Subject: ***Notice for seeking stakeholder inputs on the DFC (Draft For Comment) of Indian Telecom Security Assurance Requirements (ITSAR) for Vehicle Tracking Device***

Dear Stakeholders,

In exercise of the powers conferred by Section 7 of the Indian Telegraph Act, 1885 (13 of 1885), the Central Government amended the Indian Telegraph Rules, 1951 to insert Rule 528 to 537 in Part XI under the heading Testing & Certification of Telegraph. The new rules provide that every telecom equipment must undergo prior mandatory testing and certification.

2. Telecom Engineering Centre (TEC) came out with Procedure for Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) in December 2017. The MTCTE document outlines the procedure to operationalise the new Rules.

3. The testing and certification described in the MTCTE procedure document requires that the equipment meets the Essential Requirements (ER). Security Requirement is part of ER for which the equipment must be tested and certified against. The responsibility for framing Security requirements and for Security testing and certification lies with National Centre for Communication Security (NCCS), a centre under Department of Telecommunications headquartered at Bengaluru.

4. Security Assurance Standards (SAS) vertical under NCCS is responsible for drafting and finalizing ITSARs for communication equipment. In this regard, an online meeting is scheduled for discussion with the stakeholders (TSPs, M2M service providers, Application service providers, Device manufacturers, OEMs, prospective labs, industry bodies, and academia) on the Draft ITSAR for **Vehicle Tracking Device.** The details of the online meeting and registration link are as follows:

- Date of meeting: **To be notified soon**
- Registration link: will be shared later

The comments received from stakeholders will form the basis for discussion. Stakeholders are hereby requested to participate in the above meeting & send their suggestions/comments/inputs to the following e-mail addresses on or before **21.04.2023**

Shri R. Babu Srinivasa Kumar Director (SAS-II), NCCS - dirnccs5.bg-dot@ gov.in
2) Ms. Mounika Adepu ADET-I (SAS-II), NCCS - adet1sasf.nccs-dot@gov.in

In case of any queries, Please call Sh. R. Babu Srinivasa Kumar, at +91 9444000960 or Ms. Mounika Adepu at +91 77804 39890

Thanks and regards

R. Babu Srinivasa Kumar
Director (SAS-II)
O/o Sr DDG(NCCS), NCCS, DoT, Bengaluru-27.

सत्यमेव जयते

Indian Telecommunication Security Assurance Requirements (ITSAR)

Vehicle Tracking Device

(Consumer IoT Category)

NCCS
Securing Networks

[1]

Draft for Comments

Release Date: Version: 1.0.0

Enforcement Date:

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

[1]

About NCCS

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

Document History

Sl. No	ITSAR Reference	Title	Remarks
1			

Contents

A. Outline

The objective of this document is to present comprehensive, country-specific security requirements for the Vehicle Tracking Device. A Vehicle Tracking Device uses satellite-based location technology to determine and record the precise location of a vehicle at regular intervals. The location data so determined can be stored within the device, and/or can be transmitted to the Backend Control Centre using a wireless communication modem built in the device.

There are various international standardisation bodies/associations working on the security aspects, relevant to the IoT devices security and the specifications produced by these various regional/ international standardisation bodies/ organisations/associations like ISO, ETSI, NIST, IoTSF, Agelight, GSMA, ENISA and OWASP along with the country-specific security requirements from TEC ER, BIS, AIS are the basis for this document.

This document commences with a brief description of vehicle tracking device architecture, and then proceeds to address the common and device entity security requirements of vehicle tracking device.

B. Scope

This document targets the security requirements of the vehicle tracking device for consumer use mentioned in TEC ER NO. TEC28732108 4.1.3. As per BIS IS 16833: 2018, vehicle tracking devices are classified into following three use cases.
a) ATD with an integrated emergency system.
b) ATD with an integrated emergency system and fare metre.
c) CCTV system with in-built tracking system and integrated emergency system.

This document applies to vehicle tracking devices intended to be used in Private transport vehicles. Therefore, the security requirements are applicable to the automotive tracking device (ATD) with an integrated emergency button system.

C. Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above.

Chapter 1 – Overview

1.1 Introduction: Vehicle tracking Device is an emerging technology and is very much in use for public transport. With increasing theft rate, vehicle security has become one of the biggest consumer concerns and therefore use of vehicle tracking devices for consumer vehicles is encouraged. A consumer vehicle tracking device uses Global Navigation Satellite System (GNSS) and provides real-time information about a vehicle's location all the time with digital maps.

ATD with an integrated emergency system: - In this type of vehicle tracking system the device provides the position, speed, direction of travel and time to a network communication centre as well as there is an embedded emergency button which when pressed sends an alert to the endpoint device or to the designated authority.

Most of the vehicle tracking devices are both active and passive since they can track in real-time as well as store the tracking information for some time period into the device which can be downloaded for future analysis.

1.2 explains how a vehicle tracking device works in real-time.

1.2 Scenario: Following is a scenario for a typical vehicle tracking for private use presuming that a private vehicle has been deployed with a vehicle tracking device.

The vehicle owner wishes to track the vehicle, that is, wants to know the location, fuel level, speed of the vehicle etc. The tracking device gathers all such information and uses Global Positioning System (GPS) satellites to know the location of the vehicle and transmits the data using wireless or cellular network. Through the network provider the data travels to the server which processes the data and allows the owner to access the tracking details.

[Ref: ETSI TR 102 898 V 1.1.1]

1.3 Vehicle Tracking Device architecture: VTD architecture can be divided into two parts:-

Endpoint Ecosystem:

1. A simple Graphic User Interface (GUI) that allows a user to:
   - Log in with a username and password
   - Disable tracking
   - Enable tracking
   - Identify and visualise current location

2. A cellular module for connecting to back-end services
3. A SIM card for the cellular module
4. A Lithium-Polymer battery for back-up power
5. A Central Processing Unit (CPU)
6. An embedded application in Non-Volatile RAM
7. RAM
8. EEPROM

Service Ecosystem:

1. Cellular Data connectivity
2. Secure Private APN
3. Service Access Point
4. Cellular Modem OTA management service
5. SIM Card OTA management service

This document briefly covers the security requirements for the endpoint ecosystem only. The security requirements for the service ecosystem is beyond the scope of this document.

Chapter 2 – Common Security Requirements

Section 1: Authentication

1.1 Requirement:

Devices shall have authentication and authorization schemes (unique per device) based on the system-level threat models.

[Ref: ENISA Baseline recommendations for IoT November 2017, GP-TM-21]

1.2 Requirement:

Authentication credentials shall be salted, hashed, and/or encrypted. Authentication credentials, including but not limited to user passwords, shall be salted, and hashed. Applies to all stored credentials to help prevent unauthorized access and brute force attacks.

[Ref: ENISA Baseline recommendations for IoT November 2017, GP-TM-24]

1.3 Requirement:

existing enterprise authenticators and authentication mechanisms should be used device.

[Ref: NIST 8228 Example 11]

1.4 Requirement:

Where a user can authenticate against a device, the device shall provide the user or an administrator with a simple mechanism to change the authentication value used.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-4]

1.5 Requirement:

Authentication mechanisms shall use strong passwords or personal identification numbers (PINs), and shall consider two-factor authentication (2FA) or multi-factor authentication (MFA) like OTP-based, Biometrics, etc., on top of certificates.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-23]

1.6 Requirement:

Manufacturer shall give undertaking that authentication credentials for users, devices, or services are not hardcoded in firmware or ecosystem applications.

[Ref: OWASP ISVS 2.1.9]

1.7 Requirement:

The manufacturer shall give undertaking if Trusted Computing Base has been implemented, the identity is cryptographically authenticated using the TCB.

[Ref. GSMA CLP.12 4.2]

1.8 Requirement:

Manufacturer shall provide generally accepted username and password recovery mechanisms using multi-factor verification and authentication and shall provide notification of password and/or user ID reset or changes utilizing secure authentication and /or out-of-band notice(s).

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 15 and 17]

1.9 Requirement:

Brute force attacks shall be impeded by introducing escalating delays following failed user account login attempts, and/or a maximum permissible number of consecutive failed attempts.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.13.15, 2.4.8.7, ENISA Baseline security recommendations for IoT November 2017 GP-TM-25]

1.10 Requirement:

The device shall have a limitation on the number of authentication attempts within a certain time interval. It shall also use increasing time intervals between attempts.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-5 Example 6]

1.11 Requirement:

The client application shall be able to lock an account or to delay additional authentication attempts after a limited number of failed authentication attempts.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-5 Example 7]

1.12 Requirement:

The device shall authenticate each user and device attempting to logically access it.

[Ref: NIST 8228 Expectation 10]

1.13 Requirement:

Entity's identity shall be authenticated before granting access if the entity is a human (e.g., PIN, password, passphrase, two-factor authentication) or system/device (e.g., API keys, certificates).

[Ref: NIST 8259 Activity 3]

1.14 Requirement:

Devices shall provide notice and/or request user confirmation when pairing, onboarding, and/or connecting with other devices, platforms, or services.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 19]

1.15 Requirement:

Mutual authentication shall be used

[Ref: GSMA CLP.13 7.6]

1.16 Endpoint Password Management

1.16.1 Requirement

Where passwords are used and, in any state, other than the factory default, all consumer device passwords shall be unique per device or defined by the user. If password-less authentication is used, the same principles of uniqueness apply.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-1, IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.3]

1.16.2 Requirement:

Where pre-installed unique per-device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-2]

1.16.3 Requirement:

Where a user interface password is used for login authentication, the factory issued or reset password shall be randomly unique for every device in the product family.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.3]

1.16.4 Requirement:

Provisioned credentials such as username for device authentication shall be unique per device.

[Ref: OWASP ISVS 2.1.10]

1.16.5 Requirement:

The default passwords and even default usernames shall be changed during the initial setup, and that weak, common, null, or blank passwords shall not be allowed.

[Ref: ENISA Baseline security recommendations for IoT November GP-TM-22]

1.16.6 Requirement:

The product shall allow the factory issued or OEM login accounts to be disabled or erased or renamed when installed or commissioned.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.12]

1.16.7 Requirement:

The product shall support all the factory default user login passwords altered when installed or commissioned.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.13]

1.16.8 Requirement:

The default user or device credentials shall be changed by authorized administrators or end-users.

[Ref: OWASP ISVS 2.1.8]

1.16.9 Requirement:

Multiple user accounts with varied levels of controls shall be created.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-4 example 4 and 5]

1.16.10 Requirement

The product shall not allow new and common passwords containing the user account name with which the user account is associated.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.5]

1.16.11 Requirement

User authentication password change mechanism shall ask for the user's current password.

[Ref: OWASP ISVS 2.1.6]

1.16.12 Requirement

The passwords used for device authentication shall be sufficiently long, complex and shall follow industry practices.

[Ref: OWASP ISVS 2.1.7]

1.16.13 Requirement:

The device shall conceal password characters from display of user credentials on login interfaces when a person enters a password for a device. Device shall disable the use of default or hardcoded passwords.

[Ref: NIST 8228 Expectation 9, IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.15]

1.16.14 Requirement:

Password recovery or reset mechanism should be robust. It should not readily be abused by an unauthorized party or supply any information indicating a valid account.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-26 and IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.14]

1.16.15 Requirement:

Devices shall have thresholds and incremental delays for invalid password attempts Users.

[Ref: GSMA CLP.13 6.9]

Section 2: Identity Management

2.1 Device Identification

2.1.1 Requirement:

The device shall be uniquely identified logically and physically, only authorized entities should have access to the physical identifier, which may or may not be the same as logical identifier.

[Ref: NIST 8259A Device Identification]

2.1.2 Requirement:

The unique logical identifier shall be used for device authentication; however, an appropriate identifier should be used.

[Ref: NIST 8259A Device Identification]

2.1.3 Requirement:

Hard-coded unique per device identity shall be used in a device. It shall resist tampering by means such as physical, electrical or software.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.4.2]

2.1.4 Requirement:

The device shall uniquely identify each user and device attempting to logically access it.

[Ref: NIST 8228 Expectation 8]

2.1.5 Requirement:

The device manufacturer shall ensure that the exposed identity of the device shall not be linked by unauthorized actors to the end user, to ensure anonymity and compliance with relevant local data protection law.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.16.6]

2.1.6 Requirement:

The Service Provider shall not have the ability to do a reverse lookup of device ownership from the device identity.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.16.3]

2.1.7 Requirement:

Root of Trust-backed unique logical identity shall be used to identify them in logs of their physical chain of custody.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.4.12]

2.1.8 Requirement:

The manufacturer shall give an undertaking that all authentication pathways and identity management APIs shall implement consistent authentication security control strength, such that there are no weaker alternatives per the risk of the application.

