CONNECTIVITY STANDARDS ALLIANCE
CERTIFICATION POLICY

Sept 22nd, 2022
CSA Document Numbers
Published as: 07-4842-16
Editor’s Copy: 15-0288 r16
Copyright and Disclaimer

Copyright © Connectivity Standards Alliance, Inc. (2022). All rights Reserved. The information within this document is the property of Connectivity Standards Alliance and its use and disclosure are restricted.

The document is subject to change at the discretion of Connectivity Standards Alliance.

The above notice and this paragraph must be included on all copies of this document that are made.
# Table of Contents

## Introduction
- Scope and Purpose 7
- Structure of this Document 7
- References 7
- Abbreviations and Terminology 8

## CSA Certified Program
- Description 10
- Testing Versus Certification 10
- Connectivity Standards Alliance Responsibilities 10
- Alliance Director of Certifications 10
- Expert Review Panel 10
- Appeals 11
  - Appeals Process 11
  - Appeals Committee 12
- Certification Types 12
  - Compliant Platform 12
  - Certified Product 12
  - Certified Software Component 12
  - Requirements for Certification 12
  - Membership 12
  - Conformance to Standard 13
  - Documentation of Product 13
- Process for Certification 13
- Certificates 14
- Logo Usage 14
- Length of Certification 14
- Revocation of Certification 14
- Testing and Certification Fees 15
  - Manufacturer-specific identification and information usage 15

## Testing 17
Underlying Software Component Testing 44
Certified Underlying Software Component Reuse 44
Underlying Software Component Recertification 46
Policy for User Interface Component (UIC) Certification Program 46
UIC Type 2, making use of only Simple Interfaces of a Certified Underlying Software Component 47
UIC Type 2, making use of Complex Interfaces of a Certified Underlying Software Component 47
UIC recertification: usage of Complex Interface of Certified Underlying Software Component 48
Change of Certified Underlying Software Component 48
Type 1 UIC (not making use of Certified Underlying Software Component) 48
Guidelines for Software Component Certification Program 48

Certification Programs 49
Compliant Platform: Zigbee PRO Stack 49
Zigbee PRO Compliant Platform Certification Program 49
Zigbee Stack Software Component Certification 50
Certified Product based on Zigbee PRO Compliant Platform 50
Legacy Profile Product Certification Program 50
Zigbee 3.0 Product Certification Program 51
Certified Product: Green Power Device 52
Green Power Device Product Certification Program 52
RF4CE 52
RF4CE Compliant Platform Program 52
Remote Control Product Certification Program 52

APPENDIX A: Testing Exemption Request Form 61

APPENDIX B: MATTER CERTIFICATION ATTESTATION QUESTIONS 66
1 INTRODUCTION

This document defines policies related to CSA Certified, the certification and testing program of the Connectivity Standards Alliance. It describes:

- The CSA Certified Program
- Certification Types:
  - Compliant Platform
  - Certified Product
  - Certified Software Component
- Certification Programs, including Zigbee PRO stack, Zigbee 3.0 and, Green Power Device, and Matter
- Authorized Test Laboratories
- Golden Units and processes for selection and revision
- Test Harnesses
- Certification paths, including:
  - Testing
  - Certification by Similarity and guidelines for retesting
  - Certification Transfer Program
  - Product Family Certification and guidelines for retesting

1.1 Scope and Purpose

This document defines the Certification Programs supported by the Connectivity Standards Alliance. This includes the process and rules for the entire life cycle of a program including Specification validation, testing, grace period, etc. It is not the intent of this document to define the organizational entities responsible for managing any part of this process, except those required to be visible outside the Connectivity Standards Alliance, such as the authority to certify and resolve conflict.

1.2 Structure of this Document

This document first defines processes and rules that are common to many programs. Even in the common process there are levels and dependencies. After the common Sections, this document then defines each active program (legacy and current), in terms of requirements and additions to the common process.

1.3 References

This document refers to several other documents related to details of the certification policy.

[R2] CSA document 08-0123: Test Event Rules of Engagement
[R3] CSA document 05-3739: CSA Certified Logo and Trademark Policy
[R4] CSA document 08-5185: Qualification and Validation of Test Service Providers
[R5] CSA document 11-5456: Master Cluster List
[R8] CSA document 20-27538: Zigbee Direct Test Specification
[R10] CSA document 21-27760: Zigbee Stack Functionality Test Specification (for ZVD)
1.4 Abbreviations and Terminology

Table 1 – Abbreviations and Terminology

<table>
<thead>
<tr>
<th>ATL</th>
<th>Authorized Test Laboratory</th>
</tr>
</thead>
<tbody>
<tr>
<td>CbS</td>
<td>Certification by Similarity</td>
</tr>
<tr>
<td>Certification Program</td>
<td>A well-defined process, that approves interpretation, validates conformance and interoperability to a set of Specifications, and when successfully completed, allows the certification authority to issue a certificate</td>
</tr>
<tr>
<td>Certified Product</td>
<td>A Product that has been certified under the Product Certification Program</td>
</tr>
<tr>
<td>Certified Software Component</td>
<td>A Software Component (a UIC or Underlying Software Component), that has been certified under the Software Component Certification Program</td>
</tr>
<tr>
<td>Compliant Platform</td>
<td>A Platform that has been certified under the Compliant Platform Certification Program</td>
</tr>
<tr>
<td>Compliant Platform Certification Program</td>
<td>A Certification Program that validates a Platform for purposes of certification</td>
</tr>
<tr>
<td>CSA</td>
<td>Connectivity Standards Alliance</td>
</tr>
<tr>
<td>CSA Product</td>
<td>Product</td>
</tr>
<tr>
<td>CSA Standard</td>
<td>Standard</td>
</tr>
<tr>
<td>CTP</td>
<td>Certification Transfer Program</td>
</tr>
<tr>
<td>DUT</td>
<td>Device Under Test</td>
</tr>
<tr>
<td>ERP</td>
<td>Expert Review Panel</td>
</tr>
<tr>
<td>Golden Unit</td>
<td>A Compliant Platform or Certified Product chosen to be used as part of a Program to test interoperability.</td>
</tr>
<tr>
<td>GU</td>
<td>Golden Unit</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>ODM</td>
<td>Original Design Manufacturer</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>PFC</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>PICS</td>
<td>Protocol Implementation Conformity Statement (list of supported functions)</td>
</tr>
<tr>
<td>Platform</td>
<td>An implementation of a Stack</td>
</tr>
<tr>
<td>Product</td>
<td>An implementation of a Standard</td>
</tr>
<tr>
<td>Product Certification Program</td>
<td>A Certification Program validating a Product for purposes of certification</td>
</tr>
<tr>
<td><strong>Program</strong></td>
<td>See Certification Program</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>RF</strong></td>
<td>Radio Frequency</td>
</tr>
<tr>
<td><strong>SKU</strong></td>
<td>Stock Keeping Unit (unique model identifier)</td>
</tr>
<tr>
<td><strong>SOE</strong></td>
<td>Supported Operating Environment</td>
</tr>
<tr>
<td><strong>Software Component</strong></td>
<td>umbrella term referring to all software components irrespective of their kind, i.e. both User Interface Component (UIC) and Underlying Software Component.</td>
</tr>
<tr>
<td><strong>Stack</strong></td>
<td>An approved set of base Specifications upon which a Standard is built (e.g. Zigbee PRO, RF4CE, etc.).</td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td>An approved set (or vertical Stack) of Specifications, built upon a Stack, defining interoperable behavior, on which interoperable applications can be built (e.g. ZSE, Zigbee 3.0, ZRC, etc.).</td>
</tr>
<tr>
<td><strong>Test Event</strong></td>
<td>Organized event to test and validate Specification implementations</td>
</tr>
<tr>
<td><strong>Test Harness</strong></td>
<td>Test harness that is developed for use in executing compliance testing and approved by Connectivity Standards Alliance</td>
</tr>
<tr>
<td><strong>UIC</strong></td>
<td>User Interface Component. The highest layer software component</td>
</tr>
<tr>
<td><strong>Underlying Software Component</strong></td>
<td>Software Component other than the UIC. Software component used by UIC or another Software Component</td>
</tr>
<tr>
<td><strong>ZCP</strong></td>
<td>Zigbee Compliant Platform</td>
</tr>
<tr>
<td><strong>ZDD</strong></td>
<td>Zigbee Direct Device</td>
</tr>
</tbody>
</table>

●
2 CSA CERTIFIED PROGRAM

This Section describes the general process and rules that are common for all Certification Programs.

2.1 Description

CSA Certified is the overall program which enables certification of Products and Compliant Platforms that conform to Connectivity Standards Alliance Standards. The program defines various types of certifications and related policies including requirements for certification and testing programs and leverages the expertise of hundreds of engineers and business people to ensure only quality Products earn CSA Certified Product status.

