Indian Telecom Security Assurance Requirements (ITSAR)

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

Smart Electricity Meter
Draft for comments

ITSAR Number: ITSAR30905YYMM
ITSAR Name: NCCS/ITSAR/Access Equipment/IoT End Devices/Smart electricity meter

Date of Release: DD.MM.YYYY
Date of Enforcement:

Version: 1.0.0

MTCTE के तहत जारी:
Issued under MTCTE by:

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

About NCCS

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

Document History

Sl no	Title	ITSAR No.	Version	Date of Release	Remark
1	Smart Electricity Meter	ITSAR30905YYMM	1.0.0.	DD.MM.YYYY	First release

Table of Contents

A) Outline

The objective of this document is to present a comprehensive, country-specific security requirements for the Smart electricity meter. The smart electricity meters (Single phase & Three phase whole current smart electricity meters) is responsible to comply with the enclosed technical specifications. The supplier and Manufacturer would furnish valid BIS certification before supply of meters.

The specifications produced by various regional/ international standardization bodies/ associations like ISO, ETSI,NIST, IOTSF, Agelight, GSMA,OWASP, ENISA along with the country-specific(e.g BIS) security requirements are the basis for this document.

This document commences with a brief description of Smart electricity meter , its functionalities and then proceeds to address the common and device specific security requirements of smart electricity meters.

B) Scope

This document provides security requirements of consumer IoT -Smart electricity meters installed in residential or office environments. The requirements specified herein shall be complied by TSPs, M2M Service Providers, M2M Application Service Providers, OEMs and IoT/M2M device manufacturers. These specifications shall be applicable to smart electricity meter as mentioned in TEC ER NO. TEC28732108. The smart electricity meter has bidirectional communication facility & remote connect/disconnect switch. The meter shall communicate with Head End System (HES) on any one of the communication technologies mentioned in IS16444 Part 1, as per the requirement of the utility.

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

A Smart electricity meter is an electronic device that records consumption of electricity, and communicates that information for monitoring and billing. Smart electricity meters send meter readings to the utility company automatically. They also come with in-home displays, which give users real-time feedback on their energy and what it is costing.It is designed to measure 'forwarded only' or 'import and export' energy, store and communicate the same along with other parameters defined in this standard. It shall be remotely accessed for collecting data/events, programming for selected parameters.

Basic Features

The Smart electricity meter would have the following minimum basic features-

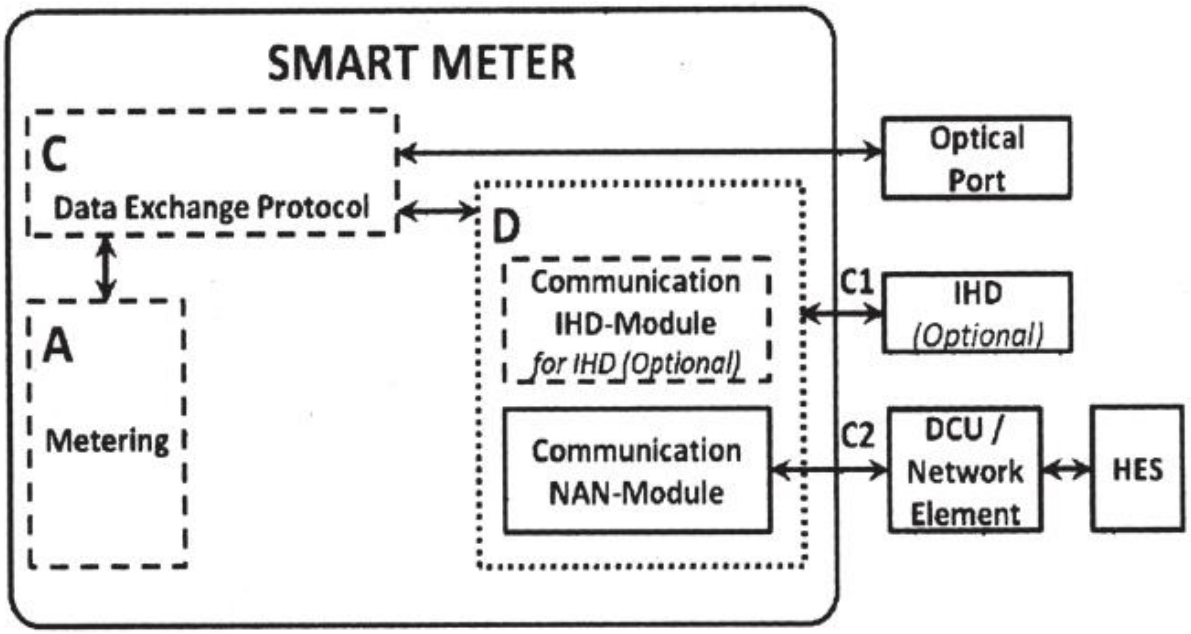
- Measurement of electrical energy parameters
- Bidirectional Communication
- Integrated Load limiting /connect/disconnect switch
- Tamper event detection, recording and reporting
- Power event alarms as per IS 16444 Part 1
- Remote firmware upgrade
- Pre-paid features at MDM end (as per IS 15959 Part 2)
- TOD features Net Metering(kWh) features (optional as per requirement of utility)
- On demand reading

Smart electricity meter Architecture:

The smart electricity meter is a component of Advanced Metering Infrastructure(AMI). For the purpose of this standard the smart electricity meter is conceived as single unit comprising of following functional zones:
a) Metering
b) Load switch
c) Data exchange and communication protocol, and
d) Communication modules.

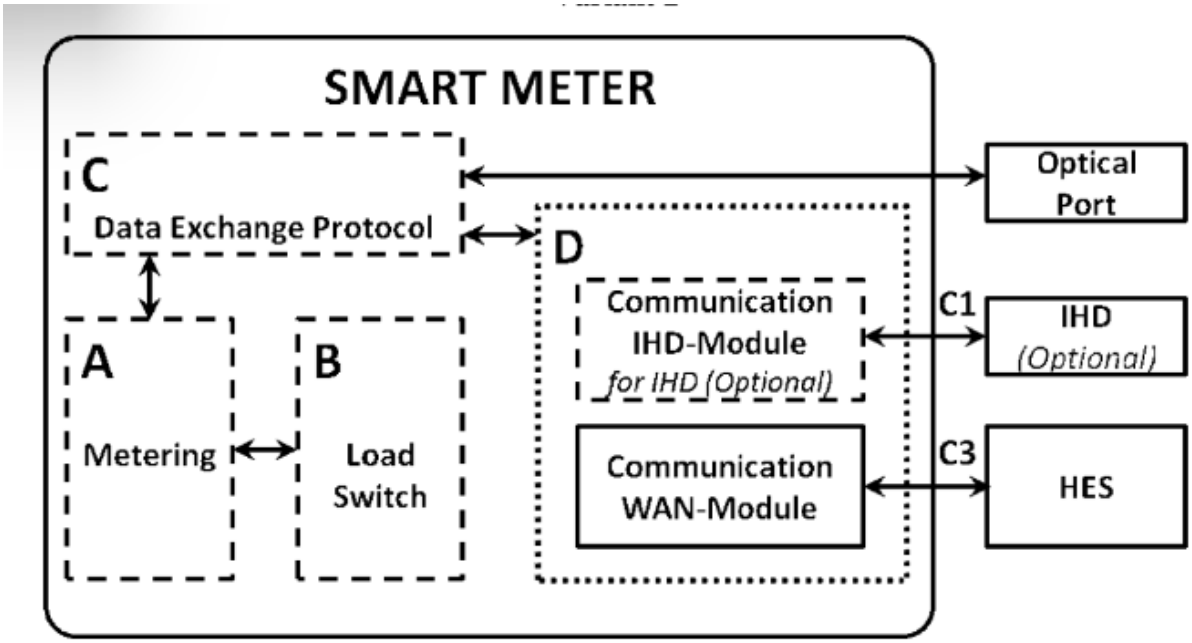
The Smart electricity meters may have wide usage and the buyer may like to choose desired features to meet the objectives of their overall system and site conditions. In order to facilitate such a flexible approach, the Smart electricity meter architecture are categorized into two variants. Based on the technical feasibility buyer may choose the combination of

