Subject: ***Notice for seeking stakeholder inputs on the DFC (Draft for Comment) of Indian Telecom Security Assurance Requirements (ITSAR) for Feedback 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 **Feedback Device.** The details of the online meeting and registration link are as follows:

- Date of meeting: **28.04.2023 (at 10:30 hrs onwards)**
- 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)

Feedback Device

Securing Networks

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

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 of ICT equipments 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

Contents

A) Outline

The objective of this document is to present a comprehensive, country-specific security requirements for the IoT Feedback device to be used in non-critical areas where any cybersecurity breach incident will result in little discernible impact on the organization (i.e non-critical, best effort and non-sensitive category of the deployment scenarios. As per TEC ER No TEC 23232106, the feedback device may use cellular/non-cellular LP WAN connectivity i.e. LTE or LTE-A, GSMA or GPRS or EDGE, WCDMA or HSPA, LPWAN(LoRa)

The specifications produced by various regional/ international standardization bodies/ organizations, government agencies, non-profit organizations and foundations, professional associations like One M2M, ETSI, ENISA, IoT SF, GSMA, OWASP, Agelight, ISO, IEEE, NIST, ANSI/CTA,CSDE,ANSSI etc. along with the country-specific security requirements are the basis for this document. The references made in this document implies that the respective clause has been adopted as it is or with certain modifications.
This document commences with a brief description of feedback device and then proceeds to address the common and entity specific security requirements of IoT feedback device.

B) Scope

This document lays down the security requirements of the Consumer IoT Feedback Device. The associated services are out of scope.
The requirements specified herein shall be complied by TSPs, M2M Service Providers, M2M Application Service Providers, OEMs and IoT/M2M device manufacturers.

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

Introduction:

Customer feedback devices can be installed in any outlet/Public Space to get the feedback from the end users or from the employees. The device requires only a simple press of button to answer the customizable question displayed on the device. Hardware uses a configurable front panel with a customizable feedback question, micro-controller based highly configurable & remote upgradeable firmware with variety of connectivity (GSM etc.) technologies to deliver the feedback in real time.
The response captures the customer/employee satisfaction from the use of relevant service, recording the date – time of the feedback and delivers the user feedback to the central server in real time, currently these devices are being used in public toilets under Swachh Bharat mission from the Mandate of Ministry of housing & Urban Affairs.

Common interfaces used are:

1. LTE or LTE-A
2. GSM or GPRS or EDGE
3. WCDMA or HSPA
4. CDMA
5. LPWAN- LoRa

Types of Feedback Devices:

1. Anonymous Feedback Devices – in malls, shopping complexes etc.,
2. Identifiable Feedback Device –ask for some sort of personal identification, usually mobile number and/or email, like in polling booths, hospital

❖ Based on nature of information collected

i. **Anonymous Feedback Devices** – As the name suggests, this kind of feedback devices collect feedback anonymously i.e., without having the need to log in to give feedback. Due to less complex nature of the devices, these are usually compact and cost – effective options offering a more generic and non-actionable or somewhat actionable feedback.

a) ‘Yes’ or ‘No’ Response Feedback

b) Numeric Response Feedback (Rating product/service from a scale of say, 0 to 5 or 0 to 10)

Features:

- plug-and-play setup
- No PII is collected
- Single Question, quick and simple feedback
- Wall-mount, Floor Standing, Tabletop Installations
- 3G/4G Wireless Setup (US, UK, UAE); GPRS, GSM (India)
- Online/Cloud Based Administrative Panel
- Battery/Power Supply Operated
- Simple and easy data collection and Report generation (additional feature, not mandatory)
- Places of Deployment - malls, shopping complexes etc.,

ii. **User Identifiable Feedback Device** – These devices mandatorily ask for some sort of personal identification Information, usually mobile number and/or email, like in polling booths, hospitals, banks etc., and are used for specific and usually actionable feedback.

