Cybersecurity Certification Test Plan for IoT Devices

Version 2.0

December 2021

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

The purpose of this document is to define the CTIA Certification Program testing requirements for CTIA 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 either 4G LTE, 5G or Wi-Fi®.

The CTIA Cybersecurity Certification Test Plan harmonizes IoT device requirements from ETSI and NIST into a common test plan for the industry. In particular, the test plan encompasses requirements from the three documents that follow:

- ETSI EN 303 645 V2.1.1: Cyber Security for Consumer Internet of Things: Baseline Requirements [2]
- NIST IR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks [3]
- NIST IR 8259A: IoT Device Cybersecurity Capability Core Baseline [4]

1.2 Scope

This test plan defines the cybersecurity tests that will be conducted in CTIA Certification Authorized Test Labs (ATLs) on devices submitted for CTIA Cybersecurity Certification. 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 such that accurate, repeatable testing may be conducted among all ATLs. Detailed step-by-step test procedures and specific test equipment configurations are left to the ATL and will be presented to CTIA Certification as part of the ATL authorization process as defined in the *CTIA Certification Policies and Procedures for Authorized Test Labs* document [1].

CTIA Cybersecurity Certification 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 test plan. 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.

Testing assumes that the device firmware or software can be updated, either through patch management and/or software upgrades procedure. If the device firmware or software can be updated, then the device architecture is out of scope of this test plan.

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 goal of this test plan is to ensure the widest adopted standards are used across cybersecurity systems. The test plan mandates a number of standards: AES key size standards

[11], end-to-end encryption standards, syslog compatible formats, etc. These are intended to allow for a baseline of security standards that are compatible with most systems.

This test plan 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 equivalent or more cryptographic security.

This test plan assumes the use of standard security protocols to protect data in transit. Devices must use IPsec (IP Security) [16][17][18], SSH (Secure Shell) [19][20][21][22], TLS (Transport Layer Security) [12][13], or DTLS (Datagram TLS) [14] to provide interoperable security capability; however, devices may also support other security protocols.

This test plan specifies certain situations in which, during the testing process, an ATL may accept an attestation from an IoT OEM in lieu of testing. In the event that an attestation is accepted, evidence to support the validity of the attestation shall be provided by the OEM to the ATL (e.g. a photograph, a signed document of attestation provided by a certified OEM representative, etc.).

1.2.1 Level 1 IoT Cybersecurity Tests (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.
- 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 and Software Upgrades – 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 Personal Data – Device protects personal data.
- Design-In Features – Device includes features to fail secure, provide boundary security, and ensure function isolation.
- Tamper Evidence – Devices protects security-sensitive data from tampering.

1.2.2 Level 2 IoT Cybersecurity Tests (Enterprise Devices)

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

- 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 using IPsec, SSH, TLS, or DTLS for encryption and integrity protection.

1.3 Applicable Documents

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

[1] CTIA Certification Policies and Procedures for Authorized Test Labs, CTIA Certification
[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

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]
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.
Fresh Character String	To attempt to modify the password with an acceptable set of characters where the system correctly accepts the new password. Section 3.2.1.4.
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.
Personal Data	Any information relating to an identified or identifiable natural person.
Personal Identifiable Information	Synonym for personal data.

Term	Definition
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][9][10] provides a severity level capability, which allows more severe events to be reported to the EMS more promptly than routine ones.
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 Reserved

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

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

Purpose: Confirm availability of 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. This test 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 3.1.

Test Cases:

3.1.1 Try to obtain the Terms of Service or Use for the device (e.g., included in the box or download from the OEM web page). If the Terms of Service or Use for the device is obtained, then this test passes; otherwise it fails.

3.1.2 Within the Terms of Service or Terms & Conditions for the device, locate the portion of the document that covers “end of life” or “end of your term” for the device. If the terms provide the defined support period in a manner that is clear and transparent to the user, then this test passes; otherwise it fails.

3.1.3 Try to obtain the privacy policy for the device (e.g., included in the box or download from the OEM web page). If the privacy policy for the device is obtained, then this test passes; otherwise it fails.

3.1.4 Within the privacy policy for the device, locate the portion that covers processing of personal data. If the documentation provides clear and transparent information about what personal data is processed, how personal data is used, who uses the personal data (e.g., third parties, including advertisers), and for what purposes, then this test passes; otherwise it fails.

3.1.5 Within the privacy policy for the device, locate the portion that covers deletion of personal data. If the documentation provides clear instructions to delete the user’s personal data and how to obtain confirmation that the user’s personal data has been deleted from the device as well as services and applications associated with the device, then this test passes; otherwise it fails.

