Cybersecurity Certification Program for IoT Devices

Version 1.3.1

November 2020

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

1.202.785.0081

programs@ctiacertification.org

Table of Contents

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 three levels. The first level identifies core IoT device security features; and the second and third levels identify security elements of increasing device complexity, sophistication and manageability.

Testing assumes that the device provides an execution environment for IoT applications that makes use of the 5G or 4G LTE 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. The Test Plan [1] mandates 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 Tests

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.

Password Management – Device supports local password management and one-time password management

Authentication – Device supports user authentication.

Access Controls – Device enforces role-based access control.

Patch Management – Device supports automatic and manual installation of patches from an authorized source.

Software Upgrades – Device supports manual installation software upgrades from an authorized source.

1.2.2 Level 2 IoT Cybersecurity Tests

The Level 2 IoT security features expand on the Level 1 IoT security features and add:

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.

Encryption of Data in Transit – Device supports encrypted communications using IPsec, SSH, TLS or DTLS.

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).

Threat Monitoring – Device supports logging of anomalous or malicious activity based on configured polices and rules.

IoT Device Identity – Device provides an IoT Device Type and a globally unique IoT Device Identity.

1.2.3 Level 3 IoT Cybersecurity Tests

The Level 3 IoT security features expand on the Level 1 and Level 2 IoT security features and add:

Encryption of Data at Rest– Device supports an effective mechanism for encrypting data stored on the device.

Digital Signature Generation and Validation – Device supports generation and validation of digital signatures.

Tamper Evidence – Device has the ability to alert a monitoring system when it is physically opened.

Design-In Features – Device includes features to fail secure, provide boundary security, and ensure function isolation.

1.3 Applicable Documents

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

[1] *Cybersecurity Certification Test Plan for IoT Devices*, CTIA Certification
[2] RFC 5652
[3] RFC 5751
[4] NIST SP 800-53 Rev 4
[5] NIST SP 800-63B Authentication and Lifecycle Management
[6] Council on CyberSecurity (CCS) Critical Security Controls (CSC)
[7] NIST SP 800-40 Rev 3

[8] CTIA Consumer Code for Wireless Service
[9] ISO/IEC 27001:2013
[10] ANSI/ISA 62443-2-1:2009
[11] NIST SP 800-92
[12] RFC 5424
[13] RFC 5425
[14] RFC 6012
[15] NIST Cybersecurity Framework v1.1
[16] NIST SP 800-113
[17] FIPS PUB 197
[18] RFC 5246
[19] NIST SP 800-147
[20] NIST SP 800-63-3
[21] NIST SP 800-25
[22] NIST SP 800-49
[23] NIST SP 800-89
[24] FIPS PUB 186-4
[25] RFC 5280
[26] NIST SP 800-160
[27] GSM AA.39
[28] NIST Cybersecurity for IoT Program
[29] NIST SP 800-41 Rev 1
[30] NIST SP 800-111
[31] SP800-90A
[32] RFC 4301 -- Security Architecture for the Internet Protocol
[33] RFC 4303 -- IP Encapsulating Security Payload (ESP)
[34] RFC 4306 -- Internet Key Exchange (IKEv2) Protocol
[35] RFC 5282 -- Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
[36] RFC 4251 -- The Secure Shell (SSH) Protocol Architecture
[37] RFC 4252 -- The Secure Shell (SSH) Authentication Protocol
[38] RFC 4253 -- The Secure Shell (SSH) Transport Layer Protocol
[39] RFC 4254 -- The Secure Shell (SSH) Connection
[40] RFC 8308 -- Extension Negotiation in the Secure Shell (SSH) Protocol
[41] RFC 6749
[42] RFC 8252
[43] CTIA Certification Policies and Procedures for Authorized Test Labs

1.4 Definitions

Term	Definition
Adequate Privilege	Adequate Privilege is any account that has the ability to upgrade the device software (Section 3.6)
ATL	CTIA Certification Authorized Test Lab
Device Deactivation	A deactivated device is unable to communicate with any network using any port or protocol.
Digital Signature	A digital signature is a cryptographic mechanism for checking authenticity. The Test Plan [1] makes use of RSA and ECDSA digital signatures, which are based on different cryptographic primitives. The Test Plan [1]. accommodates one variant of the RSA digital signature: RSASSA-PKCS1-v1_5. The Test Plan [1]. accommodates one variant of the ECDSA digital signature: ECDSA with curve P-256. Both variants depend upon the SHA-256 hash function.
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.
Fresh Character String	To attempt to modify the password with an acceptable set of characters where the system correctly accepts the new password. Section 3.2.
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 an 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, 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.
P7S Format	The file format of a digital signature using the Cryptographic Message Syntax (CMS), which is also known as PKCS#7. The most recent version of CMS can be found in RFC 5652 [2]. In addition, RFC 5751 [3] defines the application/pkcs7-signature media type for digitally signed content using this same format.
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.
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 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 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 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.

