Cybersecurity Certification Program for IoT Devices

Version 2.1

February 2022

CTIA Certification LLC
1400 16th Street, NW
Suite 600
Washington, DC 20036

1.202.785.0081

programs@ctiacertification.org

Table of Contents

Section 1 Introduction

1.1 Purpose

This document defines the CTIA Certification Program requirements for Cybersecurity Certification of managed Internet of Things (IoT) devices. For the purpose of this document, an IoT device contains an IoT application layer that provides identity and authentication functionality and at least one communications module supporting 5G, 4G LTE Wi-Fi®.

1.2 Scope

This document includes the requirements and processes of the CTIA Cybersecurity Certification Program ("Program") for IoT devices. An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc. The device might include hardware, software, sensors, actuators and network connectivity. Tests are defined in the CTIA Cybersecurity Certification Test Plan for IoT Devices ("Test Plan") [1].

While the Program covers a wide range of requirements, network operators may require compliance with additional specifications and tests to satisfy their unique security requirements. It is highly recommended to understand the target operator's security requirements prior to seeking certification.

The Program is defined in two levels. The first level identifies core IoT device security features; these features must be supported by all consumer and enterprise IoT devices. The second level identifies security features of increasing device complexity, sophistication and manageability; these devices must be capable of being connected to an enterprise management system (EMS).

Testing assumes that the device provides an execution environment for IoT applications that makes use of the 4G LTE or 5G communications module and/or the Wi-Fi communications module. If the IoT application is not associated with at least one of these communications modules, then the device architecture is out of scope of this document. If the IoT application supports more than one of these communications modules, then tests that involve network communications shall be tested with each supported communications module to ensure the same security features are available for all network environments.

Many different mechanisms may be used to achieve the security goals. The IoT device manufacturer (OEM) may select the mechanisms that are deemed most relevant for the intended market. One of the goals of this document is to make sure the widest adopted standards are used to ensure compatibility across cybersecurity systems. This document and the Test Plan [1] mandate a number of standards: AES key size standards, end-to-end encryption standards, syslog standards, etc. These are intended to allow for a baseline of security standards that are compatible with most systems.

This document assumes minimum support for encryption based on AES with a 128-bit key. Support for this algorithm and key size by all devices provides an interoperable cryptographic capability; however, devices may also support other algorithms and key sizes that provide the same or more cryptographic security.

1.2.1 Level 1 IoT Cybersecurity Requirements (Consumer and Enterprise Devices)

The Level 1 IoT security features are:

- Terms of Service and Privacy Policies – Device Terms of Service and privacy policy are readily available. The Terms of Service cover "end of life" for the device.

- Authentication – Device supports local password management and one-time password management.
- Access Controls – Device enforces role-based access control.
- Patch Management and Software Upgrade – Device supports installation software upgrades from an authorized source.
- IoT Device Identity – Device provides an IoT Device Type and a globally unique IoT Device Identity.
- Encryption of Data at Rest – Device supports an effective mechanism for encrypting data stored on the device.
- Encryption of Data in Transit – Device supports encrypted communications using IPsec (IP Security), SSH (Secure Shell), TLS (Transport Layer Security), or DTLS (Datagram TLS).
- Use of Subscription Related Information – Device protects subscription related information.
- Design-In Features – Device includes features to fail secure, provide boundary security, and ensure function isolation.
- Tamper Protection and Evidence – Devices protects security-sensitive data from tampering.
- Constrained IoT Devices – Device cannot support software update capabilities and can be isolated from the network in case of vulnerability.

1.2.2 Level 2 IoT Cybersecurity Requirements (Enterprise Devices)

- Audit Log – Device supports the gathering audit log events and reporting them to an EMS using IPsec, SSH, TLS, or DTLS for encryption and integrity protection.
- Multi-Factor Authentication – Device supports multiple authentication factors.
- Remote Deactivation – Device can be remotely deactivated by the EMS.
- Secure Boot – Device supports a secure boot process to protect its hardware (e.g., UEFI (Unified Extensible Firmware Interface)).
- Threat Monitoring – Device supports logging of anomalous or malicious activity based on configured polices and rules.
- Secure Backup – Device supports backup.