3.1.6 Try to obtain the documentation on telemetry data collection for the device (e.g., included in the box or download from the OEM web page). If the documentation covers what telemetry data is collected, how telemetry data is used, who uses the telemetry data, and for what purposes, then this test passes; otherwise it fails. If telemetry data is not collected, then this test is not applicable.

3.1.7 Try to obtain the list of cloud services that the device requires access to for normal operation device (e.g., included in the box or download from the OEM web page). If the documentation says there are no dependencies on cloud services or the documentation provides a list of cloud service dependencies or it covers “Back Up and Cloud Services” for the device, then this test passes; otherwise it fails.

3.1.8 Try to obtain the vulnerability disclosure policy (e.g., included in the box or download from the OEM web page). If the documentation includes contact information for the reporting of issues, a commitment to act on disclosed vulnerabilities in a timely manner, a commitment to act on critical vulnerability with appropriate priority, a timeline for initial acknowledgement of receipt after a report is made, and a timeline for status updates until the reported issue is resolved, then this test passes; otherwise it fails.

3.1.9 Try to obtain the procedures to update the device software (e.g., included in the box or download from the OEM web page). If the documentation includes the means by which the device will notify the user if the software update will disrupt the basic functioning, then this test passes; otherwise it fails. If no software update is able to be disruptive, then this test in not applicable.

3.1.10 Try to obtain the installation and maintenance documentation for the device (e.g., included in the box or download from the OEM web page). If the documentation shows minimal decisions by the user, provides guidance on securely setting up the device, and provides guidance on how to check whether their device is securely set up, then this test passes; otherwise it fails.

3.1.11 Try to obtain the documentation of the external sensing capabilities of the device (e.g., included in the box or download from the OEM web page). If the device has any external sensing capabilities and these capabilities are described in a manner that is clear and transparent to the user, then this test passes; otherwise it fails. If the device has no external sensing capabilities, then this test is not applicable.

3.2 Authentication

Confirm that the device supports user passwords according to Section 3.2.1, confirm that the device offers straightforward password management, uses passwords that are unique to each device, any default passwords get changed on first use, limits the number of successive failed attempts to reduce the risk of brute-force attacks. Confirm that the device supports one-time passwords according to Section 3.2.2, or both.

3.2.1 Password

Purpose: If local password management is supported, confirm that devices that support locally managed passwords offer straightforward password management, use passwords that are unique to each device, and any default passwords get changed on first use. Confirm that the device supports 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. If local password management is supported, confirm that the device supports a mechanism that limits the number of successive failed attempts to reduce the risk of brute-force attacks.

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.

- 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.

Evidence Attestation Guideline:

- Initial- If only one test sample is provided, ATL can accept the attestation in Test Case 3.2.1.1 and 3.2.1.2. No attestation is allowed in the rest of the test cases in Section 3.2.
- ECO- This section shall be tested after software/firmware changes. If only one test sample is provided, ATL can accept the attestation in Test Case 3.2.1.1 and 3.2.1.2. No attestation is allowed in the rest of the test cases in Section 3.2.

Test Cases:

3.2.1.1 Try to login with the factory set password. If the factory set password is the same for many devices (e.g., a password of “admin” or one that is formed in an obvious way from information sent of the network), then this test fails; if the factory set password is specific to the device (e.g., based on the serial number of the device), then this test passes.

NOTE: Confirm with OEM that the password is unique and generated in a manner that reduces the risk of automated attacks against the device if only one DUT is provided.

3.2.1.2 If the same default password appears in multiple devices, then try starting initial normal operation before changing any passwords. If the device refuses to begin normal operation or forces the user to change the default passwords, then this test passes; otherwise it fails. If device specific passwords are uniquely generated by the manufacturer, then this test is not applicable.

NOTE: Device passwords are either uniquely generated by the manufacturer or provided by the user.

3.2.1.3 Try to locate the password management mechanism. If the password change mechanism is readily accessible, then this test passes; otherwise it fails.

3.2.1.4 Try setting a password to a fresh character string, and then perform the procedure to restore the device to factory settings. If the device refuses to begin normal operation or forces the user to change the default passwords, then this test passes; otherwise it fails.

3.2.1.5 Try setting a password to a fresh character string less than 8 characters. If the device refuses to set the password to the provided string or device gives a notification message by asking to input at least 8 characters, then this test passes; otherwise it fails.

3.2.1.6 Try setting a password back to the default value. If the device refuses to set the password to the provided string, then this test passes; otherwise it fails.

