1.7, can be achieved seamlessly on a National basis to protect every mobile user from any security threat.

(D) Innovate on bug free mobile device hardware, operating system, peripheral interface, application software, and user data protection. See Section 3.1.

(E) Explore on SIM Security and personalization issues. Innovate on secure element of Mobile Device useful to store private and public key pairs of digital certificate of Mobile User under mobile PKI implementation issued by Controller of certifying authority. This would help not only in mobile voting in general elections but to securely do all transactions.

(F) Investigate on open source secure APIs, libraries for developing secure mobile services.

(G) Innovate on 5G and beyond to develop low cost, efficient and secure communication services as per Indian requirements.

(H) Innovate on how session management can be faster.

(I) The mobile Browser has various security challenges such as Weak Operating system/plugin, Man-in-the-Middle (MitM) Attacks, Weak cryptography of Browser Advanced Jailbreaking and Rooting Techniques. See Section 5.2 and innovate on improved methods.

(J) There are various existing and emerging standards on mobile security by various bodies both nationally and internationally. It is a challenge for engineers, scientists and researchers to bridge the gap in understanding them, moving in pace with the developments there and transforming them quickly to realistic implementation for the benefit of society.

6.8 Security Guidelines for Mobile Device Users (U)

Here, security tips for Mobile Users are given, which are categorized under Device Level, Communication Level and Service Level Security Measures. Mobile User needs to be aware of these basic security precautions and follow them to safeguard from the mobile device security threats. It is also important for the mobile user to enrich the knowledge on the various security tips and follow best practices of security measures. For Data Privacy of Mobile User's, one may refer to Section 1.8 and for identification of the Level of a Mobile User, see Section 1.2

(A) Device Level Security Measures:

(i) Keep mobile phone device safely with self only: Like a purse or ornament, mobile device should be kept safely with the Mobile User only and should not be left un-attended, particularly when going to outside and public places.

(ii) Know the security features of own mobile phone device: Read the security settings of the User Manual of the Mobile Phone being used. Each brand and model of mobile phone may have common and specific security settings. Using Mobile Device Settings menu, security options may be chosen.

(iii) Use a Pin/Password/Pattern to lock mobile user phone: Locking the mobile device with a Pin/Password/Pattern is a basic security measure that every user should comply with. Without this basic security measure, an attacker may get direct access to data stored in the mobile device once gets physical access to the mobile device. Register password for screen lock. Use different passwords for important folders or files secure and private. Further, it is very important not to share the security Pin/Password/Pattern with anyone and keep it a secret. Change the Password periodically, at least once in 6 months.

(iv) Keep mobile user operating system and applications updated: Make sure to keep the operating system and applications up to date by installing the updates as and when they are available. Apart from the functionality updates and the functional bug fixes, these updates often include security fixes & vulnerability patches to patch the newly discovered security vulnerabilities. This ensures that the mobile device is secured against the known vulnerabilities.

(v) Ensure no jailbreaking and no rooting of mobile device: By default, mobile device platforms such as Android/iOS provide stringent security at the operating system level in order to secure the data stored on the devices. But once the device is jail-broken or rooted, the stringent security provided by the operating systems would become void. This makes the critical data stored on the device insecure and accessible to malicious applications or attackers. Always ensure that own mobile device is never jailbroken/rooted. Never purchase or use any rooted or jailbroken device, particularly pre-owned mobile device.

(vi) Avoid charging of mobile devices using public charging points: Users have to understand that it would be possible to hack a mobile device just by connecting the device to public charging points such as the one's available in public transport, shopping malls and other public places. If a particular charging point is compromised by the attacker, it would be possible to get access to the sensitive data stored on the user's device. This technique of hacking phones using USB charging points is known as Juice Jacking. So, it is advisable not to charge mobile devices using charging points available in untrusted public places to avoid any possible security breach into the mobile devices.

(vii) Follow safe disposal practices: In case the user is planning to dispose of the mobile device either through an exchange offer to purchase a new mobile device or selling the device by other means, even to a person of close contacts, make sure that the device is cleaned and data is wiped off properly. This can be done by taking the backup of the complete data and using the options such as Factory Reset the Device before disposing of the device. This would protect personal sensitive data from falling into the wrong hands.

(B) Communication Level Security Measures:

(i) Note down own Mobile Phone Number, Mobile Phone IMEI Number, SIM Card Number and Mobile Network Operator's Phone Number: These numbers are essential to be recorded by a Mobile User in a paper or diary and to be kept safe, so that in crisis times, they need to be provided to report for lodging compliant to trace it. SIM Card Number is available on the SIM Card or its cover in printed form. International Mobile Equipment Number (IMEI) of the Mobile Phone, which can be seen printed on its packed box or manual. If You press *#06# in the phone dialing pad of the mobile phone, then IMEI Number gets displayed. For phones with dual SIMs one may get two IMEI (International Mobile Equipment Identity) Numbers.

(ii) Avoid suspicious links: Attackers may lure the users by asking to click on malicious links which are communicated to the users over various channels such as SMS, email or social media platforms such as WhatsApp, Facebook etc. pretending to be from a popular bank or someone whom the user may know or trust. Once the user clicks on these malicious links, it would be possible for the attackers to hack into the user's mobile devices, inject malware and steal sensitive user data. So, one should strictly avoid clicking on any suspicious links appearing in text, image or video icons or received over SMS, email or any social media platforms.

(iii) Block cookies of unknown websites: Websites which are unknown and whose cookie policy is not published in the website, their cookies may be blocked by the mobile browser using settings. Follow: (i) Cookies services and their policy must be read carefully while surfing/accessing the web page. (ii) Some cookies collect analytics data, it is recommended to block the third-party cookies for safe surfing, (iii) Carefully set the Privacy setting in the browser, (iv) Download browser from safe source such as application stores (Google play, Apple stores and Microsoft) and keep it updated, (v) Always use mobile phones recommended security and keep it updated.

(iv) Turn off Bluetooth/Wi-Fi/NFC when not in use: It is possible for attackers to hack into mobile devices through the services such as Bluetooth/Wi-Fi/NFC. So, it is always a good practice to turn off these network services when not in use. Turn on these services as and when they are required and make sure to turn them off immediately after use.

(v) Log out of sites after performing a financial transaction: It is a good practice to log out of any banking or payment service after performing financial transactions and then close the mobile application. This would ensure preventing access by unauthorized users to mobile user financial services by making use of any active sessions on mobile user device.

(vi) Encrypt hotspots from being used by other devices: When a mobile device is turned into a personal hotspot, it is a best practice to secure the hotspot with Wireless Protected Access 2, or WPA2 in order to prevent unauthorized access to the mobile device by malicious actors/IoT device/wireless device or higher standard.

(C) Service Level Security Measures:

(i) Keep Secure storage of passwords and do not use same password for every online account. Do not store passwords related to online accounts in plain text in mobile devices. Rather, it is recommended to use reputed password managers to securely store the passwords in an encrypted format. Further, it is recommended to use a unique separate password for every online account and avoid reusing the same password across multiple accounts. This ensures security to other accounts even if the password of one online account is compromised. The best practice is to use a password manager to create unique, hard-to-crack passwords.

(ii) Keep data connections off when not in use: It is safe to keep data connections off when not in use and make it on only when necessary. Auto on/off feature of mobile phone can be set as default during sleeping hours, for example, auto off at 10 PM to and auto on at 6 AM. This habit has made users safer compared to those who keep the data on all time.

(iii) Download mobile apps from official/reputable app stores and certified as tested:

Mobile Applications may come pre-installed at the time of purchasing a mobile phone or the mobile user may download and install on demand. Ensure that mobile app is downloaded from trustworthy sites only. If several mobile apps with similar name appears, choose appropriate one by looking at what functionalities it provides, whether it is certified, whether it is latest, has maximum downloads, what permissions it asks for etc.

(iv) Use only official play-stores/app-stores for installing and using mobile applications: Usage of third-party play-stores/app-stores should be avoided unless the user is pretty sure about the authenticity of such app-stores and the applications downloaded from these app-stores. It is a very common practice for attackers to host malicious applications through these third-party app stores. The reason being the official play-stores/app-stores deploy stringent security measures before publishing the applications which avoid to the extent possible entering of malicious applications into these official app stores. Further, before installing any application even from the official play-stores/app-stores, it's a good practice to check the user ratings & reviews to get a glimpse of the application and the other user's experience with the application. This gives first-hand information about the application. Also, it is important to read the privacy policy of the application which gives an understanding of the data being accessed by the application from the mobile device and what the application will be doing with the accessed data.

(v) Though there are stringent security measures in place to keep the malicious applications away from the play-stores/app-stores, sometimes, these malicious applications manage to make their way to the play stores. So, it is always important as a user to be cautious about what applications the user is installing on the mobile device, what are the ratings/reviews of the applications by other users, what permissions the application is seeking from the user and what is the application's privacy policy. Also, make sure to review the permissions granted to the applications installed on the device on a regular basis.

(vi) Use a security protection application: In spite of proper security measures and best practices followed by the users, sometimes, it would be very difficult for naive users to detect and avoid any attempts by the attackers to attack and hack into the user's mobile devices. Hence, it is recommended to use any popular and trusted antivirus software on the mobile device to protect the devices from any possible security breaches/attacks.

