



# Indian Telecom Security Assurance Requirements (ITSAR) भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

## Group-VI Devices Common Security Requirements ITSAR

ITSAR Number: ITSAR702062603

ITSAR Name: NCCS/ITSAR/Standards Applicable for Group of Equipment/CSR  
Group of Devices/Group-VI Devices-V1.0.0

Date of Release: 05.03.2026

Date of Enforcement:

Version: 1.0.0

© रा.सं.सु.के., २०२६

© NCCS, 2026

MTCTE के तहत जारी:

Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.के.)

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. Security Assurance Standards (SAS) division of 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

Sr. No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Group-VI Devices Common Security Requirements ITSAR	ITSAR702062603	1.0.0	05.03.2026	First release

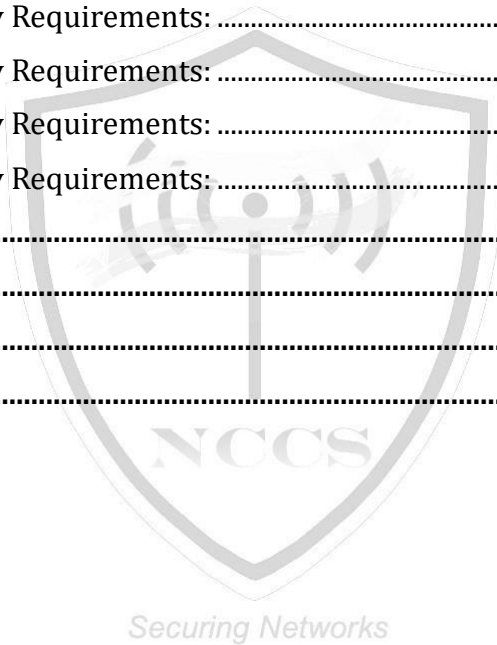


# Table of Contents

Chapter 1: Introduction .....	8
<b>Chapter 2 – Common Security Requirements</b> .....	<b>12</b>
<b>Section1: Authentication</b> .....	<b>12</b>
A. Level-1 Security requirements: .....	12
B. Level-2 Security Requirements: .....	13
C. Level-3 Security Requirements: .....	14
D. Level-4 Security Requirements: .....	15
<b>Section 2: Identity Management</b> .....	<b>15</b>
A. Level-1 Security Requirements: .....	15
B. Level-2 Security Requirements: .....	16
C. Level-3 Security Requirement: .....	17
D. Level-4 Security Requirements: .....	17
<b>Section 3: Authorization and access controls</b> .....	<b>17</b>
A. Level-1 Security Requirements: .....	17
B. Level-2 Security Requirements: .....	19
C. Level-3 Security Requirements: .....	19
D. Level-4 Security Requirements: .....	19
<b>Section 4: Securely storing sensitive information.</b> .....	<b>19</b>
A. Level-1 Security Requirements: .....	19
B. Level-2 Security Requirements: .....	19
C. Level-3 Security Requirements: .....	20
D. Level-4 Security Requirements: .....	22
<b>Section 5: Data Protection</b> .....	<b>22</b>
A. Level-1 Security Requirements: .....	22
B. Level-2 Security Requirements: .....	23
C. Level-3 Security Requirements: .....	23
D. Level-4 Security Requirements: .....	23
<b>Section 6: Secure input and output handling</b> .....	<b>23</b>
A. Level-1 Security Requirements: .....	23
B. Level-2 Security Requirements: .....	23
C. Level-3 Security Requirements: .....	24
D. Level-4 Security Requirements: .....	25
<b>Section 7: Communicate Securely</b> .....	<b>25</b>