the variants best suited for a given geographical area. The Smart electricity meter shall have either NAN or WAN module as mandatory communication module for communicating to DCU or HES respectively. The two variants are diagrammatically represented in Fig. 1 and Fig. 2.



A – Metrology C1 – IHD Connectivity SM IHD (optional)
C – Data Exchange and Metering Protocol C2 – NAN Connectivity SMDCU
D – Communication
NOTES
1 The smart electricity meter variant based on Fig. 1 shall provide connectivity C2 for two way communication with DCU using a NAN module.
2 If IHD is chosen this smart electricity meter shall provide connectivity C1 for two way communication with IHD using the same NAN module or a suitable additional module as per buyer-seller agreement.

Fig.1. Smart electricity meter architecture(Variant 1)



LEGEND

A – Metrology Optical port — As per IS 15959 (Part 2)

B – Load switch for control C1 – IHD Connectivity SM IHD (Optional)

C – Metering protocol C3 – WAN Connectivity SM HES

D – Communication

NOTES

1 The Smart electricity meter variant based on Fig. 2 shall provide connectivity C3 for two way communication with HES using a WAN module.

2 If IHD is chosen this Smart electricity meter shall provide connectivity C1 for two way communication with IHD using a suitable additional
module as per buyer-seller agreement.

Fig.2. Smart electricity meter architecture (variant 2)

Neighborhood Area Network [NAN] — This is a network comprising of group of smart electricity meters and any other network elements such as DCU all of which
communicate in a two way mode.

Data Concentrator Unit [DCU] — This device is part of NAN. It acts as a secured aggregate router and is an interface between smart electricity meter and HES. It shall facilitate secured two way data transfer either in transparent/store and forward mode as per system designs.

Head End System [HES] — This entity is a set of ICT based systems situated at the head of AMI. HES is responsible for handling security keys, passwords intended for smart electricity meter programmability and firmware upgrade and host applications such as remote connect/disconnect, analytics, billing, messaging etc.

In Home Display [IHD] — This is a compact display module meant for mounting inside the consumer premises. The IHD shall receive data/ messages from smart electricity meter and send responses to smart electricity meter as and when required from HES.
Hand Held Unit [HHU] — This is a device used to communicate locally over the optical port to the smart electricity meter.

Keeping in view of the device functionality and capabilities and referring to various standards on IoT security, specifically ETSI EN 303 645 V2.1.1 (2020-06), ENISA Baseline security recommendations for IoT November 2017, IoTSF IoT Security Assurance Framework Release 3.0 Nov 2021 Security Assurance Framework, GSMA CLP suitable common security requirements for the smart electricity meter are developed in this document. Also, specific security requirements are developed considering the industry specifications for the consumer smart electricity meter.

Classification of IoT devices based on Security Features

Making the whole diversity of IoT-class applications adhere to a common security objective is a subjective endeavour. Even within vertical sectors such as consumer and enterprise, the security measures and strength of controls will vary depending on the actual use case. Though international standards exist for IoT security viz., ETSI 303 645, IoT SF security framework for IoT, there is no harmonization of these standards. In an endeavour to classify IoT devices based on Security features, TEC (Telecom Engineering Centre) has mapped the device classifications from various standard bodies in its technical report- "Security by Design for IoT Device Manufacturers".
In the above report, TEC has also proposed "***Classification for IoT devices in India".*** This classification has IoT devices varying from Level-1 to Level-4 covering the CIA (Confidentiality, Integrity and Availability) triad requirements along with authentication and authorization covering baseline security requirements and principles of security by design.
The proposed classification has Level-1 meeting the baseline requirements, Level-2 adhering to international cybersecurity standards for IoT, Level-3 meeting the principles of security by design and having no known software vulnerabilities and Level-4 device being resistant to cyber security attacks by undergoing penetration testing.
To develop Indian Telecom Security Assurance Requirements (ITSARs) for the gamut of Consumer IoT devices, National Centre for Communication Security (NCCS) adopts the cybersecurity device classification proposed in the "Security by Design for IoT Device Manufacturers" report of TEC.

The TEC report also explains the four levels of IoT devices as below.

a) Level-1: Devices of this level must use a protocol stack specifically designed for IoT devices with constraints, such as Constrained Application Protocol (CoAP). Device examples in this category can include environmental sensors. Devices in this category should meet the baseline requirements of ETSI EN 303 645 i.e. no default password, ensuring the availability of security updates and implementing means to manage vulnerability reporting.
b) Level-2: Security requirement of Level-1 and adherence to international standards (secure identity, software asset security etc.).
c) Level-3: Absence of Known Common Software Vulnerabilities. The devices must meet the Security assurance requirements of Level-2 and also the software used in the connected device must be evaluated by a test laboratory using automated binary analysers to ensure that there is no known critical software weakness, vulnerabilities or malware.
d) Level-4: The device should perform well against the penetration tests by approved third party test labs, and fulfil Level-3 requirements. The IoT device undergoes penetration testing by a test laboratory to provide a basic level of resistance against common cybersecurity attacks.

Proposal for Device Classification						
Security Features	Security Requirements	Level-0	Level-1	Level-2	Level-3	Level-4
Confidentiality	Message Encryption	X	√	√	√	√
	Attack Protection	X	X	√	√	√
	Data Encryption	X	√	√	√	√
	Tamper Resistance	X	X	√	√	√
	Security Assessment Certificates	X	X	√	√	√
	Device ID Management (Physical/ Logical)	√	√	√	√	√
Integrity	Data Integrity	X	X	√	√	√
	Platform Integrity	X	X	√	√	√
	Secure Booting and Integrity Test / Self Test	X	X	X	√	√
Availability	Logging	√	√	√	√	√
	External Attack Prevention & Response	X	X	X	√	√
	Secure Monitoring	X	X	X	√	√
	Secure Firmware Update & Patch Update	X	√	√	√	√
	Software Assets Protection & Response	X	X	√	√	√
	Vulnerability Management & Response	X	√	√	√	√
	Security Policy Update & Response	X	X	X	√	√
Authentication/ Authorization	Biometrics	X	X	X	X	√
	User Authentication	X	√	√	√	√
	Data Authentication	X	X	√	√	√
	Password Management	X	√	√	√	√
	Access Control	√	√	√	√	√
	Device ID Verification	X	X	√	√	√

Security Assement and standard	Level-0	Level-1	Level-2	Level-3	Level-4
Meet Baseline Security Requirement					
Adherence to cyber security based on International Standards					
Adherence to the principles of Security by Design, and absence of known common software vulnerabilities					
Resistance against common cyber-attack and undergo for penetration testing					

Proposed levels for IoT devices[Ref: Table 7 Proposed levels for IoT devices from "Security by Design for IoT Device Manufacturers" published by TEC]

Classification of Security Requirements:

In order to apply an appropriate level of security assurance to an IoT product, This ITSAR has four levels of security requirements classified based on the classification of IoT devices proposed in "Security by Design for IoT Device Manufacturers" report of TEC.