(vii) Avoid giving out personal information: Avoid sharing personal/sensitive information in response to SMS or email communications received from a bank or a person from your known circles. These may be phishing messages or emails from an attacker pretending to be a genuine request seeking sensitive information.

(viii) Backup data at regular intervals: Frequent backups of the data stored on the mobile device in personal storage device or online cloud providers storage would ensure that one does not lose data in the event of loss/theft of the mobile device. Backing up of data also ensures that one's data is protected against any ransomware attack on the mobile device. If one keeps mobile data in online sites, they should be trustworthy and have agreement not to misuse it and share to other parties.

(ix) Enable remote locking and wiping of the mobile device: It is always a good practice to enable remote locking/wiping off the mobile device. This enables the users to protect personal/sensitive data from falling into the hands of unauthorized users in the event of a loss/theft of the device. Further, it would be possible for the users to restore that data into a new device from the data backup. For example, Apple mobile phone users have to Find My iPhone, and Android users can enable Find My Device to see the last known location of the device. Both features allow the users to remotely wipe the smartphone's data if it's stolen or can't be retrieved.

(x) Use two-factor authentication: Some services/applications provide an additional layer of authentication such as OTP in addition to username/password to access their services. Some services may provide two-factor authentication by default and some services make the two-factor authentication optional. In case it is optional, make sure to enable the two-factor authentication. This ensures that mobile user critical financial/business/personal data is protected from unauthorized access even if the passwords are compromised.

7. References

[1] Mobile Security, Prof. V. N. Sastry, IDRBT Staff Paper Series, Cyber Security, Vol.4, No.1, March 2019, pp.50-128 https://idrbt.ac.in

[2] https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05i-Testing-Code-Quality-and-Build-Settings.md

[3] https://developer.android.com/studio/publish/app-signing#certificates-keystores

[4] https://embeddedbits.org/introduction-to-trusted-execution-environment-tee-arm-trustzone/

[5] https://source.android.com/security#security-program-overview

[6] https://developer.android.com/*guide*/topics/permissions/overview

[7] https://uk.norton.com/internetsecurity-online-scams-11-social-media-threats

[8] https://www.businessinsider.in/slideshows/miscellaneous/10-ways-to-makeyour-phone-safer-according-to-security-experts/slidel-ist/71235078.cms#slideid=71235080

[9] https://blog.avast.com/9-smartphone-tips-privacy-security

[10] https://www.verizon.com/articles/8-common-sense-tips-to-keep-yoursmartphone-secure/

[11] https://lunarline.com/lunarline-blog/top-mobile-security-tips/

[12] https://www.identityforce.com/blog/15-mobile-device-security-tips#:~:text=Here%2015%20mobile%20device%20secu-rity,apps%20from%20third%2Dparty%20sites

[13] https://preyproject.com/blog/en/phone-security-20-ways-to-secure-your-mobile-phone/

[14] https://pratum.com/blog/477-mobile-device-security-best-practices

[15] https://www.ntiva.com/blog/top-5-mobile-device-security-best-practices

[16] https://www.hindawi.com/journals/misy/2020/8828078/

[17] https://www.it.ucla.edu/security/resources/security-best-practices/guidelines-for-securing-mobile-devices

[18] https://www.verizon.com/business/content/dam/resources/infographics/2021/2021-msi-executive-summary-infographic.pdf

[19] https://www.whitehatsec.com/wpcontent/uploads/2016/01/Mobile_SDLC_White_Paper-1.pdf

[20] https://source.android.com/security/overview/implement

[21] https://www.isaca.org/resources/isaca-journal/issues/2017/volume3/safeguarding-mobile-applications-with-secure-development-life-cycle-approach

[22] https://www.veracode.com/security/android-security

[23] https://resources.infosecinstitute.com/topic/android-tips-and-settings/

[24] https://brave.com/learn/most-secure-android-browser/#secure-browsing-on-your-android

[25] https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8271994

[26] https://link.springer.com/chapter/10.1007/978-3-319-33630-5_23

[27] https://mobile-security.gitbook.io/mobile-security-testing-guide/android-testing-guide/0x05h-testing-platform-interaction

[28] https://hackernoon.com/mobile-api-security-techniques-682a5da4fe10

[29] https://core.ac.uk/download/pdf/143854065.pdf

[30] http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Layer-1-The-Physical-Layer.pdf

[31] https://www.sciencedirect.com/topics/computer-science/communication-security

[32] https://coek.info/pdf-mobile-wireless-network-security-.html?

[33] https://www.technology.pitt.edu/help-desk/how-to-documents/wireless-network-standard

[34] https://www.wi-fi.org/discover-wi-fi/security

[35] https://nfc-forum.org/faq/nfc-forum-security-faqs/?

[36] https://mts.intechopen.com/storage/books/446/authors_book/authors_book.pdf?

[37] Hamid Jahankhani, Sufian Yousef. "Evolution of TETRA through the integration with a number of communication platforms to support public protection and disaster relief (PPDR)", Elsevier BV, 2014

[38] http://net-informations.com/q/diff/generations.html

[39] Petros Mashwama, Stephen Gbenga Fashoto, Elliot Mbunge, Simanga Gwebu. "Development of a Mobile Inter-Vehicular Communication System Based on Gossip Algorithm", International Journal of Interactive Mobile Technologies (iJIM), 2020

[40] epdf.pub

[41] https://www.e-spincorp.com/importance-of-mobile-device-forensics/?

[42] https://athenaforensics.co.uk/wp-content/uploads/2019/01/NIST-Guidelines-on-Mobile-Device-Forensics-05-2014.pdf?

[43] https://info-savvy.com/mobile-forensic-overview/?

[44] Mobile Device Security (Parts 1-4), BIS LITD-17 Standard, Dec.2021, Bureau of Indian Standards.

8. List of Annexures

Annexure A: Abbreviations

Abbreviation	Full form
3GPP	3rd Generation Partnership Project
AC	Access Control
AES	Advanced Encryption Standard
AMPS	Advanced Mobile Phone Service
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
APP	Application
BTS	Base Trans-receiver System
CBC	Cipher Block Chaining
CC	Cellular Communication
C-DAC	Center for Development of Advanced Computing
CDMA	Code-Division Multiple Access
CDPD	Cellular Digital Packet Data
CE	Credential Encrypted
CFB	Cipher Feedback
CHTML	Compact HTML
CIS	Center of Internet Security
COAI	Cellular Operators Association of India
COMSEC	Communications Security
DAC	Discretionary AC
DE	Device Encrypted
DES	Data Encryption Standard
DMZ	De-materialized Zone
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic-curve Diffie–Hellman exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
e-Gov	Electronic Governance
eID	Enrolment ID
EMI	Electromagnetic Interference
eMMC	Embedded Multimedia Cards
eSIM	Embedded/Shouldered SIM
ESN	Electronic Serial Number

Abbreviation	Full form
ETSI	European Telecommunications Standards Institute
eUICC	Embedded/Shouldered UICC
FANETs	Flying Ad Hoc Networks
FDE	Full Disk Encryption
GCMP	Galois/Counter Mode Protocol
GoI	Government of India
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GSMA	Global System for Mobile Association
HCE	Host Card Emulation
HD	High Definition
HMAC	Hashed Message Authentication Mode
HTTP	Hypertext Transfer Protocol
IAMAI	Internet and Mobile Association of India
IC	Integrated Circuit
ICCID	Integrated Circuit Card Identifier
ID	Identity
IDRBT	Institute for Development and Research in Banking Technology
IDS	Intrusion Detection Systems
IDT	Integrated Device Technology/Intrusion Detection System
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter-Process Communication.
IRDA	Insurance Regulatory and Development Authority
iSIM	Integrated SIM
ISIM	IP Multimedia Services Identity Module
ISM	Industrial, Scientific and Medical
ISP	Internet Service Provider
ITU	International Telecommunication Union
IVC	Inter-Vehicle Communication
KYC	Know Your Customer
LCD	Liquid Crystal Display
LK	Little Kernel

Abbreviation	Full form
LLCP	Logical Link Control Protocol
LNCG	Non-Linear Congruential Generator
LTE	Long Term Evolution
MA	Mobile Application
MAC	Mandatory AC
MACs	Message Authentication Codes
MANETs	Mobile Ad Hoc Networks
MD	Mobile Device
MDM	Mobile Device Management
MDS	Mobile Device Security
MDSS	Mobile Device Security Standard
MEID	Mobile Equipment Identifier
MeitY	Ministry of Electronics and Information Technology
m-Gov	Mobile Governance
MIMO	Multiple Input Multiple Output
MIN	Mobile Identification Number
MitM	Man-in-the-Middle
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MNO	Mobile Network Operator
MPFI	Mobile Payment Forum of India
MS	Mobile Subscriber
MSCM	Mobile Security Control Measures
MSG	Mobile Security Guidelines
MSG	Mobile Security Guideline
MT	Mobile Transaction
MU	Mobile User
NFC	Near Field Communication
NGOs	Non-Governmental Organization
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OFB	Output Feedback
OFDM	Orthogonal Frequency Division Multiplexing
OPC	One Person Company
OS	Operating System
OSI	Open System Interconnection
OTA	Over The Air