A. Level-1 Security Requirements: .....	25
B. Level-2 Security Requirements: .....	28
C. Level-3 Security Requirements: .....	28
D. Level-4 Security Requirements: .....	30
<b>Section 8: Cryptography .....</b>	<b>30</b>
A. Level-1 Security Requirements: .....	30
B. Level-2 Security Requirements: .....	31
C. Level-3 Security Requirements: .....	32
D. Level-4 Security Requirements: .....	32
<b>Section 9: Minimize Exposed Attack Surfaces.....</b>	<b>32</b>
A. Level-1 Security Requirements:.....	32
B. Level-2 Security Requirements:.....	32
C. Level-3 Security Requirements:.....	34
D. Level-4 Security Requirements:.....	34
<b>Section 10: Vulnerability Management.....</b>	<b>34</b>
A. Level-1 Security Requirements:.....	34
B. Level-2 Security Requirements:.....	35
C. Level-3 Security Requirements:.....	35
D. Level-4 Security Requirements:.....	36
<b>Section 11: Incident Management.....</b>	<b>36</b>
A. Level-1 Security Requirements:.....	36
B. Level-2 Security Requirements:.....	36
C. Level-3 Security Requirements:.....	36
D. Level-4 Security Requirements:.....	36
<b>Section 12: Keep Software Updated.....</b>	<b>36</b>
A. Level-1 Security Requirements: .....	36
B. Level-2 Security Requirements: .....	38
C. Level-3 Security Requirements: .....	39
D. Level-4 Security Requirements: .....	39
<b>Section 13: Ensure Software Integrity.....</b>	<b>39</b>
A. Level-1 Security Requirements: .....	39
B. Level-2 Security Requirements: .....	40
C. Level-3 Security Requirements: .....	40
D. Level-4 Security Requirements: .....	41

<b>Section 14: Firmware and Bootloader Security .....</b>	<b>41</b>
A. Level-1 Security Requirements: .....	41
B. Level-2 Security Requirements: .....	41
C. Level-3 Security Requirements: .....	42
D. Level-4 Security Requirements: .....	44
<b>Section 15: Secured Execution Platform.....</b>	<b>44</b>
A. Level-1 Security Requirements: .....	44
B. Level-2 Security Requirements: .....	44
C. Level-3 Security Requirements: .....	44
D. Level-4 Security Requirements: .....	44
<b>Section 16: Collection of Logs .....</b>	<b>44</b>
A. Level-1 Security Requirements: .....	44
B. Level-2 Security Requirements: .....	46
C. Level-3 Security Requirements: .....	46
D. Level-4 Security Requirements: .....	46
<b>Annexure-I.....</b>	<b>47</b>
<b>Annexure-II.....</b>	<b>51</b>
<b>Annexure-III.....</b>	<b>53</b>
<b>Annexure-IV .....</b>	<b>54</b>



## A) Outline

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies Common Security Requirements for Group-VI devices which include IoT devices namely “Vehicle Tracking Device, Smart Electricity Meter and Feedback device.”

**A Vehicle Tracking Device** is an electronic system installed in automobiles to monitor and record their location, movement, and usage. It typically uses GPS and cellular networks to transmit real-time data to a central server, enabling fleet management, theft prevention, and route optimization.

**A smart electricity meter** is a digital device that measures and records electricity consumption in real time. Unlike traditional meters, it can communicate usage data automatically to utility providers via secure communication channels, supporting accurate billing, demand management, and energy efficiency programs.

**A Feedback Device** is an electronic system used to collect user responses or operational data for analysis. It can take the form of kiosks, handheld units, or embedded sensors, and is commonly used in customer service, quality control, and performance monitoring to improve processes and user experience.

This document begins with an overview of Grouping, including its scope and objectives, classification of IoT devices and then proceeds to outline the Common Security Requirements of the ITSARs applicable to Group VI devices.

## B) Scope

This document defines Common Security Requirements for Indian Telecom Security Assurance Requirements (ITSARs) of Group VI devices (Vehicle Tracking Device, Smart Electricity Meter and Feedback device).

It serves as the basis for designating labs as TSTLs for testing the Common Security Requirements of these devices and security certification of these devices till TSTL capable of testing SSR is available.

## 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 a 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.

## D) Applicability of the clauses

If a requirement explicitly specifies the applicability to a particular device, it applies and is tested only on that device; otherwise, it applies to and is tested on any one or all Group VI devices.