Features:

- Application is installed on the tablets or it has a web-based interface/web-app.
- PII like Name, Mobile number, Email-id etc., is collected
- Touch screen typed/smiley face feedback options
- Ability to get Textual-Based Inputs/Comments of the Customer using On-screen Keyboard
- Ability to Collect Multiple Question Based Feedbacks
- Customizable Surveys and Questions
- Connectivity via LAN (RJ45 Ethernet port), Wi-Fi, and 3G/4G (US, UK)
- Ability to integrate Email and SMS based notifications and alerts

Inbuilt RTC (Real Time Clock) is provided so that we can know the date and time of each feedback.

Feedback device architecture:

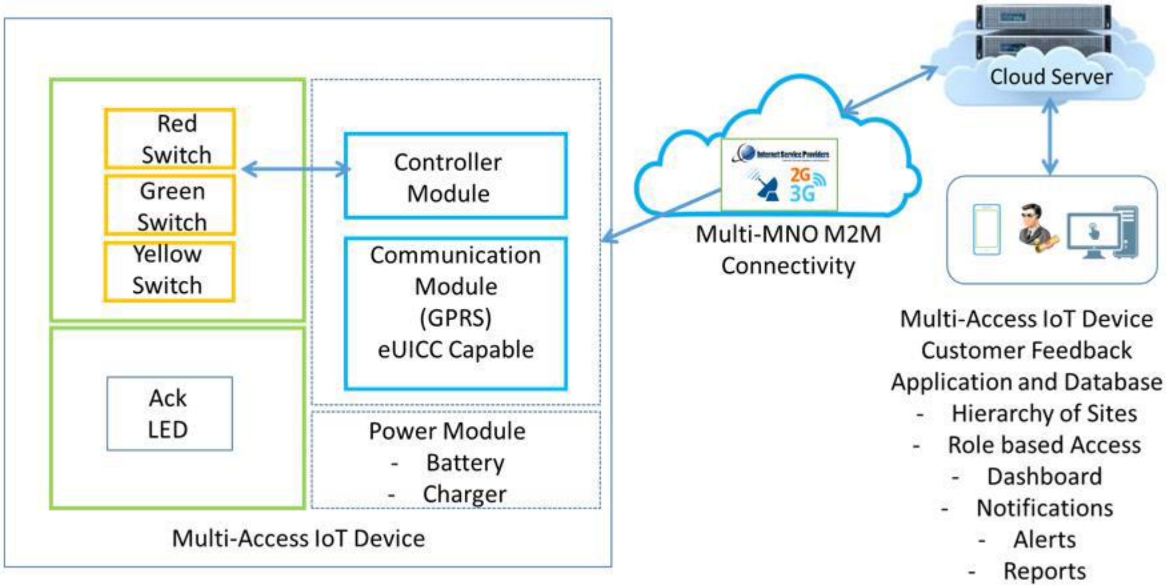

Fig.1 Feedback Device architecture

The architecture of a typical IoT feedback device is shown above. It contains a control module along with touch pad or push button, power module and a communication module

Chapter 2 – Common Security Requirements

Section 1: Authentication

1.1. Password Management

1.1.1. Requirement

Where passwords are used and, in any state, other than the factory default, all device passwords shall be unique per device or defined by the user. The factory issued or reset password shall be randomly unique for every device in the product family.
If a password less authentication is used the same principles of uniqueness apply.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.1-1 and IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.8.3.]

1.1.2. Requirement:

Default usernames and passwords shall be changed during the initial setup. No weak, null or blank passwords and common usernames shall be allowed.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-23]

1.1.3. Requirement:

Device owner-user shall be notified 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 - 17]

1.1.4. 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 V2.1.1 (2020-06) Provision 5.1-2]

1.1.5. Requirement:

The product allows 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]

1.1.6. Requirement

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

[Ref: OWASP ISVS 2.1.7 and IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.8.14]

1.1.7. Requirement

Password reset mechanism shall be robust and does not supply an attacker with information indicating a valid account. It shall be ensured that this mechanism is not abused by an unauthorized party.