Abbreviation	Full form
OTP	One Time Programmable
OU	Organization Unit
OWASP	Open Web Application Security Project
PaSS	Planning, Attention, Simultaneous and Successive
PBL	Primary Boot Loader
PCBC	Propagating Cipher Block Chaining
PDAs	Personal Digital Assistants
PEAP	Protected Extensible Authentication Protocol
PIM	Personal Information Management
PIN	Personal Identification Number
PMF	Protected Management Frames
PoS	Point-of-Sale
POTS	Plain Old Telephone Service
PSK	Pre-shared Key
PSTN	Public Switched Telephone Network
PUK	Personal/Public Unlocking Key
QoS	Quality of Service
R&D	Research and Development
RAM	Random Access Memory
RBAC	Role Based AC
RBI	Reserve Bank of India
RNG	Random Number Generators
ROM	Read Only Memory
RSP	Remote Service provisioning
RTD	Record Type Definition
SaaS	Software as Service
SAE	Simultaneous Authentication of Equals
SANS	System Administration, Networking and Security
SBL	Secondary Boot Loader
SCI	Supreme Court of India
SD	Secure Digital
SDK	Software Development Kit
SE	Secure Element
SEBI	Securities and Exchange Board of India
SETS	Society of Electronics Transaction and Security
SIM	Subscriber Identity Module
SMS	Short Message Service

Abbreviation	Full form
SoC	System on Chip
STQC	Standardization Testing and Quality Certification
TEE	Trusted Execution Environment
TEMPEST	Test for Electromagnetic Propagation and Evaluation for Secure Transmissions
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TRAI	Telecom Regulatory Authority of India
TSDSI	Telecommunications Standards Development Society, India
TV	Television
UE	User Experience/User Equipment in 5G
UEFI	Unified Extensible Firmware Interface
UI	User Interfaces
UICC	Universal Integrated Circuit Card
UIDAI	Unique Identification Authority of India
UMTS	Universal Mobile Telecommunications System
USIM	UMTS Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
UTs	Union Territories
VANET	Vehicular ad hoc Networks
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRC	Vehicle to Road Communication
WEP	Wired Equivalent Privacy
WG	Working Group
WLAN	Wireless Local Area Network
WML	Wireless Markup Language
WPA	Wi-Fi Protected Access
XBL	eXtensible Boot Loader
xG	x-th. Generation (x=1,2,3,4,5,6)

Annexure B: Terms and Definitions

1. **Standard**: A Standard defines common practices, methods, measures and metrics. It provides interoperable solutions that have been evaluated by experts in relevant areas, reviewed by the public and subsequently accepted by a wide community of users. It helps in uniformity and common understanding by stakeholders so that organizations can reduce costs, provide acceptable solutions and protect their investments in technology.
2. **Mobile Device (MD):** A Mobile Device (MD) is referred here to mean a mobile phone or a smartphone or a handheld tablet or a mobile wearable device used by a Mobile Subscriber (MS) registered with a mobile network operator (MNO) or Internet Service Provider (ISP).
3. **Mobile User (MU):** A Mobile User (MU) is referred here to mean an authorized Mobile Subscriber (MS) using a Mobile Device (MD) linked with the registered SIM/USIM.
4. **Mobile Governance (m-Gov):** Mobile Governance (m-Gov) focuses on the delivery of all Government services of information on to citizens mobile Device. The major area of concern under e-Governance/m-Governance services is Mobile Device Security.
5. **Mobile Security Goals:** Mobile security goals which are also referred to as security properties or security principles, that need to be fulfilled by the mobile ecosystem entities:
6. **Mobile Device Manufacturers (M):** They are accountable for design, manufacturing, hardware, interfaces, OS, Library, embedded API and their security
7. **Mobile Network Operators (N):** They are accountable for providing seamless connectivity to the Mobile Device as per the Quality of Service requirements of the Mobile User ensuring end to end security.
8. **Mobile Service Providers (S):** Government bodies providing mobile governance services, Semi-Government, Private bodies, Social Media organizations, integrators, data analytics organizations and others providing mobile services to Mobile Users in India.
9. **Mobile Application and API Developers (D):** They should ensure that besides functional and performance testing, proper security testing of Mobile Apps and APIs is done as per the prescribed guidelines of secure coding practices.
10. **Mobile Security Testing and Forensics Bodies (T):** Mobile Security Testing, Mobile Forensics, Quality Assurance and Assessment organizations should periodically upgrade their infrastructure, testing tools, software's, simulation environment and skilled manpower.
11. **Regulators, Legal and Government Bodies (R):** Mobile ecosystem encompasses mobile services of service providers catering to various verticals monitored by respective regulators of India such as TRAI for Telecom, RBI for Banking, IRDA for Insurance, SEBI for financial markets etc. Regulators, Legal bodies and Government Departments should work together to exchange information coordinated by Inter-ministerial group

for proper directions and implementation to ensure safety and security of Mobile Users in India.

12. **IC (Integrated Circuit) Platform:** This is an old generation SIM based on 8085 instruction code with less EEPROM that can hold one application/profile used mostly for 2G and 3G GSM connectivity.
13. **UICC (Universal Integrated Circuit Card) platform:** This is also based on 8085 instruction code developed by UMTS, with an advanced platform facilitating the multiple applications for GSM and Non-GSM networks.
14. **SIM (Subscriber Identity Module):** GSM application based on IC platform.
15. **E-SIM** (Embedded SIM/USIM in the machine with the capability of GSMA eSIM) or normal 3GPP SIM)- As defined in TEC Interface Requirement), Any SIM form factor (iii, iv and vii) soldered in the machine is defined as E-SIM
16. **iSIM (Integrated SIM):** This is the next generation of SIM form factors. In iSIM, the substantial change is from the perspective of integrating SoCs (System on Chip) with the cellular modem to get the benefit of tightly coupled architecture. The major change is that the SIM hardware is integrated into system-on-chip (SOC) architectures that combine a processor and cellular modem.
17. **USIM (UMTS Subscriber Identity Module):** GSM/UMTS/3GPP applications based UICC platform.
18. **ISIM (IP Multimedia Services Identity Module):** 3GPP application for IP multimedia services reside in UICC.
19. **GSMA eSIM (Embedded/Soldered SIM):** This is GSMA specified form factors shouldered in the machine for M2M (Machine to Machine) business and consumer business, could be personalized remotely, using GSMA specification with GSMA RSP (Remote Service Provisioning) services.
20. **eUICC:** Embedded Universal Integrated Circuit Card platform.
21. **Soldered UICC:** It is commonly known as eUICC, features are the same as SIM/USIM but it is not GSMA eSIM
22. **Network eavesdropping:** Network eavesdropping, also known as eavesdropping attack, sniffing attack, or snooping attack, is a method that retrieves user information through the internet.
23. **Interprocess communication (IPC):** Interprocess communication (IPC) refers specifically to the mechanisms an operating system provides to allow the processes to manage shared data.
24. **Secure Element (SE):** Secure Element (SE), which is dedicated, separate tamper-resistant hardware to store cryptographic data
25. **Denial of Service (DoS):** The prevention of authorized access to a system resource or the delaying of system operations and functions.

26. **Buffer overflow:** A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.
27. **Privilege Escalation:** The exploitation of a bug or flaw that allows for a higher privilege level than what would normally be permitted.
28. **Spyware:** Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
29. **Jailbreaking:** Jailbreaking refers to privilege escalation on an Apple device to remove software restrictions imposed by Apple on iOS, iPadOS, tvOS, watchOS, bridgeOS and audioOS operating systems
30. **Address space layout randomization (ASLR):** Address space layout randomization (ASLR) is a computer security technique involved in preventing exploitation of memory corruption vulnerabilities.
31. **Stack canaries** : Stack canaries or security cookies are tell-tale values added to binaries during compilation to protect critical stack values like the Return Pointer against buffer overflow attacks.
32. **Virtual private network (VPN**): Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
33. **File encryption:** It protects individual files or file systems by encrypting them with a specific key, making them accessible only to the keyholder. The goal is to prevent malicious or unauthorized parties from accessing files that are stored on the disk. Support for file encryption can be built into an operating system or file system.
34. **Full disk encryption:** Full disk encryption allows users to secure all the data stored on a device. It encrypts the whole hard drive as well as the data that needs to be protected. When the user turns on their mobile device, they will enter one or more factors of authentication before their data can be decrypted.
35. **Application Programming Interface (API):** A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.
36. **Side-Channel Attack:** An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions.
37. **Trusted Execution Environment (TEE):** A trusted execution environment (TEE) is a secure area of a main processor. It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity
38. **Sensor:** A sensor is a transducer that converts a physical, biological or chemical parameter into a electrical signal.