1.3 Applicable Documents

The following documents are applicable to or referenced in this document. Unless otherwise specified, the latest released version shall be used

[1] CTIA Cybersecurity Certification Test Plan for IoT Device
[2] ETSI EN 303 645 V2.1.1

[3] NIST IR 8228
[4] NIST IR 8259A
[5] NIST SP 800-40 Rev 3
[6] CTIA Consumer Code for Wireless Service, CTIA
[7] NIST SP 800-92
[8] RFC 5424 -- The Syslog Protocol
[9] RFC 5425 -- Transport Layer Security (TLS) Transport Mapping for Syslog
[10] RFC 6012 -- Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog
[11] FIPS PUB 197
[12] RFC 5246 -- Transport Layer Security (TLS) Protocol Version 1.2
[13] RFC 8446 -- The Transport Layer Security (TLS) Protocol Version 1.3
[14] RFC 6347 -- Datagram Transport Layer Security Version 1.2
[15] RFC 4301 -- Security Architecture for the Internet Protocol
[16] RFC 4303 -- IP Encapsulating Security Payload (ESP)
[17] RFC 4306 -- Internet Key Exchange (IKEv2) Protocol
[18] RFC 5282 -- Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
[19] RFC 4251 -- The Secure Shell (SSH) Protocol Architecture
[20] RFC 4252 -- The Secure Shell (SSH) Authentication Protocol
[21] RFC 4253 -- The Secure Shell (SSH) Transport Layer Protocol
[22] RFC 4254 -- The Secure Shell (SSH) Connection
[23] RFC 8308 -- Extension Negotiation in the Secure Shell (SSH) Protocol
[24] RFC 6749 -- The OAuth 2.0 Authorization Framework
[25] RFC 8252 -- OAuth 2.0 for Native Apps
[26] NIST IR 8425
[27] CTIA Certification Policies and Policies and Procedures for Authorized Test Labs

1.4 Definitions

Table 1.4-1 Acronyms and Definitions

Term	Definition
Adequate Privilege	Adequate Privilege is any account that has the ability to upgrade the device software.
Associated Service	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. [2]
Critical Vulnerability	A critical vulnerability has potentially adverse effects of a large scale. Due to the complex software structures and the pervasive of communication platforms, multiple stakeholders might be involved in an update to address a critical vulnerability.
Critical Security Parameters	Security-related secret information whose disclosure or modification can compromise the security of a security module. For example, secret cryptographic keys, authentication values such as passwords, PINs, private components of certificates. [2]
Constrained IoT 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. [2]

Term	Definition
Default password	A default password may be used on multiple devices and is not allowed during normal operation. In order to start normal operation the user is forces to change the default password.
Device Deactivation	A deactivated device is unable to communicate with any network using any port or protocol.
Enterprise Management System (EMS)	A large-scale application software package that supports business processes, account management, device audit log monitoring, and data analytics in complex organizations. The EMS may be a collection of unique services (such as active directory) that may be diversified with a service provider (such as a cloud based service) feeding information to a corporate EMS.
Factory set password	A factory set password is unique to each device but not based on the generic approach (e.g. not serial number, “password1”).
Fresh Character String	To attempt to modify the password with an acceptable set of characters where the system correctly accepts the new password.
Inventory Information	Inventory information to support asset management, which maintains a current, accurate inventory of all IoT devices and their relevant characteristics throughout the devices’ lifecycles in order to use that information for cybersecurity and privacy risk management purposes
IoT Device	An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc. An IoT device might include hardware, software, sensors, actuators and network connectivity.
IoT Device ID	The IoT Device ID is the unique identifier for a single device. This identifier is permanently set by the OEM and is not changeable.
IoT Device Type	A permanently assigned identifier for a group of devices that share common characteristics, functions or behaviors.
Normal Operation	This means to allow the device to be turned on, performing all the device’s startup routines to completion. At this point the device is in normal operation mode, it may or may not have connectivity to a 4G LTE, 5G or Wi-Fi network and be awaiting further commands. When device is under normal operation the first time, the device may have some additional setup activities, such as setting the password, connecting to the network for the first time, performing patching / updates [5] that may be unique during the first time setup.
OEM	Original Equipment Manufacturer
One-Time Password (OTP)	A password that is valid for only a single login session on an IoT device.
Subscription related information	Any information associated to user roles on the device (privileged and non-privileged), including user configuration and cryptographic material such as user passwords, certificates or keys.
Remote Deactivation	Disable the IoT device from the EMS. A deactivated device cannot generate network traffic. A manual reset may be needed to reactivate the device or configure it to work on another network.
Security Best Practice on Usability	The user is presented with a subset of configuration options using consistent defaults and appropriate security options turned on by default.
Severity Based Deadline	Within the EMS, a policy can be established so that the audit log entries will be sent to the EMS upon the severity level specified in the configuration. Rather than waiting on a time-based reporting threshold (every 5 minutes) or a size based reporting threshold (log reaches 100k), SysLog [8 – 10] provides a severity level capability, which allows more severe events to be reported to the EMS more promptly than routine ones.