# Chapter 1: Introduction

## 1.1. Grouping (scope and objectives)

The ITSARs are consisting of Common Security Requirements (CSR) and Specific Security Requirements (SSR). The CSR clauses are common across most of the ITSARs. SSR clauses are specific to the Communication device. However, the testing infrastructure requirement, skill set requirement may vary from device to device or from group of devices to group of devices.

In an endeavour to mandate testing CSR clauses of a group of devices and designate the TSTL for testing CSR clauses of a group of devices ***“Grouping of devices”*** is done.

Chapter 2 of this ITSAR outlines the Common Security Requirements applicable for designating the labs for CSR testing of Group VI device ITSARs.



## 1.2. 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-0 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-0 meeting no security requirements, 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 five levels of IoT devices as below.

**Level 0:** Such devices are very constrained devices with very low processing power, no data encryption and message encryption. Such type of devices may not enable a secure communication and should be allowed to work through such gateways which can add the required measure of security. Without the security augmentation by a Gateway, such type of devices should not be permitted for use in mission critical infrastructure. It is required that the Gateways used to connect such devices will follow the security assurance at Level 2 / Level 3.

**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.

**Level-2:** Security requirement of Level-1 and adherence to international standards (secure identity, software asset security etc.).

**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.

**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 Assessment 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]**

Level ‘0’ type of devices may not enable secure communication and they do not meet baseline security requirements. They can be allowed to work through only gateways

which can add the required measure of security. For ITSAR purpose, the level '0' classification is not considered as these devices do not meet baseline security requirements and hence, it is not possible to carry out security certification at Level '0'.

### **Classification of Security Requirements:**

In order to apply an appropriate level of security assurance to an IoT device, 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 device 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 device 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 device 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 device shall have resistance against common cyber-attacks, it undergoes penetration testing and incorporates the usage of biometric authentication.

## Chapter 2 – Common Security Requirements

---

### Section 1: Authentication

---

#### A. Level-1 Security requirements:

##### 2.1.A.1 Default passwords and user names

Requirement:

- a) The Group-VI device shall enforce the factory-issued/OEM login accounts and factory-default usernames to be disabled or erased or renamed when installed or commissioned.
- b) The Group-VI 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: a) ENISA Baseline security recommendations for IoT November 2017 GP-TM-22,  
b) 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: a) ETSI EN 303 645 V2.1.0 (2020-04) Provision 5.1-1, b) 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 Group-VI 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:

Group-VI 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 Group-VI 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 Group-VI 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 user enters a password for a device. Group-VI 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 use 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 device shall implement a trusted computing base. The manufacturer shall give an undertaking that the Trusted Computing Base has been implemented, and the identity is cryptographically authenticated using the TCB. The Group-VI 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 Group-VI 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 identity per Group-VI device shall be used in a device. It shall resist tampering by means such as physical, electrical or software. The unique ID may be as prescribed by National Trust Centre or MoRTH, Govt of India.

[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 Group-VI 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 Group-VI 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 Group-VI device 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 Group-VI 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]

---

### **2.3.A.12 Access control during initial connection**

Requirement:

The Group-VI 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:**

#### **2.3.C.1 Trusted service layer**

Requirement:

The Group-VI device 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 shall be used 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 Group-VI 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 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.2 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.3 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.4 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.5 Tamper-resistant storage of sensitive data**

Requirement:

UICC /embedded 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.6 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.7 Trust Anchor**

Requirement:

- a) Tamper resistant Trust Anchor shall be used.
- b) 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, 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: Data Protection**

---

#### **A. Level-1 Security Requirements:**

##### **2.5.A.1 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]

---

##### **2.5.A.2 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]

---

##### **2.5.A.3 Personally Identifiable Information collection**

Requirement:

Manufacturer shall share details of the PII collected by the device and the Group-VI 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]

---

## **B. Level-2 Security Requirements:**

### **2.5.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 6: Secure input and output handling**

---

### **A. Level-1 Security Requirements:**

Nil

---

### **B. Level-2 Security Requirements:**

#### **2.6.B.1 Validation of input data and transferred data**

Requirement:

The Group-VI 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.