[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]

1.1.8. Requirement

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

[Ref: OWASP ISVS 2.1.6]

1.1.9. Requirement

Protection against brute force and/or other abusive login attempts (such as automated login bots, etc.) shall be in place.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-25]

1.2. Authentication

1.2.1. Requirement:

An unconstrained device shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interfaces impracticable.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.1-5]

1.2.2. Requirement:

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

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.1-4]

1.2.3. Requirement:

Authentication mechanisms used to authenticate users against a device shall use cryptography, appropriate to the properties of the technology, risk and usage.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.1-3]

1.2.4. Requirement:

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

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-24]

1.2.5. Requirement:

Authentication mechanisms shall use strong passwords or personal identification numbers (PINs), and should consider using 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]

1.2.6. Requirement:

User authentication for external connections: Appropriate authentication methods shall be used to control access by remote users. Remote authentication methods if any, like SSH shall be mutually authenticated.

[Ref: ISO 27001 A.11.4.2]

1.2.7. Requirement:

Verify that authentication credentials for users, devices, or services are not hardcoded in firmware or ecosystem applications.

[Ref: OWASP ISP 2.1.9]

1.2.8. Requirement:

The device can conceal password characters from display when a person enters a password for a device, such as on a keyboard or touch screen.

[Ref: NIST 8228 Expectation 9]

1.2.9. 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]

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:

Root of trust backed unique authenticable logical identity should be provided.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.8.18]

2.1.3. Requirement:

If any hard-coded unique per device identity is implemented for security purposes, it shall be implemented in such a way that it resists tampering by physical, electrical or software means.

[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 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]

2.1.6. 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]

Section 3: Authorization and access controls

3.1. Requirement:

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]

3.2. 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]

3.3. Requirement:

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

[Ref: NIST 8228 Expectation 19 and Expectation 21]

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

[Ref: NIST 8228 Expectation 12]

3.6. Requirement:

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

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

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:

Principle of least privilege shall be enforced by limiting applications and services that run as root or administrator. Applications shall operate at the lowest privilege level possible.

[Ref: OWASP ISVS 2.2.2 and ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-27]

3.9. 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]

3.10. 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]

3.11. Requirement:

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

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-29]

3.12. Requirement:

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

[Ref: OWASP ISVS 2.2.4]

3.13. Requirement:

The product or service shall records 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]

3.14. Requirement:

Access control shall be in place for management of removable media.

[Ref: ISO 27001 A.10.7.1]

3.15. Requirement:

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

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.8.16]

3.16. Requirement:

Ownership shall be validated upon registration and as part of decommissioning when devices move across accounts such as device reselling, leasing, and renting.

[Ref: OWASP ISVS 2.2.3]

3.17. Requirement:

The OEM shall 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 2. 4.14.22]

Section 4: Storing Sensitive Information Securely

4.1. 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 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 V2.1.1 (2020-06) Provision 5.4-1]

4.3. Requirement:

Hard-coded critical/ security parameters in device software source code shall not be used; if needed these should be injected in a separate (secure) process.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.5.40]

4.4. Requirement:

Security parameters and passwords shall not be hard-coded into source code or stored in a local file. If passwords absolutely must be stored in a local file, then the password file(s) shall be owned by, and are only accessible to and writable by, the Device's OS most privileged account and are obfuscated.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.6.5]

4.5. Requirement:

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

[Ref: OWASP ISVS 5.1.4]

4.6. Requirement:

The product/service shall ensure that all Personal Information is encrypted for confidentiality both when stored and if communicated out of the device and only accessible after successful authentication and authorization.

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

4.7. Requirement:

UICC may also be used for tamper-resistant storage of sensitive data for services, including security keys controlled by Service Provider (Recommendatory).

[Ref: GSMA CLP.14 5.1.1.4]

4.8. Requirement:

Memory protection shall be enabled in the underlying hardware architecture, and the operating system must have a concept of privilege levels. Unprivileged software must be restricted from accessing privileged resources, such as drivers, configuration files, or other objects.