39. **Accelerometer:** An accelerometer is a device that measures non-gravitational accelerations. The accelerometer can tell when the mobile phone is tilted, rotated, or moved.
40. **Magnetometer:** A magnetometer is a device that measures magnetic field or magnetic dipole moment.
41. **Global Positioning System (GPS)**: A system for determining position by comparing radio signals from several satellites.
42. **Spearphone:** A lightweight speech privacy exploit via accelerometer-sensed reverberations from smartphone loudspeakers
43. **SD card**: A secure digital card (SD card) is a small flash memory device designed to provide high-capacity memory in a portable size.
44. **Firmware:** Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
45. **Near Field Communication (NFC)**: A form of contactless, close proximity, radio communications based on radio-frequency identification (RFID) technology.
46. **Testing:** Testing is the act of conducting a trial or test to check an entity, how good it is with respect to a criterion. It helps in verifying the expected performance or deviation from a target of an entity in a given environment. For example, a mobile app undergoes functional testing to check whether it executes its intended functionality or not.
47. **Security Testing:** It is a methodology to check whether an entity fulfils a security goal/requirement or not. Unlike Functional testing, Security Testing of the mobile app is more challenging as it requires threat modelling and vulnerability assessment. Mobile Device Security Testing covers the security testing of a mobile device (H/W, OS & Firmware), mobile communication, mobile application, mobile interfaces and mobile user.
48. **App Vetting:** Mobile app vetting is a process which consists of activities aiming to assess the extent of conformance of the app to the specified security requirements. It involves testing and analysis of mobile app’s compiled, binary representation or source code in an organized manner. Application Security and Mobile Device Security Controls to fulfill security goals.
49. **Forensics:** It is the scientific approach to collect and analyze evidence in a suspected crime investigation. Digital forensics deals with digital assets of evidence and mobile forensics focus on investigative evidence analysis of mobile phone and its data.
50. **Cookie**: A cookie is a piece of software code that an internet web site sends to mobile browser to access information at that site. A cookie is stored as a simple text file on the mobile device by a website’s web server and only that server will be able to retrieve or read the contents of that cookie. Cookies let one to navigate between pages

efficiently as they store mobile user preferences to improve user experience of a website.

51. **Data**: It is a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means.
52. **Data principal**: It means the natural person to whom the personal data relates. Here, it refers to a Mobile User.
53. **Personal data:** It means data about or relating to a Mobile User who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.
54. **Personally identifiable information (PII):** Any representation of information that permits the identity of an individual or Mobile User to whom the information applies to be reasonably inferred by either direct or indirect means.
55. **Personal data breach**: It means any unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal, that is to Mobile User.
56. **Data fiduciary**: It means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.
57. **Data processor**: It means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.
58. **Processing of Personal Data**: It means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.
59. **Biometric data:** It means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations short title and commencement.
60. **Financial data**: It means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history.
61. **Health data**: It means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.

Annexure C: Standards

SR.No	Document No.	Title/Document Name
1	ISO 7816-1	"Identification cards - Integrated circuit(s) cards with contacts, Part- 1: Physical characteristics"
2	ETSI TS 101 220	Smart Card ETSI Numbering system for telecommunication application provider
3	ETSI TS 101 180	Digital cellular telecommunications system (Phase 2+); Security mechanisms for the SIM Application Toolkit; Stage 1
4	ETSI TS 102 221	Smart cards; UICC-Terminal interface; Physical and logical characteristics
5	3GPP TS 11.11	3rd Generation Partnership Project; Technical Specification Group Terminals Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
6	3GPP TS 11.14	3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
7	3GPP TS 51.011	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
8	3GPP TS 51.014	3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
9	GSM 11.12	Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
10	GSM 11.18	Digital cellular telecommunications system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module Mobile Equipment (SIM - ME) interface
11	3GPP TS 43.019	3rd Generation Partnership Project; Technical Spec-

SR.No	Document No.	Title/Document Name
		ification Group Terminals; Subscriber Identity Module Application Programming Interface (SIM API) for Java Card™ Stage 2
12	3GPP TS 31.111	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)
13	3GPP TS 03.19	3rd Generation Partnership Project; Technical Specification Group Terminals; Subscriber Identity Module Application Programming Interface (SIM API) for Java Card™; Stage 2
14	3GPP TS 03.48	3rd Generation Partnership Project; Technical Specification Group Terminals; Security mechanisms for the SIM application toolkit; Stage 2
15	3GPP TS 23.048	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Security mechanisms for the (U)SIM application toolkit; Stage 2
16	Global Platform	Global Platform, Card Specification
17	ETSI TS 102 221	Smart cards; UICC-Terminal interface; Physical and logical characteristics
18	ETSI TS 102 222	Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications
19	ETSI TS 101 116	Digital cellular telecommunications system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module Mobile Equipment (SIM - ME) interface
20	3GPP TS 42.017:	3rd Generation Partnership Project; Technical Specification Group Terminals; Subscriber Identity Modules (SIM); Functional characteristics
21	3GPP TS 31.101	3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics
22	3GPP TS 31.102	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Char-

SR.No	Document No.	Title/Document Name
		acteristics of the Universal Subscriber Identity Module (USIM) application
23	3GPP TS 31.111	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)
24	3GPP TS 33.102	3GPP Technical specifications for 3G security
25	3GPP TS 33.103	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects. 3G security; Integration guidelines
26	3GPP TS 35.206	3GPP Technical specifications for GSM-MILENAGE ALGORITHM
27	Remote Provision-able eUICC Profiles	SIM ALLIANCE eUICC Profile Package: Interoperable Format Technical Specification Version 2.1, 24 February 2017
28	Business Process for Remote SIM Provisioning	Business Process for Remote SIM Provisioning in M2MVersion 1.018 February 2015
29	GSMA SGP 0.6	GSMA eUICC Security Assurance Principal
30	GSMA SGP .21	eSIM architecture Specifications
31	GSMA SGP .22	GSMA RSP Technical Specification
32	GSMA SGP .02	GSMA Remote Provisioning Architecture for Embedded UICC Technical Specification
33	GSMA SGP .24	eSIM compliance Process
34	GSMA SGP .25	GSMA Embedded UICC for Consumer Devices Protection Profile
35	IS 16333, Part-1,2015 & Indian Standard Reaffirmed, BIS,2021	Mobile Phone Handsets - Safety Requirements
36	IS 17737, Part-1 to 4, BIS, Dec 2021	Mobile Device Security, Part-1 to 4

Annexure D: Categories of Sensors

There are two categories of sensors in smartphones:

(i) Permission-imposed Sensor (PS): The application needs user permission to access some of the sensors in smartphones. These types of sensors are categorized as PS. Examples are camera, microphone, speaker, GPS. These sensors have an on/off (binary) state. So, the other names for the PS are binary sensors and logic-oriented sensors.

(ii) No Permission-imposed Sensor (NPS): The application does not need user permission to access some of the sensors in smartphones. These types of sensors are categorized as NPS. Examples are an accelerometer, gyroscope, light sensor and Proximity sensor. Applications can access these sensors through the generic sensor API. These sensors are not having an on/off state and they produce numeric readings. So, other names for the NPS are numeric sensors and data-oriented sensors.

(iii) There have been attacks reported where adversaries were able to unlock Android phones with as fast as three attempts. Also there have been attacks where adversaries were able to evolve a 3D map of the user's physical environment. Similarly attacks on guessing passwords by using the microphone sensor and Artificial Intelligence, when user's type password, was also demonstrated by Researchers. Another attack called the spearphone eavesdropping has been reported where the adversaries were able to guess gender, identity etc. by using speakerphone and accelerometer.

(iv) It is recommended to check at the permissions given to applications specifically to access the sensors. The operating systems should incorporate mechanisms to authenticate sensor data access for applications and also should have mechanisms to detect background access of sensor data, when the application is not active.

Annexure E: Diagrams/Charts/Figures

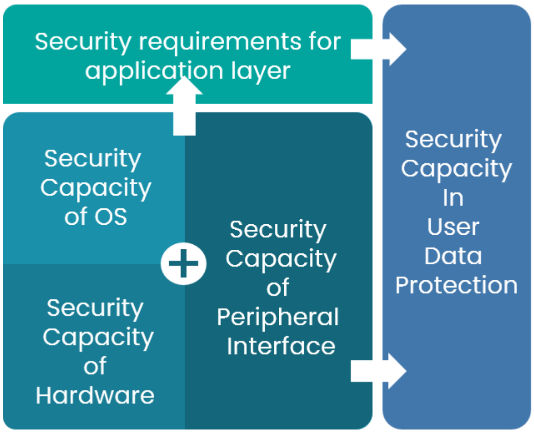
Security requirements for application layer
Security Capacity of OS
Security Capacity of Hardware
Security Capacity of Peripheral Interface
Security Capacity In User Data Protection