CSA Certified generally follows international Standards for the definition and operation of a Certification Program. In particular, CSA Certified is designed as a Type 1b Certification Program as defined in ISO/IEC Guide 67: 2004. Type 1b systems consist of several types of activities:

- Determination of Product characteristics: This is achieved through testing of submitted samples performed by independent authorized test laboratories,
- Evaluation: This is achieved by formally evaluating the results of testing,
- Decision: This is the stage that controls granting, maintaining and extending suspending or withdrawing certification, and
- Licensing: Licensing refers to granting, suspending, or withdrawing the rights to use certificates or marks such as logos.

2.2 Testing Versus Certification

The CSA Certified program maintains a strict distinction between testing and certification. Testing is the process verifying conformance to CSA Standards. Certification is granting official recognition that a Product conforms to a CSA Standard and that a Product manufacturer conforms to all the relevant policies of the CSA Certified program.

Only the Connectivity Standards Alliance may grant certification.

2.3 Connectivity Standards Alliance Responsibilities

The Test and Certification Oversight Committee (TCOC) of the Alliance Board of Directors shall be responsible for development of policies related to certification (including this document) and working with the various CSA working groups on certification related issues. The TCOC is made up of volunteers from members of the Alliance Board of Directors.

2.4 Alliance Director of Certifications

The Alliance Director of Certifications shall be named by Alliance management and will be responsible for a variety of functions related to administering the CSA certified program including processing of certification applications, issuing of certificates, consulting with the TCOC on certification and testing policy matters, and interpreting certification policies on a day-to-day basis.

In accordance with ISO/IEC Guide 65, the Alliance Director of Certifications has decision making authority in regard to granting certifications and other related tasks.

2.5 Expert Review Panel

The Expert Review Panel is a team of volunteers from member companies nominated by working groups for a particular expertise area and approved by the TCOC. The Panel provides expert technical advice to the CSA Certified program. The function of the Panel is defined in document 08-5185 “Qualification and Validation of Test Service Providers”. An up-to-date list of the current Panel members is maintained in the CSA document repository, within the Certification Resources folder underneath the All Members main folder.
Aside from their role in validation of test laboratories, the Expert Review Panel may be called on from time to 
time to provide other expert advice in regard to other matters such as review of test plans, review of 
interoperability concerns discovered in the field or to assist the Alliance Director of Certifications in resolution 
of disputes.

2.6 Appeals

The Connectivity Standards Alliance has a procedure for the resolution of issues regarding the granting of 
certification.

Certification applicants may appeal a decision regarding certification if they believe this certification policy was 
applied in error. The basis of the appeal shall be (1) a specific concern about the misapplication of the policy, or 
(2) an error on the part of an authorized test laboratory or the Alliance Director of Certifications.

2.6.1 Appeals Process

The process for appeals shall be:

- Applicant shall send an appeal request to certification@csa-iot.org. The request shall 
document the issue, the specific basis of the appeal and the corrective action requested.

- Acknowledgement of receipt of the appeal by either the Alliance Director of Certifications or 
the President and Chief Executive Officer of Connectivity Standards Alliance shall be 
provided.

- The Alliance Director of Certifications and the President and Chief Executive Officer of 
Connectivity Standards Alliance shall consider the appeal.

- A preliminary decision shall be made either to have Connectivity Standards Alliance take 
corrective action or to reject the appeal.

- If corrective action by Connectivity Standards Alliance is to be taken, the Alliance Director of 
Certifications or the President and Chief Executive Officer of Connectivity Standards Alliance 
shall implement the corrective action.

- If the appeal is proposed for rejection, the appeal shall be forwarded to the Appeals 
Committee for consideration.

- A report on the status of the appeal shall be given to the applicant.

- The Appeals Committee shall consider the appeal.

- A decision shall be made either to have Connectivity Standards Alliance take corrective action 
or to reject the appeal.

- If corrective action by Connectivity Standards Alliance is to be taken, the Alliance Director of 
Certifications or the President and Chief Executive Officer of the Connectivity Standards 
Alliance shall implement the corrective action.

- If the appeal is rejected, the specific basis for rejection shall be documented.

- A report on the final disposition of the appeal shall be given to the applicant by either the 
Alliance Director of Certifications or the President and Chief Executive Officer of 
Connectivity Standards Alliance.

All parties shall treat any information related to an appeal as confidential information during the process.
2.6.2 Appeals Committee

The Connectivity Standards Alliance shall have a committee to address appeals. The Appeals Committee shall consist of the Chief Executive Officer of the Alliance, the chairperson of the TCOC and three representatives from authorized test laboratories chosen at the discretion of the Chief Executive Officer. The Chief Executive Officer of the Alliance shall act as chairperson of the Appeals Committee.

To ensure the impartiality of the appeals process, any member of the Committee who may have any conflict of interest with the party making the appeal shall disclose the conflict. The member will not be allowed to vote or participate in Committee activities regarding the appeal. Conflicts of interest are defined as, at a minimum, a financial or competitive relationship with the appealing party. The Committee members themselves shall decide if other issues are conflicts of interest.

2.7 Certification Types

The Connectivity Standards Alliance offers three types of Standards compliance – Compliant Platform, Certified Product and Certified Software Component.

2.7.1 Compliant Platform

The Compliant Platform program defines a rigorous evaluation and certification process for a Platform before it can be certified as a Compliant Platform and engineered into a Product. Each Platform is comprised of a radio and a microprocessor with storage running CSA firmware. The Platform is tested for compliance to a set of CSA Specifications (see Section 11 Certification Programs).

This program ensures the supply chain has a solid foundation for Products destined for personal or commercial use. Successfully completing this testing allows the member to have its Platform recognized by the Alliance as a Compliant Platform.

2.7.2 Certified Product

A Certified Product program defines the testing requirements and a process to validate a Product’s conformance to a Standard (see Section 11 Certification Programs). The Product must be fully compliant to the Standard(s) and successfully execute all mandatory and implemented optional commands. Successful certification allows the Product to be recognized by the Alliance as a Certified Product and use a Certified Product logo. A Compliant Platform is a fundamental building block of a Certified Product. With few exceptions (defined in this document), the use of a certified Compliant Platform is a mandatory prerequisite to assessment as a Certified Product.

2.7.3 Certified Software Component

The CSA Certified Software Components program defines the testing requirements and a process to validate a Software Component implemented in software on feature rich Supported Operating Environments (SOE). The certification policy for Software Components is covered in Section 10 Certified Software Component.

2.7.4 Requirements for Certification

Certification may be awarded based on a Product’s successful completion of the process defined in a Certified program (see Section 11 Certification Programs).

2.7.5 Membership

To submit a Product, Platform or a Software Component for certification or compliance testing and to be granted certification, a company must be a member in good standing of the Connectivity Standards Alliance. The Alliance has several different types of membership which are documented on its web site: http://www.csa-iot.org.
2.7.6 Conformance to Standard

Conformance is verified by testing performed by an authorized test laboratory and demonstrated by a test report documenting successful completion of the entire test plan including all test cases for mandatory features and test cases for any implemented optional features as identified by the PICS. The authorized test laboratories shall report any information relevant regarding the Product’s conformance to a Standard in the test report.

2.7.7 Documentation of Product

The Connectivity Standards Alliance shall require information sufficient to identify a Product before granting certification including:

1) Declaration of Conformity (DoC or DOC):
   a) Version numbers of Product hardware, software, and firmware
   b) For a Product, a Stock Keeping Unit (SKU) and/or Universal Product Code
   c) For a Product, the Compliant Platform upon which the Product is based
   d) Signature of a representative of the Product, Platform or Software Component manufacturer
   e) Signature of a representative of the authorized test laboratory performing Product, Platform or Software Component testing
   f) Where required, answering self attestation questions

2) Protocol Implementation Conformance Statements (PICS):
   a) including mandatory and optional features supported by the Product, Platform or Software Component

3) Non-declaratory information that is also requested:
   a) Product, Platform or Software Component description
   b) Product photo

2.8 Process for Certification

The certification process begins after the manufacturer completes development of the Product, Platform or Software Component to be certified.

Testing: Testing for conformance to a Standard is performed by Alliance authorized test laboratories using test plans developed by the Alliance. The Alliance maintains a list of authorized test laboratories on its web site at http://www.csa-iot.org. Each authorized test laboratory has a process for Product submission and will provide details on how to submit a Product, Platform or a Software Component. All authorized test laboratories will require submission of a Declaration of Conformity and a Protocol Implementation Conformance Statement for the submitted Product, Platform or Software Component. To successfully pass test plans, a Product, Platform or Software Component must pass all mandatory test cases and any optional test cases that are applicable to the Product, Platform or Software Component based on the functionality it supports. In addition to the explicit functionality being checked by the test cases, the submitted Product, Platform or Software Component must not exhibit any behavior which is contrary to the behavior detailed in the underlying Specifications, to be considered to have passed a test plan.

Reporting: Authorized test laboratories will submit test results directly to the Alliance.

Application: The Alliance grants certifications based on an application. The application is web based and is available in the Member’s Area of http://www.csa-iot.org and consists of the information described in Section 2.7.7 above.

