	Government of India **Ministry of Electronics & IT (MeitY)** **STQC Directorate** **IT &eGov Division**	Document No. STQC/IoTSCS/F03, Issue No. 04 Date: 13-09-2024
Technical Construction File (TCF) for IoT Device		

Security Requirements for IoT Devices (for security, privacy and supply chain)

IoT device is defined as “an entity of an IoT system that interacts and communicates with the physical world through sensing or actuating” [Source: ISO/IEC 27400:2022]. With the increasing number of Internet of Things (IoT) devices and increasing reliance on such devices, the security and privacy risks relating to those “things” are expected to grow. Their widespread deployment in networks and systems make them easy and prime targets for cyber-attacks.

This document provides a set of security, privacy and supply chain requirements for IoT devices. Adhering to these requirements will provide adequate confidence to the users in respect of security, privacy and supply chain security of these devices.

Not all requirements outlined in this document are universally applicable to every IoT device. Users or organizations have to assess and determine the specific security, privacy, and supply chain requirements relevant to their use of these devices.

This document defines four assurance levels, with each level increasing in depth of testing. Users/organizations can choose the appropriate assurance level depending on area of applicability, sensitivity of data and operational needs.

- Level 0 is for minimal assurance level. Within 01 year of obtaining Level 0 compliance the IoT devices has to seek certification for Level 1/Level 2/Level 3
- Level 1 is for low assurance levels and all IoT devices are expected to meet these requirements
- Level 2 is for IoT devices that contain sensitive data, which requires protection and is the recommended level for most IoT devices
- Level 3 is for the most critical IoT devices - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.

Each IoT device can undergo certification any of these four levels as provided below:

Certification Level	Testing Level	Objective	Requirements	Methodology
Level 0	Minimal	Level 0 provides certification based on declaration and limited	Annexure A	Test Laboratory required to verify declaration are appropriate and

		Testing/Audit		perform limited testing/audit
Level 1	Basic	Level 1 provides minimum security, privacy and supply chain requirements for adequate confidence to the user.	Refer Annexure A, B and C	Test Laboratory required to verify the claim made by developer through testing, demonstration, site visit and audit.
Level 2	Intermediate	In addition of Level 1 requirements, Level 2provides extra security requirements related to hardware and software. It also defines specific security requirements pertaining to Intellectual Property protection technologies, reverse engineering, firmware update process etc.	Refer Annexure A, B and C	Test Laboratory required to verify the claim made by developer through testing, demonstration, site visit and audit.
Level 3	Advanced	In addition of Level 2 requirements, Level 3 provides extra security requirements related to hardware and software. It also defines specific security requirements pertaining to side channel attacks,	Refer Annexure A, B and C	Test Laboratory required to verify the claim made by developer through testing, demonstration, site visit and audit.

		encrypted inter chip communication, tampering etc.		

Note:

1. Level 0 certification is valid for only one year and is a onetime occurrence. Developers are encouraged to pursue Level 1/Level 2/Level 3 certification within this timeframe.

2. Level 1, Level 2, and Level 3 certifications are valid for three years, with one surveillance audit required each year.

Annexure 'A'