Figure 1: Security Capability Framework of Mobile Device

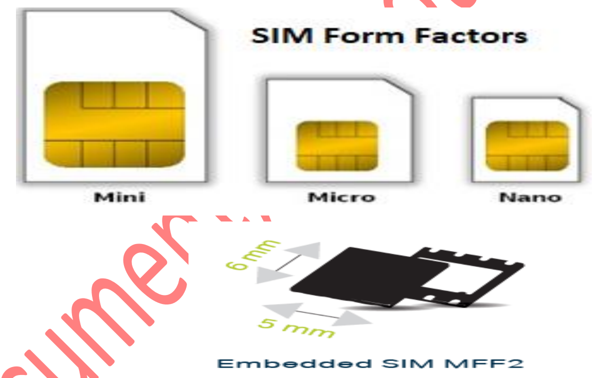

Figure 2: SIM Form Factors

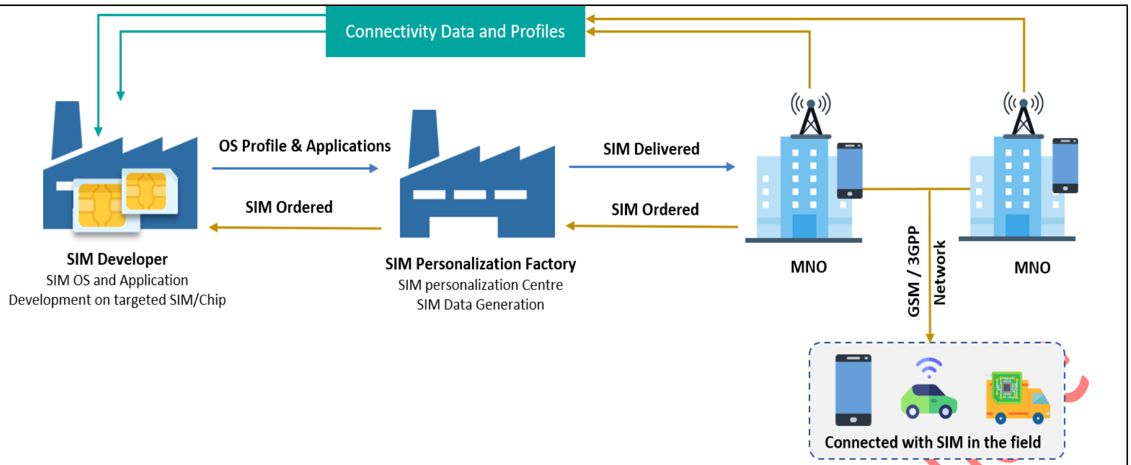
Connectivity Data and Profiles
OS Profile & Applications
SIM Ordered
SIM Delivered
SIM Ordered
SIM Developer
SIM OS and Application
Development on targeted SIM/Chip
SIM Personalization Factory
SIM personalization Centre
SIM Data Generation
MNO
MNO
GSM / 3GPP
Network
Connected with SIM in the field