[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]

---

#### **2.6.B.2 Validation of inputs and outputs**

Requirement:

- a) 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, use "Fuzzing" tests to check for acceptable responses or output for both expected (valid) and unexpected (invalid) input stimuli.
- b) All input (HTML form fields, REST requests, URL parameters, HTTPS headers, cookies, batch files, RSS feeds, etc.) shall be validated using positive validation (allow lists).

- c) 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: a) IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.10.12, 2.4.11.9 and 2.4.5.23

b) OWASP ISVS 5.1.3, 5.1.4]

---

### **2.6.B.3 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]

---

### **2.6.B.4 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]

---

## **C. Level-3 Security Requirements:**

### **2.6.C.1 HTTPS parameter pollution attacks**

Requirement:

The application shall have defences against HTTPS 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]

---

### **2.6.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]

---

### **2.6.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 7: Communicate Securely**

---

#### **A. Level-1 Security Requirements:**

### **2.7.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]

---

### **2.7.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]

---

### **2.7.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]

---

#### **2.7.A.4 Secure connection with remote servers**

Requirement:

Where the application communicates with a device 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]

---

#### **2.7.A.5 Access via network interface**

Requirement:

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

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

---

#### **2.7.A.6 Configuration changes via network interface**

Requirement:

The Group-VI Device functionality that allows security-relevant changes in configuration via a network interface shall be accessible only after mutual 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]

---

#### **2.7.A.7 Web interfaces**

Requirement:

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

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

---

#### **2.7.A.8 Communication of sensitive data between device and associated services**

Requirement:

The confidentiality of sensitive personal data communicated between the Group-VI 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]

---

#### **2.7.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 2.4.10.19 and 2.4.13.35]

---

#### **2.7.A.10 Sensitive data through HTTP message**

Requirement:

If HTTP is used, sensitive data shall not 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:**

### **2.7.B.1 Authentication of data received from other devices**

Requirement:

The Group-VI 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]

---

### **2.7.B.2 Authentication of connections at all levels of protocols**

Requirement:

The Group-VI device shall make intentional connections, shall prevent unauthorized connections to it or other devices the device is connected to, at all levels of the protocols. Protocols to be used shall be latest and must be patched for all vulnerabilities.

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

---

## **C. Level-3 Security Requirements:**

### **2.7.C.1 Cloud service**

Requirement:

If run as a cloud service, TCP based communications (such as MQTT connections) shall be encrypted using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” and authenticated using latest DTLS 1.2 and above standard 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]

---

### **2.7.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]

---

### **2.7.C.3 Webservice devices**

Requirement:

Where a device related to a webservice 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]

---

### **2.7.C.4 Verification of X.509 certificate - TLS**

Requirement:

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

[Ref: OWASP ISVS 4.1.3]

---

### **2.7.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]

---

### **2.7.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]

---

### **2.7.C.7 Replay attacks**

Requirement:

Protection against replay attacks shall be built into the device.

[Ref: OWASP ISVS 4.1.1]

---

### **2.7.C.8 Security for email notifications**

Requirement:

The Group-VI 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: Age light IoT Safety Architecture & Risk Toolkit v4.0 38]

---

#### **D. Level-4 Security Requirements:**

Nil

---

## **Section 8: Cryptography**

---

#### **A. Level-1 Security Requirements:**

### **2.8.A.1 Cryptographic controls**

Requirement:

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 used.

[Ref: ISO:27001 A.12.3.1]

---

### **2.8.A.2 Cryptographic keys**

Requirement:

Cryptographic secrets and keys shall be unique per device. 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: a) OWASP ISVS 2.4.1

b) IoT SF IoT Security assurance framework Release 3.0 November 2021 2.4.14.9]

---

### **2.8.A.3 Cryptographic key chain**

Requirement:

The OEM 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]

---

### **2.8.A.4 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]

---

## **B. Level-2 Security Requirements:**

### **2.8.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]

---

### **2.8.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]

---

### **2.8.B.3 Storage of sensitive unencrypted parameters**

Requirement:

The Group-VI device 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]