Term	Definition
Software Patch	A software patch is safely installed in a manual or an automated manner while the device is operating. A patch does not make major changes to the device configuration or add new features that change the security posture of the device.
Software Upgrade	A software upgrade is installed in a manual or an automated manner. A software upgrade may change the IoT device configuration or features in a security relevant way. Upgrades are expected to be installed when the device is operational in a stable environment.
Telemetry Data	Data from a device that can provide information to help the manufacturer identify issues or information related to device usage. For example, a consumer IoT device reports software malfunctions to the manufacturer enabling them to identify and remedy the cause. [2]

Section 2 Program Procedures

2.1 Test Facilities

Multiple laboratories are authorized to perform certification testing according to the Test Plan.

A current listing of CTIA Certification Authorized Test Labs (ATLs) can be found within the CTIA Certification database and on the CTIA Certification website at https://www.ctiacertification.org/test-labs/.

OEMs may utilize ATLs for pre-certification testing as per Section 2.2 of this document.

2.2 Use of the CTIA Cybersecurity Certification Test Plan for IoT Devices

As noted in the copyright statement of the Test Plan, only ATLs are authorized to use the Test Plan for commercial testing purposes. No other test labs are authorized to use the Test Plan. The Test Plan may not be altered or reproduced in any way without prior permission from CTIA Certification. No portions of the Test Plan may be used in other documents without prior permission from CTIA Certification.

ATLs shall refer to the CTIA Certification Policies and Procedures for Authorized Test Labs [27] document and the ATL License and Service Agreement for the terms and conditions under which the Test Plan may be used.

2.3 OEM Submission

OEMs shall submit certification requests via the CTIA Certification database at https://certify.ctiacertification.org/. User login accounts may be requested by selecting “Register now” on the login page.

The OEM shall select IoT Cybersecurity Certification Program, Submit New Request. Then select the appropriate request type:

- Initial Certification Request
- ECO Certification Request

The OEM shall enter the requested information about the device and select an ATL. The OEM shall select the main PoC and billing PoC for the request.

The OEM shall select the operators allowed to view the certification record on the CTIA Certification database once it is certified.

The OEM shall upload a Product Description, such as a product brochure or user manual, and may upload any optional supporting documentation to assist with the evaluation of the device.

The OEM shall read and agree to the certification license agreement terms and conditions.

The OEM shall submit the OEM Questionnaire (see Appendix A) to the ATL.

After the request is submitted and accepted by ATL for testing, the certification database will generate an invoice for the CTIA Certification fee (see Appendix B) which will be available in the Billing & Payment tab.

The ATL will receive an email notification of the certification request. The ATL will log into the certification database to review and accept/reject the request. The database will send an email notification to the submitter once the ATL has accepted/rejected the request. If the request is rejected, the submitter may re-assign the request to another ATL.

Once the request has been accepted by the ATL, the OEM may no longer make changes to the request. The OEM shall contact the ATL or CTIA Certification if any changes need to be made to the data entered.

The OEM shall then send a minimum of three (3) units for testing directly to the ATL per the ATL's instructions.

2.4 Device Evaluation

The ATL shall test the devices according to the current version of the Test Plan at the time of submission. Results shall be recorded in the test report template provided by CTIA Certification.

Upon completion of the evaluation, the ATL shall log into the CTIA Certification database and:

- Enter the requested information about the testing
- Upload the completed test report template, along with a summary test report (PDF file) that complies with ISO/IEC 17025 requirements
- Confirm if the devices has a 5G/NR interface
- Confirm if the device has an 4G/LTE interface
- Confirm if the device has a Wi-Fi interface

The test results and the information submitted by the OEM during the submission process will be maintained in confidence by CTIA Certification and the ATL.

2.5 Certification

Upon completion of the following items, the device will be certified:

- Product Description uploaded by the OEM
- Acceptance of the certification license agreement terms and conditions
- Completed test report template and summary test report uploaded by the ATL
- Certification of the parent product, in the case of ECO Certification Requests
- Payment of the CTIA Certification fee

The certification will apply to the specific HW/ SW version of the device evaluated by the ATL. Certification of additional HW/SW versions may be accomplished as per Section 2.6 of this document.

2.6 Certification of HW/SW Updates to a Model

Should the OEM wish to certify a different HW/SW version of a model an ECO certification request shall be submitted (by logging into the CTIA Certification database, selecting Submit New Request and choosing ECO Certification Request).

The OEM and ATL shall determine the scope of testing. The ATL shall test the device according to the current version of the Test Plan.

2.7 Certification of Re-Labeled Devices

A re-labeled device is defined as a device that is identical to a currently certified device, but has a different OEM name and model name/number.

The re-labeling OEM may certify a re-labeled device by entering the device into the CTIA Certification database as an Initial certification:

- The re-labeled OEM name and model name/number shall be entered
- The ATL used for the originally certified device shall be chosen
- The ATL shall upload the test reports of the originally certified device along with two additional documents:
    - A Product Equality Letter from the re-labeling OEM. This letter shall state that the re- labeled device is the same as the originally certified device (referenced by OEM name and model name/number as it appears in the certification database) and that no changes have been made other than the OEM name and model name/number. The letter shall be signed and dated.
    - An Authorization of Use Letter from the OEM of the originally certified device. This letter shall state that the OEM of the originally certified device allows the ATL to use the test reports from this device for certification of the relabeled device. The letter shall be signed and dated.