[Ref: GSMA CLP.13 7.9]

4.9. Requirement:

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

[Ref: OWASP ISVS 1.2.6]

4.10. Requirement:

The feedback device 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]

4.11. Requirement:

Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.4-4]

Section 5: Make it easy for 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 V2.1.1 (2020-06) Provision 5.11-1, 11-2]

5.2. Requirement:

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

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.11-3]

5.3. Requirement:

The supplier or manufacturer of 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 V2.1.1 (2020-06) 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:

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:

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]

5.8. Requirement:

Minimise the data collected and retained. Stakeholders shall 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]

Section 6: Data Protection & Privacy

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 V2.1.1 (2020-06) Provision 6-1]

6.1.2. Requirement:

Data processed by a third-party shall be protected by a data processing agreement. An undertaking in this regard shall be submitted.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-OP-12]

6.1.3. 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]

6.1.5. 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:

Personal data shall be collected and processed fairly and lawfully, it shall not be collected and processed without the data subject's consent.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-10]

6.2.2. Requirement:

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

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

6.2.3. 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]

6.2.4. Requirement:

It shall be conspicuously disclosed what personally identifiable and sensitive data types and attributes are collected and how they are used. The users shall be provided the ability to opt-in for any other purposes.

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

6.2.5. 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 is mandatory.

[Ref: GSMA CLP.11 PDR 1.7]

6.2.6. Requirement:

Clear language and text/images appropriate to the target audience shall be used Local language shall also be considered.

[Ref: GSMA CLP.11 PDR 1.9]

6.2.7. 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 V2.1.1 (2020-06) Provision 6-3]

6.2.8. Requirement:

Sharing of the personal data of the consumers with third parties shall be done with 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-OP-13]

6.2.9. Requirement:

Bundle consent must be avoided, granular choice must be provided. Individuals must be made aware of the persistency of consent and how it can be revoked. Evidence of Consent revocation shall be captured and retained.

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

6.2.10. Requirement:

Users must be allowed to choose the presentation of their identity. Personal identifiers shall be collected for only when unavoidable (such as a MSISDN, or name or email address).

[Ref: GSMA CLP.11 PDR 2.1]

6.2.11. Requirement:

Unauthorized linking of identifiers and authentication protocols across different services must be prevented. Tracking of identifiers or user behavior must be limited to the extent necessary to provide or protect a service (such as authentication and authorization).

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

6.2.12. Requirement:

Individuals shall be provided with an 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]

6.2.13. Requirement:

Individuals must be provided with the means to associate, disassociate and re-assign their IoT service identities.

[Ref: GSMA CLP.11 PDR 3.3]

6.3. Anonymization

6.3.1. Requirement:

Anonymization of Personal Information must be done whenever possible particularly in reports.

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

6.3.2. Requirement:

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

[Ref: GSMA CLP.11PDR 4.1]

6.4. Minimize the Data Collected and Retained

6.4.1. Requirement:

Data retention classification must be done for sensitive personal information to delete old or out-of-date data automatically, on a schedule, or as the situation requires.

[Ref: OWASP ASVS 8.3.8]

6.4.2. 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]

6.4.3. 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]

6.4.4. Requirement:

Minimum attributes needed to meet a specific IoT use case must 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]

6.5. Backup and Storage

6.5.1. Requirement:

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

[Ref: NIST 8228 Expectation 19 and 21]

6.5.2. Requirement:

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

[Ref: NIST 8228 Expectation 20]

6.5.3. Requirement:

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

[Ref: OWASP ASVS 8.1.6]

6.5.4. Requirement:

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

[Ref: OWASP ASVS 8.2.2]

6.5.5. 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]

6.5.6. Requirement:

Methods to remove or export data on demand by users must be in place.

[Ref: OWASP ASVS 8.3.2]

6.5.7. 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]

6.6. Information Security

6.6.1. Requirement:

Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

[Ref: ISO 27001 A.15.1.4]

6.6.2. Requirement:

Legal basis for processing personal data must be identified (such as it is necessary for performance of a contract to give access to an account and data, or consent).