---

### **2.8.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:**

Nil

---

#### **D. Level-4 Security Requirements:**

Nil

---

## **Section 9: Minimize Exposed Attack Surfaces**

---

### **A. Level-1 Security Requirements:**

#### **2.9.A.1 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]

---

### **B. Level-2 Security Requirements:**

#### **2.9.B.1 Physical decapsulation, side channel and glitching attacks**

Requirement:

The Group-VI devices shall have tamper resistant device 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]

---

### **2.9.B.2 Debugging and Testing Technologies**

Requirement:

Disable Debugging and Testing Technologies: The final configuration of the device to be deployed shall never contain debugging, diagnostic, or testing interfaces that could be abused by an adversary. Such interfaces are:

- a) Command-line console interfaces
- b) Consoles with verbose debugging, diagnostic, or error messages
- c) Hardware debugging ports such as JTAG or SWD
- d) Network services used for debugging, diagnostics, or testing
- e) Administrative interfaces, such as SSH or Telnet

All such technologies should be disabled in the final configuration.

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

[Ref: a) GSMA CLP:13 8.2

c) OWASP ISVS 5.1.7]

---

### **2.9.B.3 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]

---

### **2.9.B.4 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]

---

### **2.9.B.5 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 10: Vulnerability Management**

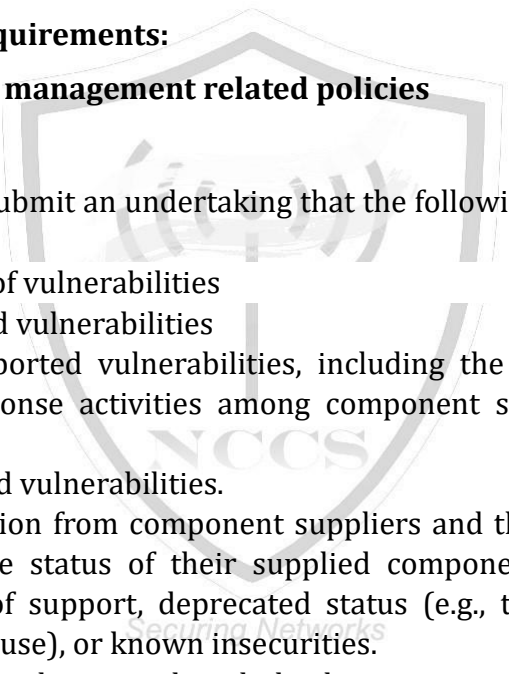
---

**A. Level-1 Security Requirements:**

**2.10.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 devices 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 device or service.
  - j) Informing users and relevant stakeholders when vulnerabilities affect devices through established communication channels (website, e-mail, security advisory pages, changelogs, etc.).
- 

**2.10.A.2 Vulnerability scanners**

Requirement:

The device shall support the use of vulnerability scanners.

[Ref: NIST 8228 Expectation-7]

---

### 2.10.A.3 Third party and open-source software

Requirement:

The manufacturer shall verify the potential areas of risk that come with the use of third-party and open-source software and take actions to mitigate such risks.

[Ref: OWASP ISVS 1.2.2]

---

## B. Level-2 Security Requirements:

### 2.10.B.1 Abnormal number of requests

Requirement:

The Group-VI 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:

### 2.10.C.1 Review of device OS/source code

Requirement:

- a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at Telecom Security Testing Laboratory (TSTL) premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).
- b) Also, OEM shall submit the undertaking as below:
  - i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the device which includes OEM developed code, third party software and open-source code libraries used/embedded in the device.
  - ii) device software shall be free from Common Weakness Enumeration (CWE) top 25, Open Worldwide Application Security Project (OWASP) top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.
  - iii) The binaries for device and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

[Ref: a) [https://cwe.mitre.org/top25/archive/2022/2022\\_cwe\\_top25.html](https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html)

b) <https://owasp.org/www-project-top-ten/>

c) <https://owasp.org/www-project-api-security/>]

---

**D. Level-4 Security Requirements:****2.10.D.1 Penetration testing strategy**

Requirement:

The Group-VI device shall implement a complete persistent penetration-testing strategy.  
[Ref: GSMA CLP-13 7.11]