Processing: The Alliance staff processes applications under the direction of the Director of Certifications. Applications are processed for completeness to all requirements as described in Alliance policies including:

- Submission of all required documentation
- Membership in the Alliance
- Completion of testing
- Payment of applicable fees

**Certification:** Only Connectivity Standards Alliance may grant certification and a Product, a Platform or a Software Component is only certified when the Alliance issues certification. The Alliance will issue certificates as evidence of successful certification.

**Issuing of Manufacturer Code / Vendor ID (VID):** Only CSA may issue a Manufacturer Code/Vendor ID (VID). See also Section 2.14 Manufacturer-specific identification and information usage.

While all new and updated Platforms, Products, and Software Components SHALL be certified by the Alliance, this does not mean that they SHALL all require testing. Two additional routes available for achieving certification are Certification by Similarity and the Certification Transfer Program. Details on both of these routes are covered in later sections of this document.

An authorized test laboratory may occasionally submit non-compliant results to the Alliance Director of Certifications for him/her to make a decision on the issue of certification.

### 2.9 Certificates

The Connectivity Standards Alliance shall provide a certificate which will serve as evidence that a particular Product, Platform or Software Component is CSA Certified.

### 2.10 Logo Usage

The Connectivity Standards Alliance owns the trademarks and logos that may be used to identify various Products, Platforms or Software Components that are CSA Certified.

Use of any Connectivity Standards Alliance trademarks and logos, including for labelling Products, Platforms or Software Components as certified by Connectivity Standards Alliance is limited to Alliance members and is subject to the Connectivity Standards Alliance Trademark and Logo Usage Guidelines and Terms available at [www.csa-iot.org](http://www.csa-iot.org).

### 2.11 Length of Certification

Once a Product, Platform or Software Component is certified, it remains certified for the lifetime of the Product/Platform/Software Component unless Connectivity Standards Alliance revokes the certification or the Product/Platform/Software Component is modified.

Modifications include any changes to the Product/Platform/Software Component. However, not all modifications will require retesting of a Product/Platform/Software Component in order to be certified. The Alliance maintains guidelines about modifications that require retesting and will determine whether retesting is required for any particular modification.

For complete information, refer to Section 6 Certification by Similarity and Section 10 Certified Software Component.

### 2.12 Revocation of Certification

The Connectivity Standards Alliance may also revoke certification or participation in the certification process if one or more of the following occurs:

- Modifications which impact the test results of the Product or Software Component or instances where an SOE qualification is revoked for any reason
- A Product is found to be hazardous as defined in ISO Guide 17030-2021.
- The manufacturer has made any material misstatement of fact, or omission of fact, to the Alliance or its authorized test laboratories.
● The manufacturer fails to follow all Alliance certification requirements.

● The manufacturer fails to use Connectivity Standards Alliance trademarks and logos in accordance with the Connectivity Standards Alliance Trademark and Logo Usage Guidelines and Terms available at www.csa-iot.org. Examples of failure to use in accordance with the Connectivity Standards Alliance Trademark and Logo Usage Guidelines and Terms include (but are not limited to) misapplying logos/icons, and using logos with Products or Software Components that have not been certified.

● The manufacturer has engaged in any form of misconduct which compromises the integrity of Connectivity Standards Alliance or the CSA Certified program.

● The manufacturer leaves Connectivity Standards Alliance and continues using logos, trademarks or any other Connectivity Standards Alliance branding.

● The member is in violation of the member agreement, other agreement with Connectivity Standards Alliance, or a Connectivity Standards Alliance policy or procedure.

Prior to revoking any certification, the Alliance shall notify the manufacturer with details and steps needed to resolve issues and take corrective action. After revocation, and the manufacturer has made corrective action and successfully resolved all issues, the Alliance may, at its discretion, restore the certification or issue a new certification.

Corrective action shall follow ISO/IEC 17030:2021 “Conformity assessment – General requirements for third-party marks of conformity”.

Note that security incidents and security vulnerabilities are not addressed here since they are covered by the Security Incident Response Plan document.

2.13 Testing and Certification Fees

There are two fees associated with the CSA Certified program: testing and certification.

Testing fees are set by the individual authorized test laboratories.

Certification fees are set by Connectivity Standards Alliance and vary based on the type of membership in the Alliance. The current fee schedule is available at http://www.csa-iot.org or by contacting the Alliance.

The different Certification fees include:

● Full Certification
● Certification by Similarity (CbS)
● Certification Transfer Program (CTP)
● Product Family Certification (PFC)
● CTP Listing (an Annual fee for companies making use of CTP)

2.14 Manufacturer-specific identification and information usage

Upon request, the Connectivity Standards Alliance assigns to a Member a manufacturer-specific identification which is maintained by the Alliance. An example of a manufacturer-specific identification is a unique Manufacturer Code, maintained in one of the following:

● “CSA Manufacturer Code Database” [R6]

● A unique pool of GPD SourceIDs, maintained in the “Zigbee Green Power SrcID database” [R7]

Member companies are responsible for obtaining the applicable manufacturer-specific identification prior to certifying a product with the Alliance, and for using it correctly.
Members are responsible for correctly identifying manufacturer-specific functionality, if any, following the Alliance technical Specifications.

A company SHALL only use their own manufacturer-specific identification to identify their own devices and their functionality. Usage of another party’s manufacturer-specific identification is only permitted with a proof of consent of that party.

This usage policy also applies to the Certification Transfer Program. A company certifying a product via the Certification Transfer Program SHALL obtain its own manufacturer-specific identification to use within their newly certified product. Usage of the manufacturer-specific identification of the previously Certified Product is only permitted with a proof of consent of the manufacturer of that Product.
3 TESTING

This Section defines the process for testing that is common to Certification Programs and the final development of Certification Programs. Testing for conformance to CSA Standard or Stack is performed by Alliance authorized test laboratories using test plans developed by the Alliance.

3.1 Test Plans

The test plan must, at a minimum, cover all PICS related items. This must be confirmed by means of a PICS-to-Test-Case mapping. The test plan will undergo standard approval as part of the process detailed in Policies & Procedures (document 13-0625) before formal release. To be finalized, and approved, a test plan must undergo validation at a Specification Validation Event (SVE). More details regarding the SVE can be found in document 08-123 Test Event Rules of Engagement. Features that are certifiable are listed in each Specification set.

The Connectivity Standards Alliance will maintain the list of current test plans, associated PICS, any errata on the Connectivity Standards Alliance member area.

3.2 Authorized Test Laboratories

The Connectivity Standards Alliance authorizes independent test laboratories to administer the testing associated with the CSA Certified program. The process for selecting and qualifying test laboratories is maintained in document 08-5185.

The current list of authorized test laboratories is maintained at the Alliance web site: http://www.csa-iot.org.

3.3 Test Harness

A Test Harness is an automated test tool that is designed to execute a defined test procedure and deliver Pass/Fail decision based on the observed behavior of a Device Under Test based on well-defined criteria. Test harnesses could be in use in the various CSA Certified test programs.

3.3.1 Connectivity Standards Alliance Test Harness

The Connectivity Standards Alliance may have a Test Harness developed for use in one or more of its Certification Programs defined in this document. Where the Alliance has its own Test Harness, this harness shall be the one official Test Harness used by all authorized test laboratories in the execution of testing activities for the given Certification Program.

Maintenance of a Connectivity Standards Alliance Test Harness and associated test scripts is managed, updated and validated through existing Connectivity Standards Alliance processes (supported by member efforts).

3.4 Requirements for Testing

3.4.1 Compliant Platform Testing

The guidelines for Compliant Platform testing are as follows:

- Platforms submitted for testing must fulfill all dependencies and requirements, incl. if applicable, a proof of underlying certifications, as defined by the particular Compliant Platform Certification Program,
- Manufacturers must provide any technical support structure required to assist in the implementation of their Product into the test environment,
- The test is non-destructive and will be applied using the functionalities given by the specific Platform tested, and
3.4.2 Certified Product Testing

The guidelines for Certified Product testing are:

- A Product submitted for testing must be built on a certified Compliant Platform,
- Manufacturers must provide any technical support structure required to assist in the implementation of their Product into the test environment,
- The test is non-destructive and will be applied using the functionalities given by the Product tested,
- Authorized Test Laboratories can provide more information, and
- For the purposes of testing test (security) certificates are to be used.

3.4.3 Certified Software Component Testing

The guidelines for Certified Software Component testing, applicable to both UIC and Underlying Software Component, are:

- Software Component vendors shall clearly list the applicable Supported Operating Environments (SOE) for the Software Component to be certified. Any stated SOE or range of SOEs must align with the range of SOEs supported by the Specification of the respective software component.
- Software Component vendors shall clearly list any dependencies including Software Components on which the Software Component under test depends on. Where applicable, any dependencies must have undergone Software Component Certification prior to the testing.
- Manufacturers must provide any technical support structure required to assist in the implementation of their Product into the test environment,
- The test is non-destructive and will be applied using the functionalities given by the specific Platform tested, and
- Test service providers can provide more information.