[Ref: GSMA CLP.11 PDR 1.2]

6.6.3. 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]

6.6.4. Requirement:

In case a device is decommissioned, or the owner changes, all sensitive information such as PII data and credentials shall be removed from the device.

[Ref: OWASP ISVS 2.3.2]

6.6.5. Requirement:

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

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

6.6.6. Requirement:

System and procedural controls must 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]

6.6.7. Requirement:

Changes in personal information of the user must be authorized.

[Ref: GSMA CLP 11 PDR 5.4]

6.6.8. Requirement:

Security measures to be adopted through entire data life cycle must be documented.

[Ref: GSMA CLP11 PDR7.1]

6.6.9. 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 V2.1.1 (2020-06) Provision 6-5]

Section 7: Secure input and output handling

7.1 Data Input Validation

7.1.1. Requirement:

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

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-54]

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.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.13-1]

7.1.3. 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]

7.1.4. 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]

7.1.5. 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]

7.1.6. 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]

7.1.7. 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]

7.1.8. Requirement:

URL redirects and forwards shall only allow destinations which 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 defences 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]

Section 8: Communicate Securely

8.1. Requirement:

The feedback device shall use best practice cryptography to communicate securely. Such cryptographic algorithms and primitives must 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 and 5.5-3]

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 Recommendations 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.

[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 must 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 TCP based communications (such as MQTT connections), UDP based communication shall be encrypted and authenticated using the latest TLS 1.2 or above and DTLS 1.2 or above respectively.

[Ref: 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 webserver encrypts communications using TLS and requests a client certificate, the server(s) shall establish a connection only if the client certificate and its chain of trust are valid.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.13.9]

8.9. Requirement:

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]

8.10. 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]

8.11. 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 objective]

8.12. Requirement:

Unauthorized connections to the feedback device or other devices the product is connected to, must be prevented at all levels of the protocols by letting only intentional connections.

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

8.13. Requirement:

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

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.11.4]

8.14. Requirement:

Disable deprecated or known insecure algorithms and ciphers.

[Ref: OWASP V4 Communication requirements control objective]

8.15. Requirement:

Access to device functionality specially the one which allows security-relevant changes in configuration via a network interface in the initialized state shall only be possible after authentication on that interface.

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

8.16. Requirement:

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

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

8.17. Requirement:

The feedback device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.5-7]

8.18. Requirement:

Specific ports and/or network connections for selective connectivity must be disabled. Internal or external traffic must not expose the device credentials.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP TM-40 and GP TM-45]

Section 9: Cryptography

9.1.1. Requirement:

The device and associated applications shall support current generally accepted security and cryptography protocols. All personally identifiable data in transit (wireless and wired) and in storage (in rest), must be encrypted using generally accepted security standards.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-34]

9.1.2. Requirement:

End-point communication security: Secure session must be established after each disconnected session to prevent intentional and unintentional denial of device [DoS].

[Ref: GSMA CLP.13 9.1]

Section 10: Minimize Exposed Attack Surfaces

10.1. Requirement:

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

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

10.2. 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]

10.3. Requirement:

Device shall have tamper resistant product cas~~t~~ing and shall be provided protection against physical decapsulation, side channel and glitching attacks.

[Ref: OWASP ISVS 5.1.9 and GSMA CLP 7.3]

10.4. 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 authorised and authenticated entities.

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

10.5. Requirement:

All unused network and logical interfaces shall be disabled.

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

10.6. Requirement:

The debug information shall not contain sensitive information, such as PII, credentials or cryptographic material.

[Ref: OWASP ISVS 1.3.14]

10.7. Requirement:

The debug and release firmware shall not be signed using same keys.

[Ref: OWASP ISVS 1.3.13]

10.8. Requirement:

The hardware shall have no unofficially documented debug features, such as special pin configurations that can enable or disable certain functionality. ~~(Undertaking)~~
An undertaking in this regard shall be submitted.