3.2.1.7 Try setting the password to a string with repetitive (e.g., ‘aaaaaaaa’) or sequential (e.g., ‘12345678’,’abcdefgh’) characters. If the device refuses to set the password to the provided string, then this test passes; otherwise it fails.

3.2.1.8 If the device supports more than one user password, login as the most privileged user and try to obtain the passwords of other users. If the device discloses the password of another user, then this test fails; otherwise it passes. If the device does not support more than one user password, then this test case is not applicable.

NOTE: The most privileged user might be able to set the passwords for other users but doing so should not allow them to learn the current password for other users.

3.2.1.9 If the device has a display, enter the password. If the device conceals the password, then this test passes; otherwise it fails. If the device does not have a display, then this test case is not applicable.

3.2.1.10 Try to login with the default password. If the login to the device is unsuccessful, then this test passes; otherwise it fails.

3.2.1.11 Try to login with an incorrect password. If the login to the device is unsuccessful, then this test passes; otherwise it fails.

3.2.1.12 Try to login with the incorrect password several times in a row. If the device restricts password attempts to at most 5 per minute after a number of failed attempts as specified by the manufacturer, then the test passes; otherwise it fails. If local password management is not used, then this test is not applicable.

3.2.1.13 Try to login with the correct password. If the login to the device is successful, then this test passes; otherwise it fails.

3.2.1.14 If the device supports more than one authenticated role, try to login to each role with an incorrect password. If the login to the device is unsuccessful in each case, then this test passes; otherwise it fails. If the device does not support more than one authenticated role, then this test case is not applicable.

3.2.1.15 If the device supports more than one authenticated role, try to login to each role with the correct password. If the login to the device is successful in each case, then this test passes; otherwise it fails. If the device does not support more than one authenticated role, then this test case is not applicable.

3.2.2 One-Time Password

Purpose: Confirm that 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 3.2.2.

Test Cases:

3.2.2.1 From the documentation, determine the size of the OTP and the duration that the OTP can be used. If the OTP is at least 6 pseudo-random characters or digits and the validity duration is at most 2 minutes, then this test passes; otherwise it fails.

3.2.2.2 Try to login with a freshly generated OTP. If login is successful, then this test passes; otherwise it fails.

3.2.2.3 Try to login using the same OTP a second time. If login is successful, then this test fails; otherwise it passes.

3.2.2.4 Capture the traffic between the device and the external OTP management server. Capture the traffic between the device and the user. If the OTP is transferred in plaintext more than once, then this test fails; otherwise it passes.

3.3 Access Controls

Purpose: Confirm that the device enforces role-based access control. The intent of this test 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 3.3.

Test Cases:

3.3.1 Prior to login, try to perform a privileged action described in the device documentation. If the privileged action is performed, then this test fails; otherwise it passes.

3.3.2 After login as a user with adequate privilege, try to perform a privileged action. If the privileged action is performed by the device, then this test passes; otherwise it fails.

3.3.3 If the device supports more than one authenticated role, test that the user must provide a valid password associated with the proper role in order to perform each privileged action. If the privileged action is performed by the device only after login to the proper role, then this test passes; otherwise it fails. If the device does not support more than one authenticated role, then this test is not applicable.

NOTE: Simple devices will have a single administrative role, but more complex devices may have many different roles with different, potentially overlapping, sets of privileges.

3.3.4 If the device is network accessible, try to access the device via the available network interface. If the device requires authentication prior to access, then this test passes; otherwise it fails. If the device is not network accessible, this test is not applicable.

3.3.5 If the device is network accessible and supports updating security-relevant configuration from the network, then try to make a change. If the device requires authentication prior to the change, then this test passes; otherwise it fails. If the device is not network accessible, this test is not applicable.

3.4 Patch Management and Software Upgrade

Purpose: Confirm that the device supports 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.

Evidence Attestation Guideline:

- For Test Case 3.4.1, 3.4.4, and 3.4.5, ATL can accept the attestation regarding authorized source, device specific security parameters, and security parameter generation. No attestation is allowed in the rest of test cases in Section 3.4.

Test Cases:

3.4.1 Obtain the documentation on the mechanism used to create any critical security parameters used for software patches or upgrades. If the mechanism generates per device security parameters, then this test passes; otherwise it fails.

NOTE: The device specific critical security parameters provide integrity and authentication or confidentiality.

3.4.2 Without any user login, test that the device will observe that a software patch or upgrade is available; inform the user about the software patch or upgrade, what vulnerability it remediates, and any disruption to the device as result of the installation; download the patch or upgrade; check that the patch or upgrade is unmodified from an OEM specified authorized source; and then at an appropriate time installs the software patch or upgrade. If the software patch or upgrade is installed, then this test passes; otherwise it fails. If the device does not support automatic installation of software patches or upgrades, then this test case is not applicable.