Mandatory for All Levels

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
5.1	**Requirements for IoT device policies and documentation**				
5.1.1	**Risk management**				
5.1.1.1.1	IoT devices shall have documentation recording the results of a risk assessment process performed at the IoT device level in the context of a risk assessment at the system level.	a) Verify risk assessment and documentation are complete and accurate. b) Check implementation and effectiveness of controls. c) Assess device management under resource constraints. d) Ensure	i. Risk Assessment Report ii. Risk Treatment Plan iii. Risk Assessment Methodology iv. Constraints Documentation v. Review Records vi. Interested Parties Analysis		
5.1.1.1.2	The risk assessment process shall take into account intended outcomes for				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	the intended use case.	documentation is maintained and accessible throughout the device's lifecycle.			
5.1.1.1.3	The risk assessment process shall also take into account the needs and expectations of interested parties (e.g. those parties on networks to which the IoT device is connected), including physical and logical undesired effects.				
5.1.1.1.4	The risk assessment shall take into account that IoT devices can be constrained (e.g. limited battery, little memory, 'weak' CPU),				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	which informs the risk treatment process.				
5.1.1.1.5	Risk assessment and treatment processes shall be defined and applied.				
5.1.1.1.6	IoT devices shall implement the features and controls identified as necessary in its Statement of Applicability, as well as features and controls.				
5.1.1.1.7	The documentation shall be available for the supported lifetime of the product.				
5.1.2	**Information disclosure**				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
5.1.2.1.1	IoT devices shall have user documentation that lists the features that the IoT device provides to support controls for security and privacy, making it clear if any of the IoT device requirements in 5.2 are not included.	a) Verify user documentation lists all security and privacy features clearly. b) Check documentation availability throughout the device's support period. c) Confirm the existence and clarity of the security support policy and update discontinuation notices.	i. User Documentation ii. Security Support Policy iii. Product Lifecycle Documentation iv. Risk Assessment Report		
5.1.2.1.2	Such information shall be publicly available for the period of time the IoT device is supported.				
5.1.2.1.3	IoT devices shall be covered by a security support policy and other				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	supporting documentation wherein users are made aware in advance of when security updates will be discontinued.				
5.1.3	**Vulnerability disclosure and handling processes**				
5.1.3.1.1	IoT devices shall have documentation that defines the vulnerability disclosure and handling processes that will apply for the supported lifetime of the device.	a) Verify comprehensive documentation for vulnerability reporting and handling processes. b) Test accessibility and functionality of the public reporting system.	i. Vulnerability Disclosure Policy ii. Vulnerability Handling Procedures iii. Public Reporting Mechanism Documentation iv. Product Lifecycle Documentation		
5.1.3.1.2	Vulnerability disclosure and handling processes shall include, at a				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	minimum, a capability to receive reports of potential vulnerabilities from the public.	c) Ensure defined steps for acknowledging, assessing, and resolving vulnerabilities. d) Confirm adherence to relevant standards and regulations.			
5.2	**Requirements for IoT device capabilities and operations**				
5.2.1	**It includes IoT device features to be used with a risk assessment and treatment process in accordance with 5.1.1.**				
5.2.2	**Configuration**				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
5.2.2.1.1	If the configuration settings of the IoT device can be modified, only authorized entities shall be able to modify the configuration settings of the IoT device.	a) Test that only authorized entities can modify the device's configuration settings. b) Validate that configuration changes affecting other devices are permitted only when properly authorized.	i. Access Control Policy ii. Authorization Procedures iii. Configuration Management Documentation		
5.2.2.1.2	If IoT devices are capable of changing the configuration of IoT and other devices, they shall only be capable of making such changes when authorized.				
5.2.3	**Software reset**				
5.2.3.1.1	If IoT devices have the capability to be reset, that process shall be secure.	a) Verify that the reset process is secure and prevents unauthorized access.	i. Reset Procedure Documentation ii. Authorization and Access Control Policy		
5.2.3.1.2	This capability				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	shall only be executable by an authorized entity.	b) Confirm that only authorized entities can initiate the reset process.			
5.2.4	**User data removal**				
5.2.4.1.1	If the IoT device stores user data, it shall provide a function for deleting appropriate user data stored on the device in any type of memory.	a) Verify that the device provides a function to delete user data from all types of memory. b) Ensure that the data deletion function is accessible only to authorized entities.	i. Data Deletion Procedure ii. Access Control Policy		
5.2.4.1.2	The function shall be restricted to authorized entities only.				
5.2.5	**Protection of data**				
5.2.5.1.1	IoT devices shall be capable of	a) Verify that the device employs	i. Data Protection Policy ii. Software Security		