3.5 Testing Samples

Manufacturers applying for certification must leave at least one sample of the Device Under Test (DUT), if required by the authorized test laboratory to satisfy ISO17025. These samples will be used for traceability and reference in case of future contention of results or when deemed necessary. A sample consists of:

- Exact hardware that the device will be certified with,
- Same firmware as the one the DUT passed the compliance testing on, and
- Any software/tools pertaining to the device and its certification necessary to reproduce the test plan testing.

For large physical size product testing, the actual product does not need to be submitted. A company may alternatively submit a sub-portion of the original product (a smaller physical form factor). This sub-portion shall be the exact HW, SW, FW, etc. that is in the full-size product, for the purposes of the standard being certification tested, and not an equivalence representation. If other portions (i.e. in the case where the compliant portion is on a circuit board or a sub assembly where the knobs, buttons, display, etc.) of the full product are needed in order to properly perform certification testing, then the company must provide that capability as well. The ultimate decision of whether or not a specific sub-portion and other portions is allowable for certification testing is at the sole discretion of the Alliance Director of Certifications.

In the case where the authorized test laboratory in question already has the hardware configuration (from previous certification or otherwise), and if the authorized test laboratory has the tools (both hardware and software) needed to flash new firmware onto the devices, a manufacturer may simply send the authorized test laboratory a copy of the new firmware as the sample for the DUT.
3.6 Reporting of Test Results

The authorized test laboratory shall report results of successful tests directly to Connectivity Standards Alliance. Unsuccessful test results are not reported to the Alliance unless an application for certification has been made and the Alliance requests reporting of test results.

The test reports shall conform to reporting as defined by ISO/IEC 17025:2005 Section 5.10 and at a minimum shall include:

- Test Information: Location and dates of testing, any tracking or other information necessary to trace results such as test project numbers, responsible testing engineer,
- Tested Device: Company, address, contact information, Product name, hardware and software Product versions, serial number, device type, and other information necessary to identify the device,
- Certification Type: Compliant Platform, Certified Product, or Certified Software Component
- Standards: Name and version information,
- Test Plan: documentation of Test Plan and version numbers used or a list of test cases if a complete test plan is not used,
- Test Equipment: Documentation of any equipment used in the test including Test Harness, script, sniffers, GU>s, and other information necessary to identify the testing equipment including version information,
- Test Results: List of individual tests conducted with individual test results,
- Test Results Summary: Overall Pass / Fail,
- Test Results Observations: Observations outside the scope of the test cases, and
- Signatures: Test engineer, any reviewer or quality engineers.

3.7 Certification by Similarity

The Connectivity Standards Alliance offers a Certification by Similarity program. The program allows a Product that is derived from a previously tested and certified Product to be considered for certification based on its similarity to the previously tested certified Product and depending on the differences between the two. The purpose of the program is to speed up time-to-market and to minimize costs. For complete information on this process, see Section 6 Certification by Similarity.

3.8 Testing Events

A Connectivity Standards Alliance Test Event is defined in document 08-0123 Test Event Rules of Engagement.
3.9 Features Not Previously Certified

A feature that has not been previously tested during an official Specification Test Event cannot be certified. A feature is defined as an attribute of an implementation such as support for a particular cluster in a Connectivity Standards Alliance Standard. A feature becomes validated (and therefore testable and certifiable) only when the following condition(s) are satisfied:

Three separate implementations of the feature must be tested against three separate implementations of the complementary side of that feature (e.g. server against client) through Connectivity Standards Alliance:

- One of the implementations, but no more than one, may be a Test Harness.
- A “separate implementation” is defined as an implementation developed independently from other implementations by a different member of Connectivity Standards Alliance.
- When a test case is testing the handling of illegal or non-standard behavior the requirement to test against three implementations is relaxed and testing against a single implementation (Test Harness or Golden Unit) that exhibits the non-standard behavior is acceptable. Otherwise the requirement is to test against three implementations.
- The testing described above will be subject to the same rules and requirements as Specification Validation Events, defined in document 08-0123 Test Event Rules of Engagement.
- Once all testing is complete, the Specifications for which the testing has been done shall be updated to reflect the change.
- For a device using a previously non-certifiable feature to become certified, all requirements for certification must be met including successful completion of the entire test plan as described in this policy.
- If three separate implementations are not available for testing, the feature cannot be validated. A device implementing that feature may not be certified and the manufacturer has a choice to either:
  - Wait for the other implementations to become available
  - Certify the rest of the Product and identify the non-certifiable feature(s) as Manufacturer Specific (i.e., cluster ID, profile ID, command ID, or other Connectivity Standards Alliance approved method)
4 GOLDEN UNIT

A Golden Unit (GU) is a Compliant Platform or a Certified Product that is designated as reference instantiation of the Specification(s) it implements. A GU is a specific combination of hardware, software, firmware and/or errata including revision numbers for each. GUs represent an important infrastructure for Certification Programs.

GUs are used to test against Platforms and Products during the testing leading towards certification. Specifically, they are used for:

- Evaluating the expected behavior of the device under test (DUT)
- Testing the DUT for interoperability and conformance to the test Specification

When the Specification is silent or ambiguous, the behavior of the GUs will be used as the reference for evaluating the expected behavior of the device under test.

GU providers are Connectivity Standards Alliance members and are likely to have been actively involved in creation of the relevant Specification and have been actively participating in the interoperability testing series in vendor-neutral environments. This represents a significant commitment by the GU manufacturers.

4.1 Golden Unit Selection

For each release of a Specification, the following procedure will be used to establish GUs for that release.

The Connectivity Standards Alliance will announce a Specification release interoperability testing series associated with the development of a new standard Specification or the revision of an existing one. This interoperability testing series will constitute the GU selection round. During the development process for new (or revised) Specifications there are three phases of testing:

Phase 1. Proof of Concept & Interoperability Test Events – These events are held while the test plan is being developed and implemented to prove concepts being considered for inclusion in the Specification and to begin testing and validation of early implementations.

Phase 2. Gating Test Events – These events mark the end of the Proof of Concept & Interoperability Test Events. Participation at all prior Gating Test Events is required to continue participating in subsequent Gating Test Events. A variety of Gating Test Events may be scheduled.

Phase 3. Specification Validation Event(s) (SVEs) – This is the final Gating Test Event where participants must test all mandatory features. Attendance at each Gating Test Event is required to participate in the SVE. Participation in a SVE implies a desire to become a Golden Unit.

Upon completion of the three phase testing series, implementations which have successfully completed the series will be eligible for certification provided that all testing requirements have been met at the final SVE.

Participation in the Specification Validation Event does not guarantee being selected as a GU. Implementations become GUs after completing certification and the Alliance Director of Certifications confirms in writing the GU candidate provider’s conformance to Section 4.2 Manufacturer Commitments as a Golden Unit Provider.

The Alliance Director of Certifications shall select the GU candidates. The selection will be made from implementations that participated in the SVE with preference given to those that tested against the most implementations.

An additional requirement in becoming a GU provider is that the authorized test laboratory provides the GU test logs to Connectivity Standards Alliance which will post them to the document server. The Alliance Director of Certifications will work with the manufacturer in making the test log files anonymous.
During the GU selection process, GU candidates will be notified by the Alliance Director of Certifications with regards to any outstanding items required regarding their implementation in order to finalize its certification and complete its selection as a GU. GU candidate providers will be provided with a timeframe by which all outstanding items must be completed, in order for their GU candidacy to remain valid. The timeframe for outstanding item completion will be the same for all GU candidates.

Upon the conclusion of the timeframe allowed for completion of outstanding items, the Alliance Director of Certifications will make final GU selections from those candidates that successfully completed all outstanding items. If there is an insufficient number of candidates within the prescribed time frame, the Alliance Director of Certifications may extend the timeframe, which extension shall be applicable to all GU candidates. For purposes of determining an appropriate number of candidates, the Alliance Director of Certifications will make such determination based on the guidelines set forth in this policy.

Once the timeframe has expired (including any extensions), provided there are a sufficient number of GUs selected, the Alliance Director of Certifications will provide written notice to GU candidates that the GU selection process is closed. Any GU candidate who failed to complete its outstanding items by the date of the notice will not be eligible for selection as a GU. Any Connectivity Standards Alliance member that proposed a failed GU candidate is eligible to participate in future Specification revisions in accordance with the terms and conditions in this policy.

GUs must be established and provided to the authorized test laboratories before a Certification Program can be open to the Connectivity Standards Alliance general membership. The approved authorized test laboratories will then be in a position to commence testing of additional implementations as part of the certification process. A test program may not begin until GUs have been selected and provided to the authorized test laboratories.