[Ref: OWASP ISVS 1.2.4]

Section 3: Authorization and access controls

3.1 Requirement:

It shall be ensured that IoT system accounts across users, services and devices share a common authorization framework.

[Ref: OWASP ISVS 2.2.1]

3.2 Requirement:

The application shall enforce access control rules on a trusted service layer, especially if client-side access control shall be present and could be bypassed.

[Ref: OWASP ASVS 4.1.1]

3.3 Requirement:

The access controls shall fail securely, including when an exception occurs.

[Ref: OWASP ASVS 4.1.5]

3.4 Requirement:

Administrative interface shall use appropriate multi-factor authentication to prevent unauthorized use.

[Ref: OWASP ISVS 4.3.1]

3.5 Requirement:

The administration interfaces shall be accessible only by authorized operators. Mutual Authentication over administration interfaces such as certificates.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.10.13]

3.6 Requirement:

Directory browsing shall be disabled unless deliberately desired. Additionally, applications should not allow discovery or disclosure of file or directory metadata, such as Thumbs. db, .DS_Store, .git or .svn folders.

[Ref: OWASP ASVS 4.3.2]

3.7 Requirement:

User and data attributes and policy information used by access controls shall not be manipulated by end users unless specifically authorized.

[Ref: OWASP ISVS 4.1.2]

3.8 Requirement:

Control Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

[Ref: ISO 27001 A.10.1.3]

3.9 Requirement:

The access control privileges shall be defined, justified, and documented.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.10]

3.10 Requirement:

The principle of least privilege shall exist. Users shall only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege.

[Ref: OWASP ASVS 4.1.3]

3.11 Requirement:

The principle of least privilege shall be enforced by limiting applications and services that run as root or administrator.

[Ref: OWASP ISVS 2.2.2]

3.12 Requirement:

The device shall restrict each user, device, and process to the minimum logical access privileges necessary.

[Ref: NIST 8228 Expectation12]

3.13 Requirement:

The product shall support access control measures to the root/highest privilege account to restrict access to sensitive information or system processes.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.8.9]

3.14 Requirement:

The product only allows controlled user account access; access using anonymous, or guest user accounts is not supported without justification.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.11]

3.15 Requirement:

Data integrity and confidentiality shall be enforced by access controls with a defined security policy.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-29]

3.16 Requirement:

Authorized access to device debug capabilities shall be in place along with monitoring and logging such access.

[Ref: OWASP ISVS 2.2.4]

3.17 Requirement:

The product or service shall record audio/visual/or any other data in accordance with the authorization of the user only, no passive recording without explicit authorization shall be done.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.12.14]

3.18 Requirement:

Control Media shall be disposed of securely and safely when no longer required, using formal procedures.

[Ref: ISO 27001 A.10.7.2]

3.19 Requirement:

Control Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.

[Ref: ISO 27001 A.10.7.3]

3.20 Requirement:

Control System documentation shall be protected against unauthorized access.

[Ref: ISO 27001 A.10.7.4]

3.21 Requirement:

The OEM shall provide an undertaking to retain authorization of secure production control methods to prevent a third-party manufacturer (CEM etc.) from producing overproduction and/or unauthorized devices.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 4.14.22]

3.22 Requirement:

The product allows an authorized and complete factory reset of all the device's authorization information.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.16]

3.23 Requirement:

The ownership shall be validated upon registration and as part of decommissioning when devices move across accounts (e.g., device reselling, leasing, and renting)

[Ref: OWASP ISVS 2.2.3]

Section 4: Securely storing sensitive information

4.1 Requirement:

There shall be a process for the secure provisioning of security parameters and keys that includes random and individual (unique) generation, distribution, update, revocation, and destruction.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.9.3]

4.2 Requirement:

Sensitive security parameters in persistent storage shall be stored securely by the device.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.4-1]

4.3 Requirement:

Security parameters and passwords shall not be hard-coded into source code or stored in a local file.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.5]

4.4 Requirement:

For unconstrained devices, sensitive data such as private keys and certificates should be stored leveraging dedicated hardware security features.

[Ref: OWASP ISVS 5.1.4]

4.5 Requirement:

Sensitive information, such as personal identifiable information (PII) and credentials shall be stored securely using strong encryption to protect from data leakage and integrity checking to protect against unauthorized modification.

[Ref: OWASP ISVS 2.3.1]

4.6 Requirement:

The product shall securely store any passwords using an industry-standard cryptographic algorithm.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.8]

4.7 Requirement:

Passwords shall be stored in a form that is resistant to offline attacks. Passwords shall be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash.

[Ref: OWASP ASVS 2.4.1]

4.8 Requirement:

Salt shall be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash shall be stored.

[Ref: OWASP ASVS 2.4.2]

4.9 Requirement:

If PBKDF2 is used, then the iteration count should be as large as verification server performance will allow, typically at least 100,000 iterations.

[Ref: OWASP ASVS 2.4.3]

4.10 Requirement:

If bcrypt is used, then the work factor should be as large as the verification server performance will allow, with a minimum of 10.

[Ref: OWASP ASVS 2.4.4]

4.11 Requirement:

An additional iteration of a key derivation function shall be performed using a salt value that is secret and known only to the verifier. The secret salt value shall be stored separately from the hashed password.

[Ref: OWASP ASVS 2.4.5]

4.12 Requirement:

UICC should be used for tamper-resistant storage of sensitive data for services, including security keys controlled by the service provider.

[Ref: GSMA CLP.14 5.1-1.4]

4.13 Requirement:

The unique identifier should be stored in the TCB's trust anchor.

[REF: GSMA CLP.13 6.6]

4.14 Requirement:

Critical sections of the memory should be locked.

[REF: GSMA CLP.13 5.4 /5.6/6.16]

4.15 Requirement:

Internal memory shall be used for Secrets.

[REF: GSMA CLP.13 5.7/7.1]

4.16 Requirement:

Devices should be provisioned with a cryptographic root of trust that is hardware-based and immutable.

[Ref: OWASP ISVS 1.2.6]

4.17 Requirement:

Devices shall be shipped with readily accessible physical identifiers derived from their ROT-backed IDs. This is to facilitate both tracking through the supply chain and for the user to identify the device-type/model and SKU throughout the support period.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.14.11]

4.18 Requirement:

Tamper resistant Trust Anchor shall be used.

[Ref: GSMA CLP.13 6.3]

Section 5: Make it easy for the user to delete data

5.1 Requirement:

The user shall be provided with functionality such that user data can be erased from the device and associated services in a simple manner.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.11-1, 11-2]

5.2 Requirement:

Clear instructions shall be provided to the users on how to delete personal data.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.11-3]

5.3 Requirement:

The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all personal information from the device and any associated services.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.12.11]

5.4 Requirement:

Users shall be provided with clear confirmation that personal data has been deleted from services, devices, and applications.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.11-4]

5.5 Requirement:

The user shall have the ability to perform a factory reset, including the ability to delete all user data in the event of device transfer, rental, loss, or sale to a third party.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 34]

5.6 Requirement:

The device shall have the ability for the user to delete or make anonymous, personal, or sensitive data stored on company servers (other than purchase transaction history).

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 33]

5.7 Requirement:

The manufacturer should minimize the data collected and retained. Stakeholders should delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion shall take place at the nearest point of data collection of raw data (e.g., on the same device after processing).

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-12]

5.8 Requirement:

An end-of-life disposal process shall be provided to ensure that retired devices are permanently disconnected from their cloud services and that any confidential user data is securely erased from both the device and the cloud services.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.24]

Section 6: Data Protection

6.1 Consumer Intimation Policy

6.1.1 Requirement:

The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 6-1]

6.1.2 Requirement:

Provide a Short Contextual Privacy Notice at the point at which an individual is asked to use personal data attributes for the purposes of the IoT service, and that notifies the user of:

–identity of controller
–data to be processed
–data uses (unless obvious from context)
–how to contact the controller, especially regarding how to exercise privacy rights.

[Ref: GSMA CLP.11 PDR1.1]

6.1.3 Requirement:

The product or service shall only record audio/visual/or any other data in accordance with the authorization of the user (e.g., no passive recording without explicit authorization).

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.14]

6.1.4 Requirement:

Data processed by a third-party shall be protected by a data processing agreement. (Undertaking)

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-OP-12]

6.1.5 Requirement:

The Product Manufacturer or Service Provider shall ensure that a detailed data retention policy is in place, documented for users. The same shall be disclosed to users.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.12.5]

6.1.6 Requirement:

There shall be a method or methods for each user to check/verify what personal information is collected.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.12.7]

6.2 Consent Management

6.2.1 Requirement:

The users shall be provided in clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.

[Ref: OWASP ASVS 8.3.3]

6.2.2 Requirement:

The Product Manufacturer shall conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used. The user shall have the ability to opt-in for any other purposes.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 22]

6.2.3 Requirement:

The user shall be prompted to opt-in or opt out of sharing data, the benefits or consequences shall be clearly and objectively explained, including any potential impact to product features or functionality.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 30]

6.2.4 Requirement:

If user credential or 'identity' is used to track the profile of an individual for the purpose of gaining insights into product use and targeting of commercial products - then consent of the user shalll be mandatory.

[Ref: GSMA CLP.11 PDR 1.7]

6.2.5 Requirement:

Use clear language and text/images appropriate to the target audience and context to ensure the user understands what is being asked of them and what they are agreeing to. Local language should also be considered.

[Ref: GSMA CLP.11 PDR 1.9]

6.2.6 Requirement:

Users shall be notified of the 'purpose' of data processing in a privacy policy.

[Ref: GSMA CLP.11PDR2.4]

6.2.7 Requirement:

Personal data shall be collected and processed fairly and lawfully, it should never be collected and processed without the user's consent.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-10]

6.2.8 Requirement:

Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 6-3]

6.2.9 Requirement:

The personal data shall be used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects shall be informed.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-11]

6.2.10 Requirement

Users of IoT products and services shall be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing and objection to processing.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-14]

6.2.11 Requirement:

Consumers personal data to be shared with third parties shall require consent of the consumers, unless otherwise required and limited for the use of product features or service operations.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-13]

6.2.12 Requirement:

If relying on consent, granular choices should be provided– do not bundle consent – and ensure individuals are aware of the persistence of consent and how to revoke it.

[Ref: GSMA CLP.11 PDR1.3 and PDR 1.4]

6.2.13 Requirement:

Evidence of consent and its revocation shall be captured and retained.

[Ref: GSMA CLP.11PDR 1.4]

6.2.14 Requirement:

Users should choose the presentation of their identity and only require the presentation of personal identifiers where unavoidable (such as a MSISDN, or name or email address).

[Ref: GSMA CLP.11 PDR 2.1]

6.2.15 Requirement:

The manufacturer shall prevent the unauthorized linking of identifiers and authentication protocols across different services. Limit the tracking of identifiers or user behavior to that necessary to provide or protect a service (such as authentication and authorization).

[Ref: GSMA CLP.11 PDR2.2 and PDR 2.7]

6.2.16 Requirement:

The manufacturer shall provide individuals with the opportunity to determine their IoT service 'identity' and the personal data and attributes used in the creation and presentation of such identities.

[Ref: GSMA CLP.11 PDR 3.1]

6.2.17 Requirement:

The manufacturer shall provide individuals with the means to associate, disassociate and re-assign their IoT service identities.

[Ref: GSMA CLP.11 PDR 3.3]

6.2.18 Requirement:

Processing of personal data (such as it is necessary for performance of a contract to give access to an account and data, or consent) shall be identified on a legal basis.

[Ref: GSMA CLP.11 PDR 1.2]

6.3 Requirement:

Personal Information shall be anonymized whenever possible and, in particular, in any reporting.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.6-1]

6.4 Requirement:

The product or service should be made compliant with the local and/or regional Personal Information protection legislation where the product is to be sold.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.12.8]

6.5 Requirement:

The manufacturer shall identify any legal obligation to provide notices in a specific language or languages.

[Ref: GSMA CLP.11 PDR 1.8]

6.6 Requirement:

The supplier or manufacturer shall submit an undertaking on performing a privacy impact assessment (PIA) to identify Personally Identifiable Information (PII) and design approaches for safeguarding user privacy compliant with the legal requirements of the user's location. This should extend to data gathered via Web APIs from third party platform suppliers.