Figure 3: Pluggable SIM form Factor lifecycle

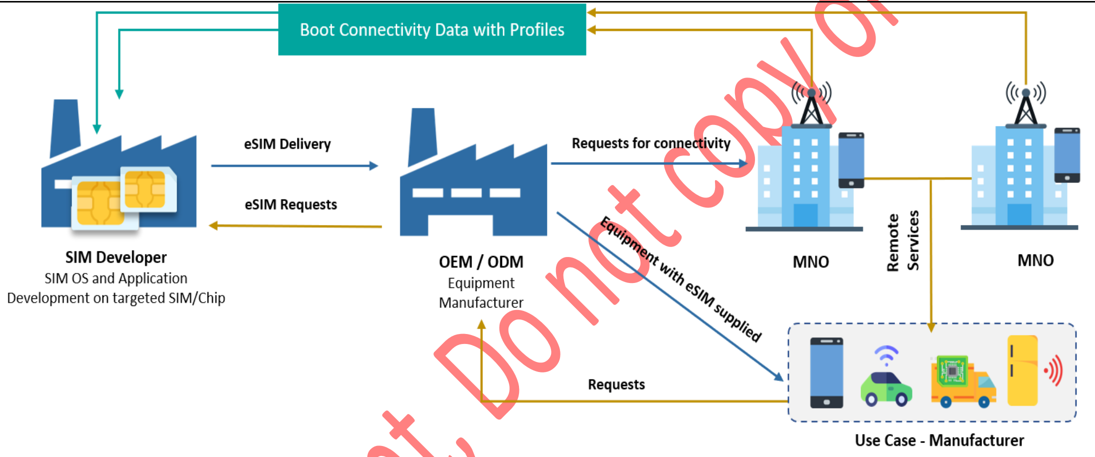

Figure 4: Embedded soldered SIM lifecycle and Order Management

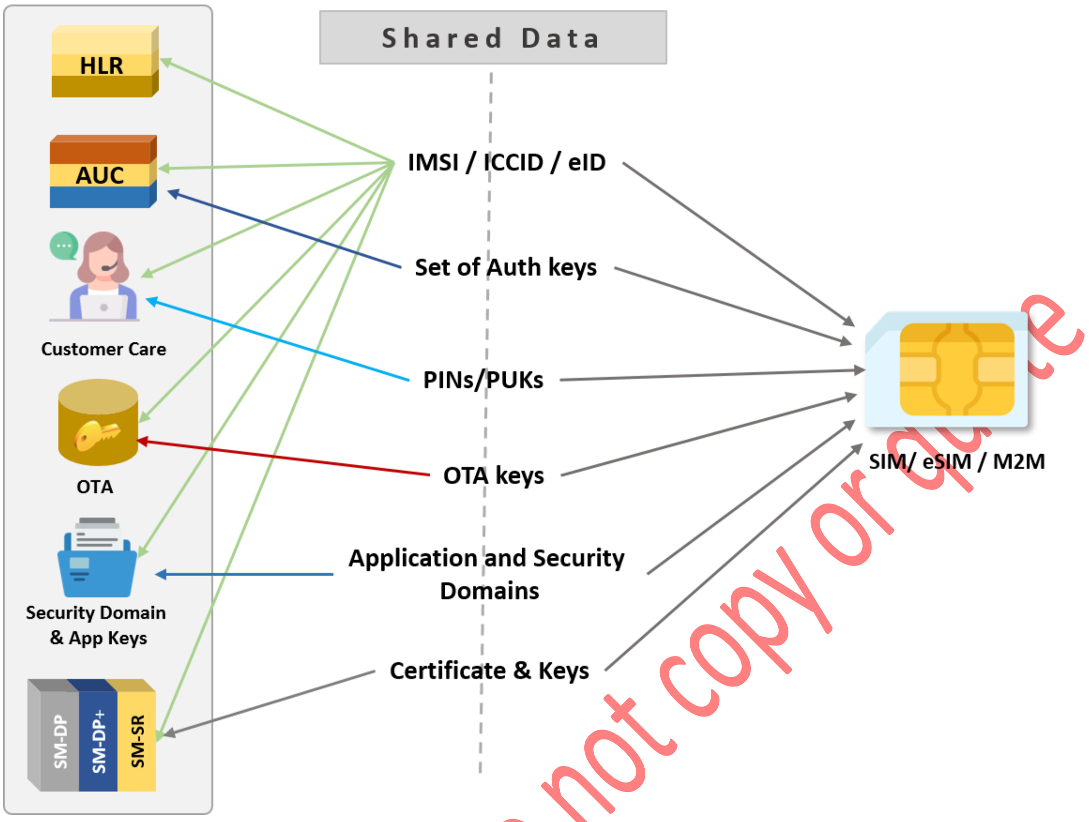

Figure 5: SIM Critical contents and echo system

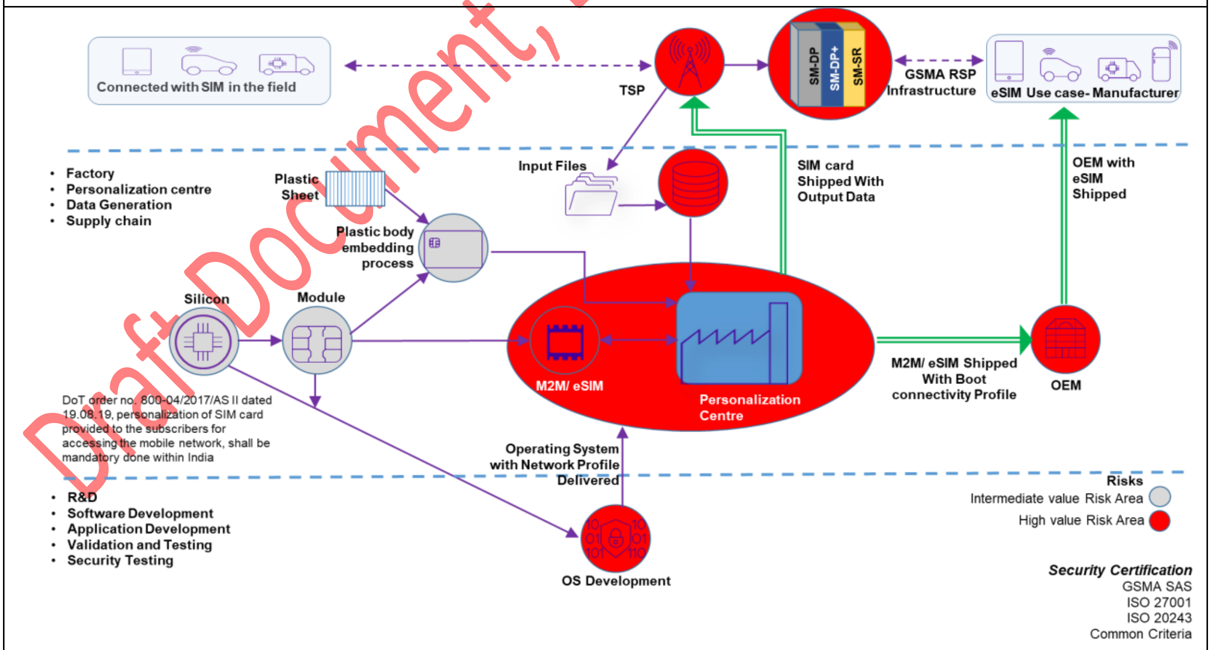

Figure 6: SIM/eSIM development and product delivery

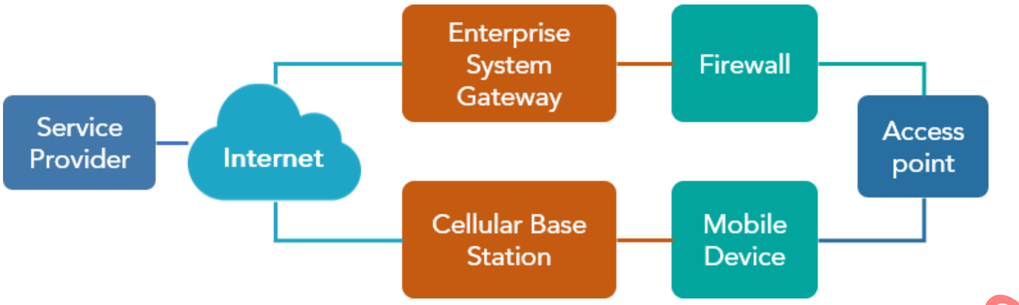

Figure 7: Communication level security

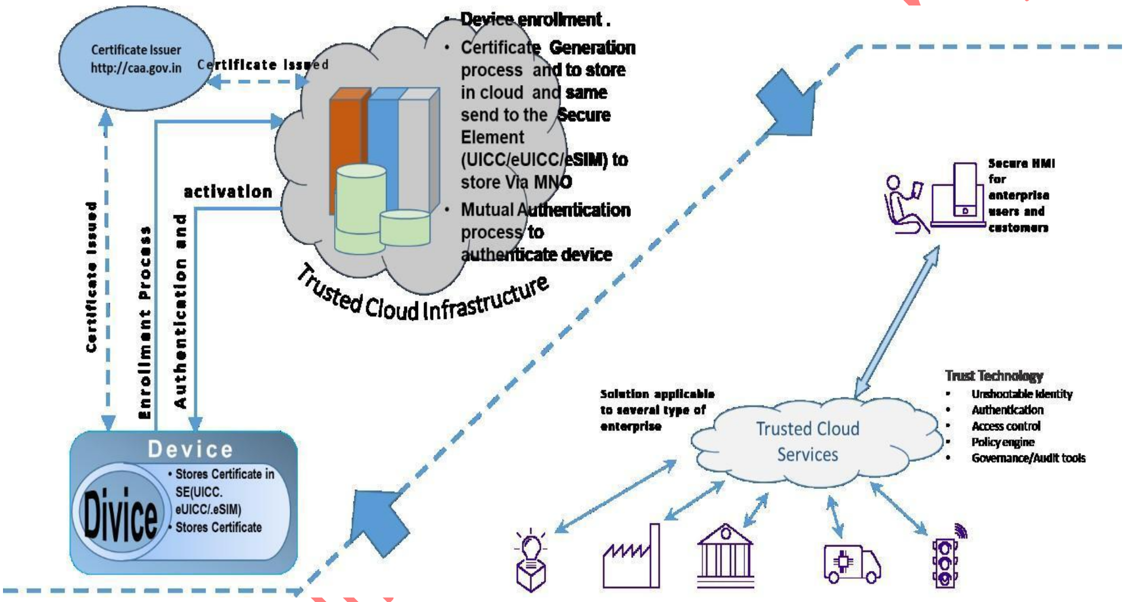
Certificate Issuer http://caa.gov.in
Certificate Issued
Certificate Issued
Enrollment Process
Authentication and activation
Device enrollment .
Certificate Generation process and to store in cloud and same send to the Secure Element (UICC/eUICC/eSIM) to store Via MNO
Mutual Authentication process to authenticate device
Trusted Cloud Infrastructure
Device
Divice
Stores Certificate in SE(UICC. eUICC/.eSIM)
Stores Certificate
Secure HMI for enterprise users and customers
Solution applicable to several type of enterprise
Trusted Cloud Services
Trust Technology
Unshootable Identity
Authentication
Access control
Policy engine
Governance/Audit tools