2.8 Waiver Process

The objective of the waiver process is to provide OEMs the opportunity to work with CTIA Certification and sponsor operator(s) to document the waiver of a specific test case. The waiver request will be assessed on a case by case basis by CTIA Certification and/or the sponsor operator(s).

Step 1:

The OEM is allowed to submit a waiver for any specific test case. One Waiver Request Form is required for one specific test case OEM seeks to waive. The OEM should complete sections 1-3 of the CTIA Certification IoT Cybersecurity Waiver Request Form (Waiver Request Form) to initiate the process. The Waiver Request Form is available in the zip file.

The ATL shall review and comment in section 4 of the Waiver Request Form prior to the waiver submission.

OEM to submit the waiver request into the CTIA Certification database at https://certify.ctiacertification.org/ by uploading the Waiver Request Form to the Optional Supporting Documentation section.

Example Waiver justifications:

- IoT Cybersecurity Requirements from Level 1 may be covered by corresponding Level 2 requirements.
- If a device does not support defined IoT Cybersecurity Requirements (e.g. local passwords and user management) it is acceptable, if more sophisticated/complex security features (e.g. mutual authentication via X.509 certificates) are supported instead.
- Device does not support certain test case requirement.
- Device does not support certain test case procedure. The list of examples is not exhaustive.

Step 2:

With a sponsor operator chosen in the certification request:

- CTIA Certification to circulate the waiver request to the sponsor operator(s) for approval via email Without a sponsor operator chosen in the certification request:
- CTIA Certification to evaluate the waiver request for approval

Waiver approval will be based on the assessment of the impact of the waiver.

The sponsor operator(s) or CTIA Certification shall review and comment in section 5 of the Waiver Request Form.

Step 3:

Sponsor operator(s) or CTIA Certification to approve/reject the waiver request within 5 business days after the submission. The decision is based on the assessment of the impact of the waiver.

CTIA Certification shall assign a Waiver ID (a unique identifier) and fill out section 6 of the Waiver Request Form.

Step 4:

OEM to upload the approved Waiver Request Form to the certification database. The certification request will not be approved if there is a pending waiver request.

Step 5:

The ATL shall list the approved Waiver ID instead of a “Not Tested” indication in the test report.

Section 3 Level 1 IoT Cybersecurity Requirements (Consumer and Enterprise Devices)

This section describes the first level of CTIA Cybersecurity Certification requirements for IoT devices on a managed network. To achieve a Level 1 CTIA Cybersecurity Certification, the device must meet all of requirements in this section.

There shall be no interruption of power or battery while the device is being tested.

3.1 Terms of Service and Privacy Policies

Requirement: The OEM shall make Terms of Service, privacy policy, telemetry data collection capabilities, cloud services dependencies, vulnerability disclosure policy, software update procedure, installation and maintenance documentation, and external sensing capabilities for the device available. This requirement ensures the OEM provides the lifetime of the product and ensures that important information about the device and the way it operates as well as the external entities it interacts with is available to the customer.

Procedure:

- Confirm the availability documentation for the Terms of Service, privacy policy, telemetry data collection capabilities, cloud services dependencies, vulnerability disclosure policy, software update procedure, installation and maintenance, and external sensing capabilities related to the device.

3.2 Authentication

The device shall support user locally managed passwords according to Section 3.2.1; and the device shall support one-time passwords according to Section 3.2.2

3.2.1 Password

Requirement: Devices shall support locally managed passwords to offer straightforward password management, uses either factory set passwords that are unique to each device or any default passwords get changed on first use. Device shall support user authentication to be able to make changes to the device configuration with the goal to require authentication before changes are made, reducing risk to the device that anyone can walk up and make anonymous changes to the device. The device shall support a mechanism that limits the number of successive failed attempts to reduce the risk of brute-force attacks.

Procedure:

- Confirm that factory set passwords are unique per device, not generic.
- Confirm that default passwords are rejected during normal operation.
- Confirm that the device can change locally managed passwords, and the password contains at least 8 characters.
- Confirm that the password for one user cannot be accessed by any other user.
- Confirm that the password can be concealed during input.
- Confirm that the device requires user login to perform any privileged action.

- Confirm that the device limits the number of successive failed attempts.

3.2.2 One-Time Password

Requirement: The device shall only allow login to the device can only occur with an externally managed short-lived, one-time password (OTP) that is not easily guessable. A short-lived OTP will be accepted for at most 2 minutes. A difficult to guess OTP is at least 6 pseudo-random characters or digits.