The security requirements to be met by the IoT device under each level are explained below.

Level 1: Baseline Security Requirements

The level 1 product shall meet the requirement of no default password, ensuring the availability of security updates and implementing means to manage vulnerability reporting. It also shall meet the basic security requirements such as message encryption, data encryption, device ID management (Physical/Logical), logging availability, secure firmware update and patch update, vulnerability management and response, user authentication, password management and access control mechanisms.

Level 2: Adherence to Cybersecurity based on International Standards

In addition to fulfilling Level 1 requirements, the level 2 product shall have integrated features to provide adherence to cybersecurity such as attack protection, tamper resistance, security assessment certificates, data integrity, platform integrity, software assets protection and response, data authentication and device ID verification.

Level 3: Adherence to the Principles of Security-by-Design, and Absence of Known Common Software Vulnerabilities

In addition to fulfilling Level 2 requirements, the level 3 product shall have adherence to the principles of Security-by Design and absence of known common software vulnerabilities by using features like secure booting and integrity test / self-test, external attack prevention and response, secure monitoring and secure policy update and response.

Level 4: Resistance against Common Cyber-Attacks and undergo for penetration testing

In addition to fulfilling Level 3 requirements, the level 4 product shall have resistance against common cyber-attacks, it undergoes penetration testing and incorporates the usage of biometric authentication.

Minimum level of Security Certification

For the Smart Meter, the minimum-security certification required shall be at least Level 2 and above. In other words, for smart meters to get Security Certified as per this ITSAR, the minimum-security requirements to be met are Level 2 and above.

Chapter 2 – Common Security Requirements

Section1: Authentication

A. Level-1 Security requirements:

2.1.A.1 Default passwords and user names

Requirement:

a) The device shall enforce the factory-issued/OEM login accounts and factory-default usernames to be disabled/erased or renamed when installed or commissioned.

b) The device shall enforce all the factory default user login passwords altered when installed or commissioned. Weak, common, null, or blank passwords shall not be allowed.

[Ref: 1. ENISA Baseline security recommendations for IoT November 2017 GP-TM-22,
2. IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.8.12 and 2.4.8.13]

2.1.A.2 Hardcoded authentication credentials

Requirement:

The manufacturer shall submit an undertaking that authentication credentials for users, devices, or services are not hardcoded in firmware or applications.

[Ref: OWASP ISP 2.1.9]

2.1.A.3 Unique passwords

Requirement:

Where passwords are used and, in any state, all consumer IoT 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]

2.1.A.4 Multiple user accounts

Requirement:

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

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

B. Level-2 Security Requirements:

2.1.B.1 Authentication credentials

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 security recommendations for IoT November 2017, GP-TM-24]

2.1.B.2 Username and password reset

Requirement:

Manufacturer shall provide generally accepted username and password reset 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]

2.1.B.3 Logical access

Requirement:

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

[Ref: NIST 8228 Expectation 10]

2.1.B.4 Pairing and connecting with other devices

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]

2.1.B.5 Provisioned credentials

Requirement:

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

[Ref: OWASP ISVS 2.1.10]

2.1.B.6 Changing authentication value

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]

2.1.B.7 New and common passwords

Requirement:

The device 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]

2.1.B.8 Changing authentication password

Requirement:

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

[Ref: OWASP ISVS 2.1.6]

2.1.B.9 Display of user credentials

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]

C. Level-3 Security Requirements:

2.1.C.1 Multi-factor authentication

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, certificates etc.

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

2.1.C.2 Trusted Computing Base (TCB)

Requirement:

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

[Ref. GSMA CLP.12 4.2]

2.1.C.3 Brute force Attacks

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 within a certain time interval

[Ref: 1. IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.13.15, 2.4.8.7,
2. ENISA Baseline security recommendations for IoT November 2017 GP-TM-25 and ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-5]

2.1.C.4 Locking of account

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]

D. Level-4 Security Requirements:

Nil

Section 2: Identity Management

A. Level-1 Security Requirements:

2.2.A.1 Physical and logical identifiers

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 the logical identifier.

[Ref: NIST 8259A Device Identification]

B. Level-2 Security Requirements:

2.2.B.1 Hardcoded unique identity

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]

2.2.B.2 Root of Trust

Requirement:

Manufacturer shall submit an undertaking that 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]

2.2.B.3 Consistent authentication security

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]

C. Level-3 Security Requirement:

Nil

D. Level-4 Security Requirements:

Nil

Section 3: Authorization and access controls

A. Level-1 Security Requirements:

2.3.A.1 Common authorization framework

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]

2.3.A.2 Failure of access controls

Requirement:

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

[Ref: OWASP ASVS 4.1.5]

2.3.A.3 Directory browsing

Requirement:

Directory browsing shall be disabled. 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]

2.3.A.4 Manipulation of user and data attributes

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]

2.3.A.5 Access control privileges

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]

2.3.A.6 Protection against spoofing

Requirement:

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

2.3.A.7 Access to sensitive information

Requirement:

The device 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]

2.3.A.8 Controlled user account access

Requirement:

The device shall only allow controlled user account access; access using anonymous, or guest user accounts shall not be supported.

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

2.3.A.9 Access to debug capabilities

Requirement:

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

[Ref: OWASP ISVS 2.2.4]

2.3.A.10 Recording of data

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]

2.3.A.11 Reset of authorized information

Requirement:

The device 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]

B. Level-2 Security Requirements:

Nil

C. Level-3 Security Requirements:

2.3.C.1 Trusted service layer

Requirement:

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

[Ref: OWASP ASVS 4.1.1]

2.3.C.2 Administration interfaces

Requirement:

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

[Ref: 1. IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.10.13] and 2. OWASP ISVS 4.3.1]

D. Level-4 Security Requirements:

Nil

Section 4: Securely storing sensitive information.

A. Level-1 Security Requirements:

Nil

B. Level-2 Security Requirements:

2.4.B.1 Sensitive security parameters

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]

2.4.B.2 Hardcoded security parameters

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]

2.4.B.3 Secure storing of passwords

Requirement:

The device shall securely store any passwords using secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)”.

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

2.4.B.4 Salting and hashing of passwords

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 shall take a password, a salt, and a cost factor as inputs when generating a password hash. 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 2.4.1 & OWASP ASVS 2.4.2]

2.4.B.5 bcrypt

Requirement:

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

[Ref: OWASP ASVS 2.4.4]

C. Level-3 Security Requirements:

2.4.C.1 Secure provisioning of security parameters

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]

2.4.C.2 Storing of sensitive data

Requirement:

OEM shall ensure that sensitive data, such as private keys and certificates, shall be stored securely by leveraging dedicated hardware security features.