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	protecting the data they store and transmit from unauthorized access, modification and disclosure.	mechanisms to protect stored and transmitted data (e.g., encryption, access controls). b) Confirm that the device's software and firmware are secured against unauthorized access and modification. c) Check the implementation of cryptographic measures (encryption, hashing, digital signatures) for	Documentation iii. Cryptographic Implementation Guidelines		
5.2.5.1.2	This shall include configuration settings, identifying data, user data, event logs and sensitive security parameters.				
5.2.5.1.3	IoT devices shall be capable of protecting their software (including firmware) from unauthorized access and modification.				
5.2.5.1.4	IoT devices shall use cryptography				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	(e.g. encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of data requiring protection from being compromised.	safeguarding data integrity and confidentiality.			
5.2.6	**Interface access**				
5.2.6.1.1	IoT devices shall have mechanisms to limit logical access to its interfaces to authorized entities only.	a) Verify mechanisms for restricting logical access to interfaces and ensure only authorized entities can access them. b) Assess the	i. Access Control Policy ii. Authentication and Authorization Procedures iii. Identifier Management and Security Policy iv. Default Values and Parameter Management Documentation		
5.2.6.1.2	IoT devices shall employ appropriate authentication and access control				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	mechanisms.	implementation of authentication and access control mechanisms to confirm they are appropriate and effective. c) Ensure that unique identifiers are created and common values for security parameters are replaced with unique or external values before deployment.			
5.2.6.1.3	Security and privacy requirements shall be assessed when designing and implementing the functions of IoT devices regarding creation and use of identifiers.				
5.2.6.1.4	IoT devices shall ensure that common values for critical security parameters, such as global private keys or standard passwords, are replaced by values that are unique per device or explicitly defined by an				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	appropriate external entity before they are put into operation.				
5.2.7	**Software and firmware updates**				
5.2.7.1.1	If the IoT device supports software updates, updates shall be performed using a secure procedure.	a) Verify that software updates are performed using secure procedures, including encryption and integrity checks. b) Ensure that only authorized entities can initiate software updates. c) Assess the device's ability to handle	i. Software Update Procedure ii. Authorization Policy for Updates iii. Update Failure Recovery Plan		
5.2.7.1.2	Updates shall only be initiated by authorized entities.				
5.2.7.1.3	Unexpected interruption of an update shall leave the IoT device in a state that minimizes potential for harm, taking				

Cl. No.	Requirements for IoT security and privacy — Device baseline requirements	What to be Tested/ audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	into account the risks of the IoT device not functioning as expected.	unexpected interruptions during updates, ensuring it minimizes potential harm and maintains operational integrity.			

Annexure B

Below Security Requirements need to be selected based on Levels

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
Level 1/2/3					
1.	Verify that application layer debugging interfaces such USB, UART, and other serial variants are disabled or protected by a complex password.	a) Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being used in the device under test. b) Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation. c) Testing, in presence of OEM team, to verify the enabling/disabling of all the ports and	i. Datasheet of the SoC being used in the device. ii. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. iii. Process flow of the Manufacturing/Provisioning of the device		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		debugging interfaces such as USB, UART, and other serial variants using their relevant hardware-based debuggers and access control mechanisms in case the interface is enabled. d) Process audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/ disabled during provisioning. [For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/ peripherals.]			