---

**Section 11: Incident Management**

---

**A. Level-1 Security Requirements:****2.11.A.1 Operational and security events**

Requirement:

The Group-VI device shall log its operational and security events.  
[Ref: NIST Expectation 15]

---

**B. Level-2 Security Requirements:****2.11.B.1 Detection of potential incidents**

Requirement:

The Group-VI 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 12: Keep Software Updated**

---

**A. Level-1 Security Requirements:****2.12.A.1 Remote update**

Requirement:

Where remote update is supported, there shall be an established process or 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]

### **2.12.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]

---

### **2.12.A.3 Authenticate to update server**

Requirement:

The Group-VI device shall authenticate to the update server component prior to downloading the update.

[Ref: OWASP ISVS 3.4.10]

---

### **2.12.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]

---

### **2.12.A.5 Automatic updates and/or update notifications**

Requirement:

If the Group VI 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]

---

### **2.12.A.6 Checking for security updates**

Requirement:

The Group-VI 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]

---

### **2.12.A.7 Notification during software update**

Requirement:

The Group-VI 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]

---

### **2.12.A.8 Over-The-Air (OTA) update**

Requirement:

The manufacturer shall ensure that the Group-VI 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]

---

### **2.12.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:**

### **2.12.B.1 Authenticity and integrity of software updates**

Requirement:

- a) Software package integrity shall be validated during the software update stage.
- b) The Group-VI device shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only. To this end, the device has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update originated from only these sources.
- c) Tampered software shall not be executed or installed if integrity check fails.
- d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update and modify the list mentioned in (b) above. Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Ref : TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

---

### **2.12.B.2 Authenticity and integrity of firmware**

Requirement:

Firmware binary should be made available with the version matching one in the Group-VI device as well as binary size & modification timestamp and/ or checksum should match for the binary provided and one installed on device.

[Ref: AIS-140 Amendment-2, Page 14, Point 6, Table -2 Clause No 8.5]

---

### **C. Level-3 Security Requirements:**

#### **2.12.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 13: Ensure Software Integrity**

---

### **A. Level-1 Security Requirements:**

#### **2.13.A.1 Back doors**

Requirement:

Manufacturer shall submit an undertaking that the application source code and third-party libraries:

- i. Do 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
- ii. Do 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

*Securing Networks*

[Ref: OWASP ASVS 10.2.3, 10.2.5 and 10.2.6]

---

#### **2.13.A.2 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]

---

#### **2.13.A.3 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.

---

## **B. Level-2 Security Requirements:**

### **2.13.B.1 Persistent filesystem storage**

Requirement:

Persistent filesystem storage volumes must be encrypted.

[Ref: OWASP ASVS 3.2.5]

---

## **C. Level-3 Security Requirements:**

### **2.13.C.1 Secure boot mechanisms**

Requirement:

The Group-VI device shall verify its software using secure boot mechanisms.

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

---

### **2.13.C.2 Unnecessary Services Removal**

Requirement:

The Group-VI 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.

- 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]

---

### **2.13.C.3 Controls against mobile code**

Requirement:

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]

---

#### **D. Level-4 Security Requirements:**

Nil

---

## **Section 14: Firmware and Bootloader Security**

---

#### **A. Level-1 Security Requirements:**

##### **2.14.A.1 Configuration of firmware**

Requirement:

The Group-VI 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]

---

##### **2.14.A.2 Design of device firmware**

Requirement:

The Group-VI 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:**

### **2.14.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]

---

### **2.14.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]

---

### **2.14.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]

---

### **2.14.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]

---

---

### **2.14.C.5 Executable image of first-stage boot loader**

Requirement:

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

[Ref: GSMA CLP.13 6.17]

---

### **2.14.C.6 Sensitive information in boot loader stages**

Requirement:

Boot loader 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]

---

### **2.14.C.7 Code loading of boot loader**

Requirement:

The boot loader 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]

---

### **2.14.C.8 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 15: Secured Execution Platform**

---

**A. Level-1 Security Requirements:**

**2.15.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:**

**2.15.B.1 Minimum Viable execution Platform**

Requirement:

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

[Ref: GSMA CLP.13 6.7]

---

**C. Level-3 Security Requirements:**

Nil

**D. Level-4 Security Requirements:**

Nil

---

**Section 16: Collection of Logs**

---

**A. Level-1 Security Requirements:**

**2.16.A.1 Security logs**

Requirement:

The Group-VI device shall generate logs of all the important events including the events with security implications, such as connection logs, access logs, successful and failed authentication attempts, access to debugging functionality etc.