[Ref: OWASP ISVS 5.1.4]

2.4.C.3 Personal Identifiable Information (PII)

Requirement:

Sensitive information, such as personal identifiable information (PII) and credentials shall be stored securely using secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)".

[Ref: OWASP ISVS 2.3.1]

2.4.C.4 PBKDF2

Requirement:

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

[Ref: OWASP ASVS 2.4.3]

2.4.C.5 Secret salt value

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]

2.4.C.6 Tamper-resistant storage of sensitive data

Requirement:

UICC should be used for tamper-resistant storage of sensitive data for services, including security keys controlled by the service provider. In case the device utilizes SIM, requirements as per the latest document on "Pluggable (U)ICC (SIM, USIM and other (U)ICC based applications/applets)," shall be fulfilled. (e)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]

2.4.C.7 Trusted Computing Base (TCB)

Requirement:

If Trusted Computing Base has been implemented, the unique identifier shall be stored in the TCB's trust anchor.

[Ref: GSMA CLP.13 6.6]

2.4.C.8 RoT backed IDs

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]

2.4.C.9 Trust Anchor

Requirement:

Tamper resistant Trust Anchor shall be used.

[Ref: GSMA CLP.13 6.3]

D. Level-4 Security Requirements:

2.4.D.1 Cryptographic Root of Trust

Requirement:

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

[Ref: OWASP ISVS 1.2.6]

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

A. Level-1 Security Requirements:

2.5.A.1 Erasing user data

Requirement:

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

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

2.5.A.2 Deletion of personal data

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]

2.5.A.3 Conformation of personal data deletion

Requirement:

Users shall be provided with clear confirmation that personal data has been deleted from the device.

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

B. Level-2 Security Requirements:

Nil

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 6: Data Protection

A. Level-1 Security Requirements:

2.6.A.1 Privacy notice about personal data collection

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:
» data to be processed
» data uses (unless obvious from context)

[Ref: GSMA CLP.11 PDR1.1]

2.6.A.2 Authorization for recording data

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]

2.6.A.3 Data retention policy

Requirement:

If the device manufacturer retains any data, data retention policy shall be disclosed to users.

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

2.6.A.4 Consequences of sharing of personal data

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

[Ref: 1. Agelight IoT Safety Architecture & Risk Toolkit v4.0 30,
2. ETSI EN 303 645 V2.1.0 (2020-04) Provision 6-3]

2.6.A.5 IoT service identity

Requirement:

In case the device supports IoT service identity, 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]

2.6.A.6 Re-assignment of service identities

Requirement:

In case the device supports IoT service identity, the manufacturer shall provide individuals with the means to associate, disassociate and re-assign their IoT service identities.

2.6.A.7 Data in browser storage

Requirement:

Data stored in browser storage (such as local Storage, session Storage, Indexed DB, or cookies) shall not contain sensitive data.

[Ref: OWASP ASVS 8.2.2]

2.6.A.8 Clearance of authenticated data

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]

2.6.A.9 Remove or export data on demand

Requirement:

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

[Ref: OWASP ASVS 8.3.2]

2.6.A.10 Updating of personal information

Requirement:

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

[Ref: GSMA CLP.11 PDR 5.3]

2.6.A.11 Telemetry data collection

Requirement:

If telemetry data is collected from the device, 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]

B. Level-2 Security Requirements:

2.6.B.1 Sensitive information in memory

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]

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 7: Secure input and output handling

A. Level-1 Security Requirements:

Nil

B. Level-2 Security Requirements:

2.7.B.1 Validation of input data and transferred data

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]

2.7.B.2 Validation of inputs and outputs

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]

2.7.B.3 Verification of inputs and outputs

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]

2.7.B.4 Validation checks

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]

2.7.B.5 Validation of application output data

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]

2.7.B.6 Warning regarding potentially untrusted content

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]

2.7.B.7 Validation of inputs

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]

2.7.B.8 Structured data validation

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]

C. Level-3 Security Requirements:

2.7.C.1 HTTP parameter pollution attacks

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]

2.7.C.2 Mass parameter assignment attacks

Requirement:

Mass parameter assignment attacks shall be protected by frameworks, or the application shall have countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.

[Ref: OWASP ISVS 5.1.2]

2.7.C.3 OS command injection

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]

D. Level-4 Security Requirements:

Nil

Section 8: Communicate Securely

A. Level-1 Security Requirements:

2.8.A.1 Cryptographic algorithms and primitives

Requirement:

Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” shall only be used. Such cryptographic algorithms and primitives shall be updateable.

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

2.8.A.2 Internal or external traffic

Requirement:

Internal or external traffic must not expose the device credentials.

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

2.8.A.3 Enabling specific ports

Requirement:

Only specific ports that are necessary shall be enabled and all other ports shall be disabled.

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

2.8.A.4 Secure connection with remote servers

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]

2.8.A.5 Access via network interface

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]

2.8.A.6 Configuration changes via network interface

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]

2.8.A.7 Web interfaces

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]

2.8.A.8 Communication of sensitive data between device and associated services

Requirement:

The confidentiality of sensitive personal data communicated between the device and associated services shall be protected. Critical security parameters should be encrypted in transit. 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 5.8-2]

2.8.A.9 Communication of personal data between device and web interface

Requirement:

Any personal data communicated between the web interface/mobile app and the device shall be encrypted. Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used.

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

2.8.A.10 Sensitive data through HTTP message

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 shall not contain sensitive data.

[Ref: OWASP ASVS 8.3.1]

B. Level-2 Security Requirements:

2.8.B.1 End-user security and privacy alerts

Requirement:

End-user security and privacy alerts and communications, including but not limited to email and SMS, shall be adopted by the 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]

2.8.B.2 Authentication of data received from other devices

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]

2.8.B.3 Authentication of connections at all levels of protocols

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]

C. Level-3 Security Requirements:

2.8.C.1 Cloud service

Requirement:

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

2.8.C.2 TLS

Requirement:

TLS 1.2 and above shall be used regardless of the sensitivity of the data being transmitted. Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used.

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

2.8.C.3 Webserver products

Requirement:

Where a product related to a webserver encrypts 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 SF IoT Security assurance framework Release 3.0 November 2021 2.4.13.9]

2.8.C.4 Verification of X.509 certificate - TLS

Requirement:

If TLS 1.2 and above is used, then the device shall cryptographically verify the X.509 certificate.

[Ref: OWASP ISVS 4.1.3]

2.8.C.5 Certificate and keys - TLS

Requirement:

If TLS 1.2 and above is used, 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]

2.8.C.6 Client server model

Requirement:

If client server model is used for communication, then 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]

2.8.C.7 Insecure algorithms and ciphers

Requirement:

Disable deprecated or known insecure algorithms and ciphers.

[Ref: OWASP V4 Communication requirements control objective]

2.8.C.8 Replay attacks

Requirement:

Protection against replay attacks shall be built into the device.

[Ref: OWASP ISVS 4.1.1]

2.8.C.9 Security for email notifications

Requirement:

The device shall implement transport-level security as per Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” for email notifications to ensure the privacy of the communication while in transit.

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

D. Level-4 Security Requirements:

Nil

Section 9: Cryptography

A. Level-1 Security Requirements:

2.9.A.1 Cryptographic controls

Requirement:

A policy on the use of Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” for the protection of information shall be developed and implemented.