Procedure:

- Confirm that the device accepts only externally generated OTP of at least 6 pseudo-random characters or digits.
- Confirm that the device will not accept the same OTP more than once.
- Confirm that the device will not accept a never-used OTP after it expires.

3.3 Access Controls

Requirement: The device shall enforce role-based access control. The intent of this requirement is to make sure user or low-level accounts cannot perform privileged actions; that roles are clearly separated and enforced.

Procedure:

- Confirm that login to an administrative role is required to perform any action at a privilege level.

3.4 Patch Management and Software Upgrade

Requirement: The device shall support automatic or manual installation of unmodified software patches or unmodified security upgrades from an authorized source in order to correct software problems and fix vulnerabilities. These patches are expected to not reset the existing configuration.

Procedure:

- Confirm that the device supports automatic or manual installation of unmodified software patches or upgrades from an authorized source without causing the device configuration to be reset.

3.5 IoT Device Identity

Requirement: The device shall identify itself with an IoT Device Type and a globally unique IoT Device Identity.

NOTE: There are many ways that an OEM can assign an IoT Device Type and a globally unique IoT Device Identity; this document does not require the use of any particular approach.

Procedure:

- Confirm that the device can provide an IoT Device Type that can be used to determine the capabilities of the device.

- Confirm that the device can provide a globally unique IoT Device Identity that is available logically and physically.

3.6 Encryption of Data at Rest

Requirement: The device shall include an effective mechanism for encrypting data stored in the device using 128-bit AES at minimum.

Procedure:

Confirm that the device implements either an encrypting file system or a file encryption mechanism that uses 128-bit AES at minimum.

3.7 Encryption of Data in Transit

Requirement: The device shall support encrypted communications using SSH, IPsec, TLS or DTLS. The devices must support 128-bit AES at minimum.

Procedure:

- Confirm that the device supports encryption of data communications using SSH, IPsec, TLS, or DTLS with 128-bit AES.

3.8 Use of Subscription Related Information

Requirement: Subscription related information shall only be stored after obtaining consent, and then the subscription related information can easily be removed from the device and associated services.

Procedure:

- Confirm that subscription related information is not stored without consumer consent.
- Confirm that consent to use subscription related information can be withdrawn.
- Confirm that subscription related information can easily be removed from the device.
- Confirm that subscription related information can easily and promptly be removed from the services associated with the device.

3.9 Design in Features

Requirement: The security design of the device shall avoid hard-coded critical security parameters, disables unused logical and network interfaces, disables debug interfaces, minimizes the disclosure of security-relevant information prior to authentication, and validates input data.

Procedure:

- Confirm that the security design of the device prevents hard-coded critical security parameters in device software source code.
- Confirm that the security design of the device disables any unused network and logical interfaces.

- Confirm that the security design of the device disables any debug interfaces.
- Confirm that the security design of the device minimizes the disclosure of security-relevant information prior to authentication.
- Confirm that the security design of the device validates input data, whether it is provided by the user or received over the network.

3.10 Tamper Protection and Evidence

Requirement: A device with a hard-coded unique device identity shall provide tamper protection.

Procedure:

- Confirm that the security design of the device provides tamper protection for hard-coded unique device identity, if the device has one.
- Confirm that the tamper protection mechanisms in the security design are on a basic level implemented.

3.11 Constrained IoT Devices

Requirement: The device shall meet the requirements of a device that cannot support software update capabilities, due to limitations with respect to storage, processing, communications, user interaction, or overall intended use case and that the device can be isolated from the network in case of a vulnerability.

Procedure:

- Confirm the Terms of Service or Use for the device (e.g., included in the box or download from the OEM web page) includes information that covers the rationale for the absence of software updates, when the device will need to be replaced, the method of device replacement, and a defined support period for the hardware and software.
- Confirm the device can be isolated from the network in case of vulnerability.
- Confirm a remote deactivation command to the device deactivates/permanently shuts down the device
- Confirm a deactivated device removes all subscription related information

Section 4 Level 2 IoT Cybersecurity Requirements (Enterprise Devices)

This section describes the second level of CTIA Cybersecurity Certification requirements for IoT devices on a managed network. To achieve a Level 2 CTIA Cybersecurity Certification, the device must meet all requirements in this document; the test plan [1] will verify the requirements noted in Section 3 and this section.

There shall be no interruption of power or battery while the device is being tested.

4.1 Terms of Service and Privacy Policies

Requirement: The device shall recover cleanly after power failure.

Procedure:

- Confirm that the design supports clean recovery after power failure.

4.2 Authentication

The device authentication shall implement multiple factors for authentication according to Section 4.2.3, and also implement either passwords (something you know) according to Section 4.2.1 or one-time passwords (something you have) according to Section 4.2.2.