3.4.3 After login as a user with adequate privilege, locate the software patch or upgrade mechanism. If the software patch or upgrade mechanism is readily accessible, then this test passes; otherwise it fails. If the device does not support manual installation of software patches, then this test case is not applicable.

3.4.4 Try to install an unmodified software patch or upgrade from an OEM specified authorized source. If the device installs the software patch, then this test passes; otherwise it fails.

3.4.5 Try to install a software patch or upgrade from an OEM specified authorized source that has been modified. If the device refuses to install the software patch, then this test passes; otherwise it fails.

3.4.6 After successfully installing a software patch or upgrade, determine whether the installation processing has reset the device configuration. If the device configuration has not been reset, then this test passes; otherwise it fails.

NOTE: This test case ensures that installation of the patch or upgrade does not reset custom settings to their default values. The device is expected to retain its custom settings if a patch or upgrade is applied. New settings that exist only after the patch or upgrade is applied, may be initially set at default values.

3.4.7 Try to install a software patch or upgrade from an unauthorized source. If the device refuses to install the software patch or upgrade, then this test passes; otherwise it fails.

3.5 IoT Device Identity

Purpose: Confirm that the device can 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 test plan 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 3.5.

Test Cases:

3.5.1 Obtain the IoT Device Type and globally unique IoT Device Identity from the device packaging or labeling. If they are present, then this test passes; otherwise it fails.

3.5.2 Perform an action where the device response includes its logical IoT Device Type and globally unique IoT Device Identity. If they are present and they match the ones from the device packaging or labeling, then this test passes; otherwise it fails.

3.6 Encryption of Data at Rest

Purpose: To validate the device includes 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 3.6.

Test Cases:

3.6.1 If multiple encryption algorithms are supported, login as a user with sufficient privilege and then configure the device to use the encrypting file system or a stored data encryption mechanism using AES with a 128-bit key. If the device continues to operate normally, then this test passes; otherwise it fails.

3.7 Encryption of Data in Transit

Purpose: Confirm that the device supports 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 3.7.

Test Cases:

3.7.1 Perform actions that will generate network traffic, and view the network traffic monitor. If the traffic is protected with SSH, IPsec, TLS, or DTLS using 128-bit AES, then this test passes; otherwise it fails.

NOTE: If the device is set at a level beyond AES with a 128-bit key, set the device to 128-bit AES for compatibility purposes.

3.7.2 Perform actions (e.g., Authentication, Authorization, or an OTA (over the air) update) that will generate network traffic to the cloud services that the device depends upon, and view the network traffic monitor. If the traffic is protected with SSH, IPsec, TLS, or DTLS using 128-bit AES and no plaintext personal data is visible, then this test passes; otherwise it fails.

3.8 Use of Personal Data

Purpose: Confirm that personal data is only stored after obtaining consent, and then the personal data can be easily be removed from the device and associated services.

Procedure:

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

Evidence Attestation Guideline:

- Attestation is not allowed in Section 3.8.

Test Cases:

3.8.1 If it is possible to use personal data on the device, perform the actions to provide personal data. If consent must be provided before personal data is provided, then this test passes; otherwise it fails.

3.8.2 If it is possible to use personal data on the device, after previously providing consent, perform the actions to withdraw consent to use personal data. If the use of personal data by the device and associated services promptly ceases, then this test passes; otherwise it fails.

3.8.3 If it is possible to store personal data on the device, perform the actions to delete it. If the personal data is removed from the device, then this test passes; otherwise it fails.

3.8.4 If it is possible to store personal data on one or more services associated with the device, perform the actions to delete it. If the personal data is promptly removed from all of the services associated with the device, then this test passes; otherwise it fails.

3.9 Design in Features

Purpose: Confirm that the security design of the device avoids 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.

Evidence Attestation Guideline:

- Attestation is allowed for 3.9.1, 3.9.2, 3.9.3, 3.9.4, and 3.9.5.
- Attestation is not allowed for 3.9.6.

Test Cases:

3.9.1 Try to obtain a declaration from the OEM that the device software does not contain hard-coded critical security parameters. If a declaration is obtained, then this test passes; otherwise it fails.

3.9.2 Try to obtain a declaration from the OEM that any unused network and logical interfaces in the device have been disabled in the software. If a declaration is obtained, then this test passes; otherwise it fails.