[Ref: OWASP ISVS 5.1.7]

10.9. Requirement:

Debug interface shall communicate only with authorised and authenticated entities on the production devices. The functionality of any interface should be minimised to its essential task.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.4.5]

10.10. 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]

10.11. Requirement:

The platform shall support memory and I/O protection capabilities using a memory management unit (MMU) to isolate sensitive memory regions .

[Ref: OWASP ISVS 5.1.8]

Section 11: Vulnerability Report Management

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.
3) Vulnerability disclosure policy

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.2-1]

11.2. Requirement:

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 2.4.3.21]

11.3. Requirement:

A dedicated security email address and/or secure online page for vulnerability disclosure communications must be provided.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.3.12]

11.4. Requirement:

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

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.3.16]

11.5. Requirement:

Disclosed vulnerabilities shall be acted on in timely manner.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.10-1]

11.6. 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]

11.7. Requirement:

Manufacturers shall 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]

11.8. Requirement:

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

[Ref: OWASP ISVS 1.1.6]

Section 12: Vulnerability Management

12.1. Requirement:

Systems logging and monitoring approach must be clearly defined

[Ref: GSMA CLP-12 5.7]

12.2. Requirement:

The device application shall do 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]

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

[Ref: OWASP ISVS 1.2.2]

12.5. 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]

12.6. Requirement:

The manufacturer shall provide patches or upgrades for all software and firmware throughout the device’s lifespan.

[Ref: NIST 8228 Expectation-5]

Section 13: Incident Management

13.1. Requirement:

Restore to secure state: The device shall return to a secure state after a security breach has occurred or if an upgrade has not been successful.

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

13.2. Requirement:

Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state shall be in place.

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-16]

13.3. Requirement:

Procedures for analysing and handling security incidents shall be established.

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

Section 14: Make Systems Resilient to Outages

14.1. Requirement:

The device 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 V2.1.1 (2020-06) Provision 5.9-2]

14.2. Requirement:

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

[Ref: NIST Cyber security Whitepaper pg6]

14.3. Requirement:

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

[Ref: IoT SF 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 feedback device 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 conditions for and period of replacement support shall be clear. 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 users shall have the ability to disable updating.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.3.22.1]

15.4. Requirement:

Where remote update is supported, there shall be an established process/plan for validating "updates" 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:

If the device supports automatic updates and/or update notifications, these shall 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]

15.7. Requirement:

Automatic firmware update mechanism shall be offered. Backward compatibility of firmware updates shall be in place. Automatic firmware updates shall not modify user-configured preferences, security, and/or privacy settings without user notification

[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-20]

15.8. 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]

15.9. Requirement:

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

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-8 and OWASP ISVS 3.4.2 and 3.4.12]

15.10. Requirement:

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

[Ref: OWASP ISVS 2.4.6.1]

15.11. Requirement:

The firmware, software updates shall be stored encrypted on server side and are transmitted by using encrypted communication channel.

[Ref: OWASP ISVS 3.4.11 and 12]

15.12. Requirement:

The device shall verify the authenticity and integrity of software updates.

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]

15.13. 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]

15.14. 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]

15.15. Requirement:

The user shall be informed via a notification on the user interface or via email which can include extra detail, such as the approximate expected duration for which the device will be offline.

[Ref: ETSI EN 303 645 V2.1.1 (2020-06) Provision 5.3-11]

15.16. 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]

15.17. Requirement:

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

[Ref: OWASP ISVS 1.2.9]

15.18. Requirement:

There is a minimum support period during which security updates will be made available to all stake holders. 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]

15.19. Requirement:

The device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server shall be secure, that the update file shall be transmitted via a secure connection. It shall be signed by an authorized trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.
[Ref: ENISA Baseline Security Recommendations for IoT November 2017 GP-TM-18]

15.20. 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 feedback 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, shall 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 must 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:

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]

16.5. Requirement:

Protection against malicious and mobile code shall be implemented.