4.2 Manufacturer Commitments as a Golden Unit Provider

4.2.1 Requirements for Compliant Platforms Golden Units

Manufacturers of GUs used for Compliant Platform testing shall:

- Implement all mandatory and optional functions.
- Act as all applicable device types/roles defined by the Specification
- Support all device operations defined by the Specification.
- Allow for negative testing (i.e., be able to produce stimulus that is incorrect, or in error, with respect to the Platform Specification) as required by the test Specification.
- Provide a clearly documented interface, including descriptive operational documentation, which enables the running of all test cases and the test Specification.
- Maintain Compliant Platform status for that device, so long as the Specification to which that device applies to is in effect, See Section 4.3.
- Provide technical support to the CSA authorized test laboratories for its ongoing use as a GU;
- Provide to each CSA authorized test laboratory, free of charge, as many units as specified by the Alliance Director of Certifications. The CSA authorized test laboratory may unpack, power on and test (e.g., smoke test) each of the units prior to confirming to the Alliance Director of Certifications that the units have been delivered; and
- Make available additional GUs (to Alliance authorized test laboratories) for the purposes of breakage replacement (free of charge) and for additional purchase.

Written Confirmation of the Alliance Director of Certifications Required to Become GU – Implementations become GUs only after the Alliance Director of Certifications confirms in writing to the
applicable manufacturer that such implementation has completed certification, has successfully completed all the items in Sections 4.1 and 4.2 and is a GU. No GU applicant may publicize, represent, reference, state or otherwise claim to have a GU or be the manufacturer of a GU except with respect to the specific GU implementation for which the Alliance Director of Certifications has delivered a written confirmation as set forth above.

4.3 Updating Golden Units

4.3.1 Conditions for Updating Platform Golden Units

Updating of the GUs shall be determined by the Alliance Director of Certifications. Circumstances warranting updating a GU include:

- Approval of Change Control Board (CCB) comments that affect the behavior of the GUs
- Revision to the Specification, test Specifications or PICS document that affect the behavior of the GUs
- Errors or bugs are found in the GU
- A GUs is not available anymore (discontinued, etc.)

4.3.2 Process of Updating Platform Golden Units

If an update is deemed necessary, Connectivity Standards Alliance shall send an official note to the GU manufacturer as well as authorized test laboratories detailing the following:

- Reasons for the need to update
- Timeline to update
- All supporting information/documentation to update (example: new Specification revision, CCB references, specific bugs to fix, etc.)

Once the manufacturer implements the needed changes, the new revision(s) of the GUs need to be revalidated. Revalidation of a Golden Unit requires successful testing completion according to the retest requirements for Compliant Platform as described in Section 6 Certification by Similarity. To the end of revalidating Golden Units, there are two possibilities:

- Set a Test Event for the manufacturers and test laboratory to attend and verify the changes. This Test Event shall be only open to those GU manufacturers and the test laboratory. At least one test laboratory shall attend that event.
- Send the new revision(s) of the GUs to all test laboratories who will then test them internally and submit the results to Connectivity Standards Alliance.

If the result of the testing is considered a pass the new revisions will then be officially accepted as the new GUs and the official list of GUs pertaining to that Specification must be modified to reflect the changes.

The manufacturers shall then send the new GUs to all test laboratories (in case of a firmware upgrade, sending the revised firmware would be sufficient as long as test laboratories have the tools to upgrade the firmware on their units). At that point, the new GUs shall replace the old ones in official testing at the test laboratories.

Note that in case that new hardware is needed, the number of GUs to be sent to test laboratories shall be determined by the Alliance Director of Certifications.

If a GU manufacturer cannot update their units within the timeline specified by the Alliance Director of Certifications, the Alliance Director of Certifications can then decide to make a new request for a GU to replace that specific Platform/device.

Any Golden Unit going through the revalidation process, shall be removed from the active rosters of Golden Units until the revalidation process is successfully completed and all necessary updates (HW and/or SW) have been completed at all authorized test laboratories and shall not be used in the testing of units for the applicable Standard.
5 MODIFICATIONS AND REVISIONS

This Section describes the processes and requirements for certification when a Product has already been certified.

5.1 Modification of Products

Certification is awarded to a particular version of a Product or Software Component. Any modification to that Product or Software Component will result in a new version and that version may not claim certification without going through the CSA Certified program.

The new version of the Product or Software Component may not require testing in order to be certified. Changes that affect conformance to the Standard (hardware, firmware or software changes) will usually require testing. The Alliance maintains requirements for testing of changes to Products and Software Components. For complete information, see 6 Certification by Similarity or 10 Certified Software Component.

The original version of the Product retains certification for the life of the Product, unless revoked by action of the Alliance.

5.2 Revisions to Specifications

In the interests of continuous improvement in the quality of the compliance program, Connectivity Standards Alliance may, from time to time, change the compliance testing procedures through a change to a test plan. Because a Product’s or Software Component’s certification is good for the life of the Product or Software Component, there will be no requirements for manufacturers to go through certification again. However, Connectivity Standards Alliance encourages manufacturers to resubmit their Product or Software Component to authorized test laboratories for verification of compliance to those changes.

The Connectivity Standards Alliance will maintain records sufficient to identify the version of a test plan under which certified Products or Software Components were tested.

5.2.1 Grace Period for Testing

When a test plan or Specification is revised, Connectivity Standards Alliance will declare a grace period during which manufacturers in their development cycles can still certify to an old test plan and Specification. However, after the grace period is over, all Products or Software Components going through certification must be tested against latest test plan and Specification.

The Working Group creating the Standard will recommend a grace period for revisions affecting Products or Software Components to be approved by the appropriate Technical Sub-Committee, the Marketing Committee and the Board StratCom when the Specification has reached 1.0 status. This grace period will be based on the amount of changes introduced by the new Specification and the current state of deployment of devices based on the previous version of the Specification or similar considerations. The default grace period if the Working Group does not recommend a change is 6 months.

5.2.2 Major Revisions Affecting Interoperability

In exceptional circumstances, Connectivity Standards Alliance reserves the right to mandate resubmission of Compliant Platforms for testing against a revised Compliant Platform test plan. This may occur, for instance, where a serious deficiency in the test plan or process is uncovered, leading to Platform interoperability issues. In the event that the Alliance mandates such resubmission and the manufacturer fails to successfully complete such testing within the time specified by the Alliance Director of Certifications, the Alliance may move to revoke certification of the Compliant Platform.
6 CERTIFICATION BY SIMILARITY

The Connectivity Standards Alliance offers a Certification by Similarity program to member companies. The Certification by Similarity (CbS) program allows a CSA Product that is derived from a previously tested and certified CSA Product to be granted certification based on its similarity to a previously tested certified Product. The purpose of the CbS program is to speed time-to-market and to minimize certification costs. It is not intended to eliminate the requirement that a Product actually passes CSA compliance tests.

6.1 Certification by Similarity Policy

The only authority to grant Certification by Similarity to a Product is the Connectivity Standards Alliance. No test laboratory or any other entity is authorized to grant or pursue Certification by Similarity Testing Exemption Requests on behalf of the Connectivity Standards Alliance.

The new Product must be derived from and be substantially similar to a CSA certified Product that has successfully undergone full and complete compliance testing. CbS addresses changes such as color, enclosures, language, etc. that do not affect the conformance of the Product to CSA Standards. The new Product cannot be compared to another Product that itself has been granted Certification by Similarity without additional testing having been performed. More details on the guidelines that govern the CbS, and thus the need (or lack of) for testing, can be found in Section 6.6 Retest Requirements for Compliant Platform Certification of this document.

If the original certified Product on which the Certification by Similarity Testing Exemption Request is based is older than three years, then complete testing is required of the new Product.

CbS does not waive or change the requirement for certifiers of Products to be members of the Alliance, to follow the Connectivity Standards Alliance Trademark and Logo Usage Guidelines and Terms, or to comply with any policies of Connectivity Standards Alliance.

6.2 Certification by Similarity Guidelines

When Products are very similar, testing of one Product may allow the other similar Products to be added to the Integrators List (Approved List) without re-testing. Furthermore, some changes to certain Products may be deemed harmless to the existing certification for that specific Product, in which case the newer revision will automatically be certified by similarity.

The decision on whether or not a Product will qualify for Certification by Similarity (CbS) will be the responsibility of CSA’s Certification body according to the process highlighted above. The ultimate responsibility for making sure that all Product variations and models are certified (whether through actual certification and/or via CbS), ultimately lies with each manufacturer.

Audits by Connectivity Standards Alliance that reveal discrepancies between shipping Product and samples tested may be cause for required re-test, revocation of certification, and/or legal action. Only Connectivity Standards Alliance members have the right to use the Connectivity Standards Alliance trademarks and logo, and such usage is subject to the Connectivity Standards Alliance Trademark and Logo Usage Guidelines and Terms.

6.3 Certification by Similarity Guidelines Procedure

1) An applicant (Product developer) selects Certification by Similarity Testing Exemption Request at certification@csa-iot.org for the product(s) in question when applying for certification online. An example of the information required to be submitted for the purposes of a Certification by Similarity Testing Exemption Request can be found in Appendix A.

2) The Certification by Similarity Testing Exemption Request shall be supported by a rationale from the developer showing that the modifications or changes do not negatively affect the security of the product. The rationale can be provided as part of the Certification by Similarity Testing Exemption Request.