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
2.	Verify that cryptographic keys and certificates are unique to each individual device.	Identifying all the keys and certificates being used in the device eco-system and verification through: a) Testing, in presence of OEM team b) Code review c) Process audit of the key-life cycle process	i. List of all keys and certificates being used in the device ecosystem ii. Key management life cycle (purpose, generation, storage, destruction/ zeroization, validity, key changeover/rotation)		
3.	Verify that memory protection controls such as ASLR and DEP are enabled by the embedded/IoT operating system, if applicable.	Testing, in presence of OEM team, to verify the declared memory protection controls available and enabled in the device using command line-based tools/commands or any other open-source tool like DEP, EMET tool.	Declaration of the memory protection controls available and enabled in the device.		
4.	Verify that on-chip debugging interfaces such as JTAG or SWD are disabled or that available protection mechanism is enabled and	a) Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being	i. Datasheet of the SoC being used in the device. ii. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. iii. Process flow of the		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	configured appropriately.	used in the device under test. b) Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation. c) Testing, in presence of OEM team, to verify the enabling/disabling of all the ports and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware-based debuggers and access control mechanisms in case the interface is enabled. d) Process audit of the manufacturing	Manufacturing/Provisioning of the device		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		facility to validate the vendor's claim regarding the debugging interfaces which are closed/ disabled during provisioning. [For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/ peripherals.]			
5.	Verify that trusted execution is implemented and enabled, if available on the device SoC or CPU.	Identifying whether TEE/SE/TPM is available or not in the device through the SoC datasheet and technical documentation submitted by the vendor. Further assessment is done on the basis of scenarios as applicable to device as defined below:	i. Datasheet of the SoC being used in the device. ii. User manual/ Technical specifications of the device iii. Code snippets of the TEE API call, wherever applicable		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		CASE 1: TEE/SE/TPM is not available: No further assessment **CASE 2:** TEE/SE/TPM is available and enabled: Verification through code review that crypto functions are called through TEE/SE/TPM APIs. **CASE 3:** TEE/SE/TPM is available but not enabled by the vendor: Termed as nonconformance to the requirement. OEM is required to enable and implement the TEE/SE/TPM.			
6.	Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM, TEE (Trusted Execution Environment), or protected using strong cryptography.	Identifying all the keys and certificates being used in the device eco-system and verification through: a) Testing, in presence of OEM team b) Code review c) Process audit of the key-life cycle	i. List of all keys and certificates being used in the device ecosystem ii. List of all the sensitive data with their intended usage and secure storage mechanism(s) as implemented along with secure configurations to be enabled in the device. iii. Key management life cycle (purpose, generation, storage, destruction/		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		process	zeroization, validity, key changeover/rotation) private keys and certificates.		
7.	Verify that the firmware apps protect data-in-transit using transport layer security.	a) Verifying that strong encryption algorithms and secure TLS version is supported by the device to establish secure communication. b) Verifying that device properly validates the server's TLS certificate to ensure that it is trusted and has not been tampered with. c) Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites. d) Using tools such as Nmap to identify open ports through which device can be	Specifications and documentation related to the configurations available in the applications and firmware related to transport layer security.		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		accessed leading to unintended data retrieval. e) Verifying that the TLS session(s) are resistant to attempts of interception and decryption of network traffic using man-in-the middle attacks using tools like Burpsuite.			
8.	Verify that the firmware apps validate the digital signature of server connections.	a) Identifying the scenarios when the device establishes the server connections with the external world and verifying the following: • Security features, related to secure server connections and digital signature validation as implemented like strong cipher	Document mentioning the use cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the server connections.		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		suites, secure TLS version, SSL pinning etc. supported by code walkthrough. • Proper certificate validation, certificate chain validation and certificate revocation checks are implemented in the device. b) Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites. c) Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval. d) Verifying that TLS			