[Ref: ISO:27001 A.12.3.1]

2.9.A.2 Cryptographic libraries

Requirement:

Cryptographic libraries used to implement Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall be certified to be compliant with a recognized cryptographic security standard.

[Ref: OWSAP ISVS 2.4.6]

2.9.A.3 Cryptographic keys

Requirement:

Cryptographic secrets and keys shall be unique per device.

[Ref: OWASP ISVS 2.4.1]

2.9.A.4 Cryptographic key chain

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]

2.9.A.5 Secure sources of randomness

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]

2.9.A.6 Provisioning of security parameters and keys

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]

B. Level-2 Security Requirements:

2.9.B.1 Confidentiality, authenticity, and/or integrity of data

Requirement:

Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic

Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall be used to protect the confidentiality, authenticity, and/or integrity of data and information (including control messages), in transit and in rest.

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

2.9.B.2 Secured sessions

Requirement:

Secure session shall be established after each disconnected session to prevent intentional and unintentional Denial of Service (DoS).

[Ref: GSMA CLP.13 9.1]

2.9.B.3 Storage of sensitive unencrypted parameters

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]

2.9.B.4 Applications stored outside CPU's core EEPROM

Requirement:

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

[Ref: GSMA CLP.13 6.11]

C. Level-3 Security Requirements:

2.9.C.1 API for the TCB

Requirement:

The device shall utilize an API for the TCB.

[Ref: GSMA CLP.13 6.4]

2.9.C.2 Trust Anchor

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]

D. Level-4 Security Requirements:

Nil

Section 10: Minimize Exposed Attack Surfaces

A. Level-1 Security Requirements:

2.10.A.1 Removal of silk screens from PCBs

Requirement:

The descriptive silkscreens shall be removed from PCBs and debug paths and traces are depopulated from production PCBs.

[Ref: OWASP ISVS 5.1.10]

2.10.A.2 Secret keys in a product family

Requirement:

The manufacturer should submit an undertaking that the same secret key is not used in an entire product family. Compromising a single device would be enough to expose the rest of the product family.

[Ref: ENISA Baseline security recommendations for IoT November GP-TM-49]

2.10.A.3 Security of test/debug modes

Requirement:

The device 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]

2.10.A.4 Unused communication ports

Requirement:

All communications port(s) which are not used as part of the device's normal operation shall not be physically accessible and shall be disabled.

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

2.10.A.5 Debugging headers

Requirement:

Debugging headers shall be removed from PCBs.

[Ref: OWASP ISVS 5.1.6]

B. Level-2 Security Requirements:

2.10.B.1 Physical decapsulation, side channel and glitching attacks

Requirement:

The 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]

2.10.B.2 Debugging and Testing Technologies

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]

2.10.B.3 Unofficially documented debug features

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]

2.10.B.4 Unused network and logical interfaces

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]

2.10.B.5 Software services

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]

2.10.B.6 Software development processes

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]

2.10.B.7 Build environment of each application

Requirement:

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

[Ref: OWASP ISVS 1.3.1]

2.10.B.8 GPL-based firmware

Requirement:

The manufacturer shall submit 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]

2.10.B.9 Safe equivalents functions

Requirement:

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

[Ref: OWASP ISVS 1.3.3]

2.10.B.10 Builds of source code

Requirement:

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

[Ref: OWASP ISVS 1.3.5]

2.10.B.11 Compilers, version control clients, development utilities, and software development kits

Requirement:

The manufacturer shall submit 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]

2.10.B.12 Compilation of packages

Requirement:

The manufacturer shall submit an undertaking that packages are compiled with Object Size Checking (OSC) (e.g. -D_FORTIFY_SOURCE=2), No eXecute (NX) or Data Execution Protection (DEP) (e.g. -z,noexecstack), Position Independent Executable (PIE) (e.g. -fPIE), Stack Smashing Protector (SSP) (e.g. -fstack-protector-all), read-only relocation (RELRO) (e.g. -Wl,-z,relro)

[Ref: OWASP ISVS 1.3.7]

2.10.B.13 Release builds

Requirement:

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

[Ref: OWASP ISVS 1.3.12]

2.10.B.14 Debug and release firmware

Requirement:

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

[Ref: OWASP ISVS 1.3.13]

2.10.B.15 Debug information

Requirement:

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

[Ref: OWASP ISVS 1.3.14]

2.10.B.16 Debug interface

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]

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 11: Vulnerability Management

A. Level-1 Security Requirements:

2.11.A.1 Vulnerability management related policies

Requirement

The manufacturer shall submit an undertaking that the following policies/processes are in place for

a) receiving reports of vulnerabilities
b) recording reported vulnerabilities
c) responding to reported vulnerabilities, including the process of coordinating vulnerability response activities among component suppliers and third-party vendors.
d) disclosing reported vulnerabilities.
e) 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.
f) interacting with both internal and third-party security researcher(s) on the products or services.
g) conflict resolution process for Vulnerability Disclosures
h) Security advisory notification
i) Retention of the key security design information and risk analysis over the whole lifecycle of the product or service.
j) Informing users and relevant stakeholders when vulnerabilities affect products through established communication channels (website, e-mail, security advisory pages, changelogs, etc.).

2.11.A.2 Software Component Transparency

Requirement:

The manufacturer shall submit 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]

2.11.A.3 Vulnerability scanners

Requirement:

The device shall support the use of vulnerability scanners.

[Ref: NIST 8228 Expectation-7]

2.11.A.4 Hardening of compiler language

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]

2.11.A.5 Third party and open source software

Requirement:

The manufacturer shall identify the third party and open source software that are used in the device.

[Ref: OWASP ISVS 1.2.2]

B. Level-2 Security Requirements:

2.11.B.1 Abnormal number of requests

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]

C. Level-3 Security Requirements:

2.11.C.1 Review of device OS

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]

2.11.C.2 Continuous monitoring of security vulnerabilities

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]

D. Level-4 Security Requirements:

2.11.D.1 Pentesting strategy

Requirement:

The Device shall implement a complete persistent pentesting strategy.

[Ref: GSMA CLP-13 7.11]

Section 12: Incident Management

A. Level-1 Security Requirements:

2.12.A.1 Operational and security events

Requirement:

The device shall log its operational and security events.

[Ref: NIST Expectation 15]

B. Level-2 Security Requirements:

2.12.B.1 Detection of potential incidents

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]

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 13: Make Systems Resilient to Outages

A. Level-1 Security Requirements:

2.13.A.1 Access control during initial connection

Requirement:

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

[Ref: NIST Whitepaper]

B. Level-2 Security Requirements:

Nil

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 14: Keep Software Updated

A. Level-1 Security Requirements:

2.14.A.1 Remote update

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]

2.14.A.2 Secure update

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]

2.14.A.3 Authenticate to update server

Requirement:

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

[Ref: OWASP ISVS 3.4.10]

2.14.A.4 Authenticity of the update

Requirement:

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

[Ref: OWASP ISVS 3.4.4]

2.14.A.5 Automatic updates and/or update notifications

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]

2.14.A.6 Checking for security updates

Requirement:

The device should check after initialization, and then periodically, whether security updates are available. Security 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 5.3-5]

2.14.A.7 Notification during software update

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]

2.14.A.8 Over-The-Air (OTA) update

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. Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” shall only be used.