4.2.1 Password

Requirement: The device shall be integrated with an EMS. The device shall honor the EMS mechanism to limit the rate of unsuccessful authentication attempts to greatly increase the time needed to guess a password. The device shall support user authentication.

Procedure:

- After the device has been integrated with an EMS, confirm that the device will not allow passwords to be set to a string that is prohibited by the EMS.
- After the device has been integrated with an EMS, confirm that the device implements a rate-limiting or blocking mechanism that limits the number of unsuccessful authentication attempts as specified by the EMS.
- After a period of inactivity, confirm that the user must provide their password to continue.
- Confirm that the device honors the disabling of a user role in the EMS.

4.2.2 One-Time Password

Requirement: The device shall be integrated with an EMS.

Procedure:

- After a period of inactivity set by the EMS, confirm that the user must provide a fresh OTP to continue.

4.2.3 Multi-Factor Authentication

Requirement: The device shall be configured to require two different authentication factors for login.

NOTE: One factor will most likely be a password (i.e., something you know). The other factor could be biometric (i.e., something you are) or possession of a physical object (i.e., something you have). The OAuth 2.0 protocol **Error! Reference source not found. Error! Reference source not found.** offers one approach to multi-factor authentication, and there are many approaches.

Procedure:

- Configure the device to require at least two different authentication factors for login, and then confirm that all the factors are successfully checked at login.

4.3 Access Controls

No additional requirements for Level 2.

4.4 Patch Management and Software Management

Requirement: The device shall support the download of software patches or upgrades from a remote location at a time that is coordinated with an EMS.

Procedure:

- Confirm that the device supports download of software patches or upgrades from a remote location.

- Confirm that the device supports installation of software patches or upgrades from an authorized source at a time that is coordinated with an EMS.

4.5 IoT Device Identity

No additional requirements for Level 2.

4.6 Encryption of Data at Rest

No additional requirements for Level 2.

4.7 Encryption of Data in Transit

Requirement: The device shall support encrypted communications with the EMS to using SSH, IPsec, TLS or DTLS. The devices must support 128-bit AES at minimum.

Procedure:

- Confirm that the device supports encryption of data communications with the EMS using SSH, IPsec, TLS, or DTLS with 128-bit AES.

4.8 Use of Subscription Related Information

No additional requirements for Level 2.

4.9 Design in Features

Requirement: The design of the device shall include features to fail secure, resiliency to data network and power failure, connect to networks and services in an orderly fashion, secure software development process are followed, the principle of least privilege is followed, critical functions are isolated, reviewed or evaluated cryptographic implementations are used, boundary security is provided, function isolation is implemented, unnecessary physical interfaces are not exposed, and there is a hardware-level access control mechanism for memory.

Procedure:

- Confirm that the device was designed to fail secure.
- Confirm that the device was designed to be resilient to data network or power failure.
- Confirm that the device was designed to connect to networks and services in an orderly fashion.
- Confirm that unneeded software services are disabled, code includes only the necessary functionality, and that unused code is removed.
- Confirm that the principle of least privilege is followed.
- Confirm that critical functions are isolated from non-critical ones.
- Confirm that reviewed or evaluated implementations are used for network and security functionalities, particularly in the field of cryptography.
- Confirm that the device was designed to deny all inbound and outbound network communications, except for those that are essential for the device to operate properly.

  NOTE: The Threat monitoring functionality may play a significant role in the enforcement of a policy to “deny-all, permit-by-exception” network communications.

- Confirm that the device was designed to isolate critical functions from less critical functions with separation and segmentation mechanisms.

  NOTE: If malicious software gets into the device, these mechanisms deter the propagation to other parts of the device and other devices while critical functions continue to operate properly. For example, boundary controls within a device could be used to allow only allowed or accepted activities.

- Confirm that the device hardware does not expose unnecessary physical interfaces.
- Confirm that the device includes a hardware-level access control mechanism for memory.

4.10 Tamper Protection and Evidence

Requirement: The device shall have the ability to alert an EMS when it is physically opened.

Procedure:

- Confirm that the device alerts an EMS and records in the audit log when it is physically opened.

4.11 Audit Log

Requirement: The device shall support the gathering and reporting of audit log events to an EMS using a severity thresholds and time frequency. Collection of subscription related information is minimized and anonymized where possible.

Procedure:

- Confirm that the EMS audit log gathers at least emergency, alert, critical, and error events, and that these events are transferred to the EMS at an interval selected by the EMS in the Syslog format over a session protected with SSH, IPsec, TLS, or DTLS.
- Confirm that older audit log entries can be trimmed or reset on the device only by a privileged role.
- Confirm that the most privileged role cannot make changes to individual log entries.
- Confirm that audit logs contain minimal subscription related information and is anonymized where possible.
- If telemetry data is collected, confirm that the device provides a means to support it during incident analysis.