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		session(s) are resistant to attempts of interception and decryption of network traffic using man-in-the middle attacks using tools like Burpsuite.			
9.	Verify that wireless communications are mutually authenticated.	Testing, in presence of OEM team, to verify the process of mutual authentication as laid down in the documentation by the vendor.	The documentation regarding the process of mutual authentication as implemented in the device when wireless communications are initiated. In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.		
10.	Verify that wireless communications are sent over an encrypted channel.	Identifying all the security mechanisms being used in the communication process verification through: a) Testing, in presence of OEM team b) Code review c) Process audit of the key-life cycle process	i. Documentation regarding the security measures implemented in the device to prevent tampering of the data being sent through wireless mode of communication. ii. In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.		
11.	Verify that any	Secure code review	i. Firmware binaries for code		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	use of banned C functions are replaced with the appropriate safe equivalent functions.	[both automated and manual], in presence of OEM team, using a licensed static analysis tool through any of the following approaches: a) Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended] b) Visit to the evaluation agency by the vendor with the firmware code and any licensed static analysis tool available with them and demonstrating the code	review. ii. Internal code review reports		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		review activity in the presence of representatives of evaluation agency. c) Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them. d) Giving a remote access of the systems at vendor site to the evaluation agency containing the firmware code along with the licensed static analysis tool available with the vendors.			
12.	Verify that each firmware	a) Verification of the submitted	i. Documentation for information on software		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	maintains a software bill of materials cataloging third-party components, versioning, and published vulnerabilities.	list of third-party components by running automated tools like FACT on the firmware. b) Identifying vulnerabilities in the third-party component(s) through publically available vulnerability databases. c) Verification and validation of the process defined by the vendor for providing regular security updates and patches for the firmware to address any known vulnerabilities in third party components.	bill of materials, including third-party components and versions. ii. Organization process and policies for the following: • Addressing and patching any identified vulnerabilities in third-party components. • Informing the customers about the security issues or vulnerabilities and providing security updates and patches for the same. iii. Configuration management system and related policies for maintaining firmware and third-party binaries, libraries and frameworks along with the patches/fixes issued to the devices.		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
13.	Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).	Secure code review [both automated and manual], in presence of OEM team, using a licensed static analysis tool through any of the following approaches: a) Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended] b) Visit to the evaluation agency by the vendor with the firmware code and any licensed static analysis tool available with them and demonstrating	i. Firmware binaries for code review. ii. Internal code review reports		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		the code review activity in the presence of representatives of evaluation agency. c) Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them. d) Giving a remote access of the systems at vendor site to the evaluation agency containing the firmware code along with the licensed static analysis tool available with the vendors.			
14.	Verify that the	Independent secure	i. Firmware binaries for code		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	application and firmware components are not susceptible to OS Command Injection by invoking shell command wrappers, scripts, or that security controls prevent OS Command Injection.	code review [both automated and manual] using a licensed static analysis tool through any of the following approaches: a) Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended] b) Visit to the evaluation agency by the vendor with the firmware code and any licensed static analysis tool available with them and demonstrating the code	review ii. Internal code review reports		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		review activity in the presence of representatives of evaluation agency. c) Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them. d) Giving a remote access of the systems at vendor site to the evaluation agency containing the firmware code along with the licensed static analysis tool available with the vendors.			
Level 2/3					
15.	Verify that the	Identifying the	Document mentioning the use-		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	firmware apps pin the digital signature to a trusted server(s).	scenarios when the device establishes the server connections with the external world and verifying the following: a) Security features, related to secure server connections and digital signature validation as implemented like strong cipher suites, secure TLS version, SSL pinning etc. supported by code walkthrough. b) Proper certificate validation, certificate chain validation and certificate revocation checks are implemented	cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the server connections.		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		in the device.			
16.	Verify the presence of tamper resistance and/or tamper detection features.	Testing, in presence of OEM team, to verify the measures implemented in the device to prevent software and hardware tampering.	i. Measures available in the device to prevent software tampering. ii. Measures available in the device to prevent hardware tampering.		
17.	Verify that any available Intellectual Property protection technologies provided by the chip manufacturer are enabled.	Testing, in presence of OEM team, to verify the enabling of the Intellectual Property protection technologies provided by the chip manufacturer, if available.	i. Datasheet of the SoC ii. Documentation regarding the Intellectual Property protection technologies provided by the chip manufacturer which have been enabled. iii. In case, no Intellectual Property protection technologies are being provided by the chip manufacturer, then a declaration stating the same.		
18.	Verify security controls are in place to hinder firmware reverse engineering (e.g., removal of verbose debugging symbols).	Testing, in presence of OEM team, to verify the security controls as provided by the vendor to hinder firmware reverse engineering.	Documentation regarding the security controls in place to hinder firmware reverse engineering.		
19.	Verify the device validates	Testing, in presence of OEM team, to verify	i. Datasheet of the SoC ii. Technical specifications of		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	the boot image signature before loading.	the following: a) Device boots up successfully with the documented secure boot process when a valid boot image is provided. b) Device does not boot up when a tampered boot image (like with missing signature, invalid signature) is provided.	the device regarding secure boot (should consist of keys involved and their management life cycle, signature validation process and any other secure mechanisms if implemented.)		