6.7 Requirement:

A control policy which is in compliance with the regulatory requirements shall be in place to manage PII.

[NIST 8228 Expectation 25]

6.8 Requirement:

The manufacturer shall identify the legal basis for processing special categories of personal data such as biometrics.

6.9 Requirement:

An internal compliance programme, policies, procedures, and practices shall be established to ensure compliance and on-going oversight and redress for the remediation of non-compliances and identified privacy risks.

[Ref: GSMA CLP.11 PDR 8.2]

6.10 Minimize the Data Collected and Retained

6.10.1 Requirement:

The application shall minimize the number of parameters in a request, such as hidden fields, cookies and header values.

[Ref: OWASP ASVS 8.1.3]

6.10.2 Requirement:

The product or service shall store the minimum amount of Personal Information from users required for the operation of the service

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.12.1]

6.10.3 Requirement:

Sensitive personal information shall be subject to data retention classification, such that old or out-of-date data is deleted automatically, on a schedule, or as the situation requires.

[Ref: OWASP ASVS 8.3.8]

6.10.4 Requirement:

Pseudonymous identifiers shall be used to the extent possible as best practice

[Ref: GSMA CLP.11 PDR 4.1]

6.10.5 Requirement:

Unauthorized entities shall be prevented or restricted from observing and collecting personal data and metadata relating to the use of the IoT service credentials.

[Ref: GSMA CLP.11 PDR 4.3]

6.10.6 Requirement:

Minimum attributes needed to meet a specific IoT use case shall be identified considering the type, sensitivity and granularity of the attributes, volume, frequency of collection, and metadata generation.

[Ref: GSMA CLP.11 PDR 4.4]

6.10.7 Requirement:

The device shall prevent unauthorized access to all sensitive data transmitted from it over networks and on its storage devices.

[Ref: NIST 8228 Expectation 21 and NIST 8228 Expectation 19]

6.10.8 Requirement:

The application shall protect sensitive data from being cached in server components such as load balancers and application caches.

[Ref: OWASP ASVS 8.1.1]

6.10.9 Requirement:

All cached or temporary copies of sensitive data stored on the server shall be protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.

[Ref: OWASP ASVS 8.1.2]

6.11 Backup and Storage

6.11.1 Requirement:

The device shall have a mechanism to support data availability through secure backups.

[Ref: NIST 8228 Expectation 20]

6.11.2 Requirement:

The backups shall be stored securely to prevent data from being stolen or corrupted.

[Ref: OWASP ASVS 8.1.6]

6.11.3 Requirement:

Data stored in browser storage (such as localStorage, sessionStorage, IndexedDB, or cookies) shall not contain sensitive data.

[Ref: OWASP ASVS 8.2.2]

6.11.4 Requirement:

Authenticated data shall be cleared from client storage, such as the browser DOM, after the client or session is terminated.

[Ref: OWASP ASVS 8.2.3]

6.11.5 Requirement:

Users shall have a method to remove or export their data on demand

[Ref: OWASP ASVS 8.3.2]

6.11.6 Requirement:

Sensitive information contained in memory shall be overwritten as soon as it is no longer required to mitigate memory dumping attacks, using zeroes or random data.

[Ref: OWASP ASVS 8.3.6]

6.11.7 Requirement:

The supplier or manufacturer of any devices and/or services shall provide information about how the device removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all personal information from the device and any associated services.

[Ref: OWASP ISVS 2.3.2]

6.11.8 Requirement:

Right to transfer ownership of the device and ability to export data shall be disclosed clearly to the users.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 36]

6.12 Data Quality:

6.12.1 Requirement**:**

System and procedural controls shall be established to verify and maintain the accuracy and reliability of personal data and attributes along with procedural controls to capture and address data corruptions and mismatches.

[Ref: GSMA CLP 11 PDR 5.1 and PDR 5.2]

6.12.2 Requirement:

A process shall be established (free of charge) by which users can update their information and correct any inaccuracies

[Ref: GSMA CLP 11 PDR 5.3]

6.12.3 Requirement:

Process shall be in place to validate and authorize changes in personal information of the user

[Ref: GSMA CLP 11 PDR 5.4]

6.13 Information Security

6.13.1 Requirement:

Security measures to be adopted through the data lifecycle shall be documented**.**

[Ref: GSMA CLP 11 PDR 7.1]

6.13.2 Requirement:

The data shall be transferred securely between all parties involved in the verification or sharing of personal data and attributes. The security should be commensurate to the risks associated with the data types and sensitivity, potential for harm and impact on the user if the data is compromised, and any local regulatory or legal requirement.

[Ref: GSMA CLP.11 PDR 7.3]

6.13.3 Requirement:

If third parties process information on the controller's behalf, the controller shall ensure such 'data processors' adopt appropriate and equivalent security measures.

[Ref: GSMA CLP.11 PDR 7.5]

6.14 Examine system telemetry data:

6.14.1 Requirement:

Subject to user permission, telemetry data from the device should be analyzed for anomalous behavior to detect malfunctioning or malicious activity.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.13.36]

6.14.2 Requirement:

If telemetry data is collected from consumer IoT devices and services, the processing of personal data shall be kept to the minimum necessary for the intended functionality

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 6-4]

6.14.3 Requirement:

If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 6-5]

Section 7: Secure input and output handling

7.1 Input-Output Data Validation

7.1.1 Requirement:

Data input to applications shall be validated to ensure that this data is correct and appropriate.

[Ref: ISO 27001 A.12.2.1]

7.1.2 Requirement:

The device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices. All data being transferred over interfaces shall be validated by checking the data type, length, format, range, authenticity, origin, and frequency where appropriate.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.13-1, IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.10.10]

7.1.3 Requirement:

All inputs and outputs shall be validated using, for example, an allow list (formerly 'whitelist') containing authorized origins of data and valid attributes of such data.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.10.12, 2.4.11.9]

7.1.4 Requirement:

All inputs and outputs shall be checked for validity, e.g., use “Fuzzing” tests to check for acceptable responses or output for both expected (valid) and unexpected (invalid) input stimuli

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.5.23]

7.1.5 Requirement:

Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

[Ref: ISO 27001 A.12.2.2]

7.1.6 Requirement:

Embedded applications shall not be susceptible to OS command injection by performing input validation and escaping of parameters within firmware code, shell command wrappers, and scripts.

[Ref: OWASP ISVS 1.3.15]

7.1.7 Requirement:

Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Validate that data sent to other product components matches specified definitions of format and content.

[Ref: ISO 27001 A.12.2.4, NIST Cybersecurity Whitepaper Interface Access Control 2. a]

7.1.8 Requirement:

URL redirects and forwards shall only allow destinations that appear on an allow list or show a warning when redirecting to potentially untrusted content.

[Ref: OWASP ISVS 5.1.5]

7.1.9 Requirement:

The application shall have defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).

[Ref: OWASP ISVS 5.1.1]

7.1.10 Requirement:

Protection against mass parameter assignment attacks shall be done by frameworks, or the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.

[Ref: OWASP ISVS 5.1.2]

7.1.11 Requirement:

All input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc.) shall be validated using positive validation (allow lists).

[Ref: OWASP ISVS 5.1.3]

7.1.12 Requirement:

Structured data shall be strongly typed and validated against a defined schema, including allowed characters, length, and pattern (e.g., credit card numbers, e-mail addresses, telephone numbers, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).

[Ref: OWASP ISVS 5.1.4]

Section 8: Communicate Securely

8.1 Requirement:

The device shall use best practice cryptography to communicate securely. Such cryptographic algorithms and primitives shall be updateable. Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.5-2, 5.5-3, and 5.5-1]

8.2 Requirement:

The web interfaces shall fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-52]

8.3 Requirement:

The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage. Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk, and usage.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.8-2]

8.4 Requirement:

Any personal data communicated between the web interface/mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption shall be appropriately secure.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.10.19and 2.4.13.35]

8.5 Requirement:

Sensitive data shall be sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.

[Ref: OWASP ASVS 8.3.1]

8.6 Requirement:

If run as a cloud service, the cloud service UDP and TCP-based communications (such as MQTT connections) are encrypted and authenticated using the latest 1.2 or above DTLS and TLS standard.

[Ref: GSMA CLP.14 5.1.1.4 and IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.13.23]

8.7 Requirement:

TLS or equivalent strong encryption and authentication shall be used regardless of the sensitivity of the data being transmitted.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-39]

8.8 Requirement:

Where a product related to a web server encrypted communications using TLS and requests a client certificate, the server(s) shall establish a connection if the client certificate and its chain of trust are valid.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.13.9]

8.9 Requirement:

If TLS is used, then only strong cipher suites shall be enabled, with the strongest cipher suite set as preferred using up-to-date TLS testing tools.

[Ref: OWASP ISVS 4.1.2]

8.10 Requirement:

If TLS is used, then the device shall cryptographically verify the X.509 certificate.

[Ref: OWASP ISVS 4.1.3]

8.11 Requirement:

If TLS is used, then the device's TLS implementation shall use its own certificate store, pins to the endpoint's certificate or public key, and disallows connections to endpoints with different certificates or keys, even if signed by a trusted CA.

[Ref: OWASP ISVS 4.1.6]

8.12 Requirement:

Communications protocols should be latest versions with no publicly known vulnerabilities and/or appropriate for the product. Post product launch, communications protocols shall be reviewed throughout the product life cycle against publicly known vulnerabilities and changed to the most secure versions available if appropriate.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.7.19 and 2.4.7.20]

8.13 Requirement:

If the client server model is used for communication, then the device shall use up to date configurations to enable and set the preferred order of algorithms and ciphers used for communication, using TLS 1.2 or later.

[Ref: OWASP ASVS V9.1]

8.14 Requirement:

Since industry guidelines on secure TLS, Bluetooth, and Wi-Fi change frequently, Security Configuration of the communication protocol shall be periodically checked to ensure that secure communication is always present and effective.

[Ref: OWASP V4: Communication Requirements control object]

8.15 Requirement:

Disable deprecated or known insecure algorithms and ciphers.

[Ref: OWASP V4 Communication requirements control objective]

8.16 Requirement:

Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or shall be stored in the IoT application or in the Cloud.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-38]

8.17 Requirement:

Internal or external traffic shall not expose the device credentials.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-40]

8.18 Requirement:

Protection against replay attacks shall be built into the communication protocol.

[Ref: OWASP ISVS 4.1.1]

8.19 Requirement:

The device shall be restrictive rather than permissive in communicating.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-43]

8.20 Requirement:

The device shall not trust data received and shall always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-42]

8.21 Requirement:

The device shall make intentional connections, shall prevent unauthorized connections to it or other devices the product is connected to, at all levels of the protocols.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-44]

8.22 Requirement:

Specific ports and/or network connections for selective connectivity shall be disabled.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-45]

8.23 Requirement:

Where the application communicates with a product related remote server(s), or device, it shall be done over a secure connection.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.7.19 and 2.4.11.4]

8.24 Requirement:

Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.5-4]

8.25 Requirement:

Device functionality that allows security-relevant changes in configuration via a network interface shall be accessible only after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.
Protocols that are an exception include ARP, DHCP, DNS, ICMP, and NTP.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.5-5]

8.26 Requirement:

End-user security and privacy alerts and communications, including but not limited to email and SMS, shall adopt authentication protocols to help prevent phishing and spoofing and maximize the integrity and privacy of such communications.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 37]

8.27 Requirement:

Devices shall implement transport-level security for email notifications to ensure the privacy of the communication while in transit.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 38]

8.28 Requirement:

Manufacturers shall develop communication and alert processes to maximize user awareness of any potential security or privacy related issue, end of life notifications and possible product recalls, including in-app notifications.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 41]

Section 9: Cryptography

9.1 Requirement:

Devices shall be built to be compatible with lightweight encryption and security techniques that can, on the one hand, be usable on resource-constrained devices, and, on the other hand, be scalable to minimize the management effort and maximize their usability.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-36]

9.2 Requirement:

Proper and effective use of cryptography shall be ensured to protect the confidentiality, authenticity, and/or integrity of data and information (including control messages), in transit and in rest. Proper selection of standard, strong encryption algorithms and strong keys shall be ensured and disable insecure protocols.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-34]

9.3 Requirement:

Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations. Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used.

[Ref: ISO:27001 A.15.1.6]

9.4 Requirement:

A policy on the use of cryptographic controls for the protection of information shall be developed and implemented.

[Ref: ISO:27001 A.12.3.1]

9.5 Requirement:

Cryptographic libraries used shall be certified to be compliant with a recognized cryptographic security standard.

[Ref: OWSAP ISVS 2.4.6]

9.6 Requirement:

All the product related cryptographic functions shall have no publicly known unmitigated weaknesses in the algorithms or implementation, for example MD5 and SHA-1 are not used.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.5]

9.7 Requirement:

All key lengths shall be sufficient for the level of assurance required.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.10]

9.8 Requirement:

In systems with many layered sub devices, key management shall follow best practices. Cryptographic keys shall be securely managed.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.11]

9.9 Requirement:

Secure session shall be established after each disconnected session to prevent intentional and unintentional denial of device [DoS].

[Ref: GSMA CLP.13 9.1]

9.10 Requirement:

Perfect Forward Secrecy (PFS) shall deal with the disclosure of cryptographic keys exchanged during the setup of communications between two Endpoints.

[Ref: GSMA CLP.13 6.18,8.10, 9.4]

9.11 Requirement:

Cryptographic secrets and keys shall be unique per device.

[Ref: OWASP ISVS 2.4.1]

9.12 Requirement:

Secure sources of randomness shall be provided by the operating system and/or hardware for all security needs.

[Ref: OWASP ISVS 2.4.3]

9.13 Requirement:

In device manufacture, all asymmetric encryption private keys that are unique to each device shall be secured. They shall be truly randomly internally generated or securely programmed into each device

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.9]

9.14 Requirement:

There shall be a process for secure provisioning of security parameters and keys that includes random and individual (unique) generation, distribution, update, revocation and destruction.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.3]

9.15 Requirement:

There shall be a secure method of key insertion that protects keys against copying.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.4]

9.16 Requirement:

The product shall store all sensitive unencrypted parameters (e.g. keys) in a secure, tamper resistant location.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.7]

9.17 Requirement:

The manufacturer shall submit an undertaking that the cryptographic key chain used for signing production software is different from that used for any other test, development or other software images or support requirement.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.9.8]

9.18 Requirement:

The manufacturer shall submit an undertaking that the shared libraries (e.g., Clib or Crypto libraries) that deliver network and security functionalities have been reviewed or evaluated (note that the actual review or evaluation does not have to be conducted by the manufacturer if it has been conducted by another reputable organization or government entity). Cryptography libraries should be re-reviewed for known security vulnerabilities on each update of the device.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.5.37]

9.19 Requirement:

The device shall utilize an API for the TCB.

[Ref: GSMA CLP.13 6.4]

9.20 Requirement:

Static key or personalize key shall be used with a trust anchor device specific.

[Ref: GSMA CLP.13 6.1.1,6.1.1.1,6.1.1.2]

9.21 Requirement:

All applications stored outside of a CPU's core EEPROM shall be cryptographically authenticated.

[Ref: GSMA CLP.13 6.11]

9.22 Requirement:
The device shall support secure device decommissioning and sunsetting.

[Ref: GSMA CLP.13 8.10]

Section 10: Minimize Exposed Attack Surfaces

10.1 Requirement:

The hardware shall incorporate physical, electrical, and logical protection against tampering and reverse engineering to reduce the attack surface. The level of protection shall be determined by the risk assessment.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.4.7 and 2.4.4.8]

10.2 Requirement:

Devices shall have tamper resistant product casting and shall be provided protection against physical decapsulation, side channel and glitching attacks.

[Ref: OWASP ISVS 5.1.9 and GSMA CLP 7.3]

10.3 Requirement:

Device hardware shall not unnecessarily expose physical interfaces to attack.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.6-3]

10.4 Requirement:

The devices shall feature only the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-33]

10.5 Requirement:

All communications port(s) which are not used as part of the product's normal operation shall not be physically accessible or only communicate with authorized and authenticated Entities.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.4.9]

10.6 Requirement:

Debugging headers shall be removed from PCBs.

[Ref: OWASP ISVS 5.1.6]

10.7 Requirement:

Access to debugging interfaces (e.g., JTAG, SWD) shall be disabled or protected before shipping the device. Processors may refer to this as code protection, read back protection, CodeGuard, or access port protection.

[Ref: OWASP ISVS 1.2.4]

10.8 Requirement:

Disable Debugging and Testing Technologies: The Approved Configuration of the product to be deployed shall never contain debugging, diagnostic, or testing interfaces that could be abused by an adversary. Such interfaces are:
–Command-line console interfaces
–Consoles with verbose debugging, diagnostic, or error messages
–Hardware debugging ports such as JTAG or SWD
–Network services used for debugging, diagnostics, or testing
–Administrative interfaces, such as SSH or Telnet

[Ref: GSMA CLP.13 8.2]

10.9 Requirement:

The manufacturer shall submit an undertaking that hardware has no unofficially documented debug features, such as special pin
configurations that can enable or disable certain functionality.

[Ref: OWASP ISVS 5.1.7]

10.10 Requirement:

All unused network and logical interfaces shall be disabled, offering a configuration option that logically disables the interfaces.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.6-1 and NIST (8259) A]

10.11 Requirement:

Only necessary ports shall be exposed and available.

[ENISA Baseline security recommendations for IoT November 2017 GP-TM-50]

10.12 Requirements:

In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.6-2]

10.13 Requirement:

The manufacturer shall only enable software services that are used or required for the intended use or operation of the device.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.6-5]

10.14 Requirement:

Code shall be minimized to the functionality necessary for the service/device to operate.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.6-6]

10.15 Requirement:

The manufacturer shall give an undertaking on following secure development processes for software deployed on the device.
[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.6-9]

10.16 Requirement:

The manufacturer shall give an undertaking that each application in the ecosystem shall be built using a secure and repeatable build environment.

[Ref: OWASP ISVS 1.3.1]

10.17 Requirement:

The manufacturer shall give an undertaking that GPL-based firmware has its source code published and that no sensitive or proprietary information is accidentally included in the process.

[Ref: OWASP ISVS 1.3.2]

10.18 Requirement:

The manufacturer shall give an undertaking that banned C/C++ functions (e.g., memcpy, strcpy, gets, etc.) are replaced with safe equivalent functions (e.g. Safe C, Safe Strings library).

[Ref: OWASP ISVS 1.3.3]

10.19 Requirement:

The manufacturer shall submit an undertaking that packages are downloaded and built from trusted sources.

[Ref: OWASP ISVS 1.3.4]

10.20 Requirement:

The manufacturer shall give an undertaking that build pipelines only perform builds of source code maintained in version control systems.

[Ref: OWASP ISVS 1.3.5]

10.21 Requirement:

The manufacturer shall give an undertaking that compilers, version control clients, development utilities, and software development kits are analyzed and monitored for tampering, trojans, or malicious code.

[Ref: OWASP ISVS 1.3.6]

10.22 Requirement:

The manufacturer shall give an undertaking that packages are compiled with Object Size Checking (OSC) (e.g. -D_FORTIFY_SOURCE=2).

[Ref: OWASP ISVS 1.3.7]

10.23 Requirement:

The manufacturer shall give an undertaking that packages are compiled with No eXecute (NX) or Data Execution Protection (DEP) (e.g. -z,noexecstack).

[Ref: OWASP ISVS 1.3.8]

10.24 Requirement:

The manufacturer shall give an undertaking that packages are compiled with Position Independent Executable (PIE) (e.g. -fPIE).

[Ref: OWASP ISVS 1.3.9]

10.25 Requirement:

The manufacturer shall give undertaking that packages are compiled with Stack Smashing Protector (SSP) (e.g. -fstack-protector-all).

[Ref: OWASP ISVS 1.3.10]

10.26 Requirement:

The manufacturer shall give an undertaking that packages are compiled with read-only relocation (RELRO) (e.g. -Wl,-z,relro).

[Ref: OWASP ISVS 1.3.11]

10.27 Requirement:

The manufacturer shall give undertaking that release builds do not contain debug code or privileged diagnostic functionality.

[Ref: OWASP ISVS 1.3.12]

10.28 Requirement:

The manufacturer shall give an undertaking that debug and release firmware shall not be signed using the same keys.

[Ref: OWASP ISVS 1.3.13]

10.29 Requirement:

The manufacturer shall give an undertaking that debug information shall not contain sensitive information, such as PII, credentials or cryptographic material.

[Ref: OWASP ISVS 1.3.14]

10.30 Requirement:

The manufacturer shall give an undertaking that embedded applications are not susceptible to OS command injection by performing input validation and escaping of parameters within firmware code, shell command wrappers, and scripts.

[Ref: OWASP ISVS 1.3.15]

10.31 Requirement:

Descriptive silkscreens shall be removed from PCBs and debug paths and traces are depopulated from production PCBs

[Ref: OWASP ISVS 5.1.10]

10.32 Requirement:

Debug paths and traces shall be depopulated from production PCBs.

[Ref: OWASP ISVS 5.1.11]

10.33 Requirement:

The manufacturer should avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family

[GP-TM-49]

10.34 Requirement:

Where RF communications are enabled (e.g., ZigBee, etc.) antenna power should be configured to limit the ability of mapping assets to limit attacks such as WAR-Driving.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.7.22]

10.35 Requirement:

Debug interface shall communicate only with authorized and authenticated entities on the production devices. The functionality of any interface should be minimized to its essential task
[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.4.5]

Section 11: Implement a means to manage report of vulnerabilities

---

11.1 Requirement:

The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: contact information for the reporting of issues; and information on timelines for:

1) initial acknowledgement of receipt; and
2) status updates until the resolution of the reported issues.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.2-1]

11.2 Requirement:

Dedicated security email address and/or secure online page for Vulnerability Disclosure communications.
Ensure that the policy shall provide a clear overview of how vulnerabilities can be communicated securely and how they'll be followed up on.

[IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.3.12]

11.3 Requirement:

The manufacturer shall submit undertaking for the vulnerability management policies and processes associated with the IoT product, including:
i. Methods of receiving reports of vulnerabilities
ii. Processes for recording reported vulnerabilities.
iii. Policy for responding to reported vulnerabilities, including the process of coordinating vulnerability response activities among component suppliers and third-party vendors.
iv. Policy for disclosing reported vulnerabilities.
v. Processes for receiving notification from component suppliers and third-party vendors about any change in the status of their supplied components, such as the end of production, end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.
[Ref: NIST Cybersecurity Whitepaper g]

11.4 Requirement:

Manufacturer shall provide undertaking on Policy that has been established for interacting with both internal and third-party security researcher(s) on the products or services.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.3.5]

11.5 Requirement:

The third-party policy shall be publicly available and include contact information for reporting issues and information on timelines to acknowledge and provide status updates. There shall be a point of contact for third party suppliers and open-source communities to raise security issues.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.3.5.1 and 2.4.3.21]

11.6 Requirement:

The organization's conflict resolution process for Vulnerability Disclosures shall be developed and published.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.3.13 and 2.4.3.14]

11.7 Requirement:

Security advisory notification steps shall be developed as part of the security policy.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.3.16]

11.8 Requirement:

Coordinated disclosure of vulnerabilities should be there. For e.g., Bug Bounty program.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-OP-06 and GP-OP-08]

11.9 Requirement:

Key security design information and risk analysis shall be retained over the whole lifecycle of the product or service.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.3.29]

11.10 Requirement:

The manufacturer shall submit an undertaking to act on the Disclosed vulnerabilities in a timely manner.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.10-1]

11.11 Requirement:

Where a remote software upgrade can be supported by the device, there shall be a transparent and auditable policy with a schedule of actions of an appropriate priority, to fix any vulnerabilities in a timely manner.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.3.25]

11.12 Requirement:

To ensure information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

[Ref: ISO 27001 A.13.1]

11.13 Requirement:

Manufacturers shall submit an undertaking to continually monitor for, identify and rectify security vulnerabilities within the product and services they sell, produce, have produced and services they operate during the defined support period.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.2-3]

11.14 Requirement:

Vulnerability reporting mechanisms and processes to track and promptly respond to external reports should be established.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 9]

11.15 Requirement:

Users and relevant stakeholders should be informed when vulnerabilities affect products through established communication channels (website, e-mail, security advisory pages, changelogs, etc.).

[Ref: OWASP ISVS 1.1.6]

11.16 Requirement:

The manufacturer shall give an undertaking on Software Component Transparency - Develop and maintain a “bill of materials” including software, firmware, hardware, and cataloging third-party software libraries (including open-source modules and plugins) components, versioning, and published vulnerabilities. This applies to the device, mobile and cloud services and can help quickly remediate reported vulnerabilities.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 9 and OWASP ISVS 1.2.1]

Section 12: Vulnerability Management

12.1 Requirement:

Systems logging and monitoring approach shall be clearly defined.

[Ref: GSMA CLP-12 5.7]

12.2 Requirement:

The device application shall provide anomaly detection and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application.

[Ref: OWASP ASVS 8.1.4, GSMA CLP-13 6.13]

12.3 Requirement:

The device shall either support the use of vulnerability scanners or provide built-in vulnerability identification and reporting capabilities.

[Ref: NIST 8228 Expectation-7]

12.4 Requirement:

The manufacturer should enforce language security so that the compiler or run-time should be security hardened, where possible, to restrict the potential for a vulnerability to be abused by an adversary.

[Ref: GSMA CLP-13 7.10]

12.5 Requirement:

The potential areas of risk that come with the use of third-party and open-source software shall be identified, and actions to mitigate such risks shall be taken.

[Ref: OWASP ISVS 1.2.2]

12.6 Requirement:

Separation of duties in the application architecture shall allow administrators to diagnose and patch the vulnerable software prior to rampant abuse of the vulnerability.

[Ref: GSMA CLP-13 7.9]

12.7 Requirement:

The device OS shall be reviewed for known security vulnerabilities, particularly in the field of cryptography, prior to each update and after release. Cryptographic algorithms, primitives, libraries, and protocols shall be updateable to address any vulnerabilities.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.14]

12.8 Requirement:

The Device shall implement a complete persistent pentesting strategy.

[Ref: GSMA CLP-13 7.11]

Section 13: Incident Management

13.1 Requirement:

The device shall log its operational and security events.

[Ref: NIST Expectation 15]

13.2 Requirement:

The device shall facilitate the detection of potential incidents by internal or external controls, such as intrusion prevention systems, anti-malware utilities, and file integrity checking mechanisms.

[Ref: NIST Expectation 17]

13.3 Requirement:

The manufacturer shall give undertaking for information security events reported through appropriate channels as quickly as possible**.** To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

[Ref: ISO27001 A.13.1 and A.13.1.1]

13.4 Requirement:

Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents**.**

[Ref: ISO27001 A.13.2.1]

13.5 Requirement:

There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

[Ref: ISO27001 A.13.2.2]

13.6 Requirement:

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

[Ref: ISO27001 A.13.2.3]

13.7 Requirement:

Procedures for analyzing and handling security incidents shall be established.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-OP-05]

Section 14: Make Systems Resilient to Outages

14.1 Requirement:

The device shall maintain appropriate access control during initial connection (i.e., onboarding) and when re-establishing connectivity after disconnection or outage.

[Ref: NIST Whitepaper]

14.2 Requirement:

Where there is a loss of communications or availability it shall not compromise the local integrity of the device.

[Ref: IoT Security assurance framework Release 3.0 November 2021 2.4.7.17]

Section 15: Keep Software Updated

15.1 Requirement:

All software components in the devices shall be securely updateable.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-1]

15.2 Requirement:

For a device with no possibility of a software update the manufacturer shall clearly mention the conditions for any period of replacement support. A replacement strategy shall be communicated to the user, including a schedule for when the device should be replaced or isolated.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.5.22]

15.3 Requirement:

The security update policy for devices with a constrained power source shall be assessed to balance the needs of maintaining the integrity and availability of the device.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.5.23]

15.4 Requirement:

Where remote update is supported, there shall be an established process/plan for

validating and updating devices on an on-going or remedial basis.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.3.22]

15.5 Requirement:

The device shall authenticate to the update server component prior to downloading the Update.

[Ref: OWASP ISVS 3.4.10]

15.6 Requirement:

The update shall be applied right after the authenticity of the update is validated.

[Ref: OWASP ISVS 3.4.4]

15.7 Requirement:

Automatic mechanisms should be used for software updates.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-4]

15.8 Requirement:

If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-6]

15.9 Requirement:

The device should check after initialization, and then periodically, whether security updates are available.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-5]

15.10 Requirement:

Security updates shall be timely, and the devices shall be updated automatically upon a pre-defined schedule.

[Ref: OWASP ISVS 3.4.2 and ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-8]

15.11 Requirement:

If the network peer claims to offer a firmware-update service, the TCB shall authenticate the peer as being a part of the core IoT Service Provider network before accepting firmware updates from the peer.

[Ref: GSMA CLP.13 6.1]

15.12 Requirement:

The OS shall be implemented with relevant security updates prior to release.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.6.1]

15.13 Requirement:

Unsigned debug pre-production firmware builds shall not be flashed onto devices.

[Ref: OWASP ISVS 3.4.8]

15.14 Requirement:

The encrypted firmware images shall be securely decrypted on the device.

[Ref: OWASP ISVS 3.4.9]

15.15 Requirement:

All components, including semiconductor drivers, SDKs, and modules (e.g., 5G, LTE, Bluetooth, Wi-Fi, ZigBee etc.) shall be updated to provide security patches in alignment with the product's support or end-of-life policy.

[Ref: OWASP ISVS 1.2.9]

15.16 Requirement:

The device shall verify the authenticity and integrity of software updates, this could include but not limited to cryptographic hash comparison, code signature validation, and reliance on manufacturer-provided software that automatically performs update verification and authentication.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-9]

15.17 Requirement:

The device shall use best practice cryptography to facilitate secure update mechanisms.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-7]

15.18 Requirement:

The updates shall be cryptographically signed by a trusted source and their authenticity shall be verified before execution.

[Ref: OWASP ISVS 3.4.3]

15.19 Requirement:

Where remote software updates are supported by the device, the software images shall be digitally signed by an appropriate signing authority - e.g., manufacturer/supplier or public. The Signing Authority shall be clearly identified. Signing certificate and signing certificate chain verified by the device before the update process begins.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.5.2]

15.20 Requirement:

Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-10]

15.21 Requirement:

Where updates are supported, the software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.5.3]

15.22 Requirement:

The device shall notify the user when the application of a software update will disrupt the basic functioning of the device along with the approximate expected duration of downtime.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-12]

15.23 Requirement:

Updates shall not modify user-configured preferences, security, and/or privacy settings without notifying the user.

[Ref: OWASP ISVS 3.4.5]

15.24 Requirement:

There shall be a minimum support period during which security updates will be made available to all stakeholders. An end-of-life policy shall be published which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-13 and IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.5.35]

15.25 Requirement:

Packages and user space applications shall use over-the-air updates that are decoupled from firmware updates.

[Ref: OWASP ISVS 3.4.1]

15.26 Requirement:

The manufacturer shall ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection.

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-18]

15.27 Requirement:

In the event of an update failure, the device shall revert to a backup image.

[Ref: OWASP ISVS 3.4.7]

Section 16: Ensure Software Integrity

16.1 Requirement:

The device shall verify its software using secure boot mechanisms.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.7-1

16.2 Requirement:

Trust anchors, such as an UICC with IoT SAFE capability, should be used to authenticate not only peers during network communications, but can be augmented to store data useful for Endpoint application security.

[Ref: GSMA CLP.13 6.1]

16.3 Requirement:

The application shall employ integrity protections, such as code signing or sub resource integrity. The application shall not load or execute code from untrusted sources, such as loading includes modules, plugins, code, or libraries from untrusted sources or the Internet.

[Ref: OWASP ASVS 10.3.2]

16.4 Requirement:
Code shall be cryptographically signed to ensure it has not been tampered after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded

[Ref: ENISA Baseline Security Recommendation for IoT November 2017 GP-TM-04]

16.5 Requirement:

The manufacturer shall enforce Operating System Level Security Enhancements.

[Ref: GSMA (CLP.13) 8.1]

16.6 **Protection against malicious and mobile code.**

16.6.1 Requirement:

Controls against malicious code: Control Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented

[Ref: ISO 27001 A.10.4 and ISO 27001 A.10.4.1]

16.6.2 Requirement:

Controls against mobile code: Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.

[Ref: ISO 27001 A.10.4.2]

16.7 **Code Integrity:**

16.7.1 Requirement:

The manufacturer shall give an undertaking that a code analysis tool has been used to detect potentially malicious code, such as time functions, unsafe file operations and network connections.

[Ref: OWASP ASVS V10.1 and 10.1.1]

16.8 **Malicious Code Search:**

16.8.1 Requirement:

The application source code and third-party libraries shall not contain unauthorized phone home or data collection capabilities. Where such functionality exists, the user's permission shall be obtained for it to operate before collecting any data.

[Ref: OWASP ASVS 10.2.1]

16.9 Requirement:

The application shall not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.

[Ref: OWASP ASVS 10.2.2]

16.10 Requirement:

The application source code and third-party libraries shall not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-debugging, insecure debugging features, or otherwise out of date, insecure, or hidden functionality that could be used maliciously if discovered

[Ref: OWASP ASVS 10.2.3]

16.11 Requirement:

The application source code and third-party libraries shall not contain time bombs by searching for date and time related functions, malicious code, such as salami attacks, logic bypasses, logic bombs, Easter eggs, or any other potentially unwanted functionality.

[Ref: OWASP ASVS 10.2.3, 10.2.5 and 10.2.6]

16.12 Requirement:

Manufacturer shall share a back-up policy including details of back-up copies of information and software that are taken and tested regularly

[Ref: ISO 27001 A.10.5.1]

16.13 OS Configuration:

16.13.1 Requirement:

The operating system shall be configured according to the latest industry CIS or SCAP benchmarks (if applicable) and uses secure defaults.

[Ref: OWASP ASVS 3.2.1]

16.13.2 Requirement:

The device shall not make use of legacy or insecure protocols such as Telnet and FTP.1

[Ref: OWASP ASVS 3.2.3]

16.13.3 Requirement:

The OS kernel shall be up to date and shall not contain known vulnerabilities.

[Ref: OWASP ASVS 3.2.4]

16.13.4 Requirement:

Persistent filesystem storage volumes shall be encrypted.

[Ref: OWASP ASVS 3.2.5]

16.13.5 Requirement:

ASLR and DEP should be enabled.

[Ref: OWASP ASVS 3.2.7]

16.13.6 Requirement:

An Integrity Measurement Architecture (IMA) or similar integrity subsystem should be used and appropriately configured.

[Ref: OWASP ASVS 3.2.10]

16.13.7 Requirement:

Third-party applications should be configured to execute within a containerized runtime environment (e.g., Linux containers, Docker, etc.) that is hardened to ensure proper isolation from the host operating system.

[Ref: OWASP ASVS 3.2.11]

16.13.8 Requirement:

All unnecessary accounts or logins shall be disabled or eliminated from the software at the end of the software development process, e.g., development or debug accounts and tools.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.3]

16.13.9 Requirement:

Manufacturer shall give undertaking that files, directories, and persistent data are set to minimum access privileges required to correctly function.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.4]

16.13.10 Requirement:

All OS command line access to the most privileged accounts shall be removed from the OS.
[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.7]

16.13.11 Requirement:

All the product's OS kernel and services or functions shall be disabled by default unless specifically required. Essential kernel, services or functions are prevented from being called by unauthorised external product level interfaces and applications

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.8]

16.13.12 Requirement:

All the applicable security features supported by the OS shall be enabled.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.10]

16.13.13 Requirement:

The OS shall be separated from the application(s) and shall only be accessible via defined secure interfaces.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.11]

16.13.14 Requirement:

The OS shall implement a separation architecture to separate trusted from untrusted applications.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.12]

16.13.15 Requirement:

The product's OS kernel shall be designed such that each component runs with the least security privilege required (e.g., a microkernel architecture), and the minimum functionality needed.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.13]

16.13.16 Requirement:

The user interface shall be protected by an automatic session idle logout timeout function.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.6.15]

16.13.17 Requirement:

If LINUX is used, processes shall be isolated using Linux kernel namespaces.

[Ref: OWASP ISVS 3.3.1]

16.13.18 Requirement:

If LINUX is used, critical processes shall be configured to limit resources using control groups (cgroups).

[Ref: OWASP ISVS 3.3.2]

16.13.19 Requirement:

If LINUX is used, Linux kernel capabilities shall be configured with a minimal set for processes that require elevated access.

[Ref: OWASP ISVS 3.3.4]

16.13.20 Requirement:

If LINUX is used, SECure COMPuting (seccomp BPF) with filters shall be used and properly configured to only allow necessary system calls.

[Ref: OWASP ISVS 3.3.5]

16.13.21 Requirement:

If LINUX is used, the use of kernel security modules such as SELinux, AppArmor, GRSEC, shall be alike.

[Ref: OWASP ISVS 3.3.6]

Section 17: Firmware and Bootloader Security

17.1 Requirement:

The devices released shall have firmware configured with secure defaults appropriate for a release build (as opposed to debug versions)
[Ref: OWASP ISVS 1.2.3]

17.2 Requirement:

Device firmware images and configuration data shall be secured against unauthorized modification in manufacturing environments, including during programming. This is to prevent IP theft and reverse engineering.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.16, 2.4.14.17]

17.3 Requirement:

Firmware shall be stored in an encrypted volume at rest.

[Ref: OWASP ISVS 3.1.7]

17.4 Requirement:

Device firmware shall be designed to isolate privileged code and data from portions of the firmware that do not need access to them, and device hardware should provide isolation concepts to prevent the unprivileged from accessing security-sensitive code.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-28]

17.5 Requirement:

The secure boot process shall be enabled by default, and the product's processor system shall have an irrevocable hardware secure boot process.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.4.1, 2.4.4.4]

17.6 Requirement:

The authenticity of the first stage bootloader shall be verified by a trusted component of which the configuration in read-only memory (ROM) cannot be altered (e.g., CPU Based Secure Boot/Trusted Boot with a hardware root of trust).

[Ref: OWASP ISVS 3.1.4]

17.7 Requirement:

The authenticity of bootloader stages or application code shall get cryptographically verified before executing subsequent steps in the boot process.

[Ref: OWASP ISVS 3.1.5]

17.8 Requirement:

The bootloader configurations shall be immutable in production releases.

[Ref: OWASP ISVS 3.1.2]

17.9 Requirement:

The default/standard bootloader shall not be used if it allows alternative images or firmware flashing.

[Ref: GSMA CLP.13 6.17]

17.10 Requirement:

The first-stage bootloader executable image shall be locked in EEPROM and should only be updated through a secure process.

[Ref: GSMA CLP.13 6.17]

17.11 Requirement:

Boot loading should be outside of internal EEPROM.

[Ref: GSMA CLP.13 6.15]

17.12 Requirement:

Direct Memory Access (DMA) shall not be possible during boot.

[Ref: OWASP ISVS 3.1.8]

17.13 Requirement:

Bootloader stages shall not contain sensitive information (e.g., private keys or passwords logged to the console) as part of device start-up.

[Ref: OWASP ISVS 3.1.6]

17.14 Requirement:

The bootloader shall not allow code loaded from arbitrary locations, including both local storage (e.g., SD, USB, etc.) and network locations (e.g. NFS, TFTP, etc.).

[Ref: OWASP ISVS 3.1.1]

17.15 Requirement:

The communication interfaces such as USB, UART, and other variants shall be disabled or adequately protected during every stage of the device's boot process.

[Ref: OWASP ISVS 3.1.3]

Section 18: Hardware security

18.1 Requirement:

The product shall have hardware mechanisms to control access to memory to reduce the risk of running malicious code.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.4.18]

18.2 Requirement:

In production devices the microcontroller/ microprocessor(s) should not allow the firmware to be read out of the products non-volatile [FLASH] memory. Where a separate non-volatile memory device is used the contents shall be encrypted.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.4.13]

18.3 Requirement:

Impersonation of legitimate devices on the physical circuit shall be safeguarded by:

- Loading NVRAM contents into RAM

- Validating the application image loaded into RAM
- Executing the code directly in RAM or cache the contents in RAM

[Ref: GSMA CLP.13 9.3]

18.4 Requirement:

Inter-chip communication shall be encrypted (e.g., main board to daughter board communication).

[Ref: OWASP ISVS 4.1.7]

18.5 Requirement:

A device should support Minimum Viable execution Platform (Application Roll-Back).

[Ref: GSMA CLP.13 6.7]

18.6 Requirement:

Hardware that incorporates security features to strengthen the protection and integrity of the device should be used such as specialized security chips / coprocessors that integrate security at the transistor level, embedded in the processor.

[Ref: ENISA Baseline security recommendations for IoT November 2017 GP-TM-02]

18.7 Requirement:

The security configuration of the platform should be locked (e.g., through burning OTP fuses).

[Ref: OWASP ISVS 5.1.5]

18.8 Requirement:

Where a production device has a CPU watchdog, it shall be enabled and shall reset the device in the event of any unauthorized attempts to pause or suspend the CPU's execution.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.4.15]

18.9 Requirement:

Cryptographic accelerator functions shall be provided by the platform, leveraging dedicated functionality in the main chip or external security chips.

[Ref: OWASP ISVS 5.1.3]

18.10 Requirement:

Where the product's credential/key storage is external to its processor, the storage and processor shall be cryptographically paired to prevent the credential/key storage being used by unauthorized software.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.4.14]

18.11 Requirement:

FPGA bitstreams should be encrypted using strong, secure algorithms.

[Ref: OWASP ISVS 5.1.12]

18.12 Requirement:

The device shall use a Proven Random Number Generator.

[Ref: GSMA CLP.13 6.10]

Section 19: Installation and Maintenance of Device

19.1 Requirement:

The manufacturer shall provide users with guidance on how to securely set up their device including how to check whether the device is securely set up.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.12-2]

19.2 Requirement:

The supplier or manufacturer of any devices or services shall provide clear information about the end user’s responsibilities to maintain the devices and/or services' privacy and security.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.12.12]

19.3 Requirement:

Tamper Evident measures shall be used to identify any interference to the assembly to the end user.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.4.11]

19.4 Requirement:

Installation and maintenance of consumer IoT shall involve minimal decisions by the user and shall follow security best practice on usability.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.12-1]

19.5 Requirement:

The device shall collect logs about events with security implications, such as successful and failed authentication attempts, access to debugging functionality etc.

[Ref: OWASP ISVS 1.4.1]

19.6 Requirement:

The collected logs shall have the adequate granularity to enable actionable insights and alerts. Logs should include, at a minimum, the type of event, timestamp, source, outcome, and identification of involved actors.

[Ref: OWASP ISVS 1.4.2]

19.7 Requirement:

The devices shall contain or are synchronized with a reliable time source, to ensure the validity of log timestamps.

[Ref: OWASP ISVS 1.4.3]

19.8 Requirement:

The collected logs shall not include sensitive information, such as PII, credentials and cryptographic keys.

[Ref: OWASP ISVS 1.4.4]

19.9 Requirement:

The collected logs shall be securely retrieved from the devices over an online collection, either periodically or on-demand.

[Ref: OWASP ISVS 1.4.5]

19.10 Equipment security

19.10.1 Requirement:

Cabling security- Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

[Ref: ISO 27001 A.9.2.3]

19.10.2 Requirement:

All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal.

[Ref: ISO A.9.2.6]

19.10.3 Requirement:

The manufacturer shall provide controls and/or documentation enabling the consumer to review and revise their privacy settings and preferences.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 27]

Section 20: Supply Chain

20.1 Requirement:

It shall be ensured that the entire production test and calibration software used during manufacture is removed or secured before the product is dispatched from the factory.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.1]

20.2 Requirement:

Code integrity protection mechanisms shall be enabled and locked in hardware before shipping the device to customers. For example, ensure secure boot is enabled and the boot configuration locked.

[Ref: OWASP ISVS 1.2.7]

20.3 Requirement:

All the devices shall be logged by the product manufacturer, utilizing unique tamper resistant identifiers such as serial number so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.3]

20.4 Requirement:

The production system for a device process shall ensure that any devices with duplicate serial numbers are not shipped and are either reprogrammed or destroyed

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.4]

20.5 Requirement:

Third-party code and components shall be analyzed using static analysis tools to ensure backdoors are not introduced.

[Ref: OWASP ISVS 1.2.8]

20.6 Requirement:

Contracts with suppliers and third-party partners shall be used to implement Cyber Supply Chain Risk Management.

[Ref: NIST 8228 ID.SC-3]

20.7 Requirement:

Any hardware design files, software source code and final production software images with full descriptive annotations should be stored encrypted in off-site locations or by a 3rd party Escrow service.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.2]

20.8 Requirement:

In manufacture, all encryption keys that are unique to each device shall be either securely and truly randomly internally generated or securely programmed into each device in accordance with industry standard FIPS140-2 or equivalent.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.9]

20.9 Requirement:

A cryptographic protected ownership proof shall be transferred along the supply chain and extended if a new owner is added in the chain. This process shall be based on open standards such as Enhanced Privacy ID, Certificates per definition in ISO 20008/20009.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.7]

20.10 Requirement:

Procedures for proper disposal of scrap product shall exist at manufacturing facilities, and compliance is monitored. This to prevent scrap entering grey markets.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.14]

20.11 Requirement:

Steps shall be taken to prevent inauthentic devices from being signed into certificate chains of trust or otherwise on boarded. For example, a policy or checklist describing which devices may be on boarded exists and is followed.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.18]

20.12 Requirement:

An auditable manifest of all libraries used within the product (open source, etc.) shall be maintained to inform vulnerability management throughout the device lifecycle and whole of the support period.

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.8]

20.13 Requirement:

Products shall be shipped with information (documents or URL) about their operations and normal behavior e.g., domains contacted, volume of messaging, Manufacturer Usage Description (MUD).

[Ref: IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.13]

Chapter 3 – Specific Security Requirements

1. Requirement:

Authentication mechanisms used to authenticate users against a Vehicle Tracking Device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-3]

2. Requirement:

Password entry shall follow industry standard practice on password length, characters from the groupings and special characters.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.8.6]

3. Requirement:

The passwords used for user authentication shall be at least 12 characters long

[OWASP ISVS 2.1.5]

4. Requirement:

User authentication for external connections Appropriate authentication methods shall be used to control access by remote users.

[Ref: ISO 27001 A.10.7.2]

5. Requirement:

The application shall have additional authorization (such as step up or adaptive authentication) for lower value systems, and / or segregation of duties for high value applications to enforce anti-fraud controls as per the risk of application and past fraud.

[OWASP ASVS 4.3.3]

6. Requirement:

Manufacturer shall share what PII device collects and the device shall ensure that all PII is encrypted only accessible after successful authentication and authorisation.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 4.12.2]

7. Requirement:

The device should include a hardware-level access control mechanism for memory.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.6-8]

8. Requirement:

The manufacturer should provide patches or upgrades for all software and firmware throughout each device's lifespan.

[NIST 8228 Expectation 5]

9. Requirement:

System shall have the capability for over the air download and update of firmware as well as configuration parameters and remote administration.

[Ref: BIS, IS 16833 : 2018 (18) and (19)]

10. Requirement:

The device shall have its own secure built-in patch, upgrade and configuration management capabilities.

[NIST 8228 Expectation 6]

11. Requirement:

The device parameters given below should be configurable over the air (through SMS or cellular connectivity). The updation shall be allowed only over an 'authenticated' channel, which could be:

a) Change of the APN.
b) Change of IP and port number.
c) Setting of the primary or secondary IP.
d) Configuring the vehicle registration number.
e) Configuring the frequency of data transmission in Ignition 'ON/OFF', emergency state.
f) Configuring the time duration for emergency state.
g) Capability to reset the device.
h) Command to get the IMEI of the device.

[BIS IS 16833: 2018 A-2.2]

12. Requirement:

If a security breach occurs or an upgrade is unsuccessful, the device shall support to return to a secure state.

[Ref: ENISA Baseline recommendations for IoT November 2017 GP-TM-06]

13. Requirement:

Consumer devices shall remain operating and locally functional in the case of a loss of network access and shall recover cleanly in the case of restoration of a loss of power.

[Ref: ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.9-2]

14. Requirement:

Failed authentication attempts should be logged

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.7.5]

15. Requirement:

The Vehicle Tracking Device shall have the following information marked indelibly and legibly at an easily accessible location:

a) Name and/or trade-mark of the manufacturer,
b) Rated voltage,
c) Size,
d) Type of ATD,
e) Model number (if any),
f) Unique identification number,
g) Month and year of manufacture, and
h) Country of manufacture (if required).

[Ref: BIS, IS 16833: 2018 (6)]

16. Requirement:

Devices shall have internal cellular antenna and internal GNSS antenna.

[Ref: BIS, IS 16833: 2018 (15)]

17. Requirement:

The system shall have a unique identifier for identifying the unit and data from the unit. The unique ID shall be stored in a read only memory area so that it cannot be altered or overwritten by any person.

[Ref: BIS, IS 16833: 2018 (21)]

18. Requirement:

Devices should store/write the registration number of the vehicle in the internal non-volatile memory.

[Ref: BIS, IS 16833: 2018 (22)]

19. Requirement:

System shall have provision of secured data transmission to the backend from the devices through a secured channel. Secured channel means encrypted data transmission from device to backend using a secured tunnel on a communication medium such as 'Secured dedicated APN or 2G/3G network'.

[Ref: BIS, IS 16833: 2018 (24)]

20. Requirement:

The device should send status of system health parameters at configurable intervals and this threshold value should also be configurable over the air. It should be possible for system health parameters to be fetched on demand via command as set out in the table given below:

Sr. No.	Field	Description
i	Start Character	$
	Header	The header of the packet/identifier
ii	Vendor ID	Vendor identification header
iii	Firmware Version	Version details of the Firmware used in EX.1.0.0
iv	IMEI	Identified the sending unit. 15 digit standard unique IMEI no.
v	Battery Percentage	Indicates the internal battery charge percentage
vi	Low battery threshold value	Indicates value on which low battery alert generated in percentage
vii	Memory percentage	Indicates flash memory percentage used
viii	Data update rate when ignition 'ON'	Indicates Packet frequency on ignition ON
ix	Data update rate when ignition 'OFF'	Indicates Packet frequency on ignition OFF
x	Digital I/O status	Inputs connected to the device.
xi	Analog I/O status	Analog input status
xii	End character	*

[Ref: BIS IS 16833: 2018 A-2.3]

21. Communication Protocol:

21.1 Requirement:

Table A below contains the listing of fields that the vehicle tracking devices shall be required to send to the backend.

Sr. No	Field	Description	Sample Data
i	Start Character	$	$
ii	Header	The header of the packet/identifier	-
iii	Vendor ID	Vendor Identifies Header	-
iv	Firmware version	Version details of the Firmware used in EX.1.0.0	1.0.0
v	Packet Type	Specify the packet type— NR = Normal EA = Emergency Alert TA = Tamper Alert HP = Health Packet IN = Ignition On IF = Ignition Off BD = Battery Disconnect BR = Battery Reconnect BL = Battery Low	Depending upon the context, every frame from tracking device must carry a qualification code. This helps to determine the state in which vehicle is at that time.
vi	Packet status	L=Live or H= History	L
vii	IMEI	Identified the sending unit. 15 digit standard unique IMEI no.	123456789012345
viii	Vehicle Registration	Mapped vehicle registration	DL1PC9821

	No.	number	
ix	GPS Fix	1 = GPS fix or 0 = GPS invalid	1
x	Date	Date value as per GPS date time per GPS date time (dd-mm-yy)	220714
xi	Time	Time value as per GPS date time in UTC format (hh-mm-ss)	050656
xii	Latitude	Latitude value in decimal degrees (up to not less than 6 places)	28.758963
xiii	Latitude Direction	Latitude Direction. For example, N=North; S= South	N
xiv	Longitude	Longitude value in decimal degrees (Not less than 6 places).	77.6277844
xv	Longitude Direction	Longitude Direction. For Example, E=East, W= West	W
xvi	Speed	Speed in km/h (Up to one decimal value)	25.1
xvii	Heading	Course over ground in degrees	310.56
xviii	No. of satellites	Number of satellites available for fix	8
xix	Altitude	Altitude of the device in 'm'	183.5
xx	PDOP	Positional dilution of precision	-

xxi	HDOP	Horizontal dilution of precision	-
xxii	Network operator name	Name of Network operator	INA Airtel
xxiii	Ignition	1= Ignition On ; 0 = Ignition Off	1
xxiv	Main power status	0 = Vehicle Battery Disconnected 1= Vehicle Battery Reconnected	1
xxv	Main input voltage	Indicator showing source voltage in 'V' (Up to One Decimal Value)	12.5
xxvi	Internal battery voltage	Indicator for Level of battery charge remaining. (Up to One Decimal Value)	4.2
xxvii	Emergency status	1= On ; 0 = Off	0
xxviii	Tamper alert	C = Cover closed, O = Cover open	C
xxix	GSM signal strength	Value Ranging from 0–31	25
xxx	MCC	Mobile Country Code	404

[Ref: BIS IS 16833: 2018 A-4.1]

21.2 Requirement:

The first three fields (Start character, Header for SI and Vendor ID, who had supplied the device) shall be fixed in position as well as format (Header part of frame).

[Ref: BIS IS 16833: 2018 A-4.1]

21.3 Requirement:

Rest all other fields are required to be present in the location data sent by the devices to the backend, but can be in any sequence or with any separator between fields. The data value can be either in American Standard Code for Information Interchange

(ASCII) or in HEX format.

[Ref: BIS IS 16833: 2018 A-4.1]

21.4 Requirement:

Device shall transmit the login message whenever it establishes its connectivity with Server with the specified fields. Login message will carry below following information:

Sr. No.	Field	Description
i	$DeviceName	Vehicle number where the device was installed
ii	$IMEI	15 Digit IMEI number
iii	$Firmware	Version of the firmware used in the hardware
iv	$Protocol	Version of the frame format protocol.
v	$LastValidLocation	Last location info saved at the device.

[Ref: BIS IS 16833: 2018 A-4.1]

22. **Bluetooth**

22.1 Requirement:

Pairing and discovery shall be blocked in Bluetooth devices except when necessary.

[Ref: OWASP ISVS 4.3.1]

22.2 Requirement:

PIN or Pass-Key codes shall not be easily guessable (e.g., don't use 0000 or 1234).

[Ref: OWASP ISVS 4.3.2]

22.3 Requirement:

The devices using old versions of Bluetooth with simple modes of authentication enabled shall require a PIN for pairing.

[Ref: OWASP ISVS 4.3.3]

22.4 Requirement:

In modern versions of Bluetooth, at least 6 digits shall be required for Secure Simple Pairing (SSP) authentication under all versions except “Just Works.”

[Ref: OWASP ISVS 4.3.4]

22.5 Requirement:

Encryption keys shall be the maximum size the device supports, and this size is sufficient to adequately protect the information transmitted over the Bluetooth connection. The most secure Bluetooth pairing method available shall be used.

[Ref: OWASP ISVS 4.3.5]

22.6 Requirement:

Out Of Band (OOB), Numeric Comparison, or Passkey Entry pairing methods shall be used depending on the communicating device's capabilities.

[Ref: OWASP ISVS 4.3.6]

22.7 Requirement:

The strongest Bluetooth Security Mode and Level supported by the device shall be used. For example, for Bluetooth 4.1 devices, Security Mode 4, and Level 4 shall be used to provide authenticated pairing and encryption.

[Ref: OWASP ISVS 4.3.7]

22.8 Requirement:

Bluetooth connections should be encrypted when transmitting user IDs, passwords, and other sensitive information.

[Ref: Agelight IoT Safety Architecture & Risk Toolkit v4.0 1]

23. **Zigbee**

23.1 Requirement:

Zigbee version 3.0 shall be used for new applications.

[Ref: OWASP ISVS 4.5.1]

23.2 Requirement:

A suitable Zigbee security architecture (Centralized or Distributed) shall be selected, depending on the application's security level requirements and threat model. The Centralized architecture generally offers higher security at the cost of flexibility.

[Ref: OWASP ISVS 4.5.2]

23.3 Requirement:

The most secure way of joining the Zigbee network shall be used, depending on the selected security architecture. For example, for the Centralized architecture, use out-of-band install codes. For the Distributed one, use pre-configured link keys.

[Ref: OWASP ISVS 4.5.3]

23.4 Requirement:

The default pre-configured global link key (i.e., ZigbeeAlliance09) shall not be used to join the network, except if explicitly required for compatibility reasons and if associated risks have been considered.

[Ref: OWASP ISVS 4.5.4]

23.5 Requirement:

User interaction shall be required to activate pairing mode for both the joining nodes and the Zigbee Trust Center or router. Devices should automatically exit pairing mode after a pre-defined short amount of time, even if the pairing is unsuccessful.

[Ref: OWASP ISVS 4.5.5]

23.6 Requirement:

The network key shall be randomly generated (for example during the initial network setup).

[Ref: OWASP ISVS 4.5.6]

23.7 Requirement:

The network key shall be periodically rotated.

[Ref: OWASP ISVS 4.5.7]

23.8 Requirement:

Users shall obtain an overview of paired devices to validate that they are legitimate (for example, by comparing the MAC addresses of connected devices to the expected ones).

[Ref: OWASP ISVS 4.5.8]

24. **Wi-Fi**

24.1 Requirement:

Wi-Fi connectivity shall be disabled unless required as part of device functionality. Devices with no need for network connectivity or which support other types of network connectivity, such as Ethernet, shall have the Wi-Fi interface disabled.

[Ref: OWASP ISVS 4.4.1]

24.2 Requirement:

WPA2 or higher shall be used to protect Wi-Fi communications.

[Ref: OWASP ISVS 4.4.2]

24.3 Requirement:

If WPA is used, it shall be encrypted with AES (CCMP mode).

[Ref: OWASP ISVS 4.4.3]

24.4 Requirement:

Wi-Fi Protected Setup (WPS) shall not use to establish Wi-Fi connections between devices.

[Ref: OWASP ISVS 4.4.4]

25. **LTE**

25.1 Requirement:

LTE shall enable Confidentiality on the Air Interface.

[Ref: NIST SP 800-187 5.2]

25.2 Requirement:

LTE shall use the Ciphering Indicator

[Ref: NIST SP 800-187 5.3]

25.3 Requirement:

The device shall have User-Defined Option for Connecting to LTE Networks

[Ref: NIST SP 800-187 5.4]

25.4 Requirement:

The device shall use SIM/USIM PIN Code

[Ref: NIST SP 800-187 5.7]

25.5 Requirement:

LTE shall use Temporary Identities

[Ref: NIST SP 800-187 5.8]

26. LoRaWAN

26.1 Requirement:

LoRaWAN version 1.1 shall be used by new applications.

[Ref: OWASP ISVS 4.6.1]

26.2 Requirement:

The network, join and application servers of the LoRaWAN ecosystem shall be appropriately hardened according to industry best practices and benchmarks.

[Ref: OWASP ISVS 4.6.2]

26.3 Requirement:

All communication between the LoRaWAN gateway and the network, join and application servers shall occur over a secure channel (for example TLS or IPsec), guaranteeing at least the integrity and authenticity of the messages.

[Ref: OWASP ISVS 4.6.3]

26.4 Requirement:

Root keys shall be unique per end device.

[Ref: OWASP ISVS 4.6.4]

26.5 Requirement:

Replay attacks shall not be possible using off-sequence frame counters. For example, in case end device counters are reset after a reboot, verify that old messages cannot be replayed to the gateway.

[Ref: OWASP ISVS 4.6.5]

27. Messages and Alerts from the devices

27.1 Requirement:

Table below contains the listing of alerts that need to come from the tracking devices. These alerts are applicable for both live packets as well as the history packets.

Sr. No.	Message	Remarks
i	Location Update	Default message coming from each device
ii	Location Update (history)	Would be sent, if GPRS is not available at the time of sending the message
iii	Alert – Disconnect from main battery	If device is disconnected from vehicle battery and running on its internal battery
iv	Alert – Low battery	If device internal battery had fallen below a defined threshold, indicating that device need to get a recharge
v	Alert – Low battery removed	Indicate that vehicle internal battery is charged again
vi	Alert – Connect back to main battery	Indicate that vehicle is connected back to main battery
vii	Alert – Ignition 'ON'	Indicates that Vehicle has started (ignition ON)
viii	Alert – Ignition 'OFF'	Indicates that Vehicle has stopped (ignition OFF)
ix	Alert – GPS box opened	Message would be generated indicating GPS box opened
x	Alert – Emergency state 'ON'	When any of the emergency buttons are pressed by any passenger. System should

		also provide location of emergency button which is pressed
xi	Alert – Emergency state 'OFF'	When emergency state of vehicle is removed
xii	Alert over the air parameter change	Alerts for any parameter changed over the air/manually. Shall include the name/value of parameter changed and source of command
xiii	Harsh Braking	Alert indicating for harsh braking
xiv	Harsh Acceleration	Alert indicating for harsh acceleration
xv	Rash Turning	Alert indicating for rash turning
xvi	Tamper Alert	Alert indicating for device tampering

[Ref: BIS IS 16833: 2018 A-4.2]

28. Requirement:

The device shall have immunity to surges and resistance of 4ohM.