3.9.3 Try to obtain a declaration from the OEM that any debug interfaces in the device have been disabled in the software. If a declaration is obtained, then this test passes; otherwise it fails.

3.9.4 Try to obtain a declaration from the OEM that the device was designed to minimize the disclosure of security-relevant information prior to authentication. If a declaration is obtained, then this test passes; otherwise it fails.

3.9.5 Try to obtain a declaration from the OEM that the device was designed to perform validity checking on data received over the network interface. If a declaration is obtained, then this test passes; otherwise it fails.

3.9.6 If the device has a user interface, perform an action that requires user input, but provide improperly formatted input. If the device rejects the improperly formatted input, then this test passes; otherwise it fails. If the device does not have a user interface, this test in not applicable.

3.10 Tamper Protection

Purpose: Confirm that a device with a hard-coded unique device identity provides 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.

Evidence Attestation Guideline:

- Attestation is allowed for 3.10.1.
- Attestation is not allowed for 3.10.2 or 3.10.3.

Test Cases:

If the device does not have a hard-coded unique device identity, then perform test case 3.10.1.

3.10.1 Try to obtain a declaration from the OEM that the device does not have a hard-coded unique device identity. If a declaration is obtained, then this test passes; otherwise it fails.

If the device has a hard-coded unique device identity, then perform test case 3.10.2 and test case 3.10.3.

3.10.2 Try to obtain design documentation from the OEM that describes the mechanisms used to protect against tampering of the hard-coded unique device identity. If the documentation is obtained, then this test passes; otherwise it fails.

NOTE: Tamper protection mechanisms offer protection against physical, electrical, and software means of altering the hard-coded unique device identity.

3.10.3 Inspect the devices for evidence of the documented tamper protection mechanisms described in the design documentation from the OEM. If on a basic level the mechanisms are implemented, then this test passes; otherwise it fails.

Section 4 Level 2 IoT Cybersecurity Tests (Enterprise Devices)

This section describes the second level of CTIA Cybersecurity Certification tests for IoT devices on a managed network. To achieve a Level 2 CTIA Cybersecurity Certification, the device must pass all of the tests in Section 3 and this section.

4.1 Terms of Service and Privacy Policies

Purpose: Confirm that the device recovers cleanly after power failure.

Procedure:

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

Evidence Attestation Guideline:

- Attestation is allowed for 4.1.1.

Test Cases:

4.1.1 Try to obtain the design documentation for the device. If the documentation addresses clean recovery after power failure, then this test passes; otherwise it fails.

4.2 Authentication

Confirms that device authentication implements 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

Purpose: If local password management is supported, confirm that the device can be integrated with an EMS. Confirm that the device honors the EMS mechanism to limit the rate of unsuccessful authentication attempts to greatly increase the time needed to guess a password. Confirm that the device supports 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.2.1.

Test Cases:

4.2.1.1 Try setting the password to a string that is prohibited by the EMS. If the device forces the user to change the password, to a string that is acceptable to the EMS, then this test passes; otherwise it fails.

4.2.1.2 Login, remain inactive for a time that exceeds the documented idle login time interval, and then try to perform some action. If the device requires reentry of the password to perform the action, then this test passes; otherwise it fails.

4.2.1.3 Try to login with the incorrect password several times in a row. If there is a rate-limiting or blocking mechanism that adheres to the EMS settings, then the test passes; otherwise it fails.

4.2.1.4 Try to login with a privileged role that has been disabled in the EMS. If the login to the device is unsuccessful, then this test passes; otherwise it fails.

4.2.2 One-Time Password

Purpose: Confirm that the device can 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.2.2.

Test Cases:

4.2.2.1 Login, remain inactive for a time that exceeds the EMS configured idle login time interval, and then try to perform some action. If the device requires a fresh OTP to perform the action, then this test passes; otherwise it fails.

4.2.3 Multi-Factor Authentication

Purpose: Confirm that the device can 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 [24][25] 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.2.3.

Test Cases:

4.2.3.1 Try to login with the most privileged role supported by the device with the correct password and the incorrect additional factor. If the role logs in to the device unsuccessfully, then this test passes; otherwise it fails.

4.2.3.2 Try to login with the most privileged role supported by the device with an incorrect password and the correct additional factor. If the role logs in to the device unsuccessfully, then this test passes; otherwise it fails.

4.2.3.3 Try to login with the most privileged roles supported by the device with the correct password and the correct additional factor. If the role logs in to the device successfully, then this test passes; otherwise it fails.

4.3 Access Controls

No additional test cases for the Enterprise Level.

4.4 Patch Management and Software Management

Purpose: Confirm that the device supports 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.