20.	Verify that the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.	Testing, in presence of OEM team, to verify the following: a) Device gets successfully updated with the documented secure upgrade process when a valid update	Process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle, signature validation process and any other secure mechanisms if implemented.		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		package is provided. b) Device does not boot up when a tampered update package (like with missing signature, invalid signature) is provided.			
21.	Verify the device uses code signing and validates firmware upgrade files before installing.	Testing, in presence of OEM team, to verify the following: a) Device gets successfully updated with the documented secure upgrade process when a valid update package is provided. b) Device does not boot up when a tampered update package (like with missing	Process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle, signature validation process and any other secure mechanisms if implemented.		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		signature, invalid signature) is provided.			
22.	Verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Testing, in presence of OEM team, to verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle, signature validation process and any other secure mechanisms if implemented.		
23.	Verify usage of cryptographically secure pseudo-random number generator on embedded device (e.g., using chip-provided random number generators).	a) Verification of the documentation provided by the vendor regarding the random number generators being used in the devices. b) Verification through code review that random number generators or related libraries as applicable are being used in	Documentation regarding the random generators (either hardware based or software based or both) being used in the device with their intended usage. In case, hardware based random number generators are being used, vendors shall submit the following: i. Datasheet of the SoC ii. Technical specifications of the device regarding random generators In case, software based random number generators are being used, vendors shall provide the libraries being used for the same.		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		the device.			
24.	Verify that firmware can perform automatic firmware updates upon a predefined schedule.	Verification shall be done as per the applicable scenario: **Case 1: Automatic OTA updates are available:** A standard operating procedure for issuing automatic updates/upgrades to the in-field devices is required to be submitted by the vendor which can then be evaluated by the evaluation agency **Case 2: Automatic OTA updates are not available and vendor provides manual updates:** A standard operating procedure for issuing manual updates/upgrades to the in-field devices is required to be submitted by the vendor which can then be evaluated by the evaluation agency	i. Modes of updates available i.e. automatic, manual or both. ii. Organizational process and policies regarding the issuing of updates to the devices.		
Level 3					
25.	Verify that the	a) Confirm that	i. Tampering Detection and		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
	device wipes firmware and sensitive data upon detection of tampering or receipt of invalid message.	the device can detect tampering events and triggers a firmware and sensitive data wipe. b) Verify that the device wipes firmware and sensitive data upon receipt of an invalid message or command.	Response Procedure ii. Invalid Message Handling and Data Wiping Policy		
26.	Verify that only micro controllers that support disabling debugging interfaces (e.g. JTAG, SWD) are used.	a) Ensure datasheets and reference manuals confirm the capability to disable JTAG or SWD interfaces. b) Check that the firmware or configuration settings include options to disable debugging interfaces.	i. Datasheets ii. Reference Manuals iii. Configuration Guidelines iv. Security feature descriptions		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		c) Verify the presence and effectiveness of any security features or mechanisms related to disabling debugging.			
27.	Verify that only micro controllers that provide substantial protection from de-capping and side channel attacks are used.	a) Check datasheets and security documentation to confirm that the microcontroller includes features like physical protection against de-capping and side-channel attack mitigation (e.g., voltage and temperature monitoring). b) Evaluate if the microcontroller implements security mechanisms	i. Datasheets, ii. Security Feature Specifications iii. Any relevant security evaluation or certification reports		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		such as secure key storage, hardware random number generators, and tamper detection. c) Perform or review results of any security evaluations or certifications that assess resilience against physical attacks and side-channel vulnerabilities.			
28.	Verify that sensitive traces are not exposed to outer layers of the printed circuit board.	a) Review the PCB design files and schematics to ensure that sensitive traces are routed on inner layers rather than outer layers. b) Inspect the PCB layers visually or	i. PCB Design Documentation ii. Trace Exposure Inspection Report iii. Security Design Review Report		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		using X-ray imaging (if available) to confirm that sensitive traces are indeed protected within inner layers and not exposed. c) Verify adherence to design rules that specify trace routing and layer usage for sensitive signals.			
29.	Verify that inter-chip communication is encrypted (e.g. Main board to daughter board communication).	a) Ensure that the encryption methods used for inter-chip communication meet security standards and are properly implemented. b) Verify that data transmitted between the	i. Encryption Protocol Specification ii. Communication Security Audit Report iii. Data Integrity Verification Records		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		main board and the daughter board remains secure and unaltered.			
30.	Verify the device uses code signing and validates code before execution.	a) Confirm that the device uses code signing to authenticate software and firmware before execution. b) Verify that the device performs code validation checks to ensure that only signed and verified code is executed.	i. Code Signing Policy ii. Validation Process Documentation iii. Code Signing Audit Report		
31.	Verify that sensitive information maintained in memory is overwritten with zeros as soon as it is no longer required.	a) Confirm that sensitive information in memory is securely overwritten with zeros once it is no longer	i. Memory Management Policy ii. Data Overwriting Procedures iii. Security and Privacy Audit Report		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		needed. b) Ensure that the mechanism for overwriting data with zeros is functioning correctly and effectively clears sensitive information.			
32.	Verify that the firmware apps utilize kernel containers for isolation between apps.	a) Confirm that the firmware applications are using kernel containers to ensure isolation between different apps. b) Verify that the kernel containers effectively separate the applications to prevent unauthorized access or interference.	i. Kernel Container Configuration Guide ii. Application Isolation Verification Report iii. Firmware Security Assessment Report		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
33.	Verify that secure compiler flags such as -fPIE, -fstack-protector-all, -Wl,-z, noexecstack, -Wl, -z, noexecheap are configured for firmware builds.	a) Confirm that secure compiler flags such as -fPIE, -fstack-protector-all, -Wl,-z,noexecstack, and -Wl,-z,noexecheap are properly configured in the firmware build process. b) Ensure that the firmware build process incorporates these flags to enhance security and protect against common vulnerabilities.	i. Build Configuration Files ii. Compiler Flags Compliance Report iii. Firmware Security Review Report		
34.	Verify that micro controllers are configured with code protection (if applicable).	a) Confirm that microcontrollers are configured with code protection mechanisms where applicable to	i. Code Protection Configuration Documentation ii. Microcontroller Security Settings Report iii. Code Protection Implementation Verification Report		