When applicable, Connectivity Standards Alliance may request applicants to supply detailed technical information of both the originally certified and new Products.
3) A review of the Certification by Similarity Testing Exemption Request and Specification sheets/drawings will be performed by the Alliance Director of Certifications. One or more of the authorized test laboratories and/or other experts (e.g. Connectivity Standards Alliance Expert Review Panel) may be consulted by Connectivity Standards Alliance, keeping in mind the confidential sensitivities that come with an unreleased Product.

4) The Connectivity Standards Alliance will issue its assessment to the applicant within one (1) calendar week. One of the following outcomes is possible:
   a) Further clarification is requested by CSA in order for the review to be completed
   b) Certification by Similarity is granted. Exemption for full testing is granted and no testing is required to be granted CSA certification
   c) Spot checking (testing) is required before granting of CSA certification is considered
      i) Spot check (testing) consists of running a specific set of tests determined by CSA based on the changes made between the already certified platform/product/HW and the one being considered for Certification by Similarity
      ii) If during the spot checking, at an approved CSA test house, the spot checking reveals any issues, full testing is then required to be granted certification by the CSA

   Certification by Similarity is denied. The request for exemption from testing is rejected and a suitable description for the rejection is given. The Product is required to go through testing at one of the authorized test laboratories.

   When any testing is required the Product developer will follow standard procedures for testing and certification.

   6.4 Guidelines for “Retest”

   The guidelines for retests can be found in Sections 6.6 Retest Requirements for Compliant Platform Certification and 6.7 Retest Requirements for Certified Products of this document.

   If you think retest is not required, your company can submit a Certification by Similarity Testing Exemption Request for consideration by Connectivity Standards Alliance.

   6.5 Retest Requirements for Compliant Platform Certification

   6.5.1 Retest not required

   I/O additions on the dev board.

   6.5.2 Full retest required

   Bug fixes that substantively affect the Platform functionality require a full retest.

   6.5.3 Spot check required

   A spot check tests specific areas affected plus random spot check of other areas against Golden Units.
   - Porting of the Stack (with no changes) to a new hardware
   - Bug fixes that do not substantively affect the functionality
   - Update to the Stack (including non-program specific related code update)
   - Microcontroller change (with the PHY/MAC staying the same)
   - Addition of a new feature/module to the Zigbee firmware

   6.5.4 MAC/PHY retesting required

   See MAC/PHY retest requirements
6.6 Retest Requirements for Certified Products

6.6.1 Retest not required

- Product packaging changes (color, shape, etc.)
- Changes in interface that do not affect CSA or Radio functionality (color display v/s B&W, push button light switch v/s paddle switch, etc.)
- HW configuration changes that do not affect program specific (changing location of a read switch, change of metrology, change of button location, etc.)
- Addition of I/O’s needs that don’t degrade the security of the product (debug port, etc.)
- Changes in the Dependent Certification portions of a product, provided that the new portion is also a certified (by the same dependent certification body) portion, and meets the minimum dependent certification requirements as defined in the specific CSA’s Certification Program for the product being certified.
- Changes in the implementation of Robustness Security Requirements may be eligible for CbS with no retest but the Matter Self-Attestation Questionnaire shall be updated appropriately and submitted with the Certification by Similarity Testing Exemption Request. Depending on the type and scope of modification, the Alliance Director of Certifications may deny the CbS and ask for Spot Check or Full Retest.

6.6.2 Full retest required

- Addition/exposure of a new feature and/or cluster to the CSA firmware
- HW, SW or FW changes for the device(s) that the Stack and app are running on (with the exception of those items called out above in Retest not required)
- Layout change of the module used
- Bug fixes that substantively affect the functionality

6.6.3 Spot check required

Note: Considering that the level of effort and price to certify Products are relatively small, it would be cheaper and faster to retest fully if needed than deal with the procedures and maintenance of spot check requests and upkeep.

6.6.4 MAC/PHY retesting required

See section 6.8 MAC/PHY Retest Requirements for Compliant Radios below.

Note: The exact nature of the MAC/PHY retesting needs to be defined. As part of regulatory Radio testing, Products have to be supplied with a number of test modes. It is intended that the MAC/PHY retesting would only use these existing test modes (to reduce the development burden on the Product manufacturer)

6.7 MAC/PHY Retest Requirements for Compliant Radios

6.7.1 Full retest required

- Change in Radio IC
- Changes in SW, FW affecting Radio functionality
- Changes requiring retest by regulatory authorities
6.7.2 Spot check required

- Change/Addition of a PA (All Tx tests shall be run, Rx tests shall be spot checked)
- Change/Addition of LNA (All Rx tests shall be run, Tx tests shall be spot checked)
- Change of all other components connected externally to the Radio IC
- Change in RF/EMI/EMR enclosures
- Change in packaging affecting RF/EMI/EMR characteristics
- Change in board layout

6.7.3 Retest not required

- Change in I/O interface to the board

6.7.4 Spot check rules (Firmware/Platform)

- Full retest of functionality that has been changed or where bugs were fixed
- Full coverage of the all the other areas through spot check (one test case per function)
- In case of any failure on the spot check areas, the Product is considered as a fail and a full retest is needed

6.7.5 Spot check rules (PHY)

- Each Certification Program can define its own PHY spot check rules
- In case of any failure during the spot check, the Product is considered as a fail and a full retest is needed
7 CERTIFICATION TRANSFER PROGRAM

The Connectivity Standards Alliance certification transfer program supports the use of a previously Certified Product from a Participant or Promoter member company as part of a new Product (from a member company). Participation in the Connectivity Standards Alliance certification transfer program is subject to the terms and conditions of the Connectivity Standards Alliance Certification Transfer Program Agreement.

7.1 Certification Transfer Program details

The Connectivity Standards Alliance certification transfer program supports the embedding of a previously Certified Product (from a Participant or Promoter member company) into a new Product enclosure from any member company. The previously Certified Product SHALL NOT be changed from its certified configuration (Read: No hardware changes other than a new Product enclosure and no software changes.) The only permitted firmware changes SHALL relate to manufacturer and device specific descriptions. The manufacturer of the previously Certified Product, registered for the Certification Transfer Program, MUST make provision to configure the manufacturer and device specific data without modifying (incl. recompiling) the firmware.

The originally Certified Product implementation SHALL conform to the following Standard Specifications as appropriate to the declared PICS:

- Zigbee 3.0 Specification & requirements as defined in Section 11.2.2 Zigbee 3.0 Product Certification Program
- Zigbee Smart Energy Specification & requirements as defined in Section 11.2.1 Legacy Profile Product Certification Program
- Green Power end devices as defined in Section 11.3 Certified Product: Green Power Device
- RF4CE devices as defined in Section 11.4
- Matter products as defined in Section 11.5

The original Certified Product implementation SHALL have obtained its certification by one of the following certification paths:

- Full testing in accordance with Section 3 Testing
- Certification by Similarity as per Section 6 Certification by Similarity.

Products certified under this program SHALL conform with all additional requirements below:

- Certifying Product SHALL seek certification under the same program, device type and device capabilities as the originally Certified Product.
  - Availability of certification is subject to the same timelines and grace period as the original programs.
- Certifying companies shall submit a Certification Transfer Application via the Alliance web tool, agree to the Connectivity Standards Alliance Certification Transfer Program Agreement and remit all appropriate fees as designated by the Connectivity Standards Alliance Board of Directors.
### 7.2 Graphical Representation of the Permitted Certifications

![Graphical representation of the permitted certifications]

- **Member A**
  - Product 1
  - Product 1'
  - Product 1''

- **Certification Transfer Program**
  - Green arrows indicate certification by similarity.

- **Member B**
  - Product 1a
  - Product 1a'
  - Product 1a''

**Key**
- Fully Tested
- Not Tested
8 PRODUCT FAMILY CERTIFICATION PROGRAM

The Connectivity Standards Alliance offers a Product Family Certification program. For this program the Alliance defines a Product Family to be that where each member of the Product Family is a direct variant of a single Parent Product. The Parent Product SHALL be the most feature complete variant in the whole Family. The other products within the Family shall be termed Family Member Products of the Product Family. In addition, the differences between the variants must not affect the conformance of the Family Member Products to Alliance Specifications. Each Product Family Member must be of the same device type.

Examples of such Family Member Products are those with different regional power plug variants, or products which are depopulated or low-cost variants with less third-party physical interfaces. For the avoidance of doubt, Product Family Certification does not cover products which are Similar but not variants of a single Parent Product. Such similar products SHALL be certified using the Certification by Similarity Program.

This program allows a manufacturer to certify a Product Family, including multiple Family Member Products of the Family at the same time, on a single certification application, based on the Parent Product within the Family.

The purpose of the program is to speed time-to-market and to minimize costs, both for the Alliance and the certifying Member.

8.1 Product Family Certification Policy

The only authority to grant Product Family Certification to a Parent Product or a number of Family Member Products is the Connectivity Standards Alliance. No test laboratory or any other entity is authorized to grant or pursue Product Family Certification requests on behalf of the Connectivity Standards Alliance.

The Product Family Certification SHALL only allow changes between Product variants that do not affect the conformance of the Family Member Products to Alliance Standards.

The Parent Product in a Product Family must be certified in one of two ways. Either the Parent Product has successfully undergone full and complete compliance testing. Or, the Parent Product qualifies for Certification by Similarity, based on another, fully tested product – provided, as per CbS rules, that the certification of that fully tested product is not older than three years.

The other Family Member Products in the Product Family must be variants of the Parent Product and be substantially similar to it, with the allowable changes not affecting conformance to Alliance Standards.

The Parent product might have been originally certified as a single product, without any reference to the Product Family Certification Program, even before the launch date of the Product Family Certification program – provided, the certification of the Parent Product is not older than 3 years.

At the time of application for the initial Product Family Certification, the procedures and fees defined for the Product Family Certification program apply.
Once a Product Family has been certified, it can be extended with further Family Member Products.

The Product Family can also undergo recertification (for example in the case of updates to firmware).

More details on the guidelines that govern the Product Family Certification can be found in Section 8.2 Product Family Certification Guidelines of this document.
If the original certified Parent Product on which the Product Family Certification is based is older than three (3) years, then complete testing is required for the most feature complete product which will become the new Parent Product for that Product Family. Once this is completed, extensions with additional Family Member Products can be made.

Product Family Certification program does not waive or change the requirement for certifiers of products to be members of the Alliance, to follow the Alliance Trademark and Logo Usage Guidelines and Terms, or to comply with any policies of the Alliance.

8.1.1 Product family certification versus other certification programs

The table below provides examples illustrating applicability of the Product Family Certification program. It lists exemplary change type, i.e. different modified product features and components, and the resulting applicable certification program.

If a change type is not explicitly listed in the table, please contact the Alliance certification team for further guidance.

Table: Differences between 2 products of the same vendor – and the applicable certification program

How to read this table: The assumption is that a vendor A has a Parent Product X and another product Y, which differs from product X. Depending on what the difference is (as specified in the leftmost column of the table), a particular certification path will be applicable for product Y.

The table below applies equally in case of products X and Y submitted for certification at the same time (see section 8.3.1 Initial Procedure for submission for a Product Family Certification), and in case of product Y submitted later than product X (see section 8.3.2 Procedure to extend a Product Family Certification).

Each row of the table lists a single difference between the two products; all other product properties are assumed to be identical.

The table also applies for the case where there are multiple changes between two products. If they require different certification path, then the most demanding program is applicable; listed here from the least to the most demanding certification path: Product Family Certification, Certification by Similarity, Full testing.

A vendor can always choose to certify product Y via a more demanding program, including full testing.
<table>
<thead>
<tr>
<th>Type of change in product Y compared to a fully tested product X</th>
<th>Examples of that type of change</th>
<th>Applicable certification program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production/on-site configuration</td>
<td>Product name string, ManufacturerID string within the Basic cluster, other read only attributes of the Basic cluster (Requires same product base name, but may have different SKU numbers, ManufacturerID in the OTA image)</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Production/on-site configuration</td>
<td>Same product sold under different brand names of sub-companies (local awareness for existing popular brand) in different geographies.</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>CSA Software other than configuration: disabling a feature, no other software change; no hardware change</td>
<td>Product X was certified with 2 identical endpoints, Product Y has 1 of those endpoints; there is no other change</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>CSA Software other than configuration: disabling a feature, no other software change</td>
<td>Product X was certified with 7 optional clusters, Product Y only has 4 of those clusters; no other change</td>
<td>CbS</td>
</tr>
<tr>
<td>CSA Software other than configuration: different attribute set/different feature set within a cluster</td>
<td>Product X was certified for a cluster with a set of optional attributes, Product Y has a different set of optional attributes in that same cluster e.g. different set of controls for the motor device; different color modes of the color control cluster of a light bulb; different type of occupancy sensor with different set of attributes;</td>
<td>Full Testing</td>
</tr>
<tr>
<td>CSA Software other than configuration: enabling a new feature</td>
<td>Product X was certified with 2 identical endpoints, Product Y adds 1 endpoints;</td>
<td>Full Testing</td>
</tr>
<tr>
<td>CSA Software other than configuration: enabling a new feature</td>
<td>Product X was certified with 7 optional clusters, Product Y only has 4 of those clusters, but adds 2 more optional clusters</td>
<td>Full Testing</td>
</tr>
<tr>
<td>CSA Software other than configuration: other changes in the code</td>
<td>Code refactoring, fixing a security bug, CCB fix; new stack drop</td>
<td>Full Testing</td>
</tr>
<tr>
<td>Software NOT affecting the CSA Software</td>
<td>new language for the UI, new driver for the USB port</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Firmware (in case of multi-board solution: for (any) of the board(s) hosting CSA functionality)</td>
<td>OS update</td>
<td>Full Testing</td>
</tr>
<tr>
<td>CSA radio</td>
<td>Usage of different radio chipset</td>
<td>Full Testing</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Different external power supply</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Different power receptacle/connector pins</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Adding/removing a neutral wire connection to existing dimmer</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>different wattage of a light source (more lumens)</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>different length of a light strip (more LEDs)</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>different width of blinds</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>adding USB port (there was none before)</td>
<td>CbS</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Adding a second USB port</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>additional UI button</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Removing 1 of 2 USB ports</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Removing USB ports completely</td>
<td>CbS</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>2A light switch vs 10A switch</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Circuit breaker with same functionality but different thresholds for action.</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Smoke detector with same functionality but different thresholds for alarm.</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Electronics not affecting CSA radio</td>
<td>Circuit breaker, 120V vs 200V vs 300V</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>Different color of the casing</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>different shape for the casing for a switch module (engine) [e.g. round / rectangular, square, e.g. due to regional requirements]</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>Different finishing material of the casing for a switch module (engine)</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>Different finishing/ material of a product casing (e.g. for indoor and outdoor)</td>
<td>CbS</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>different color for the casing for a switch module (engine)</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>different light bulb form factor,</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>different socket for a light bulb (part of it being regionally-influenced)</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical form factor/casing not affecting CSA radio</td>
<td>different cable connection terminals (e.g., screwed – Norway preference vs. screw-less/spring-loaded – France preference)</td>
<td>Product Family Certification</td>
</tr>
<tr>
<td>Mechanical elements not affecting CSA radio</td>
<td>Different types of mechanical door lock mechanisms, as enumerated in the LockType attribute of the Door Lock cluster: e.g. dead bolt lock, mortise lock, latch bolt lock, tubular lock, dead latch lock. Locks with an without mechanical key override rim</td>
<td>CbS</td>
</tr>
<tr>
<td>Mechanical elements not affecting CSA radio</td>
<td>Door lock: type of keypad (e.g. pushbutton keypad or capacitive touch keypad)</td>
<td>CbS</td>
</tr>
<tr>
<td>In case of multi-board products: changing any of the boards</td>
<td></td>
<td>Full Testing</td>
</tr>
</tbody>
</table>
8.2 Product Family Certification Guidelines

The decision on whether or not a number of Products will qualify for Product Family Certification will be the sole responsibility of the Alliance’s Certification body according to the procedure highlighted above. The ultimate responsibility for making sure that all product variations and models are certified (whether through full testing, via CbS and/or via Product Family Certification), lies with each manufacturer.

Audits by Connectivity Standards Alliance that reveal discrepancies between shipping product and samples tested or certified as part of a Product Family may be cause for required re-test, revocation of certification, and/or legal action. Only Connectivity Standards Alliance member companies have the right to use the Connectivity Standards Alliance trademarks and logo, and such usage is subject to the Connectivity Standards Alliance Trademark and Logo Usage Guidelines and Terms.

8.3 Product Family Certification Procedure

8.3.1 Initial Procedure for submission for a Product Family Certification

1) The applicant must complete a standard application for certification in the Alliance Member’s Area at https://csa-iot.org/. An applicant (Product developer) submits applicable documentation of a Parent Product (incl. DoC, applicable PICS documents and, in case of Parent Product certified by full testing, the test results).

   The Parent Product must either have successfully undergone full and complete compliance testing or it must qualify for Certification by Similarity, based on another, fully tested product.

2) The applicant extends the DoC with a list of all the Family Member Products of that Product Family to be part of the same certification application, listing their unique product identifiers and the differences with respect to the Parent Product for that Product Family. Those additional Family Member Products of the Product Family are expected to use the same HW, SW and FW as the Parent Product, and as indicated in the DoC.

3) When applicable, Connectivity Standards Alliance will obtain Specification sheets/drawings of both the Parent Product and Family Member Products.

4) A review of the DoC will be performed by the Alliance Certification Team under the direction of the Alliance Director of Certifications. The review will encompass the assessment of the full documentation of the Parent Product and the Family Member Product list. One or more of the Authorized Test Laboratories and/or other experts (e.g. CSA Expert Review Panel) may be consulted by Connectivity Standards Alliance, keeping in mind the confidential sensitivities that come with an unreleased Product.