Evidence Attestation Guideline:

- For 4.4.1 and 4.4.2, ATL can accept the attestation regarding authorized source; authorized patch needs to be validated. No attestation is allowed in the rest of test cases in Section 4.4.

Test Cases:

4.4.1 Try to download an unmodified software patch or upgrade from a remote location that was produced by an OEM specified authorized source, and then try to install it. If the device installs the software patch or upgrade, then this test passes; otherwise it fails.

4.4.2 Try to download a modified software patch or upgrade from a remote location, and then try to install it. If the device refuses to install the software patch or upgrade, then this test passes; otherwise it fails.

4.4.3 Try to download a software patch or upgrade from a remote location that was produced by an unauthorized source, and then try to install it. If the device refuses to install the software patch or upgrade, then this test passes; otherwise it fails.

4.5 IoT Device Identity

No additional test cases for the Enterprise Level.

4.6 Encryption of Data at Rest

No additional test cases for the Enterprise Level.

4.7 Encryption of Data in Transit

Purpose: Confirm that the device supports 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.7.

Test Cases:

4.7.1 Perform an action that will generate network traffic to the EMS, and monitor the network traffic. If the traffic is protected with SSH, IPsec, TLS, or DTLS using 128-bit AES and no plaintext personal data is visible, then this test passes; otherwise it fails.

NOTE: If the device is set at a level beyond AES-128, set the device to AES-128 for compatibility purposes of testing the device with the EMS.

4.7.2 Perform an action that will transfer critical security parameters either to or from the EMS, and monitor the network traffic. If the transferred critical security parameters are protected with SSH, IPsec, TLS, or DTLS using 128-bit AES, then this test passes; otherwise it fails.

4.8 Use of Personal Data

No additional test cases for the Enterprise Level.

4.9 Design in Features

Purpose: Confirm that the design of the device includes 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 whitelisted 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.9.

Test Cases:

4.9.1 Try to obtain device design process documentation. If the design process includes the device going to a secure state when failure is detected, then this test passes; otherwise it fails.

4.9.2 Try to obtain device design process documentation. If the design process includes resiliency considerations regarding possible outages of data networks and power, then this test passes; otherwise it fails.

4.9.3 Try to obtain device design process documentation. If the design process includes resiliency considerations regarding connection to data networks in an orderly fashion and considers the capabilities of infrastructure, then this test passes; otherwise it fails.

NOTE: Following a power outage, all of the devices in a facility trying to reconnect at the same time can overwhelm the network infrastructure. Likewise, after a software update becomes available, all simultaneously downloading the update can overwhelm the update distribution service.

4.9.4 Disconnect or disable the data network while the device is operating, and then restore data network service. If the device remains locally functional when the data network is unavailable, and returns to full functionality after data network service is restored, then this test passes; otherwise it fails.

4.9.5 Try to obtain design documentation about the implementations of software services. If the device software design disables software services that are not used or required for the intended operation of the device, then this test passes; otherwise it fails.

NOTE: The OEM should not provision the device with any background processes, kernel extensions, commands, programs, or tools that are not required for the intended operation.

4.9.6 Try to obtain software development process documentation. If the OEM follows a secure software development process, then this test passes; otherwise it fails.

NOTE: The OEM software development process should remove "dead" or unused code.

4.9.7 Try to obtain software development process documentation. If the process ensures that the code includes only the functionality necessary for the device and associate services to operate, then this test passes; otherwise it fails.

4.9.8 Try to obtain software development process documentation. If, after taking account of both security and functionality, the process ensures that the code runs with least necessary privileges, then this test passes; otherwise it fails.

4.9.9 Try to obtain software development process documentation. If the process isolates critical functions from less critical functions, then this test passes; otherwise it fails.

NOTE: The OEM software development process should remove "dead" or unused code.

4.9.10 Try to obtain design documentation about the implementations of network and security functionalities, particularly in the field of cryptography. If the device employs reviewed or evaluated implementations, then this test passes; otherwise it fails.

4.9.11 Try to obtain the design documentation for the network security mechanisms of the device. If the device was designed to deny all inbound and outbound network communications, except for those that are essential for the device to operate properly, then this test passes; otherwise it fails.

4.9.12 Try to connect to the device from an external host using each TCP port, UDP port, and any other device-supported protocols. If the device confirms the port is open on any port or protocol that is not described in the design documentation obtained for test case 4.9.11, then this test fails; otherwise it passes.

4.9.13 Try to obtain design documentation about the device hardware. If the device hardware design does not expose unnecessary physical interfaces, then this test passes; otherwise it fails.

NOTE: A micro-USB port that is intended to provide power for the device can be physically configured to prevent command or debug operations.

4.9.14 Try to obtain design documentation about the device hardware. If the device hardware design includes a hardware-level access control mechanism for memory, then this test passes; otherwise it fails.

NOTE: A micro-USB port that is intended to provide power for the device can be physically configured to prevent command or debug operations.

4.9.15 If telemetry data is collected by the device or related services, try to obtain design documentation about handling of telemetry data. If the design includes examination of the telemetry data for anomalies, then this test passes; otherwise it fails.

4.10 Tamper Evidence

Purpose: Confirm that the device has 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.10.

Test Cases:

4.10.1 If the device supports and internal battery, disconnect it from any external power source, try to open the device case, close the case, and restore external power. If the device sends an alert to the EMS, then this test passes; otherwise it fails. If the device supports no internal battery, then this test case is not applicable.

4.10.2 If the device supports no internal battery, try to open the device case, close the case, while the device is connected to any external power source. If the device sends an alert to the EMS, then this test passes; otherwise it fails. If the device supports an internal battery, then this test case is not applicable.

4.11 Audit Log

Purpose: Confirm that the device supports the gathering and reporting of audit log events to an EMS using a severity thresholds and time frequency. Collection of personal data 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 personal data and is anonymized where possible.
- If telemetry data is collected, confirm that the device provides a means to support it during incident analysis.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.11.

Test Cases:

4.11.1 Perform actions that will create emergency, alert, critical, and error audit log entries. View the EMS audit log. If the expected audit log entries are present in the audit log, then this test passes; otherwise it fails.

4.11.2 Observe the network traffic between the device and the EMS. If the audit logs are transferred in the syslog compatible format, then this test passes; otherwise it fails.

4.11.3 Observe the network traffic between the device and the EMS. If SSH, IPsec, TLS, or DTLS is used to protect the transfer the audit log entries, then this test passes; otherwise it fails.

4.11.4 Adjust the threshold so that only emergency audit log entries are sent to the EMS, then perform actions that will create emergency, alert, critical, and error audit log entries. View the EMS audit log. If the only emergency audit log entries are present in the audit log, then this test passes; otherwise it fails.

4.11.5 Adjust the time interval for audit log entries that are sent to the EMS, then perform actions that will create emergency, alert, critical, and error audit log entries. If the audit logs are transferred at a time interval configured by the EMS, then this test passes; otherwise it fails.

4.11.6 Adjust the deadline to report emergency audit log entries to the EMS, and then perform some actions that will create emergency, alert, critical, and error audit log entries. Observe the network traffic between the device and the EMS. If the audit logs are transferred before the severity-based deadlines configured by the EMS, then this test passes; otherwise it fails.

4.11.7 Try to delete local audit log entries using a non-privileged role that is not authorized to perform these privileged actions. If these privileged actions can be performed by a role other than the ones described in the device documentation, then this test fails; otherwise it passes.

4.11.8 Login as the most privileged user and try to change an audit log entry. If the device allows an audit entry to be changed, then this test fails; otherwise it passes.

NOTE: The most privileged user might be able to delete entries from the audit log, but the user should not be able to change the content of an audit log entry.

4.11.9 If the audit logs entries contain any personal data, then examine them to confirm that it is minimal or anonymized. If the personal data is minimal or anonymous, then this test passes; otherwise, this test fails.

NOTE: Personal data should be anonymized if possible.

4.11.10 If telemetry data is collected, obtain documentation of the security incident analysis process. If the documentation describes how the process uses telemetry data, then this passes; otherwise, it fails.

4.12 Remote Deactivation

Purpose: Confirm that the unique device can be remotely deactivated by the EMS and that any personal data 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 test case is considered passing.
- Confirm a deactivated device successfully removes personal data.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.12.

Test Cases:

4.12.1 Try issuing the deactivation command at the EMS. Observe the authenticated command being sent from the EMS to the device. If the device deactivates, then this test passes; otherwise it fails.

4.12.2 Try issuing the deactivation command at the EMS, capture the command at the traffic monitor, modify the checksum, and send the modified command to the device. If the device deactivates, then this test fails; otherwise it passes.

4.12.3 Confirm that the device can be uniquely identified by the EMS. If the device can be identified uniquely by the EMS, then this test passes, otherwise it fails.

4.12.4 Try activating a device after it has been deactivated by the EMS. If the re-activated device contains no PII, then this test passes, otherwise it fails.

4.13 Secure Boot

Purpose: Confirm that the device protects the integrity of the boot process.

Procedure:

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

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.13.

Test Cases:

4.13.1 Obtain documentation of the secure boot process. If the documentation describes mechanism to verify the integrity of the device software, then this test passes; otherwise it fails.

4.13.2 Obtain documentation of the secure boot process. If the documentation describes a mechanism to notify the EMS when device software integrity checks are unsuccessful, then this test passes; otherwise it fails.

4.14 Threat Monitoring

Purpose: Confirm that the device supports 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.

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.14.

Test Cases:

4.14.1 Take actions that will trigger the device to provide inventory information to the EMS. View the EMS device inventory. If the device inventory data includes an entry for the device and the current device software version(s), then this test passes; otherwise it fails.

NOTE: These actions might include brute force password attempts, elevation of privileges, creation of new accounts, removal of accounts, system updates, CPU activity spikes, event log activity spikes, change of clock time setting, loss of communication, loss of GPS signal, network ports opened, network ports closed peripheral connection, and so on.

4.14.2 Take actions that will trigger audit log entries for the configured policies and rules. View the EMS audit log. If the expected audit log entries are present in the audit log, then this test passes; otherwise it fails.

NOTE: These actions might include brute force password attempts, elevation of privileges, creation of new accounts, removal of accounts, system updates, CPU activity spikes, event log activity spikes, change of clock time setting, loss of communication, loss of GPS signal, network ports opened, network ports closed peripheral connection, and so on.

4.14.3 Obtain documentation of the vulnerability scan process. If the documentation describes a mechanism to notify the EMS when a vulnerability scanner or a built-in vulnerability identification capability finds a potential concern, then this test passes; otherwise it fails.

4.14.4 Obtain documentation of the vulnerability discovery and correction process. If the documentation describes a means for the OEM to continually monitor for security vulnerabilities and rectify them when they are identified, then this test passes; otherwise it fails.

4.14.5 Obtain documentation of the incident investigation process. If the documentation describes a means support forensic analysis of the incident, then this test passes; otherwise it fails.

4.15 Secure Backup

Purpose: Confirm that the device has a mechanism to support data availability through secure backups.

Procedure:

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

Evidence Attestation Guideline:

- Attestation is not allowed in Section 4.15.

Test Cases:

4.15.1 After adjusting the device configuration, try to perform the secure backup process. After the secure backup process completes, reset the device to the factory configuration, and then restore the device from the secure backup. If the device configuration is properly restored, then this test passes; otherwise it fails.

Appendix A 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 that confirms that the device under test meets the requirement is provided.

A.1 NIST IR 8259A Requirements

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

A.2 NIST IR 8228 Requirements

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

A.3 ETSI EN 303 645 V2.1.1 Requirements

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:	NONE [1]
Provision 5.3-15:	NONE [1]
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 [2]
Provision 5.4-3 (M):	Section 3.10 [2]
Provision 5.4-4 (M):	Section 3.4 and Section 3.7

[1] Will not test or certify devices with no ability to update their software.

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

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 [3]

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

Appendix B Revision History

Date	Version	Description
August 2018	1.0	• Initial release
October 2018	1.0.1	• Section 2 Prerequisites: Removed • Changed “category” to “level”
June 2019	1.1	• 5G inclusion • Added one time password • Added text for substituting authentication test cases in Level 2 or 3 for Level 1 device certification
June 2020	1.2	• Added Evidence Attestation Guideline • Standardized the term, OEM • Separated the document into Cybersecurity Certification Program for IoT Devices and Test Plan. Updated Sections 3.2.1, 3.3, 3.4, 4.1, 4.7, 4.10, 4.11, and 5.7.
November 2020	1.2.1	• Changed organization name from CTIA to CTIA Certification • Changed CATL to ATL • Updated CTIA Certification URL
January 2021	1.2.2	• Updated Section 3.2.1 Local Password Management
September 2021	1.2.3	• Updated Sections 1.2.1, 1.4, 3.2.1, 3.5, 3.6, 4.5, 4.6 and 5.16

December 2021	2.0	• Reorganized from three levels to two levels of certifications. The following now have some aspect at Level 1:
		  ○ IoT Device Identity
		  ○ Encryption of Data at Rest
		  ○ Encryption of Data in Transit
		  ○ Tamper Protection
		• Aligned with NIST IR 8828 and 8259A as well as ETSI EN 303 v2.1.1. See Appendix A for a traceability matrix.
		• Merged Password Management with Authentication
		• Added Use of Personal Data section
		• Merged Patch Management and Software Updates into one section
		• Removed Digital Signature Generation and Validation section
		• Added Requirements Traceability as Appendix A
		• Moved Revision History to Appendix B