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

2.14.A.9 Failure of update

Requirement:

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

[Ref: OWASP ISVS 3.4.7]

B. Level-2 Security Requirements:

2.14.B.1 Authenticity and integrity of software updates

Requirement:

1. 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.
2. The updates shall be cryptographically signed by a trusted source and their authenticity and integrity shall be verified via a trust relationship before execution.
3. The digital signature, signing certificate and signing certificate chain of the software update package shall be verified by the device before the update process begins.
4. The Signing Authority shall be clearly identified.

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

C. Level-3 Security Requirements:

2.14.C.1 Firmware-update through peer

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]

D. Level-4 Security Requirements:

Nil

Section 15: Ensure Software Integrity

A. Level-1 Security Requirements:

2.15.A.1 Unauthorized phone home or data collection capabilities

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]

2.15.A.2 Permissions to privacy related features or sensors

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]

2.15.A.3 Back doors

Requirement:

Manufacturer shall submit an undertaking that 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

[Ref: OWASP ASVS 10.2.3, 10.2.5 and 10.2.6]

2.15.A.4 Time bombs

Requirement:

Manufacturer shall submit an undertaking that 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]

2.15.A.5 Minimum access privileges

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]

2.15.A.6 OS command line access

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]

2.15.A.7 Device's OS kernel and services

Requirement:

All the device's OS kernel and services or functions shall be disabled by default unless specifically required.

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

2.15.A.8 Device`s OS kernel design

Requirement:

The device`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]

2.15.A.9 User interface

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]

2.15.A.10 LINUX

Requirement:

If LINUX is used,

- processes shall be isolated using Linux kernel namespaces.
- critical processes shall be configured to limit resources using control groups (cgroups).
- Linux kernel capabilities shall be configured with a minimal set for processes that require elevated access.
- SECure COMPuting (seccomp BPF) with filters shall be used and properly configured to only allow necessary system calls.
- the use of kernel security modules such as SELinux, AppArmor, GRSEC, shall be alike.

[Ref: OWASP ISVS 3.3]

B. Level-2 Security Requirements:

2.15.B.1 Integrity protections

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]

2.15.B.2 Cryptographically signed code

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]

2.15.B.3 Updation of OS kernel

Requirement:

The OS kernel shall be up to date.

[Ref: OWASP ASVS 3.2.4]

2.15.B.4 Persistent filesystem storage

Requirement:

Persistent filesystem storage volumes shall be encrypted.

[Ref: OWASP ASVS 3.2.5]

2.15.B.5 Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP)

Requirement:

Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) should be enabled.

[Ref: OWASP ASVS 3.2.7]

2.15.B.6 Security features supported by the OS

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]

2.15.B.7 Separation architecture of OS

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 2.4.6.11]

C. Level-3 Security Requirements:

2.15.C.1 Secure boot mechanisms

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

2.15.C.2 Controls against malicious code

Requirement:

Controls against malicious code: Control Detection, prevention, and recovery controls to protect against malicious code

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

2.15.C.3 Unnecessary Services Removal

Requirement:

The device shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on the device by the vendor except if services are needed during deployment. In that case those services shall be disabled according to vendor's instructions after deployment is done. Disabled protocols may still need to be enabled for other reasons by the operators, e. g. remote diagnostics.

- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Telnet
- rlogin, Rate Control Protocol (RCP), Remote Shell Protocol (RSH)
- HTTP
- Simple Network Management Protocol (SNMP) v1 and v2
- SSHv1
- Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- Bootstrap Protocol (BOOTP) server
- Discovery protocols (Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP))
- IP Identification Service (Identd)
- Packet Assembler/Disassembler (PAD)
- Maintenance Operations Protocol (MOP)

Any other protocols, services that are vulnerable are also to be permanently disabled. Full documentation of required protocols and services (communication matrix) of the device and their purpose needs to be provided by the OEM as a prerequisite for the test case.

[Ref: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.2.1]

2.15.C.4 Controls against mobile code

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]

2.15.C.5 Detection of malicious codes

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]

2.15.C.6 Integrity Measurement Architecture (IMA)

Requirement:

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

Ref: OWASP ASVS 3.2.10]

D. Level-4 Security Requirements:

Nil

Section 16: Firmware and Bootloader Security

A. Level-1 Security Requirements:

2.16.A.1 Configuration of firmware

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]

2.16.A.2 Design of device firmware

Requirement:

Device firmware shall be designed to isolate privileged code and data from portions of the firmware that do not need access to them

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

B. Level-2 Security Requirements:

Nil

C. Level-3 Security Requirements:

2.16.C.1 Secure boot process

Requirement:

The secure boot process shall be enabled by default, and the device'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]

2.16.C.2 Authenticity of first stage boot loader

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]

2.16.C.3 Default/standard boot loader

Requirement:

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

[Ref: GSMA CLP.13 6.17]

2.16.C.4 Authenticity of boot loader stages

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]

2.16.C.5 Executable image of first-stage boot loader

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]

2.16.C.6 Boot loading

Requirement:

Boot loading should be outside of internal EEPROM.

[Ref: GSMA CLP.13 6.15]

2.16.C.7 Direct Memory Access (DMA)

Requirement:

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

[Ref: OWASP ISVS 3.1.8]

2.16.C.8 Sensitive information in boot loader stages

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]

2.16.C.9 Code loading of boot loader

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]

2.16.C.10 Communication interfaces

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]

D. Level-4 Security Requirements:

Nil

Section 17: Hardware security

A. Level-1 Security Requirements:

2.17.A.1 Non-volatile memory's contents

Requirement:

Where microcontroller/ microprocessor(s) reads the firmware from a separate non-volatile memory device, the non-volatile memory's contents shall be encrypted.

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

B. Level-2 Security Requirements:

2.17.B.1 Minimum Viable execution Platform

Requirement:

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

[Ref: GSMA CLP.13 6.7]

2.17.B.2 Security configuration of the platform

Requirement:

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

[Ref: OWASP ISVS 5.1.5]

C. Level-3 Security Requirements:

2.17.C.1 CPU watchdog

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]

D. Level-4 Security Requirements:

Nil

Section 18: Installation and Maintenance

A. Level-1 Security Requirements:

2.18.A.1 Security logs

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]

2.18.A.2 Contents of logs

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]

2.18.A.3 Device synchronization

Requirement:

The device shall be synchronized with a reliable time source to ensure the validity of log timestamps.

[Ref: OWASP ISVS 1.4.3]

2.18.A.4 Sensitive information in logs

Requirement:

Verify that collected logs do not include sensitive information, such as PII, credentials and cryptographic keys.

[Ref: OWASP ISVS 1.4.4]

2.18.A.5 Online collection of logs

Requirement:

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

[Ref: OWASP ISVS 1.4.5]

2.18.A.6 Privacy settings and preferences

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]

2.18.A.7 Secured set up of the device

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]

B. Level-2 Security Requirements:

2.18.B.1 Tamper Evident measures

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]

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 19: Supply Chain

A. Level-1 Security Requirements:

2.19.A.1 Shipping of device

Requirement:

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

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

B. Level-2 Security Requirements:

Nil

C. Level-3 Security Requirements:

2.19.C.1 Generation of encryption keys

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. The manufacturer shall submit an undertaking in this regard.