4.12 Remote Deactivation

Requirement: The unique device shall be remotely deactivated by the EMS and that any subscription related information associated with the device is erased from the device and protected by the EMS.

Procedure:

- Integrate the device with an EMS and configure the remote deactivation capability.
- Configure a network traffic monitor to capture network traffic between the device and the EMS.
- Send remote deactivation command from EMS and observe if device deactivates/shuts down.
- If device successfully deactivates/shuts down, then the requirement is met.
- Confirm a deactivated device successfully removes subscription related information.

4.13 Secure Boot

Requirement: The device shall protect the integrity of the boot process.

Procedure:

- Confirm that the device includes a mechanism to protect the boot process against unintended or malicious modification.

4.14 Threat Monitoring

Requirement: The device shall support asset inventory, logging of anomalous or malicious activity, scanning for vulnerabilities and correcting and rectify them when they are identified, and forensic investigation of incidents.

Procedure:

- Confirm that the device supports an EMS inventory process.
- Confirm that the EMS audit log gathers events based on anomalous or malicious activity based on configured polices and rules.
- Confirm that the device provides a vulnerability scanner or a built-in vulnerability identification capability that reports concerns to the EMS.
- Confirm that the device OEM continually monitors for security vulnerabilities and rectify them when they are identified.
- Confirm that the device provides a means to support forensic analysis of security incidents.

4.15 Secure Backup

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

Procedure:

- Confirm that the device secure backup and recovery process work as expected.

Appendix A OEM Questionnaire

The Questionnaire can be found in the zip file along with this document.

Appendix B Certification Fees

The fee for CTIA Cybersecurity Certification is:

Request Type	Fee (U.S. $)
Level 1 Initial Request	500
Level 2 Initial Request	1,000
ECO Request	500

Certification testing fees are separate from these fees and are determined independently by each ATL.

Appendix C Waiver Request Form

The Waiver Request Form can be found in the zip file along with this document.

Appendix D Requirements Traceability

This appendix provides a mapping for the requirements from NIST IR 8259A, NIST IR 8228, and ETSI EN 303 645 V2.1.1. For each requirement, the section in the test plan [1] that confirms that the device under test meets the requirement is provided.

D.1 NIST IR 8259A Requirements

NIST IR 8259A Requirements	CTIA Cybersecurity Certification Test Plan for IoT Devices Test Plan
Device Identification	Section 3.5
Device Configuration	Section 3.2
Data Protection	Section 3.6 and Section 3.7
Logical Access to Interfaces	Section 3.3
Software Update	Section 3.4
Cybersecurity State Awareness	Section 4.11

D.2 NIST IR 8228 Requirements

NIST IR 8228 Requirements	CTIA Cybersecurity Certification Test Plan for IoT Devices Test Plan
Asset Management	
Expectation 1:	Section 3.5
Expectation 2:	Section 4.1
Expectation 3:	Section 3.5 and Section 4.11
Expectation 4:	Section 3.1
Vulnerability Management	
Expectation 5:	Section 3.1
Expectation 6:	Section 4.4
Expectation 7:	Section 3.1 and Section 4.14
Access Management	
Expectation 8:	Section 4.3
Expectation 9:	Section 3.2
Expectation 10:	Section 4.2
Expectation 11:	Section 4.2
Expectation 12:	Section 4.3
Expectation 13:	Section 4.2
Expectation 14:	Section 4.10
Incident Detection	
Expectation 15:	Section 4.11
Expectation 16:	Section 4.11
Expectation 17:	Section 4.14
Expectation 18:	Section 4.11 and Section 4.14
Data Protection	
Expectation 19:	Section 3.6 and Section 3.7

Expectation 20:	Section 4.15
Expectation 21:	Section 3.7
Disassociated Data Management	
Expectation 22:	Section 4.2
Informed Decision Making	
Expectation 23:	Section 3.1 and Section 4.1
PII Processing Permission Management	
Expectation 24:	Section 3.8 and Section 4.12
Information Flow Management	
Expectation 25:	Sections 3.1, 3.8 and 4.12

D.3 ETSI EN 303 645 V2.1.1 Requirements

ETSI EN 303 645 V2.1.1 Requirements	**CTIA Cybersecurity Certification Test Plan for IoT Devices Test Plan**
5.1 No universal default passwords	
Provision 5.1-1 (M C):	Section 3.2
Provision 5.1-2 (M C):	Section 3.2
Provision 5.1-3 (M):	Section 3.2
Provision 5.1-4 (M C):	Section 3.2
Provision 5.1-5 (M C):	Section 4.2
5.2 Implement a means to manage reports of vulnerabilities	
Provision 5.2-1 (M):	Section 3.1
Provision 5.2-2:	Section 3.1
Provision 5.2-3:	Section 3.1 and Section 4.14
5.3 Keep software updated	
Provision 5.3-1:	Section 3.4
Provision 5.3-2 (M C):	Section 3.4

