CTIA Certification™

IoT Cybersecurity Certification Program Management Document

Version 1.2
April 2020

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

1.202.785.0081

programs@ctiacertification.org

testplans.ctia.org

Table of Contents

1 Overview

1.1 Purpose

The purpose of the CTIA IoT Cybersecurity Certification Program (“Program”) is to evaluate the cybersecurity components of an Internet of Things (IoT) device per the tests defined in the CTIA Cybersecurity Certification Test Plan for IoT Devices (“Test Plan”).

1.2 Document Scope

This Program Management Document (PMD) defines the requirements and processes of the Program. For device OEMs, this document describes the requirements for obtaining and maintaining CTIA Certification and the process to apply for certification. For test laboratories, this document describes the procedures to evaluate OEMs’ devices.

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

1.3 Definitions

CATL: CTIA Authorized Test Lab

ECO: Engineering Change Order. An ECO request is a request to certify a hardware or software update of a previously submitted device.

IoT: Internet of Things

OEM: Original Equipment Manufacturer

PoC: Point of Contact

PMD: Program Management Document

2 Roles and Responsibilities

This section describes the roles and responsibilities of the parties involved with the Program and mentioned throughout this document.

2.1 CTIA

As owner of the CTIA Certification Program, CTIA defines the requirements for CTIA Certification, administers the overall program and awards CTIA Certification to the OEM.

2.2 CTIA Authorized Test Laboratories (CATLs)

CATLs shall evaluate devices using criteria set forth in the Test Plan and procedures described in Section 3 of this document. CATLs shall at all times maintain compliance with the *Policies and Procedures for CTIA Authorized Testing Laboratories* document found at https://www.ctia.org/about-ctia/certification-resources.

Each CATL shall appoint a Primary Point of Contact (PoC) to interface with CTIA. The PoC is responsible for approving who within their company shall be given access to the certification database and for informing CTIA when individual user access should be disabled (for example, when a user leaves the company).

2.3 IoT Device OEM

OEMs submitting devices for certification testing shall follow the procedures described in Section 3 of this document. Testing may be conducted at any of the available CATLs per the OEM's choice.

Each OEM shall appoint a Primary Point of Contact (PoC) to interface with CTIA. The PoC is responsible for approving who within their company shall be given access to the certification database and for informing CTIA when individual user access should be disabled (for example, when a user leaves the company).

3 Program Procedures

3.1 Test Facilities

Multiple laboratories are authorized to perform certification testing for the CTIA Certification Program. Labs are authorized per CTIA Certification Test Plan.

A current listing of CATLs can be found within the CTIA certification database and on the CTIA web site at https://www.ctia.org/about-ctia/certification-resources.

OEMs may utilize CATLs for pre-certification testing as per Section 3.2 of this document.

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

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

CATLs shall refer to the *Policies and Procedures for CTIA Authorized Testing Laboratories* document per Section 2.2 and the *CATL License and Service Agreement* for the terms and conditions under which the Test Plan may be used.

The Test Plan must be run in its entirety.

3.3 OEM Submission

OEMs shall submit certification requests via CTIA's certification database at **https://ctiacert.org/.** User login accounts may be requested by selecting "I need a user name and password" on the login page.

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

- Initial Certification Request
- ECO Certification Request

The OEM shall enter the requested information about the device and select a CATL.

The OEM shall select the main PoC and billing PoC for the request.

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

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

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

The OEM shall submit the OEM Questionnaire (see **APPENDIX A: OEM Questionnaire**) to the CATL.

After the request is submitted and accepted by CATL for testing, the certification database will generate an invoice for the CTIA certification fee (see **APPENDIX B: Certification Fees**) which will be available in the Payment Info tab.

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

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

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

3.4 Device Evaluation

The CATL shall test the devices according to the current version of the Test Plan at the time of submission. Results shall be recorded in the test report template provided by CTIA (see **APPENDIX C: Test Report Template**).

Upon completion of the evaluation, the CATL shall log into CTIA's certification database and:

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

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

3.5 Certification

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

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

The certification will apply to the specific HW/ SW version of the device evaluated by the CATL. Certification of additional HW/SW versions may be accomplished as per Section 3.6 of this document.

3.6 Certification of HW/SW Updates to a Model

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

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

3.7 Certification of Re-Labeled Devices

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

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

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

APPENDIX A: OEM Questionnaire

Version 1.1 OEM Questionnaire for CT

The embedded document can be found in the Attachments Section in this PDF file.

APPENDIX B: Certification Fees

The fee for CTIA Cybersecurity Certification is:

Request Type	Fee (U.S. $)
Level 1 Initial Request	500
Level 2 Initial Request	750
Level 3 Initial Request	1,000
ECO Request	500

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

APPENDIX C: Test Report Template

Test Report Template is available on CTIA Certification Working Group site, cpwg.ctia.org.

APPENDIX D: Change History

Revision	Date	Description of Changes
1.0	October 2018	• Initial release
1.1	May 2019	• Updated Appendix A, OEM Questionnaire from Version 1.0 to 1.1.
1.2	April 2020	• Changed the term Vendor to OEM • Added additional text regarding operators requirements in Section 1.2 • Removed Appendix C: Test Report Template