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 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 [43] 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, OEM Questionnaire) 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, Certification Fees) 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.

3 Level 1 IoT Cybersecurity Requirements

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 pass all of the tests in Test Plan [1], which verifies the 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

Reference: CTIA Consumer Code for Wireless Service [8], NIST SP 800-53 Rev 4 [4]

Requirement: The OEM shall make Terms of Service and privacy policy for the device available. This ensures that the OEM provides the lifetime of the product as well as makes the customer aware of their privacy policy and where data might be stored outside of the device.

Procedure:

- Confirm that Terms of Service document, privacy policy document, and list the cloud services that the device requires access to for normal operation are available.

Testing Prerequisites:

- Verify existence and availability of the Terms of Service and the privacy policy of the device.
- The Terms of Service and the privacy policy must be applicable to the device and model submitted for certification, but may be broad enough to cover several similar models of devices.

3.2 Password Management

The device shall support locally managed user passwords according to Section 3.2.1 or one-time passwords according to Section 3.2.2.

3.2.1 Local Password Management

Reference: NIST SP 800-53 Rev. 4 [4], NIST SP 800-63B [5]

Requirement: The device shall locally manage user passwords with the intent to make passwords unique to each device; to change the default password on first use; to remove the ability of the user to set it to a commonly used / easily guessable, bad password.

Procedure:

- Confirm that default passwords are specific to the 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, but the password does not contain several repetitive or sequential characters.
- Confirm that the password for one user cannot be accessed by any other user.

Testing Prerequisites:

- Ensure that default passwords are in place at the start of this test**.**
- Determine the procedure to restore factory settings from the device documentation.

3.2.2 One-Time Password Management

Reference: NIST SP 800-63B [5], RFC 6749 [41], RFC 8252 [42]

Requirement: The device shall only allow login 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.

Testing Prerequisites:

- Obtain device documentation on external management of OTP generation and distribution.
- Configure the device for a particular external OTP management server.
- Configure a network traffic monitor to capture network traffic to and from the device.

3.3 Authentication

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

Requirement: The device shall require user authentication before changes to the device configuration are made, with the goal to reducing risk to the device that anyone can walk up and make anonymous changes to the device.

Procedure:

- Confirm that the device requires user login to perform any privileged action.

Testing Prerequisites:

- Obtain device documentation on the login roles and their privileges
- Ensure all passwords have been changed from their defaults.
- Obtain a method to unlock the device if multiple failed login attempts cause the device to lock.

3.4 Access Controls

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

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.

Test Applicability: If a device has no privileged accounts and only one user accounts, then the requirements in this section are not applicable and they are skipped.

Procedure:

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

Testing Prerequisites:

- Obtain device documentation on the roles and their privileges.
- Ensure all passwords have been changed from their defaults.

3.5 Patch Management

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4], NIST SP 800-40 Rev 3 [7]

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

NOTE: Support for download of software patches from a remote location is not required in Level 1; however, such a capability may be the most feasible approach to patch management for all of the levels.

Test Applicability: If an OEM states their device is not patchable but is upgradable, then the requirements in this section are note applicable. Skip the 'Patch Management' requirements in this section and move on to 'Software Upgrades' section.

Procedure:

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

Testing Prerequisites:

- Determine the current device software version and patch level, then locate a patch that is suitable for installation.
- Determine when it is safe and appropriate to manually install a software patch from the device documentation.
- Determine the current device configuration.

3.6 Software Upgrades

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

Requirement: The device shall support manual installation of unmodified software upgrades from an authorized source in order to migrate to a newer version, which may contain additional features.

Procedure:

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

Testing Prerequisites:

- Determine the current device software version and patch level, then locate a software upgrade that is suitable for installation.
- Determine the current device configuration.