Provision 5.3-3 (M C):	Section 3.4
Provision 5.3-4:	Section 4.4
Provision 5.3-5:	Section 4.4
Provision 5.3-6:	Section 4.4
Provision 5.3-7 (M C):	Section 3.4
Provision 5.3-8 (M C):	Section 3.1
Provision 5.3-9:	Section 3.4
Provision 5.3-10 (M):	Section 3.4
Provision 5.3-11:	Section 3.4
Provision 5.3-12:	Section 3.1 and Section 3.4
Provision 5.3-13 (M):	Section 3.1
Provision 5.3-14:	Section 3.11
Provision 5.3-15:	Section 3.11
Provision 5.3-16 (M):	Section 3.5
5.4 Securely store credentials and security-sensitive data	
Provision 5.4-1 (M):	Section 3.6
Provision 5.4-2 (M C):	Section 4.10 [1]
Provision 5.4-3 (M):	Section 3.10 [1]
Provision 5.4-4 (M):	Section 3.4 and Section 3.7
5.5 Communicate securely	
Provision 5.5-1 (M):	Section 3.7
Provision 5.5-2:	Section 4.9
Provision 5.5-3:	Section 4.4
Provision 5.5-4:	Section 3.3
Provision 5.5-5 (M):	Section 3.3
Provision 5.5-6:	Section 4.7
Provision 5.5-7 (M):	Section 3.7

Provision 5.5-8 (M):	Section 3.9
5.6 Minimize exposed attack surfaces	
Provision 5.6-1 (M):	Section 3.9
Provision 5.6-2 (M):	Section 3.9
Provision 5.6-3:	Section 4.9
Provision 5.6-4 (M C):	Section 3.9
Provision 5.6-5:	Section 4.9
Provision 5.6-6:	Section 4.9
Provision 5.6-7:	Section 4.9
Provision 5.6-8:	Section 4.9
Provision 5.6-9:	Section 4.9
5.7 Ensure software integrity	
Provision 5.7-1:	Section 4.13
Provision 5.7-2:	Section 4.13
5.8 Ensure that personal data is protected	
Provision 5.8-1:	Section 3.7
Provision 5.8-2 (M):	Section 3.7
Provision 5.8-3 (M):	Section 3.1
5.9 Make systems resilient to outages	
Provision 5.9-1:	Section 4.9
Provision 5.9-2:	Section 4.9
Provision 5.9-3:	Section 4.9
5.10 Examine system telemetry data	
Provision 5.10-1:	Section 4.1 and Section 4.11
5.11 Make it easy for consumers to delete personal data	
Provision 5.11-1 (M):	Section 3.8
Provision 5.11-2:	Section 3.8

Provision 5.11-3:	Section 3.1
Provision 5.11-3:	Section 3.1
5.12 Make installation and maintenance of devices easy	
Provision 5.12-1:	Section 3.1
Provision 5.12-2:	Section 3.1
Provision 5.12-3:	Section 3.1
5.13 Validate input data	
Provision 5.13-1 (M):	Section 3.9
6 Data protection provisions for consumer IoT	
Provision 6.1 (M):	Section 3.1
Provision 6.2 (M C):	Section 3.8
Provision 6.3 (M):	Section 3.8
Provision 6.4:	Section 4.11
Provision 6.5 (M C):	Section 4.1[2]

[1] Tamper resistance is not required for consumer level devices unless a hard-coded parameter is used in the security design

[2] The telemetry and audit are sent to the EMS.

Appendix E Revision History

Date	Version	Description
October 2018	1.0	• Initial release
May 2019	1.1	• Updated Appendix A, OEM Questionnaire from Version 1.0 to 1.1
April 2020	1.2	• Changed the term Vendor to OEM • Added additional text regarding operators requirements in Section 1.2 • Removed Test Report Template appendix
July 2020	1.3	• Added device requirements for each level • Updated OEM Questionnaire
November 2020	1.3.1	• Changed organization name from CTIA to CTIA Certification and updated contact email • Changed title of document to Cybersecurity Certification Program for IoT Devices • Changed CATL to ATL • Updated certification database URL
January 2021	1.4	• Added waiver process in Section 2.8
September 2021	1.5	• Updated Sections 1.2.1, 1.4, 3.2, 3.3, 3.4, 3.5, 3.6, 4.5, 4.7 and 5.16
February 2023	2.1	• Updated document according to CTIA-Certification-Cybersecurity-Test-Plan-for IoT Devices Version 2.1