[Ref: ISO 27001 A.10.4]

16.6. 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]

Section 17: Firmware and Bootloader Security

17.1. Requirement:

The devices released must 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. Steps have been taken to prevent inauthentic devices from being programmed with confidential firmware images and configuration data.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.14.16 and 2.4.14.17]

17.3. Requirement:

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

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.4.4]

17.4. 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]

17.5. Requirement:

Aauthenticity 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.Based Secure Boot/Trusted Boot with a hardware root of trust).

[Ref: OWASP ISVS 3.1.4]

17.6. 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]

17.7. 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: Installation and Maintenance of Device

18.1. 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]

18.2. 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]

18.3. Requirement:

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

[Ref: OWASP ISVS 1.4.4]

18.4. 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]

18.5. Requirement:

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

[Ref: ISO 27001 A.9.2.6]

Section 19: Supply Chain

19.1. Requirement:

In manufacture, all the devices shall be logged by the product vendor, 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]

19.2. Requirement:

Procedures for disposal of scrap product at manufacturing facilities must be defined and compliance to the same shall be monitored to prevent scrap entering grey markets.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.14.14]

19.3. Requirement:

Test and calibration software used during manufacture must be removed or secured before the product dispatch from the factory. This is to prevent alteration of the product post manufacture when using authorized production software, for example hacking of the RF characteristics for greater RF ERP. Where such functionality is required in a service center, it shall be removed upon completion of any servicing activities.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.14.1]

19.4. 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]

19.5. Requirement:

It shall be ensured that the devices made in India are deployed.

Chapter 3 – Specific Security requirements

1. LoRaWAN version 1.1 shall be supported.
2. LoRaWAN Root keys shall be unique per end device.
3. Private (secure) APN shall be used to connect cellular network.
4. M2M Service Providers(M2MSP) & WPAN/WLAN Connectivity Provider for M2M services shall be registered as per DoT guidelines issued.
5. It shall be possible to register the device, services etc., with the proposed National Trust Centre (NTC)
6. The SIM card used in the Feedback device shall meet the security requirements as specified in the ITSAR on “Pluggable (U)ICC”
7. **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. 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
3. 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.
4. Authentication mechanism: method used to prove the authenticity of an entity
5. Authentication value: individual value of an attribute used by an authentication mechanism
6. 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
7. Cellular: Any 3GPP standardized mobile network technology (e.g., GSM, UMTS, LTE (inc LTE-M) and NB-IoT).
8. 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
9. Consumer: natural person who is acting for purposes that are outside her/his trade, business, craft or profession
10. 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
11. Critical security parameter: security-related secret information whose disclosure or modification can compromise the security of a security module
12. Defined support period: minimum length of time, expressed as a period or by an end-date, for which a manufacturer will provide security updates
13. Device manufacturer: entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers
14. Factory default: state of the device after factory reset or after final production/assembly
15. Initialization: process that activates the network connectivity of the device for operation and optionally sets authentication features for a user or for network access
16. 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.Perform triage of issues with the device and that is not used as part of the consumer-facing functionality

17. Embedded SIM: A SIM which is not easily accessible or replaceable, is not intended to be removed or replaced in the device, and enables the secure changing of profiles.
18. Endpoint: An IoT Endpoint is a physical computing device that performs a function or task as part of an Internet-connected product or service.
19. Initialized state: state of the device after initialization
20. Internet of Things: The Internet of Things describes the coordination of multiple machines, devices, and appliances connected to the Internet through multiple networks. These devices include everyday objects such as tablets and consumer electronics, and other machines such as vehicles, monitors, and sensors equipped with machine-to-machine (M2M) communications that allow them to send and receive data.
21. IoT product: consumer IoT device and its associated services
22. IoT Service: Any computer program that leverages data from IoT devices to perform the service.
23. Logical interface: software implementation that utilizes a network interface to communicate over the network via channels or ports
24. Manufacturer: relevant economic operator in the supply chain (including the device manufacturer)
25. Mutual Authentication: Mutual authentication refers to a security process or technology in which two entities in a communications link verify the origin and integrity of each other before any sensitive data is sent over the connection. In a network, the client authenticates the server and vice-versa. It is a default mode of authentication in some protocols, such as: SSH
26. NIST: National Institute of Standards and Technology
27. Network interface: physical interface that can be used to access the functionality of consumer IoT via a network
28. On boarding: The method to register a device into its service or solution to enable device registration, configuration and data transfer
29. Owner: user who owns or who purchased the device
30. Ownership transfer: In case a device is transferred through a supply chain and changes owner, this method ensures a reliable and secure transfer of ownership
31. Personal data: any information relating to an identified or identifiable natural person
32. Public security parameter: security related public information whose modification can compromise the security of a security module
33. Physical interface: physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer
34. Remotely accessible: intended to be accessible from outside the local network
35. Secure boot: Process that ensures a device only starts software that is trusted by the OEM