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

D. Level-4 Security Requirements:

Nil

Chapter 3 – Specific Security Requirements

Section 1: Bluetooth

A. Level-1 Security Requirements:

3.1.A.1 PIN/ Pass-key code

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]

3.1.A.2 Encryption keys

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]

3.1.A.3 Pairing methods

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]

3.1.A.4 Bluetooth Security Mode and Level

Requirement:

The strongest Bluetooth Security Mode and Level supported by the device shall be used. For Bluetooth 4, Security Mode 4, Level 4 shall be used. For Bluetooth 2.1 through 4.0

devices, Security Mode 4, Level 3 shall be used, and for Bluetooth 2.0 and older devices Security Mode 3 is recommended.

[Ref: OWASP ISVS 4.3.7]

3.1.A.5 Encryption of Bluetooth connections

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]

B. Level-2 Security Requirements:

3.1.B.1 Pairing and discovery

Requirement:

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

[Ref: OWASP ISVS 4.3.1]

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 2: Zigbee

A. Level-1 Security Requirements:

3.2.A.1 Version

Requirement:

Zigbee version 3.0 and above shall be used

[Ref: OWASP ISVS 4.5.1]

3.2.A.2 Joining Zigbee network

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]

3.2.A.3 Pre-configured global link key

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]

3.2.A.4 Activation of pairing mode

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]

3.2.A.5 Network key generation

Requirement:

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

[Ref: OWASP ISVS 4.5.6]

3.2.A.6 Network key regeneration

Requirement:

The network key shall be periodically regenerated.

B. Level-2 Security Requirements:

3.2.B.1 Validation of Paired Devices

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]

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 3: Wi-Fi

A. Level-1 Security Requirements:

3.3.A.1 Disabling Wi-FI connectivity

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 4.4.2]

3.3.A.2 Protection of Wi-Fi communications

Requirement:

WPA2 or higher shall be used to protect Wi-Fi communications. In case WPA is used, it shall be encrypted with AES (CCMP mode).

[Ref: OWASP ISVS 4.4.3]

3.3.A.3 Use of Wi-Fi Protected Setup (WPS)

Requirement:

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

[Ref: OWASP ISVS 4.4.4]

B. Level-2 Security Requirements:

3.3.B.1 SSIDs

Requirement:

The SSIDs should not be the default and should be hidden for all connected devices, reducing the attack surface of a brute-force attack.

[Ref: OWASP ISVS 4.4.1]

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 4: LTE

A. Level-1 Security Requirements:

3.4.A.1 Confidentiality on the Air Interface

Requirement:

LTE shall enable Confidentiality on the Air Interface.

[Ref: NIST SP 800-187 5.2]

3.4.A.2 Ciphering Indicator

Requirement:

LTE shall use the Ciphering Indicator

[Ref: NIST SP 800-187 5.3]

3.4.A.3 SIM/USIM PIN Code

Requirement:

The device shall use SIM/USIM PIN Code

[Ref: NIST SP 800-187 5.7]

3.4.A.4 Temporary Identities

Requirement:

LTE shall use Temporary Identities

[Ref: NIST SP 800-187 5.8]

B. Level-2 Security Requirements:

Nil

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 5: LoRaWAN

A. Level-1 Security Requirements:

3.5.A.1 Version

Requirement:

LoRaWAN version 1.1 or above shall be used.

[Ref: OWASP ISVS 4.6.1]

3.5.A.2 Root keys

Requirement:

Root keys shall be unique per end device.

[Ref: OWASP ISVS 4.6.4]

B. Level-2 Security Requirements:

3.5.B.1 Replay attacks

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]

C. Level-3 Security Requirements:

3.5.C.1 Communication with LoRaWAN gateway

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]

D. Level-4 Security Requirements:

Nil

Section 6: Other Security Requirements

A. Level-1 Security Requirements:

3.6.A.1 Private Access Point Name

Requirement:

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

3.6.A.2 Compliance to Pluggable (U)ICC ITSAR

Requirement:

The SIM card used in the smart electricity meter shall meet the security requirements as specified in the ITSAR on “Pluggable (U)ICC” which is under enforcement.

B. Level-2 Security Requirements:

Nil

C. Level-3 Security Requirements:

Nil

D. Level-4 Security Requirements:

Nil

Section 7: Meter specific security Requirements

A. Level-1 Security Requirements:

3.7.A.1 Separation between measurement functionality and communication functionality

Requirement:

The Smart Meter shall separate measurement functionality from communication functionality, so that it keeps measuring electricity correctly under denial-of-service attacks.

[Ref: Security requirements for procuring smart electricity meters and data concentrators (ENCS) SRR.01.SM Separation of Measurement from Communication]

3.7.A.2 Personally Identifiable Information

Requirement:

Manufacturer shall share details of the PII collected by the device and the device shall ensure that PII is encrypted and is accessible only after successful authentication and authorization.

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

3.7.A.3 Built-in patch, upgrade, and configuration management capabilities

Requirement:

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

[Ref: NIST 8228 Expectation 6]

3.7.A.4 First breath and Last gasp detection condition

Requirement:

Smart Meter shall detect 'First breath (power on) and Last gasp (power off)' condition and communicate to Head End System (HES).

[Ref: (IS 16444 Part 1) 11.7]

3.7.A.5 Secured downloading of meter data from memory

Requirement:

The manufacturer shall provide software capable of securely downloading all the data stored in meter memory.

[Ref: Protection Profile for Smart electricity meter Minimum Security requirements(ETSI) 9.4 Software for local communication]

3.7.A.6 Isolation of ports

Recommendation:

All ports shall be optically isolated from the power circuit

3.7.A.7 Removal of unnecessary packages

Requirement:

All unnecessary packages must be removed and/or disabled from the system. Additionally, all unused operating system services and unused networking ports must be disabled or blocked. Only secure maintenance access shall be permitted and all known insecure protocols shall be disabled.

[Ref: Smart electricity meter Security: vulnerabilities, threat impacts, and countermeasures, Hardening]

3.7.A.8 Loss of network access

Requirement:

Smart Meters 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]

3.7.A.9 Reconnection of device after restoration of power

Requirement:

Following restoration of power or network connection, device shall be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect, which collectively could overwhelm a network.

[Ref: IoT SF IoT Security Assurance Framework Release 3.0 November 2021 2.4.7.25]

B. Level-2 Security Requirements:

3.7.B.1 Communication modules

Requirement:

The communication modules shall be either built in type or plug in type.The plug-in communication modules shall be properly secured on the smart meter, both physically and electrically, so as to avoid any possible tampering with adequate provision for sealing. The load switch for disconnect/ connect purpose shall be mounted inside the meter with suitable arrangement.

[Ref: IS16444(Part 1) 6.2 General Constructional Requirements]

3.7.B.2 Notifying physical tampering

Requirement:

The smart meter should monitor and notify when physical tampering of the type Magnetic interference occurs.

[Ref: Protection Profile for Smart electricity meter Minimum Security requirements(ETSI) FPT_TNN.1.1]

3.7.B.3 Effect of remote control device on meter

Requirement:

The manufacturer shall submit an undertaking that the meter shall not get affected by any remote-control device & shall continue recording energy

[Ref: Protection Profile for Smart electricity meter Minimum Security requirements(ETSI) 7.9Connection Related Tamper Conditions]

C. Level-3 Security Requirements:

3.7.C.1 Preserving secure state during failure

Requirement:

The smart meter shall preserve a secure state when the following types of failures occur:
(1) Watchdog trigger results in meter reset
(2) Failure of the random bit generator

[Ref: Protection Profile for Smart electricity meter Minimum Security requirements(ETSI) FPT_FLS.1.1]

3.7.C.2 Returning to secure state

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 IoT November 2017 , GP-TM-06]

D. Level-4 Security Requirements:

Nil

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. **Authentication** – The verification of the claimed identity of an application user.
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. **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
8. **Consumer**: Natural person who is acting for purposes that are outside her/his trade, business, craft or profession
9. **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
10. **Critical security parameter**: Security-related secret information whose disclosure or modification can compromise the security of a security module
11. **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
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. **Initialized state**: State of the device after initialization
17. **IoT product**: Consumer IoT device and its associated services

18. **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
19. **Logical interface**: Software implementation that utilizes a network interface to communicate over the network via channels or ports
20. **Manufacturer**: Relevant economic operator in the supply chain (including the device manufacturer)
21. **Master key**: HES have a record of the master key of each meter in the system. The master key is a private key and its confidentiality is to be preserved. The master key is never transmitted between the clients and servers of the system.
22. **Network interface**: Physical interface that can be used to access the functionality of consumer IoT via a
23. **Network owner**: User who owns or who purchased the device
24. **Personal data**: Any information relating to an identified or identifiable natural person
25. **Physical interface**: Physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer
26. **Public security parameter**: Security related public information whose modification can compromise the security of a security module
27. **Remotely accessible**: Intended to be accessible from outside the local network
28. **Security module**: set of hardware, software, and/or firmware that implements security functions
29. **Sensitive data**: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the device, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
30. **Security update**: Software update that addresses security vulnerabilities either discovered by or reported to the manufacturer
31. **Sensitive security parameters**: Critical security parameters and public security parameters
32. **Software service**: Software component of a device that is used to support functionality
33. **Telemetry**: Data from a device that can provide information to help the manufacturer identify issues or information related to device usage
34. **Unique per device**: Unique for each individual device of a given product class or type
35. **User**: Natural person or organization
36. **Application Security Verification**: The technical assessment of an application against the OWASP ASVS
37. **Component**: a self-contained unit of code, with associated disk and network interfaces that communicates with other components.

38. **Cryptographic module**: Hardware, software, and/or firmware that implements cryptographic algorithms and/or generates cryptographic keys
39. **Design Verification**: The technical assessment of the security architecture of an application.
40. **Hardcoded keys**: Cryptographic keys which are stored on the filesystem, be it in code, comments or files.
41. **Hardware Security Module (HSM)**: Hardware component which is able to store cryptographic keys and other secrets in a protected manner.
42. **Input Validation**: The canonicalization and validation of untrusted user input
43. **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!
44. **One-time Password (OTP)**: A password which is uniquely generated to be used on a single occasion.
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. **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.
47. **Transport Layer Security (TLS)**: Cryptographic protocols that provide communication security over a network connection
48. **Two-factor authentication (2FA)**: This adds a second level of authentication to an account log-in.
49. **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.
50. **Credentials**: Authentication material such as username and password, public and private keys, API keys, or certificate.
51. **Cryptographic material** : All material, including documents, devices, or equipment that contains cryptographic information and is essential to the encryption, decryption, or authentication of communications.
52. **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.
53. **Firmware**: Software that communicates with a device's hardware components through instructions and application interfaces.

54. **GPL**: General Public License that allows freedom to use software for any purpose, freedom to change the software, freedom to share the software, and freedom to share the changes made
55. **IoT ecosystem**: A collection of interconnected systems that includes IoT systems, and other systems, such as web and mobile applications.
56. **IoT system**: A system comprising interconnected IoT devices and their software and hardware components.
57. **PCB**: A printed circuit board is a board that contains lines (traces) and pads that connect components together via electrical signals.
58. **Privileged locations**: An area in hardware or software that requires elevated access and permission sets.
59. **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.
60. **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).

Annexure-II

Acronyms

API	Application Programming Interface
AMI	Advanced metering infrastructure
ASLR	Address Space Layout Randomization
DCU	Data concentrator unit
ENISA	European Union Agency for Network and Information Security
GSM	Global System for Mobile
GSMA	GSM Association
HHU	Hand held unit
HAN	Home area network
HES	Head end system
IoT	Internet of Things
IP	Internet Protocol
IHD	In home display
IS	Indian Standard
ISO	International Organization for Standardization
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network
MAC	Media Access Control
NIST	National Institute of Standards and Technology
OTP	One-Time Password
SWD	Serial Wire Debug
TEE	Trusted Execution Environment
TS	Technical Specification
UART	Universal Asynchronous Receiver-Transmitter
UI	User Interface
USB	Universal Serial Bus WAN Wide Area Network
BIS	Bureau of Indian Standards
OTA	Over The Air
NAN	Neighbourhood area network
PLC	Power line communication
RF	Radio frequency
WAN	Wide area network

Annexure-III

List Of Submissions

List of undertakings to be furnished by OEM for Vehicle Tracking Device (VTD) security testing

1) Hardcoded authentication credentials (Against test case 2.1.A.2)
2) Trusted Computing Base (Against test case 2.1.C.2)
3) Root of Trust (Against test case 2.2.B.2)
4) Consistent authentication security (Against test case 2.2.B.3)
5) Cryptographic key chain (Against test case 2.9.A.4)
6) Secret keys in the product family (Against test case 2.10.A.2)
7) Unofficially documenteddebug features (Against test case 2.10.B.3)
8) Software development processes (Against test case 2.10.B.6)
9) Build environment of each application (Against test case 2.10.B.7)
10) GPL based firmware (Against test case 2.10.B.8)
11) Safe equivalents functions (Against test case 2.10.B.9)
12) Builds of source code (Against test case 2.10.B.10)
13) Compilers, version control clients, development utilities, and software development kits (Against test case 2.10.B.11)
14) Compilation of packages (Against test case 2.10.B.12)
15) Release builds (Against test case 2.10.B.13)
16) Debug and release firmware (Against test case 2.10.B.14)
17) Debug information (Against test case 2.10.B.15)
18) Vulnerability management related policies (Against test case 2.11.A.1)
19) Software Component Transparency (Against test case 2.11.A.2)
20) Continuous monitoring of security vulnerabilities (Against test case 2.11.C.2)
21) Back doors (Against test case 2.15.A.3)
22) Time Bombs (Against test case 2.15.A.4)
23) Minimum access privileges (Against test case 2.15.A.5)
24) Detection of malicious codes (Against test case 2.15.C.5)
25) Generation of encryption keys (Against test case 2.19.C.1)
26) Effect of remore control device on meter (Against test case 3.7.B.3)

Annexure-IV

References

1. ER NO. TEC28732108
2. ENISA Baseline Security Recommendation For IoT November 2017 Baseline Security Recommendations
3. ETSI EN 303 645 V2.1.0 (2020-04)
4. ETSI TR 102 898 V 1.1.1
5. GSMA (CLP.11, CLP.12, CLP.13)
6. IoT SF IoT Security assurance framework Release 3.0 November 2021.
7. ISO 27001
8. NIST 8259
9. NIST 8259A
10. NIST 8228
11. NIST Cybersecurity Whitepaper
12. OWASP Application Security Verification Standard 4.0.3
13. OWASP IoT Security Verification Standard
14. BIS IS 16833
15. TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0.