Figure 8: SIM as Root of Trust secure element

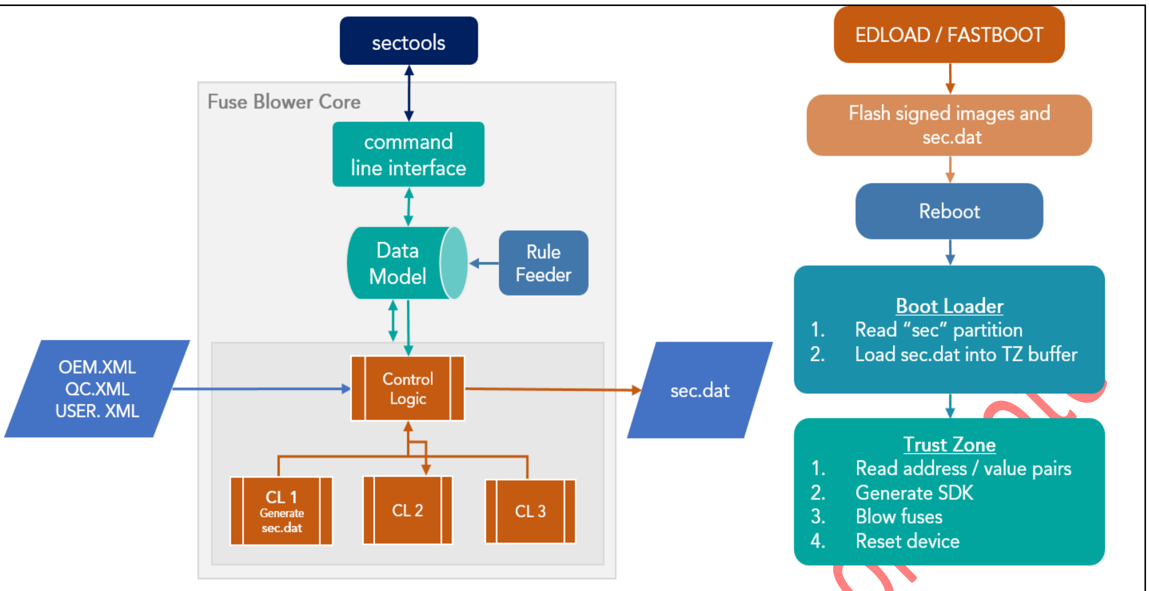

Figure 9: Fuse Provision

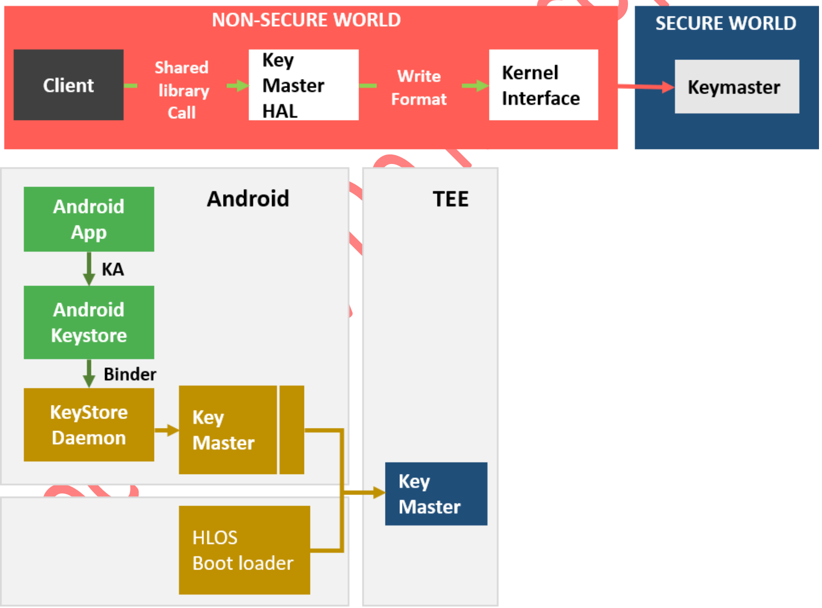

Figure 10: Key master

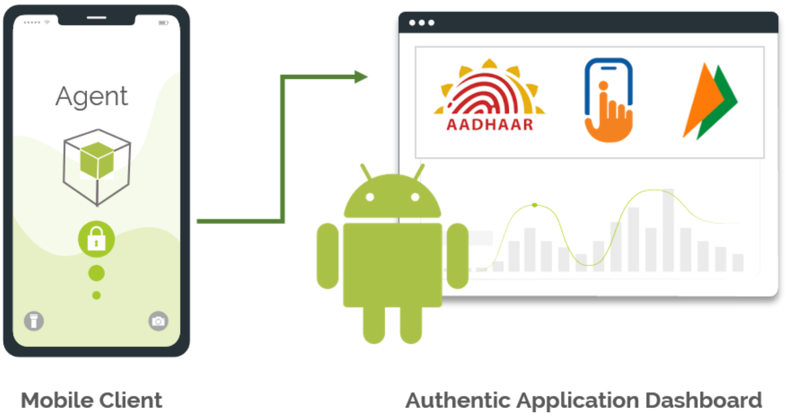

Figure 11: Agent to filter genuine government applications

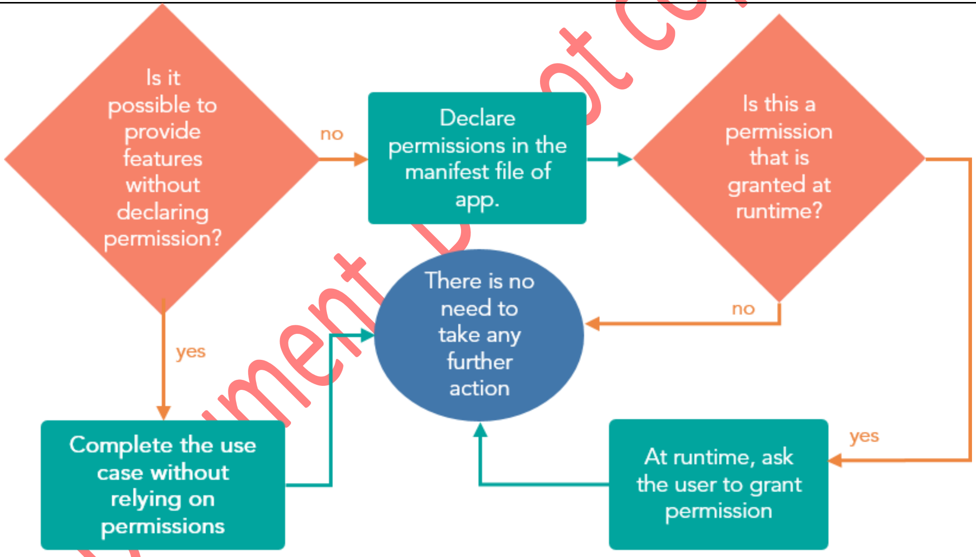
Is it possible to provide features without declaring permission?
no
Declare permissions in the manifest file of app.
Is this a permission that is granted at runtime?
yes
There is no need to take any further action
no
Complete the use case without relying on permissions
yes
At runtime, ask the user to grant permission

Figure 12: Application Permission accessing model

Annexure F: Identifying SIM/eSIM and its respective contents.

SIM/eSIM is not only a standalone entity but it is an internal part of the network. This is secured storage of algorithms, authentication keys as well as the keys for services running for encryption and decryption on subscriber mobile device.

The SIM/eSIM operating system shall be secure software for the secure operation in the SIM/eSIM ecosystem. It decides the responses, queried from smart terminals. Only the Operating system knows the location of secret keys and how they could be used.

(A) Critical Assets on SIM/eSIM:

Critical content securely injected in SIM category (a, c) e.g. OS, Network Profile, Secure Domain, Static Applications and respective Security Keys at Factory.

Whereas in GSMA Embedded SIM (Category b), Operating System, boot strap connectivity profile, eSIM security certificate is personalized in factory and at the time of activation of eSIM, network profile, security keys, security domains and respective security, application are prepared in MNO (SM-DP, SM-SR)/SMDP+) and further downloaded securely to the respective eSIM.

Assets are security-relevant elements to be directly protected. Confidentiality of assets is always intended with respect to un-trusted people or software, as various parties are involved during the first stages of the smart card product life cycle. SIM assets are classified in to two categories:

(i) Direct Assets:

(a) Authentication Keys Ki/OPC etc.

(b) Operator Constants XORing constants & Rotational Constants

(c) Administrative PIN & End-user PIN

(d) Remote File System, Remote Service provisioning and Application Management Keys

(e) SIM/eSIM Identity i.e. ICCID & IMSI, eID

(f) SIM/eSIM certificates

In Figure 5, one can see explanation of SIM critical direct assets

(ii) Indirect Assets

(a) Maximum Authentication Counter

(b) Network Access Algorithm

(c) PIN Management

(d) File System access (Read/Update)

(e) Remote File & Applet Management algorithm

(f) Remote Service provisioning (RSP) and Profile Management

(B) Functions of SIM Card Operating System.

The fundamental functions of the Card Operating System, which provide standard functionality across smart card products are:

(i) Communication between the card and outside world Management of interchanges between the card and the outside world, primarily in terms of the interchange protocol.

(a) Mechanism to manage crucial data and files held in memory via terminals or Remote management. (OTA)

(b) Management of network profile and their activation – GSMA Remote Service Provisioning.

(c) Authenticated access to crucial information and functions (examples include selection of file, Selection of network profile, activation of network profile, access data to write and read).

(d) Access to Cryptographic algorithms along with management of security of the card.

(e) Provide data reliability from the perspective of consistency and error recovery

Annexure G: SIM/eSIM Operations & Certification bodies

SR.No	Entities for M2M/GSMA eSIM and ESIM	Function	Recommended Certificate bodies
1	SIM - Category (a) and category (c)	Procuring UICC and developing Operating System. Standard Algorithms or Customer specific algorithm with security keys and testing	- GSMA SAS, - Trusted Electronic Value Chain Certificate Scheme (TEVCCS) (following National Policy of Electronics 2019) certified by STQC, - ISO 27001, Certified Physical and logical security - Protection Profile from common criteria community or GSMA - OS development shall be in India and in case OS is from foreign land, its functional testing and security testing shall be in India. - Manufacturing and Personalization shall be in India following SIM/eSIM SOPs - UICC security according to UICC ITSAR

SR.No	Entities for M2M/GSMA eSIM and ESIM	Function	Recommended Certificate bodies
2	GSMA eSIM Manufacturer as in category (b)	Procuring UICC and developing Operating System, putting PKI certificates and boot profile for very first connectivity	- GSMA SAS, - Trusted Electronic Value Chain Certificate Scheme (TEVCCS) (following National Policy of Electronics 2019) certified by STQC.ISO 27001, Certified Physical and logical security - Protection Profile from common criteria community or GSMA - OS development, Boot Profile and PKI certificate might be in India - Manufacturing and personalization might be in India.
3	Network IT Infrastructure	SM-DP, SM-SR for M2M Business. SM-DP+ SM-DS and LPA (Local profile Assistant) for Consumer device 3GPP OTA services (Remote File Management and Remote Applet Management)	- GSMA SAS certification. - ISO 27001 - Trusted Electronic Value Chain Certificate Scheme (TEVCCS) (following National Policy of Electronics 2019) certified by STQC. Network IT infrastructure Shall be India
4	OEM	OEM Manufacturer FOTA services	- Trusted Electronic Value Chain Certificate Scheme (TEVCCS) (following National Policy of Electronics 2019) certified by STQC. - Protection Profile from common Criteria community. - FOTA service IT Infrastructure Shall be India.

Annexure H: SIM assets descriptions & their Owner

SR.No		Content		Descriptions	Owner
Software on SIM	1	Operating System	OS	Smart card operating system, responsible to manage all executions/Process in smart card	SIM Manufacturer
	2	Auth. Algorithm Crypto Algorithms	Algorithm	A3/A8, MILENAGE and TUAK specified by 3GPP/GSMA or telecoms operator specific proprietary algorithms	SIM Manufacturer/ MNO/OEM
	3	Applications	Security Domain	SIM Applications for specific usage	Application owner
Security Keys common to SIM and Network	1	Identification	ICCID/eID	Physical SIM/embedded SIM identification stored in SIM	MNO/OEM
			IMSI	Subscriber identification in network stored in SIM	MNO/OEM
	2	Authentication keys Certificates	KI/OPC/others	Key used for authentication to the network	MNO**/OEM
			OTA RSP	Key to SIM Content management and service provisioning	MNO**/OEM
	3	Data Protections Keys	PINs PUKs	To protect the data like phone books etc. To unblock the PINs	MNO**

Annexure I: Informative List of Mobile Device Make/Brand

SR.No	Make/Brand	Country of origin
1	10.Or	China
2	A&K	UK
3	Acer	Taiwan
4	Adcom	India
5	AGM	China
6	Aiek	India
7	Alcatel	France
8	Alco	USA
9	Anee	India
10	iPhone	USA
11	Aqua Mobile	Canada
12	Archos	France
13	A-Star Zest	India
14	ASUS	Taiwan
15	Billion	Taiwan
16	Black Bear	India
17	Black Shark	China
18	BlackBerry	Canada
19	BlackView	China
20	BlackZone	India
21	Blaupunkt	Germany
22	Bloom	India
23	BLU	USA
24	Bluboo	Hong Kong
25	BQ	Spain
26	Brandsdaddy	India
27	CAT	USA
28	Celkon	India
29	Cellecor	India
30	Centric	India
31	Champion	USA
32	Cheers	USA
33	Citycall	India
34	Clout	India
35	Colors Mobile	China
36	Comio	China
37	CoolPad	China
38	Dami	China
39	Darago	China