4 Level 2 IoT Cybersecurity Requirements

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 pass all of the tests in Test Plan [1], which verify the requirements 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

Reference: CTIA Consumer Code for Wireless Service [8], NIST SP 800-53 Rev 4 [4]

Requirement: The OEM shall make a process to update Terms of Service and privacy policy for the device are available.

Procedure:

- Confirm that there is a process to update Terms of Service and privacy policy documents.

Testing Prerequisites:

- Conduct the tests in Section 3.1 of Test Plan [1].

4.2 Password Management

The device shall support locally managed user passwords according to Section 4.2.1 or one-time passwords according to Section 4.2.2.

4.2.1 Local Password Management

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-63B [5]

Requirement: The device shall support integration with an EMS.

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 a period of inactivity, confirm that the user must provide their password to continue.

Testing Prerequisites:

- Conduct the tests in Section 3.2.1 of Test Plan [1].
- Integrated the device with a functioning EMS.
- Specify a configuration set for the EMS for testing
- Determine the time interval of inactivity for the device to automatically end the session and require the user to enter their password to continue.

4.2.2 One-Time Password Management

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-63B [5], RFC 6749 [41], RFC 8252 [42]

Requirement: The device shall support integration with an EMS.

Procedure:

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

Testing Prerequisites:

- Conduct the tests in Section 3.2.2 of Test Plan [1].
- Integrated the device with a functioning EMS.
- Specify a configuration set for the EMS for testing.
- Determine the time interval of inactivity for the device to automatically end the session and require the user to enter a fresh OTP to continue.

4.3 Authentication

Reference: CCS CSC [6], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Requirement: The device shall support user authentication and shall honor the disabling of a user role in the EMS.

Procedure:

Confirm that the device honors the disabling of a user role in the EMS.

Testing Prerequisites:

- Conduct the tests in Section 3.3 of Test Plan [1].
- Integrate the device with an EMS and ensure that a privileged role has been disabled.
- Ensure there is no interruption of power or battery while the device is being tested.

4.4 Access Controls

No additional requirements for Level 2.

4.5 Patch Management

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4], NIST SP 800-40 Rev 3 [7]

Requirement: The device shall support the download of software patches from a remote location in order to correct software problems and fix vulnerabilities.

Test Applicability: If a device is not patchable, but is upgradable, then the requirements in this section are not applicable. Skip the 'Patch Management' requirements in this section and move on to the 'Software Upgrades' section.

Procedure:

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

Testing Prerequisites:

- Conduct the tests in Section 3.5 of Test Plan [1].
- Determine the current device software version and patch level, and then locate a patch that is suitable for installation.
- Determine when it is safe and appropriate to manually install a software patch from the device documentation.
- Determine the current device configuration.

4.6 Software Upgrades

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

Requirement: The device shall support download of software upgrades from a remote location and installation of software upgrades from an authorized source in order to migrate to a newer version, which may contain additional features.

Procedure:

- Confirm that the device supports download from a remote location and installation of software upgrades from an authorized source.

Testing Prerequisites:

- Conduct the tests in Section 3.6 of Test Plan [1].
- Determine the current device software version and patch level, and then locate a software upgrade that is suitable for installation.

4.7 Audit Log

Reference: CCS CSC [6], ISA 62443-2-1:2009 [10], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-92 [11], RFC 5424 [12], RFC5425 [13], RFC 6012 [14]

Requirement: The device shall support the gathering and reporting of audit log event to an EMS.

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 audit log older 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.

Testing Prerequisites:

- Obtain device documentation on the roles and their privileges. Make a list of the roles that can view audit log entries. Make a list of the roles that can delete audit log entries.
- Obtain device documentation on the actions that will cause audit log entries to be generated.
- Integrate the device with an EMS and ensure that an audit event reporting threshold (e.g., 0 for an emergency, and 7 for debug) has been configured.
- Configure a network traffic monitor to capture network traffic between the device and the EMS.

4.8 Encryption of Data in Transit

Reference: CCS CSC [6], NIST CSF v1.1 [15], NIST SP 800-53 Rev 4 [4], NIST SP 800-113 [16], FIPS PUB 197 [17], RFC 5246 [18], RFC 6012 [14]

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

Test Applicability: If the device does not use cloud services, then the requirements in this section are not applicable and they are skipped.