[Ref: OWASP ISVS 1.4.1]

---

### **2.16.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]

---

### **2.16.A.3 Device synchronization**

Requirement:

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

[Ref: OWASP ISVS 1.4.3]

---

### **2.16.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]

---

### **2.16.A.5 Online collection of logs**

Requirement:

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

[Ref: OWASP ISVS 1.4.5]

---

**B. Level-2 Security Requirements:**

Nil

---

**C. Level-3 Security Requirements:**

Nil

---

**D. Level-4 Security Requirements:**

Nil

---



### Definitions

1. **Administrator:** User who has the highest-privilege level possible for a user of the device, which can mean they are able to change any configuration related to the intended functionality
2. **Application Security Verification:** The technical assessment of an application against the OWASP ASVS.
3. **Associated services:** Digital services that, together with the device, are part of the overall consumer IoT product and that are typically required to provide the product's intended functionality
4. **Authentication:** The verification of the claimed identity of an application user.
5. **Authentication mechanism:** Method used to prove the authenticity of an entity
6. **Authentication value:** individual value of an attribute used by an authentication mechanism.
7. **Authorized Individuals, services, and other IoT product components:** An entity (i.e., a person, device, service, network, domain, developer, or other party who might interact with an IoT device) that has implicitly or explicitly been granted approval to interact with a particular IoT device.
8. **Component:** A self-contained unit of code, with associated disk and network interfaces that communicates with other components.
9. **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.
10. **Consumer:** Natural person who is acting for purposes that are outside her/his trade, business, craft or profession.
11. **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.
12. **Credentials:** Authentication material such as username and password, public and private keys, API keys, or certificate.
13. **Critical security parameter:** Security-related secret information whose disclosure or modification can compromise the security of a security module.
14. **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.
15. **Device manufacturer:** Entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers.

16. **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.
17. **Endpoint:** An IoT Endpoint is a physical computing device that performs a function or task as part of an Internet-connected product or service.
18. **Endpoint Ecosystem:** Any configuration of low-complexity devices, rich devices, and gateways that connect the physical world to the digital world in novel ways.
19. **Factory default:** State of the device after factory reset or after final production/assembly
20. **Firmware:** Software that communicates with a device's hardware components through instructions and application interfaces.
21. **Hardcoded:** stored on the filesystem, be it in code, comments, or files.
22. **Initialized state:** State of the device after initialization
23. **Input Validation:** The canonicalization and validation of untrusted user input
24. **IoT system:** A system comprising interconnected IoT devices and their software and hardware components.
25. **Logical interface:** Software implementation that utilizes a network interface to communicate over the network via channels or ports
26. **Manufacturer:** Relevant economic operator in the supply chain (including the device manufacturer)
27. **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!
28. **Network interface:** Physical interface that can be used to access the functionality of consumer IoT via a
29. **One-time Password (OTP):** A password which is uniquely generated to be used on a single occasion.
30. **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.
31. **Personal data:** Any information relating to an identified or identifiable natural person
32. **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.
33. **Physical interface:** Physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer
34. **Privileged locations:** An area in hardware or software that requires elevated access and permission sets.