36. Security module: set of hardware, software, and/or firmware that implements security functions
37. Security update: set of hardware, software, and/or firmware that implements security functions
38. Sensitive security parameters: critical security parameters and public security parameters
39. Software service: software component of a device that is used to support functionality
40. Tamper evident: The enclosure of the product has measures to ensure that any unauthorized attempt to open it leaves evidence of the attempt, for example, labelling across a product's enclosure joint that fragments when the joint is disturbed.
41. Tamper Resistant: The enclosure of the product has measures to prevent its unauthorised opening. Typically, with specialist fasteners or other features that require the use of specialist tooling, unique to the product
42. Telemetry: data from a device that can provide information to help the manufacturer identify issues or information related to device usage
43. Trust Anchor: In cryptographic systems with hierarchical structure, a trust anchor is an authoritative entity for which trust is assumed and not derived.
44. UICC: A Secure Element Platform specified in ETSI TS 102 221 can support multiple standardized network or service authentication applications in cryptographically separated security domains. It may be embodied in embedded form factors specified in ETSI TS 102 671.
45. Unique per device: unique for each individual device of a given product class or type
46. User: natural person or organization

Annexure-II (Acronyms)

2FA	-	Two Factor Authentication
3G	-	Third Generation
BLE	-	Bluetooth Low Energy
CA	-	Certification Authority
CPU	-	Central Processing Unit
DTLS	-	Datagram Transport Layer Security
ENISA	-	European Union Agency for Network and Information Security
ETSI	-	European Telecommunications Standards Institute
FTTH	-	Fiber to the Home
GPRS	-	General Packet Radio Service
GSM	-	Global System for Mobile communications
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

MQTT	-	Message Queue Telemetry Transport - ISO standard ISO/IEC PRF 20922
NB-IoT	-	Narrow Band-Internet of Things
NFC	-	Near Field Communication
OEM	-	Original Equipment Manufacturer
OS	-	Operating System
OWASP	-	Open Web Application Security Project
PC	-	Personal Computer
PII	-	Personally identifiable information
RFID	-	Radio-frequency identification
RoT	-	Root of Trust
SMS	-	Short Message Service
SSH	-	Secure Shell Protocol
TLS	-	Transport Layer Security
UDP	-	User Datagram Protocol
UICC	-	Universal Integrated Circuit Card
URL	-	Universal Resource Locator
Wi-Fi	-	Wireless Fidelity
WPS	-	Wi-Fi Protected Setup

Annexure-III (References)

1. TEC ER No TEC 23232106 ,the feedback device
2. ETSI EN 303 645 V2.1.1 (2020-06): Cyber Security for Consumer Internet of Things: Baseline Requirements
3. ENISA: Baseline Security Recommendations for IoT in the context of CII
4. OWASP IoT Security Verification Standard
5. OWASP Application Security Verification Standard 4.0.3 Final
6. NIST: NISTIR 8259, NISTIR 8259A, NISTIR 8228, NIST CYBERSECURITY WHITE PAPER
7. GSMA: CLP.11, CLP.12, CLP.13, CLP.14
8. Agelight: IoT Safety Architecture & Risk Toolkit v4.0
9. IoT SF: Products sold to a consumer for use in a domestic setting IoT Security Compliance Framework
10. ISO 27001

-End of Document-