SR.No	Make/Brand	Country of origin
40	Datawind	Canada
41	Dazen	China
42	Detel	India
43	Do	China
44	Doogee	Spain
45	Douzo	India
46	Easyfone	India
47	Edge	USA
48	EL	China
49	Elari	Russia
50	ELephone	China
51	Energizer	France
52	F- Fook	China
53	Forme	China
54	Fox	India
55	FRND	India
56	Gamma	UK
57	Gfive	China
58	Gionee	China
59	GLX	China
60	Gome	China
61	Good One	China
62	Google	USA
63	Green Berry	China
64	Haier	China
65	HEEMAX	India
66	Hi- Tech	India
67	Hi-Cell	India
68	HOMTOM	China
69	Honor	China
70	HPL	India
71	HSL	India
72	HTC	Taiwan
73	Huawei	China
74	Hyve	South Africa
75	i-Air	India
76	Iball	India
77	Ikall	India
78	Infinix	China
79	InFocUSA	USA

SR.No	Make/Brand	Country of origin
80	Innelo	India
81	Inovu	India
82	Inoyo	India
83	Intex	India
84	Iqoo	China
85	I-Smart	Thailand
86	Itel	China
87	IVooMi	Hong Kong
88	Ivvo	China
89	Jivi	India
90	Josh	India
91	Kara	India
92	Karbonn	India
93	Kechao	China
94	Kenxinda	India
95	Kingstar	India
96	Kult	India
97	KXD	China
98	Lava	India
99	Leagoo	China
100	LeEco	China
101	Leevo	India
102	Lemon	China
103	Lenovo	China
104	Lephone	China
105	LG	South Korea
106	Lianke	China
107	Lvtel	China
108	Lyf	India
109	Mafe	India
110	MarQ	China
111	Maxx	China
112	Maze	India
113	MBO	India
114	Megus	India
115	Meizu	China
116	Mfone	Cambodia
117	M-Horse	Malaysia
118	Mi-Tribe	Mauritius
119	Microkey	China

SR.No	Make/Brand	Country of origin
120	MicroMax	India
121	Microsoft	USA
122	Mobiistar	Vietnam
123	Monix	India
124	Motorola	USA
125	Mphone	Philippines
126	M-Tech	India
127	MTS	Russia
128	MU Phone	China
129	Mymobi	India
130	Nexian	Indonesia
131	Nextbit	USA
132	Nipda	China
133	Nocafone	India
134	Nokia	Finland
135	Nubia	China
136	NUU	USA
137	Nuvo	India
138	Obi	USA
139	OKWU	India
140	OneplUSA	China
141	Onida	India
142	Oppo	China
143	OptimaSmart	China
144	Otho	India
145	Panasonic	Japan
146	Penta	Slovakia
147	Phicomm	China
148	Philips	Netherlands
149	Phonemax	China
150	POCO	China
151	QFX	India
152	Qin	China
153	Rage	China
154	Razer	Singapore
155	Reach	India
156	Realme	China
157	Jio	India
158	Ringing Bells	India
159	Rio Mobile	India

SR.No	Make/Brand	Country of origin
160	Rokea	China
161	Salora	Finland
162	Samsung	South Korea
163	Scosmos	India
164	Seeken	Dubai
165	SeniorWorld	India
166	Sharp	Japan
167	SICT	China
168	Skywin	India
169	Smartron	India
170	Sony	Japan
171	Spice	India
172	SSKY	China
173	STK	UK
174	Subor	China
175	Sugar	France
176	Swipe	India
177	Takee	China
178	Tambo	China
179	Tara	India
180	Tashan	India
181	TCL	China
182	Tecno	China
183	Titan	India
184	T-Max	South Korea
185	Tork	Sweden
186	TP-Link	China
187	Trio	India
188	T-Series	India
189	Tymes	India
190	Ui Phones	China
191	Ulefone	China
192	UMIdigi	China
193	UNI	China
194	Unifone	China
195	Uniscope	China
196	Viaan	India
197	Videocon	India
198	Vinner	India
199	Vivo	China

SR.No	Make/Brand	Country of origin
200	Voto	China
201	Vox Mobile	Serbia
202	Wham	India
203	White Cherry	China
204	Wishtel	India
205	Xccess	India
206	Xillion	China
207	Xiaomi	China
208	XOLO	India
209	Yu	India
210	Yuho	China
211	Yxtel	India
212	Zen	India
213	Ziox	India
214	Zopo	China
215	ZTE	China

The above list is indicative only, non-exhaustive and not in any particular order.

Annexure J: Informative List of Some Mobile Security Testing Tools

Mobile Security Static Testing Tools			
SR.No	**Name**	**Open-Source Availability**	**Language Supported**
1	Microfocus Fortify Static Code Analyzer	No (HP)	Android, Java, C, C# etc.
2	PVS-Studio	No	Multiple (Supports Windows, Linux and MacOS platform)
3	Coverity Scan	Open Source (Synopsys)	Multiple
4	Mobile Security Framework	No	Android
5	QARK (Quick Android Review Kit)	Open-Source	Android
6	MARA Framework	Open-Source	Android
7	SonarQube	Open-Source	More than 20
8	Frama-C	Open-Source	C
9	Semmle	Open-Source	C and Java
10	PMD	Open-Source	C/C++, Java, JavaScript
11	FindBugs	Open-Source	Java
12	FlawFinder	Open-Source	C/C++ (UNIX)
13	OWASP Orizon	Open-Source	J2EE web applications, Android code.
14	CLANG Static Analyzer	Open-Source	C/C++

Mobile Security Dynamic Testing Tools	
SR. No.	**Name**
1	Burp Suite (Crawler, Scanner, Proxy)
2	HCL AppScan
3	Mobile Security Framework
4	Microfocus Fortify
5	Android Debug Bridge
6	Drozer

Annexure K: Informative List of Some Mobile Forensic Tools

Some Mobile Forensic Tools	
SR.No	**Name of Tool**
1	CELLEBRITE UFED TOUCH 2
2	CELEBRITE UFED 4PC
3	CELEBRITE MOBILYZE (BLACK BAG)
4	CELEBRITE PHYSICAL ANALYSER
5	MOBILeDIT FORENSIC EXPRESS PRO
6	MSAB XRY/XAMN/OFFICE
7	OXYGEN FORENSIC SUIT/DETECTIVE8
8	ELCOMSOFT MOBILE FORENSIC BUNDLE (BUNDLE CONTAINS ALL TYPES OF RECOVERY INCLUDING iOS)
9	FINAL MOBILE FORENSICS (RECOVERS DELETED DATA)
10	SUSTEEN SECURE VIEW ADVANCED MOBILE FORENSICS
11	BELKASOFT EVIDENCE CENTRE
12	PARABEN E3 (ELECTRONIC EVIDENCE EXTRACTER) UNIVERSAL
13	MAGNE AXIOM
14	AUTOPSY
15	MCMSOLUTIONS DETEGO MD
16	DB BROWSER FOR SQLITE
17	ANDRILLER
18	HANCOM MDNEXT/MDRED
19	PC 300 FLASH
20	TEEL TECHNOLOGIES CHIP OFF KIT
21	PROJECT A PHONE, ZRT2, ECLIPSE 3 Pro Kit

Annexure L: Format of Primary responsibility of a technology component to fulfill specific security goal

Security Goals	Technology Components																			
	Mobile Device	SIM	Mobile Application	API	Interface	Storage Device	Display Processor	Computing Processor	Communication Processor	Media Processor	Security Processor	Trusted Execution Environment	Sandboxing	Access Router	Network Router	Gateway	Web Server	Application Server	Sensors	Testing Tools
Confidentiality																				
Integrity																				
Availability																				
Authentication																				
Authorization																				
Non-Repudiation																				
Access Control																				
Traceability																				
Accountability																				
Trust																				
Reliability																				

Annexure M: Format for identifying primary responsibility of an entity to fulfil specific security goals

Format for identifying primary responsibility of an entity to fulfil specific security goals									
Security Goals	Entities								
	Manufacturers (M)	Developers (D)	Service Providers (S)	Network Providers (N)	Regulators (R)	Testers (T)	Researchers (R)	Mobile Users (U)	Others (O)
Confidentiality									
Integrity									
Availability									
Authentication									
Authorization									
Non-Repudiation									
Access Control									
Traceability									
Accountability									
Trust									
Reliability									

Annexure N: Format of Security Controls on Device, Communication and Service

Security Goals	Format on Security Controls on								
	Device			Communication			Service		
	Basic	Foundational	Advanced	Basic	Foundational	Advanced	Basic	Foundational	Advanced
Confidentiality									
Integrity									
Availability									
Authentication									
Authorization									
Non-Repudiation									
Access Control									
Traceability									
Accountability									
Trust									
Reliability									

Annexure O: Contact Address

<table>
<tr><th colspan="3">Contact Address for Comments, Suggestions and Feedback</th></tr>
<tr><td colspan="3"><b>Please send email with Subject “MSG” to Ms. Pallavi Dhanvijay with CC to:</b></td></tr>
<tr><td>Ms. Pallavi Dhanvijay
pallavid@cdac.in</td><td>Mr. A.K. Upadhyaya
akupadhyay@stqc.gov.in</td><td>Prof. V. N. Sastry
vnsastry@idrbt.ac.in</td></tr>
</table>