35. **Security module:** Set of hardware, software, and/or firmware that implements security functions.
36. **Security update:** Software update that addresses security vulnerabilities either discovered by or reported to the manufacturer.
37. **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.
38. **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)
39. **Sensitive security parameters:** Critical security parameters and public security parameters
40. **Trust Anchor:** In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative entity for which trust is assumed and not derived.
41. **Trusted Computing Base:** A Trusted Computing Base (TCB) is a conglomeration of algorithms, policies, and secrets within a product or service. The TCB acts as a module that allows the product or service to measure its own trustworthiness, gauge the authenticity of network peers, verify the integrity of messages sent and received to the product or service, and more. The TCB functions as the base security platform upon which security products and services can be built. A TCB's components will change depending on the context (a hardware TCB for Endpoints or a software TCB for cloud services), but the abstract goals, services, procedures, and policies should be very similar.
42. **Two-factor authentication (2FA):** This adds a second level of authentication to an account log-in.
43. **Unique per device:** Unique for each individual device of a given product class or type
44. **User:** Natural person or organization
45. **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.
46. **Internet of Things:** The Internet of Things describes the coordination of multiple machines, devices, and appliances connected to the Internet through multiple networks. These devices include everyday objects such as tablets and consumer electronics, and other machines such as vehicles, monitors, and sensors equipped with machine-to-machine (M2M) communications that allow them to send and receive data.
47. **IoT Service:** Any computer program that leverages data from IoT devices to perform the service.

48. **UICC:** A Secure Element Platform specified in ETSI TS 102 221 can support multiple standardized network or service authentication applications in cryptographically separated security domains. It may be embodied in embedded form factors specified in ETSI TS 102 671.



**Acronyms**

2FA	-	Two Factor Authentication
API	-	Application Program Interface
CLP	-	GSMA's Connected Living Programme
CPU	-	Central Processing Unit
DDoS	-	Distributed Denial of Service
EEPROM	-	Electrically Erasable Programmable Read-Only Memory
ENISA	-	European Union Agency for Network and Information Security
ETSI	-	European Telecommunications Standards Institute
GSMA	-	GSM Association
HTTP	-	Hypertext Transfer Protocol.
IoT	-	Internet of Things
IoT SF	-	Internet of Things Security Foundation
IP	-	Internet Protocol
LAN	-	Local-area Network
MFA	-	Multi Factor Authentication
MSISDN	-	Mobile Station International Subscriber Directory Number
NIST	-	National Institute of Standards and Technology
OEM	-	Original Equipment Manufacturer
OS	-	Operating System
OWASP	-	Open Web Application Security Project
PC	-	Personal Computer
PII	-	Personally identifiable information
PSK	-	Pre-Shared Key
RAM	-	Random Access Memory
ROM	-	Read Only Memory

SMS	-	Short Message Service
SSH	-	Secure Shell Protocol
TCB	-	Trusted Computing Base
UICC	-	Universal Integrated Circuit Card
Wi-Fi	-	Wireless Fidelity



## **List Of Submissions**

List of undertakings to be furnished by OEM for 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 keys (Against test case 2.8.A.2)
- 6) Cryptographic key chain (Against test case 2.8.A.3)
- 7) Debugging and testing Technologies (Against test case 2.9.B.2)
- 8) Vulnerability management related policies (Against test case 2.10.A.1)
- 9) Review of device OS/ source code (Against test case 2.10.C.1)
- 10) Back doors (Against test case 2.13.A.1)



### References

1. TEC 31328:2023 Security by Design for IoT Device Manufacturers ISO 9001 :2015
2. TEC 31188:2022 Framework of National Trust Centre for M2M/ IoT Devices and Applications
3. TEC 31318:2021: TEC Code of Practice for Securing Consumer Internet of Things (IoT)
4. AIS-140 Intelligent transportation systems (ITS)
5. ENISA Baseline Security Recommendation for IoT November 2017 Baseline Security Recommendations
6. ETSI EN 303 645 V2.1.0 (2020-04) Cyber Security for Consumer Internet of Things: Baseline Requirements
7. GSMA (CLP.11, CLP.12, CLP.13) IoT Security Guidelines
8. IoT SF IoT Security assurance framework Release 3.0 November 2021.
9. NIST 8259A IoT Device Cybersecurity Capability Core Baseline
10. NIST 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.
11. OWASP Application Security Verification Standard 4.0.3
12. OWASP IoT Security Verification Standard ISVS
13. TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0: Catalogue of general security assurance requirements