Cl. No.	Verification Requirements	What to be tested/audited	Documents Required	Implementation Details/Evidences Submitted	Comment by Developer
		safeguard against unauthorized access or tampering. b) Verify that the implemented code protection measures are effectively preventing unauthorized code modifications or access.			

Annexure C

Supply Chain Security Requirements

Sr. No.	Requirements	What to be Tested/audited	Documents Required	Implementation Details	Comment by Developer
SC1	Verify that whether trusted sources are being used for sourcing the components of the device i.e. trusted supply chain through a managed Bill of materials for critical hardware components (related to security functions like SoC) is in use.		Bill of materials for critical hardware components (related to security functions like SoC).		
SC2	Supply chain risk identification, assessment, prioritization and mitigation shall be conducted. Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents need to be submitted and demonstrate the same.		Supply chain risk identification, assessment, prioritization, and mitigation documents. Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary		

			documents.		
SC3	Verify the no proprietary network protocols are being used in the device. If yes, then complete implementation details and the source code		Document for Network protocols used in the device.		
SC4	Design and architecture details till the PCBA and SoC level to be provided to aid in counterfeit mitigation and malware detection.		Design and architecture documents till the PCBA and SoC level.		
SC5	Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.	Process and methodartifacts need to be submitted and demonstrate the same.			
SC6	One or more up-to-date malware detection tools shall be deployed as part of the code acceptance and development processes. Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date malware detection	List of components thathave been identified as requiring tracking targets of tainting/counterfeiting, CM tool. Quality assurance process need to be submitted and demonstrate the same.			

	tools).				
SC7	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.		Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents need to be submitted and demonstrate the same.		

References

1. ISO/IEC 27400 Cybersecurity — IoT security and privacy — Guidelines
2. ISO/IEC 27402 Cybersecurity — IoT security and privacy — Device baseline requirements
3. OWASP ASVS Appendix C: IoT security Requirements
4. ISO/IEC 20243 - Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS)