



OEM Questionnaire for CTIA Cybersecurity Certification Test Plan for IoT Devices

Version 2.2

October 2025

© 2018 - 2025 CTIA Certification. All Rights Reserved.

Any reproduction, modification, alteration, creation of a derivative work, or transmission of all or any part of this publication, in any form, by any means, whether electronic or mechanical, including photocopying, recording, or via any information storage and retrieval system, without the prior written permission of CTIA Certification, is unauthorized and strictly prohibited by federal copyright law. This publication is solely for use within the CTIA Certification Program. Any other use of this publication is strictly prohibited unless authorized by CTIA Certification or its assigns in writing.

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

1.202.785.0081

programs@ctiacertification.org

Table of Contents

Section 1	Testing Level Checklist.....	5
1.1	IoT Cybersecurity Testing Level Readiness Survey.....	5
Section 2	Testing Preparation Questions	6
Section 3	Level 1 Testing Questions	7
3.1	Terms of Service and Privacy Policies	7
3.2	Authentication	7
3.3	Access Control.....	7
3.4	Patch Management and Software Upgrade ¹	7
3.5	IoT Device Identity	8
3.6	Encryption of Data at Rest.....	8
3.7	Protection of Data in Transit	8
3.8	Use of Subscription Related Information	9
3.9	Design in Features.....	9
3.10	Tamper Protection and Evidence	9
3.11	Constrained IoT Devices	10
Section 4	Level 2 Testing Questions	11
4.1	Authentication	11
4.2	Design In Features	11
4.3	Tamper Protection and Evidence	12
4.4	Audit Log.....	12
4.5	Remote Deactivation	12
4.6	Secure Boot	12
4.7	Threat Monitoring.....	12
4.8	Secure Backup	13
Appendix A	Revision History	14

CTIA Certification Recommendations for Bluetooth and Zigbee Enabled Devices

For devices that include Bluetooth and/or Zigbee, CTIA Certification and its members suggest manufacturers:

- For Bluetooth, use core specification version 5.2 or later
 - When using Bluetooth Low Energy, we suggest bonding (persistent) rather than pairing (non-persistent) to reduce the cyber-attack footprint
- For Zigbee, configure devices in Secured Mode out-of-the-box
 - This supports MAC integrity and data encryption
 - We suggest Secure Level 7, 128-bit AES CCM with a 128-bit authentication tag

Section 1 Testing Level Checklist

1.1 IoT Cybersecurity Testing Level Readiness Survey

If your device has been built with the following Level 1 security features, please consider filling out the Questionnaire for Level 1 IoT Cybersecurity Certification Testing. If you have concerns about any of the noted features, discuss this with a CTIA Certification Authorized Test Lab (ATL).

Terms of Service and Privacy Policies	Authentication	Access Controls
Patch Management and Software Upgrade	IoT Device Identity	Encryption of Data at Rest
Protection of Data in Transit	Use of Subscription Related Information	Design in Features
Tamper Protection and Evidence	Constrained IoT Devices	

If devices have no ability to update software, please refer to section 3.11 Constrained IoT Devices.

If your device has been built with the following Level 2 security features, please consider filling out the Questionnaire for Level 2 IoT Cybersecurity Certification Testing. If you have concerns about any of the noted features, discuss this with an ATL.

Terms of Service & Privacy Policies	Authentication	Access Controls
Patch management & software upgrade	IoT device identity	Encryption of Data at Rest
Protection of Data in Transit	Use of Subscription Related Information	Design in Features
Tamper Protection and Evidence	Audit Log	Remote Deactivation
Secure Boot	Threat Monitoring	Secure Backup

Section 2 Testing Preparation Questions

A: Certification Level Note: To achieve a Level 2 CTIA Cybersecurity Certification, the device must pass all the applicable tests in Level 1 and all the applicable tests in Level 2. Note: IoT Network Certified for Smart Connected Infrastructure™ requires Level 2.	Click here to enter text.
B: OEM technical contact information	Name: Click here to enter text. Email: Click here to enter text. Cell Phone: Click here to enter text.
C: Name of Device and Model Number	Click here to enter text.
D: Number of devices submitted for testing (minimum 3 units)	Click here to enter text.
E: Is there any safety or handling concerns for this test sample (e.g. heat, electric shock risk, etc.)? Please list all objects that are included with the “device under testing” (DUT) including all necessary hardware accessories, software, web/cloud/mobile apps and servers.	Click here to enter text.
F: Please provide the device configuration guide.	Click here to enter text.
G: Does this device have a diagnostic/debug port for DUT?	Click here to enter text.
1. If so, please describe its testing capabilities:	Click here to enter text.
2. Please list cellular and (or) Wi-Fi chipset architecture.	Click here to enter text.
H: Does this device require a specialized equipment setup for testing purposes (like power supplies, installation locations, other data connections, sensors or interfaces, e.g. OBD2 port in car)?	Click here to enter text.
I: Are the DUT's provided by the OEM activated?	Yes <input type="checkbox"/> /No <input type="checkbox"/>
J: Is the device locked to any specific geographic location or networks?	Yes <input type="checkbox"/> /No <input type="checkbox"/>
1. If so please provide instructions how to remove these locks or restrictions for testing	Click here to enter text.
K: What primary LTE and 5G frequency bands are supported by the device? (LIST ALL SUPPORTED BANDS)	Click here to enter text.
L: Is the required software for the device available in all test locations (e.g., Android and/or IOS apps available only in US, not Europe or Asia)?	Click here to enter text.
M: Please provide four (4) software patches and four (4) software upgrades (WITH CHANGE NOTES) in the following configurations:	
1. Authorized source + Unmodified file	Click here to enter text.
2. Authorized source + Modified file	Click here to enter text.
3. Unauthorized source + Unmodified file	Click here to enter text.
4. Unauthorized source + Modified file	Click here to enter text.

Section 3 Level 1 Testing Questions

3.1 Terms of Service and Privacy Policies	
<p>A. Please provide the link to the Terms of Service for this device</p> <p>Note: The Terms of Service need to include the time period your company is willing to keep supporting this device clearly identified (the end of support for this device).</p>	Click here to enter text.
B. Please provide the link to the Privacy Policy for this device	Click here to enter text.
C. Please provide telemetry data collection	Click here to enter text.
D. Please provide the list of cloud services that the device requires access to for its normal operation	Click here to enter text.
E. Please provide the vulnerability disclosure policy	Click here to enter text.
F. Please provide the procedures to update the device software	Click here to enter text.
G. Please provide the installation and maintenance documentation for the device	Click here to enter text.
H. Please provide the documentation of the external sensing capabilities of the device	Click here to enter text.
The Privacy Policy should explicitly state all locations of data storage outside of the device itself. (e.g. cloud storage dependencies)	
I. Provide the link to any (public or private) cloud storage services this product uses	Click here to enter text.
3.2 Authentication	
A. Please list all default login accounts, passwords and each accounts role, for each test sample.	Click here to enter text.
B. What is the best way to interface the test sample for multiple login attempts and testing of passwords?	Click here to enter text.
C. How does the lab reset the password?	Click here to enter text.
D. Multiple password attempts will be made to set the password to an easily guessable password. Does this device have any automatic device resets or erasing mechanisms if too many password attempts are made during testing?	Click here to enter text.
E. How do you reset the device to factory state?	Click here to enter text.
F. Does the device support One-Time Passwords? If yes please provide documentation (e.g. size of OTP, how to generate OTP, etc.)	Click here to enter text.
3.3 Access Control	
A. Does the device support role based access control? If yes, provide documentation that describes how to perform a privileged action.	Click here to enter text.
3.4 Patch Management and Software Upgrade¹	
A. Does manufacturer include in the Terms of Service an attestation that the DUT by design cannot support software	Yes <input type="checkbox"/> /No <input type="checkbox"/>

updates because of limited capabilities and that such limitations are due to device's intended use?	
B. Does this device obtain and install patches?	Yes <input type="checkbox"/> /No <input type="checkbox"/>
C. Does this device obtain and install upgrades?	Yes <input type="checkbox"/> /No <input type="checkbox"/>
D. How do you install patches and/or upgrades from a local configurable source/file?	Click here to enter text.
E. Do the patches and/or upgrades need to be installed via a privileged account?	Click here to enter text.
F. Does this device validate patches and/or upgrades are from an authentic source?	Click here to enter text.
G. Does this device validate patches and/or upgrades are unmodified (e.g. hash, signature, etc.)?	Click here to enter text.
H. How do you physically recover a "bricked" device?	Click here to enter text.
I. Can you reset a device or flash this device to an earlier version of software?	Click here to enter text.
J. Approximately how long should the device take to apply a patch and/or upgrade once it has begun the updating process?	Click here to enter text.
K. How do you verify / validate the current patch and/or software level of the device?	Click here to enter text.
L. Does this device automatically check for available patches and/or upgrades? If Yes, describe the full process for checking, downloading and installing patches and/or upgrades automatically.	Yes <input type="checkbox"/> /No <input type="checkbox"/> Click here to enter text.
M. Please provide the documentation on the mechanism used to create any critical security parameters used for software patches or upgrades	Click here to enter text.

¹ If devices have no ability to update software, please refer to section 3.11 Constrained IoT Devices.

3.5 IoT Device Identity

A. Does this device have a globally unique ID on the device packaging or labeling?	Yes <input type="checkbox"/> /No <input type="checkbox"/>
B. Please describe how this device shares its globally unique ID via the audit log function.	Click here to enter text.
C. Please list globally unique IDs for test samples.	Click here to enter text.

3.6 Encryption of Data at Rest

A. Please provide the documentation on data encryption method(s) available for securing data on the device.	Click here to enter text.
B. Please provide the documentation for how to configure 128-bit AES encryption on the device.	Click here to enter text.

3.7 Protection of Data in Transit

A. Does your device support IPsec, SSH, TLS, or DTLS at the 128-bit AES level?	Yes <input type="checkbox"/> /No <input type="checkbox"/>
B. What actions does a user have to perform to send data over an encrypted end-to-end wireless connection? (i.e., turn on encrypted communications, etc.)	Click here to enter text.
C. Do you have an interface to test the encrypted network connection?	Click here to enter text.

D. (Optional & if EMS is used) What device actions would you suggest create encrypted traffic between the device and the enterprise management system?	Click here to enter text.
E. (Optional) If applicable, what device actions would you suggest to create encrypted traffic between the device and cloud services?	Click here to enter text.
F. If the device sends/stores data to the cloud/remote location, how can it be verified that data transmission is encrypted?	Click here to enter text.
3.8 Use of Subscription Related Information	
A. Does the device use and store subscription related information on the device or on associated services? If yes, please describe (or point to in the manual) actions that will trigger the collection of subscription related information and how to remove the subscription related information.	Yes <input type="checkbox"/> /No <input type="checkbox"/> Click here to enter text.
3.9 Design in Features	
A. Please provide a declaration that the device software does not contain hard-coded critical security parameters.	Click here to enter text.
B. Please provide a declaration that any unused network and logical interfaces in the device have been disabled in the software.	Click here to enter text.
C. Please provide a declaration that any debug interfaces in the device have been disabled in the software	Click here to enter text.
D. Please provide a declaration that the device was designed to minimize the disclosure of security-relevant information prior to authentication.	Click here to enter text.
E. Please provide a declaration that the device was designed to perform validity checking on data received over the network interface.	Click here to enter text.
3.10 Tamper Protection and Evidence	
A. If the device does not have a hard-coded unique device identity, please provide a declaration that the device does not have a hard-coded unique device identity	Click here to enter text.
B. If the device has a hard-coded unique device identity, please provide the design documentation from OEM that describes the mechanisms used to protect against tampering of the hard-coded unique device identity.	Click here to enter text.

3.11 Constrained IoT Devices

<p>A. Does device meet the requirements of a device that cannot support software update capabilities, due to limitations with respect to storage, processing, communications, user interaction, or overall intended use case and that the device can be isolated from the network in case of a vulnerability?</p>	<p>Yes <input type="checkbox"/>/No <input type="checkbox"/> Click here to enter text.</p>
<p>B. Does portion of the Terms of Service or Terms & Conditions document cover “software update” for the device and include manufacturer’s rationale for the absence of software updates, when the device will need to be replaced, the method of device replacement, and a defined support period for the hardware and software?</p>	<p>Yes <input type="checkbox"/>/No <input type="checkbox"/> Click here to enter text.</p>
<p>C. Does portion of the Terms of Service or Terms & Conditions document cover the procedure to isolate the device from the network when there is a vulnerability or at the end of support period?</p>	<p>Yes <input type="checkbox"/>/No <input type="checkbox"/> Click here to enter text.</p>
<p>D. Please list the methods by which remote deactivation can be performed on this device.</p>	<p>Click here to enter text.</p>

Section 4 Level 2 Testing Questions

A. Is your device supported by a proprietary enterprise management system? If yes, please describe.	Yes <input type="checkbox"/> /No <input type="checkbox"/> Click here to enter text.
B. What enterprise account management systems is your device compatible with?	Click here to enter text.

4.1 Authentication

A. What is the inactivity timeout period for the login of this device?	Click here to enter text.
B. What is the rate limiting or blocking mechanism / time period for the sample device?	Click here to enter text.
C. Does the device support MFA? If yes, please provide instructions to configure the device accordingly.	Yes <input type="checkbox"/> /No <input type="checkbox"/> Click here to enter text.

4.2 Design In Features

A. Please provide the device design process documentation. <i>(Note: please refer to section 4.9 including 4.9.1 – 3 of the test plan to ensure the proper design elements are included in the documentation provided).</i>	Click here to enter text.
B. Please provide the design documentation about the implementations of software services.	Click here to enter text.
C. Please provide the software development process documentation.	Click here to enter text.
D. Please provide the design documentation about the implementations of network and security functionalities, particularly in the field of cryptography.	Click here to enter text.
E. Please provide the design documentation for the network security mechanisms of the device including indication of the ports that are essential for device's proper operation (see Test plan section 4.9.12 for added details)	Click here to enter text.
F. Please provide the design documentation about the device hardware. <i>(Note: please refer to section 4.9 including 4.9.13 of the test plan to ensure the proper design elements are included in the documentation provided).</i>	Click here to enter text.
G. If telemetry data is collected by the device or related services, please provide the design documentation about handling of telemetry data.	Click here to enter text.
H. Please provide the design documentation that specifically addresses information dealing with clean recovery after power failure.	Click here to enter text.

4.3 Tamper Protection and Evidence	
A. What type of audit log event is recorded when the device detects the case has been opened?	Click here to enter text.
B. Please provide an example of an audit log event when the case has been opened.	Click here to enter text.
4.4 Audit Log	
A. Is your audit log system compatible with Syslog format?	Click here to enter text.
B. What user roles are allowed to delete audit logs?	Click here to enter text.
C. What user roles are allowed to view audit logs?	Click here to enter text.
D. Please list an action that would create an audit log entry:	Emergency : Click here to enter text. Critical : Click here to enter text. Alert : Click here to enter text. Error : Click here to enter text.
E. Is there a log entry that would clearly indicate the device is now communicating over an encrypted tunnel using TLS or DTLS at the 128-bit AES encryption level?	Click here to enter text.
F. Can audit log sizes or date ranges be adjusted on this device?	Click here to enter text.
G. If telemetry data is collected, please provide the documentation of the security incident analysis process.	Click here to enter text.
H. Does device support the gathering and reporting of audit log events that contain subscription related information to an EMS?	Yes <input type="checkbox"/> /No <input type="checkbox"/>
4.5 Remote Deactivation	
A. Please list the methods by which remote deactivation can be performed on this device.	Click here to enter text.
4.6 Secure Boot	
A. Please provide documentation of the secure boot process that describes mechanism to verify the integrity of the device software.	Click here to enter text.
B. Please provide documentation of the secure boot process that describes a mechanism to notify the EMS when device software integrity checks are unsuccessful.	Click here to enter text.
4.7 Threat Monitoring	
A. Please provide capabilities of this device to detect anomalous or malicious activity.	Click here to enter text.
B. Please provide actions that will cause the IoT device to detect an anomalous and malicious activity and record that event in the audit log as such an event.	Click here to enter text.

C. Please provide the documentation of the vulnerability scan process.	Click here to enter text.
D. Please provide the documentation of the vulnerability discovery and correction process.	Click here to enter text.
E. Please provide the documentation of the incident investigation process.	Click here to enter text.
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.	
4.8 Secure Backup	
A. Does device have a mechanism to support data availability through secure backups.	Yes <input type="checkbox"/> /No <input type="checkbox"/>
B. Please list the methods by which secure backup process can be performed on this device.	Click here to enter text.

Appendix A Revision History

Date	Version	Description
June 2018	1.0	<ul style="list-style-type: none"> Initial release
May 2019	1.1	<ul style="list-style-type: none"> Revised for conciseness, added 4 question survey at the front to determine applicability
July 2020	1.2	<ul style="list-style-type: none"> Included the informative recommendations on Bluetooth and Zigbee enabled devices
November 2020	1.2.1	<ul style="list-style-type: none"> Changed organization name from CTIA to CTIA Certification and updated contact email Changed CATL to ATL
July 2023	2.0	<ul style="list-style-type: none"> Updated the Questionnaire based on Test Plan Version 2.0 and Version 2.1 Changed personal data to subscription related information Renamed sections (e.g., Tamper Protection and Evidence)
August 2023	2.1.1	<ul style="list-style-type: none"> Updated version number to align with CTIA Certification Cybersecurity Test Plan for IoT Devices Version 2.1.X
December 2023	2.1.2	<ul style="list-style-type: none"> Updated to align with CTIA Certification Cybersecurity Test Plan for IoT Devices Version 2.1.2
April 2025	2.1.3	<ul style="list-style-type: none"> Updated Section 2 row A.
October 2025	2.2	<ul style="list-style-type: none"> Changed "Encryption of Data in Transit" headers to "Protection of Data in Transit"