Procedure:

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

Testing Prerequisites:

- Configure the device to use SSH, IPsec, TLS, or DTLS to encrypt network traffic with 128-bit AES.
- Configure a network traffic monitor to capture network traffic to and from the device.
- Determine the cloud services that the device depends upon, if any.

4.9 Multi-Factor Authentication

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4], NIST SP 800-63B [5]

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).

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.

Testing Prerequisites:

- Obtain device documentation on multi-factor authentication. Enable multi-factor authentication for the most privileged role.
- Obtain one factor for multi-factor authentication

4.10 Remote Deactivation

Reference: CCS CSC [6], NIST CSF v1.1 [15], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Requirement: The device shall support remote deactivation via EMS

Procedure:

- Integrate the device with an EMS and configure the remote deactivation capability.
- Send remote deactivation command from EMS and observe if device deactivates/shuts down.
- If device successfully deactivates/shuts down, then test case is considered passing

Testing Prerequisites:

- Confirm that the device can be remotely deactivated by an authenticated command from EMS.

4.11 Secure Boot

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4], NIST SP 800-147 [19]

Requirement: The device shall support mechanisms that protect the boot integrity process.

Procedure:

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

Testing Prerequisites:

- Confirm that the device in the out-of-the-box configuration will securely boot and begin normal operation.
- Verify the existence of documentation that describes the secure boot process.

4.12 Threat Monitoring

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Requirement: The device shall support logging of anomalous activity based on configured policies and rules.

Procedure:

- Confirm that the EMS audit log gathers events based on anomalous or malicious activity based on configured polices and rules.

Testing Prerequisites:

- Obtain device documentation on the policies and rules that can be configured to detect anomalous or malicious activity, and then configure the policies and rules to detect activities that the tester can trigger.
- Integrate the device with an EMS and ensure that an audit reporting has been configured.

4.13 IoT Device Identity

Reference: NIST SP 800-63B [5], NIST SP 800 63-3 [20]

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 requirement and Test Plan [1]. do not require the use of a 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.
- Confirm the device has the ability to include the IoT Device Type and globally unique IoT Device Identity in the EMS audit log.

Testing Prerequisites:

- Obtain the IoT Device Type and the globally unique IoT Device Identity for the device.
- Obtain device documentation on the actions that will cause audit log entries to be generated.

5 Level 3 IoT Cybersecurity Requirements

This section describes the third level of CTIA Cybersecurity Certification requirements for IoT devices on a managed network. Level 3 offers the most comprehensive level of testing for cybersecurity threats. To achieve a Level 3 CTIA Cybersecurity Certification, the device must pass all of the tests in Test Plan [1]., which verifies the requirements in Section 3, Section 4, and this section.

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

5.1 Terms of Service and Privacy Policies

No additional requirements for Level 3.

5.2 Password Management

The device shall support locally managed user passwords according to Section 5.2.1 or one-time passwords according to Section 5.2.2.

5.2.1 Local Password Management

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-63B [5]

Requirement: The device shall support a mechanism to limit the rate of unsuccessful authentication attempts to greatly increase the time needed to guess a password.

Procedure:

- 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.

Testing Prerequisites:

- Conduct the tests in Section 3.2.1 and Section 4.2.1 of Test Plan [1].
- Integrate the device with an EMS.
- Obtain the documentation of rate-limiting or blocking mechanism from OEM.

5.2.2 One-Time Password Management

No additional requirements for Level 3.

5.3 Authentication

No additional requirements for Level 3.

5.4 Access Controls

No additional requirements for Level 3.

5.5 Patch Management

Reference: CCS CSC [6], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-40 Rev 3 [7]

Requirement: The device shall support automatic installation of digitally signed software patches from an authorized source in order to correct software problems and fix vulnerabilities at a time that is coordinated with an EMS.

Test Applicability: If an OEM states their device is not patchable, but is upgradable, then the requirements in this section are not applicable. Skip the 'Patch Management' requirements in this section and move on to the 'Software Upgrades' section.

Procedure:

- Confirm that the device supports automatic installation of software patches from an authorized source at a time that is coordinated with an EMS.
- Confirm that the device validates the digital signature on the software patch immediately prior to installation.