[Ref: ER NO. TEC28732108 4.1.12 and ISO 7637-2(200A)]

29. Requirement:

Ingress protection (IP)- The device should be IP65 compliant or better.

30. Requirement:

Devices should be able to work in active mode for a period of 4 h or more at the polling/transmission rate of 60 sec.

[Ref: BIS IS 16833: 2018 A-7.2]

31. Requirement:

The device should support both IPv6 and IPv4 protocols.

[Ref: ER NO. TEC28732108 4.1.3]

32. Emergency Request:

32.1 Requirement:

Passengers or in-vehicle crew present in the vehicle should be able to make an emergency request by pressing the emergency button provided.

[Ref: BIS IS 16833: 2018 A-3 a]

32.2 Requirement:

The emergency request function should not exist as standalone. The function should be part of the Automatic Vehicle Location Tracking (AVL) system. An alert should be sent to the control center when an emergency request is activated and de-activated. De-activation should always be from an authorized government server which receives alert messages.

[Ref: BIS IS 16833: 2018 A-3 b]

32.3 Requirement:

The emergency Buttons should be 'Normally Closed' (NC) type. The form factor of Emergency Buttons should be such that the button is easy to press in the case of an emergency, and simultaneously also minimizes the possibility of accidental or unintended press thereby causing a false alert.

[Ref: BIS IS 16833: 2018 A-3 c]

32.4 Requirement:

d) On pressing of the emergency button, the system implementing AVL function should send an emergency alert to the configured IP addresses as per the communication protocol

mentioned in 10. In the absence of cellular network, the alert should be sent as an SMS message along with vehicle location data to the configured control center number(s).

[Ref: BIS IS 16833: 2018 A-3 d]

33. Regulatory provisions:

33.1 Requirement:

Private (secure) APN shall be used to connect cellular network.

33.2 Requirement:

M2M Service Providers(M2MSP) & WPAN/WLAN Connectivity Provider for M2M services shall be registered as per DoT guidelines issued.

33.3 Requirement:

It shall be possible to register the device, services etc., with the proposed National Trust Centre (NTC) [add TEC reference here]

33.4 Requirement:

The SIM card used in the Feedback device shall meet the security requirements as specified in the ITSAR on “Pluggable (U)ICC”

33.5 Requirement:

M2M SIM card provisions:

a. The requirements as specified in the Standard Operating Procedure document issued by DoT for SIM provisioning shall be complied.
b. GSM connectivity Identifier (MSISDN) for M2M use cases shall be of 13 digits.
c. The instructions issued by DoT on 16th May 2018 on M2M SIMs / e-SIMs and the related restrictive practices for bulk issuance and Know Your Customer norms shall be complied

Annexure-I (Definitions)

1. Administrator: User who has the highest-privilege level possible for a user of the device, which can mean they are able to change any configuration related to the intended functionality
2. Application Security Verification: The technical assessment of an application against the OWASP ASVS
3. Associated services: Digital services that, together with the device, are part of the overall consumer IoT product and that are typically required to provide the product's intended functionality
4. Authentication – The verification of the claimed identity of an application user.
5. Authentication mechanism: Method used to prove the authenticity of an entity
6. Authentication value: individual value of an attribute used by an authentication mechanism
7. Authorized Individuals, services, and other IoT product components: An entity (i.e., a person, device, service, network, domain, developer, or other party who might interact with an IoT device) that has implicitly or explicitly been granted approval to interact with a particular IoT device.
8. Attacker: A hacker, threat agent, threat actor, fraudster, or other malicious threat to an IoT Service. This threat could come from individual criminals, organized crime, terrorism, hostile governments and their agencies, industrial espionage, hacking groups, political activists, 'hobbyist' hackers, and researchers, as well as unintentional security and privacy breaches.
9. Best practice cryptography: Cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques
10. Component: a self-contained unit of code, with associated disk and network interfaces that communicates with other components.
11. Constrained device: Device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use
12. Consumer: Natural person who is acting for purposes that are outside her/his trade, business, craft or profession
13. Consumer IoT device: Network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as electronic wearables
14. Credentials: Authentication material such as username and password, public and private keys, API keys, or certificate.

15. Critical security parameter: Security-related secret information whose disclosure or modification can compromise the security of a security module
16. Cryptographic material: All material, including documents, devices, or equipment that contains cryptographic information and is essential to the encryption, decryption, or authentication of communications.
17. Cryptographic module: Hardware, software, and/or firmware that implements cryptographic algorithms and/or generates cryptographic keys
18. Debug interface: physical interface used by the manufacturer to communicate with the device during development or to perform triage of issues with the device and that is not used as part of the consumer-facing functionality
19. Defined support period: Minimum length of time, expressed as a period or by an end-date, for which a manufacturer will provide security updates
20. Design Verification: The technical assessment of the security architecture of an application.
21. Device manufacturer: Entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers
22. Device: Endpoint device that is capable of storing, generating, and processing data. A generic IoT device will incorporate sensors, actuators and potentially a user interface.
23. Emergency Request/Panic Alarm/Emergency Button — A button provided in vehicle for passengers or crew members to send specialized data packet/SMS
    human or natural disaster or vehicle accident, etc.
24. Endpoint: An IoT Endpoint is a physical computing device that performs a function or task as part of an Internet-connected product or service.
25. Endpoint Ecosystem: Any configuration of low-complexity devices, rich devices, and gateways that connect the physical world to the digital world in novel ways.
26. Factory default: State of the device after factory reset or after final production/assembly
27. Firmware: Software that communicates with a device's hardware components through instructions and application interfaces.
28. Hardcoded keys: Cryptographic keys which are stored on the filesystem, be it in code, comments or files.
29. Hardware Security Module (HSM): Hardware component which is able to store cryptographic keys and other secrets in a protected manner.
30. Initialization: Process that activates the network connectivity of the device for operation and optionally sets authentication features for a user or for network access
31. Initialized state: State of the device after initialization
32. Input Validation: The canonicalization and validation of untrusted user input
33. Input Validation: The canonicalization and validation of untrusted user input

34. IoT ecosystem: A collection of interconnected systems that includes IoT systems, and other systems, such as web and mobile applications.
35. IoT product: Consumer IoT device and its associated services
36. IoT system: A system comprising interconnected IoT devices and their software and hardware components.
37. Isolable: Able to be removed from the network it is connected to, where any functionality loss caused is related only to that connectivity and not to its main function; alternatively, able to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured
38. Logical interface: Software implementation that utilizes a network interface to communicate over the network via channels or ports
39. Manufacturer: Relevant economic operator in the supply chain (including the device manufacturer)
40. Malicious Code: Code introduced into an application during its development unbeknownst to the application owner, which circumvents the application's intended security policy. Not the same as malware such as a virus or worm!
41. Network interface: Physical interface that can be used to access the functionality of consumer IoT via a
42. Network owner: User who owns or who purchased the device
43. One-time Password (OTP): A password which is uniquely generated to be used on a single occasion.
44. Organizational Root of Trust: A set of cryptographic policies and procedures that govern how identities, applications, and communications can and should be cryptographically secured.
45. Password-Based Key Derivation Function 2 (PBKDF2): A special one-way algorithm used to create a strong cryptographic key from an input text (such as a password) and an additional random salt value and can therefore be used make it harder to crack a password offline if the resulting value is stored instead of the original password.
46. PCB: A printed circuit board is a board that contains lines (traces) and pads that connect components together via electrical signals.
47. Personal data: Any information relating to an identified or identifiable natural person
48. Personally Identifiable Information (PII): is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
49. Physical interface: Physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer
50. Privileged locations: An area in hardware or software that requires elevated access and permission sets.

51. Public security parameter: Security related public information whose modification can compromise the security of a security module.
52. Remotely accessible: Intended to be accessible from outside the local network
53. Security chip: Security chips provide the foundation for secure boot, secure storage, encrypting data at rest, and are the basis for a hardware root of trust. They are often coprocessors within system on chips (SoC) and field-programmable gate arrays (FPGA) but are also referred to as trusted platform modules (TPM), and secure enclaves.
54. Security module: set of hardware, software, and/or firmware that implements security functions
55. Security update: Software update that addresses security vulnerabilities either discovered by or reported to the manufacturer
56. Sensitive information: Data that requires protection against unauthorized access such as personal identifiable information (PII), protected health information (PHI), card holder data, private keys, credentials, and personal data as defined by The EU General Data Protection Regulation (GDPR)
57. Sensitive security parameters: Critical security parameters and public security parameters
58. Software service: Software component of a device that is used to support functionality to centralized regulatory server to indicate safety/panic situation caused by
59. Telemetry: Data from a device that can provide information to help the manufacturer identify issues or information related to device usage
60. Transport Layer Security (TLS): Cryptographic protocols that provide communication security over a network connection
61. Trust Anchor: In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative entity for which trust is assumed and not derived.
62. Trusted Computing Base: A Trusted Computing Base (TCB) is a conglomeration of algorithms, policies, and secrets within a product or service. The TCB acts as a module that allows the product or service to measure its own trustworthiness, gauge the authenticity of network peers, verify the integrity of messages sent and received to the product or service, and more. The TCB functions as the base security platform upon which security products and services can be built. A TCB's components will change depending on the context (a hardware TCB for Endpoints or a software TCB for cloud services), but the abstract goals, services, procedures, and policies should be very similar.
63. Two-factor authentication (2FA): This adds a second level of authentication to an account log-in.
64. Unique per device: Unique for each individual device of a given product class or type
65. User: Natural person or organization

66. X.509 Certificate: An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

Annexure-II (Acronyms)

2FA	-	Two Factor Authentication
3G	-	Third Generation
API	-	Application Program Interface
APN	-	Access Point Name
BIS	-	Bureau of Indian Standards
BLE	-	Bluetooth Low Energy
BT	-	Bluetooth
CLP	-	GSMA's Connected Living Programme
CPU	-	Central Processing Unit
DDoS	-	Distributed Denial of Service
EEPROM	-	Electrically Erasable Programmable Read-Only Memory
ENISA	-	European Union Agency for Network and Information Security
ETSI	-	European Telecommunications Standards Institute
ER	-	Essential Requirement
GSMA	-	GSM Association
HTTP	-	Hypertext Transfer Protocol.
I/O	-	Input-Output
IoT	-	Internet of Things
IoT SF	-	Internet of Things Security Foundation

IP	-	Internet Protocol
LAN	-	Local-area Network
LoRA	-	Long Range Radio
LPWAN	-	Low-Power Wide-Area Network
LTE-M	-	Long Term Evolution-Machine Type Communication
MFA	-	Multi Factor Authentication
MSISDN	-	Mobile Station International Subscriber Directory Number
MCU	-	Micro Controller Unit
NB-IoT	-	Narrow Band-Internet of Things
NIST	-	National Institute of Standards and Technology
NFC	-	Near Field Communication
NVRAM	-	Non-Volatile Random Access Memory
OEM	-	Original Equipment Manufacturer
OS	-	Operating System
OWASP	-	Open Web Application Security Project
PC	-	Personal Computer
PII	-	Personally identifiable information
PSK	-	Pre-Shared Key
RAM	-	Random Access Memory
RFID	-	Radio-frequency identification
ROM	-	Read Only Memory
SMS	-	Short Message Service
SSH	-	Secure Shell Protocol
SRAM	-	Static Random Access Memory

TCB	-	Trusted Computing Base
TLS	-	Transport Layer Security
UICC	-	Universal Integrated Circuit Card
Wi-Fi	-	Wireless Fidelity

Annexure-III (References)

1. AIS-140
2. BIS IS 16833
3. ENISA Baseline Security Recommendation for IoT November 2017 Baseline Security Recommendations
4. ER NO. TEC28732108 4.1.3
5. ETSI EN 303 645 V2.1.0 (2020-04)
6. ETSI TR 102 898 V 1.1.1
7. GSMA (CLP.11, CLP.12, CLP.13)
8. IoT SF IoT Security assurance framework Release 3.0 November 2021.
9. ISO 27001
10. NIST 8228
11. NIST 8259
12. NIST 8259A
13. NIST Cybersecurity Whitepaper
14. OWASP Application Security Verification Standard 4.0.3
15. OWASP IoT Security Verification Standard

-End of Document-