NOTE: Digital signature validation depends on the functionality in Section 5.14.

Testing Prerequisites:

- Conduct the tests in Section 3.5 and Section 4.5 of Test Plan [1].
- Integrate the device with an EMS.
- Determine the current device software version and patch level, then locate a patch that is suitable for installation.
- Modify a copy of the patch by altering the digital signature, creating an invalid patch.

5.6 Software Upgrades

Reference: CCS CSC [6], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Requirement: The device shall support automatic installation of digitally signed software upgrades from an authorized source in order to migrate to a newer version at a time that is coordinated with an EMS.

Procedure:

- Confirm that the device supports automatic installation of software upgrades from an authorized source at a time that is coordinated with an EMS.
- Confirm that the device validates the digital signature on the software upgrade immediately prior to installation.

NOTE: Digital signature validation depends on the functionality in Section 4.13.

Testing Prerequisites:

- Conduct the tests in Section 3.6 and Section 4.6 of Test Plan [1].
- Integrate the device with an EMS.
- Determine the current device software version and patch level, then locate a software upgrade that is suitable for installation.

- Modify a copy of the software upgrade by altering the digital signature, creating an invalid software upgrade.

5.7 Audit Log

Reference: CCS CSC [6], ISA 62443-2-1:2009 [10], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-92 [11], RFC 5424 [12], RFC5425 [13], RFC 6012 [14]

Requirement: The device shall support the gathering of audit log events and reporting them to an EMS within a severity-based deadline.

Procedure:

- Confirm that emergency, alert, critical, and error events are transferred to the EMS event within a severity-based deadline.

Testing Prerequisites:

- Conduct the tests in Section 4.7 of Test Plan [1].
- Configure a network traffic monitor to capture network traffic between the device and the EMS.
- Configure delivery deadlines for emergency, alert, critical, and error events.

5.8 Encryption of Data in Transit

No additional requirements for Level 3.

5.9 Multi-Factor Authentication

No additional requirements for Level 3.

5.10 Remote Deactivation

No additional requirements for Level 3.

5.11 Secure Boot

No additional requirements for Level 3.

5.12 Threat Monitoring

No additional requirements for Level 3.

5.13 IoT Device Identity

No additional requirements for Level 3.

5.14 Digital Signature Generation and Validation

Reference: NIST SP 800-25 [21] , NIST SP 800-49 [22], NIST SP 800-53 Rev 4 [4], NIST SP 800-89 [23], FIPS PUB 186-4 [24], RFC 5280 [25], RFC 5652 [2], RFC 5751 [3]

Requirement: The device shall be capable of generating an RSA or ECDSA digital signature, and validate RSA and ECDSA digital signatures using a set of trust anchors.

Procedure:

Confirm the following:

- the device can generate an RSA or ECDSA digital signature in the P7S format, and
- the device can validate RSA and ECDSA digital signatures in the P7S format.

Testing Prerequisites:

- Generate or install a digital signature private key for use with either the RSA or ECDSA algorithm.
- Obtain an X.509 certificate that includes the public key that corresponds to the digital signature private key.
- Configure at least one trust anchor that can be used to validate an RSA digital signature.
- Configure at least one trust anchor that can be used to validate an ECDSA digital signature.

5.15 Encryption of Data at Rest

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-113 [16], FIPS PUB 197 [17]

Requirement: The device shall support 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.

Testing Prerequisites:

- Obtain device documentation on encryption of data stored in the device.

5.16 Tamper Evidence

Reference: NIST SP 800-53 [4]

Requirement: The device shall support 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.

Testing Prerequisites:

- Integrate the device with the EMS.
- Configure a network traffic monitor to capture network traffic between the device and EMS.

5.17 Design-In Features

Reference: NIST SP 800-53 [4], NIST SP 800-160 [26]

Requirement: The device shall have security design which includes features to fail secure, provide boundary security, and ensure function isolation.

Procedure:

- Confirm that the device was designed to fail secure.

  NOTE: When failure is detected, the device goes to a secure state.

- 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 whitelisted activities.

Testing Prerequisites:

- Verify existence and availability of design documentation for the security mechanisms of the device.

Appendix A OEM Questionnaire

The OEM Questionnaire can be found in the Zip file created for 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	750
Level 3 Initial Request	1,000
ECO Request	500

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

Appendix C 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