5) The Connectivity Standards Alliance will issue its assessment to the applicant within one (1) calendar week. One of two outcomes is possible:

   a. Product Family Certification is granted for the Parent Product and all listed Family Member Products of the Product Family and the Alliance will process the application as any other certification.

   b. Product Family Certification is denied for one or more Family Member Products of the Product Family.

      Those Family Member Products for which Product Family Certification is denied, need to go through a different form of certification, as applicable: testing at one of the Authorized Test Laboratories or Certification by Similarity.

      For the Family Member Products for which the certification is granted, including the Parent Product, the Alliance will process the application as any other certification.

6) At the time that the Product Family certification is issued, a unique Family identifier shall be assigned. This will uniquely identify the Family for certification purposes in the future.
8.3.2 Procedure to extend a Product Family Certification

Once a Product Family Certification has been issued, the original applicant of the Product Family may submit a new application to extend the Product Family by adding extra Family Member Products.

1) When extending the Product Family Certification, the applicant shall submit a new DoC which lists the originally certified Parent Product, the originally certified Family Member Products which continue to be part of this Family, and the new Family Member Products to be added. The DoC SHALL include the unique Family identifier (from step 6 in section 8.3.1 Initial Procedure for submission for a Product Family Certification) to reference the specific Family to be extended. The applicant SHALL provide a listing of the unique product identifiers of the Family Member Products and the differences with respect to the Parent Product that has undergone full testing (as listed in step 1 in section 8.3.1 Initial Procedure for submission for a Product Family Certification). Those additional Family Member Products of the Product Family are expected to use the same HW, SW and FW as the Parent Product, and as indicated in the DoC.

2) For such extension submissions, the Parent Product of the Product Family must have been certified against the applicable Alliance Standards less than 3 years prior to the submission date of the Product Family application for extension.

3) When applicable, Connectivity Standards Alliance will obtain new Specification sheets/drawings of both the Parent Product and new Family Member Products to be added.

4) A review of the DoC will be performed by the Alliance Certification Team under the direction of the Alliance Director of Certifications. The review will encompass the assessment of the full documentation of the Parent Product (excluding the original test result) and the further Family Product Family list, to ascertain that the previously certified products are unmodified. One or more of the Authorized Test Laboratories and/or other experts (e.g. CSA Expert Review Panel) may be consulted by Connectivity Standards Alliance, keeping in mind the confidential sensitivities that come with an unreleased Product.

5) The Connectivity Standards Alliance will issue its assessment to the applicant within one (1) calendar week. One of two outcomes is possible:
   a. Product Family Certification is granted for all the new listed Family Member Products of the Product Family and the Alliance will process the application as any other certification.
   b. Product Family Certification is denied for one or more of the new listed Family Member Products of the Product Family.
   Those Family Member Products for which Product Family Certification is denied, need to go through a different form of certification, as applicable: testing at one of the Authorized Test Laboratories or Certification by Similarity.
   For the new Family Member Products for which the certification is granted, the Alliance will process the application as any other certification.

8.3.3 Procedure to re-certify a Product Family

Once a Product Family Certification has been issued, the original applicant of the Product Family may submit a new application to re-certify the Product Family (e.g. because of a SW update due to fixing SW bugs).

1) The applicant SHALL submit a new DoC including the unique Family identifier (from step 6 in section 8.3.1 Initial Procedure for submission for a Product Family Certification) to reference the specific Family to be recertified.

2) The Parent Product of the Family as submitted for the Product Family recertification SHALL be the most feature rich device in this Family.

3) At the time of the recertification, all Family Member Products for which the certification is being applied for SHALL be listed in the application. Those Family Member Products may have been certified as part of original Product Family Certification (see sec. 8.3.1 Initial Procedure for submission
for a Product Family Certification) and/or Product Family extension (see sec. 8.3.2 Procedure to extend
a Product Family Certification).

4) The process for recertification shall then follow the steps 1-5 as detailed in section 8.3.1 Initial
Procedure for submission for a Product Family Certification.

When testing is required the Product developer will follow standard procedures for testing and certification.

8.4 Procedure to re-certify products using the same HW, SW and FW

A vendor might have certified a number of products that are exactly identical in terms of their CSA-defined
functionality: use the same HW (radio), SW and FW. If the SW/FW in those products requires update, and thus
re-certification, the vendor is allowed to fully test the new software on one of the previously certified products
and list the other previously certified products on the certification submission as part of Product Family
Certification, so that all products can be recertified for the new software.

This procedure can be used regardless of how the products that are exactly identical in terms of their CSA-
defined functionality have been initially certified: through full certification, CbS or Product Family
Certification.

8.5 Product Family Certification vs Certification Transfer Program

Every certified Family Member Product can be offered for Certification Transfer Program.

9 CERTIFIED PRODUCTS SOLD IN SETS

If an individual product was certified with the Connectivity Standards Alliance, that product can subsequently
be sold without any modification as a part of any set (e.g. blister pack) with other unmodified certified products,
without a need for re-certification or registration of the product set as such.
10 CERTIFIED SOFTWARE COMPONENT

The Software Component Certification Program is only applicable to Software Components that run within the context of an SOE and the underlying hardware configurations supported by the SOE. Each Certification Program may define the set of capabilities that is certifiable as a Software Component running on an SOE. These Underlying Software Components encapsulate the functionality defined in the CSA Specification(s). This in turn allows the UIC developers to choose if they want to use ready-made certified building blocks (Type 2 UIC), or implement the Alliance-defined functionality from scratch (Type 1 UIC).

Products that meet the criteria for a HW device shall be certified under the Product Certification Program. The Software Component Certification Program is not intended to replace the existing Product Certification Program or the Compliant Platform certification program.

If a component vendor decides to not maintain a component anymore and it is known to not work with recent SOEs, the vendor SHOULD retract the component from App -Stores, package managers and other means of distribution, or clearly state the limited range of SOEs.

10.1 Definitions

Supported Operating Environment (SOE): A platform abstraction layer, such as an Operating System or platform, allowing (downloadable or pre-installed) components to be run (in source or binary) on underlying hardware configurations supported by the SOE. The SOE must allow for components to be installable and upgradeable, and ensure interoperability, fairness, and be non-discriminatory. UICs shall be allowed to package their own implementation of Alliance Specifications (eg. An Alliance SDK or a proprietary implementation).

An SOE has normal policies and processes for approval of UICs and may provide reasonable runtime checks to ensure user consent. CSA does not interfere with these approval processes in any way except that they shall not disadvantage those UICs with non-SOE software components, and ensure interoperability without limiting commissioning or control flows defined in CSA Specifications. The user must be able to choose which ecosystem to use. The Supported Operating Environment as a whole does not represent certifiable Alliance technology.

In case there is doubt whether a component vendor declared SOE qualifies as such, it is under the discretion of the Alliance Director of Certifications to make a judgment call. In case the component vendor disagrees with the judgment of the Alliance Director of Certifications, the vendor can appeal the decision as noted in section 2.6 who created the original component Specification for final clarification.

Software Component: umbrella term referring to software components irrespective of their kind, i.e. both UIC and Underlying Software Component.

Underlying Software Component: An Underlying Software Component is a piece of software that supports, at minimum, all the mandatory requirements for an Underlying Software Component Specification. An Underlying Software Component is intended to be used by the User Interface Component (UIC), possibly with other intermediate Underlying Software Components.

An Underlying Software Component may be a separate piece of software or be integrated into the Supported Operating Environment. In the latter case of a fully integrated underlying software component a change to the package containing the certified underlying software component would require recertification, unless the component is upgradeable separately to the complete package.
**Certified Software Component:** A Software Component that has successfully completed the Software Component Certification Program and obtained certification.

**User Interface Component (UIC):** The component which on its next higher layer component interface is connecting to the user, and that performs functionality defined in a Connectivity Standards Alliance Specification, corresponding to at least one device type or role. The typical user of the user interface exposed by the UIC is human (using voice, a touchscreen, a command line etc), though there can be non-human consumers of this interfaces such as interfaces not covered by other CSA certification programs to remote cloud server(s), an AI controller, event scheduler, protocol bridge or an additional UIC.

A UIC definition SHALL contain a list of dependencies.

**Type 1 UIC:** A UIC implementing the Alliance-defined protocol functionality, by either not depending on one or multiple Certified Underlying Software Component(s) at all, or by extending the functionality provided by a Certified Underlying Software Component.

**Type 2 UIC:** A UIC NOT implementing any protocol functionality defined in the Connectivity Standards Alliance Specifications; It relies completely on the functionality provided by one or more Certified Underlying Software Component(s) (or implements any manufacturer-specific functionality), as exposed via the Next Higher Layer Component Interface.
Software Component Specification: A Specification defined by a Balloting Group/Sub-Group of a Working Group based on one or multiple Draft, Working or Adopted Specifications. The Component Specification defines the protocol layers and/or functionality blocks that shall be implemented and certified as a Software Component, and optional functionality blocks, if any. For that purpose, the Software Component Specification can simply refer to the appropriate sections of the main Specification. The Software Component Specification also defines the mandatory and optional functionality to be exposed to the Next Higher Layer and the functionality expected to be provided by the Next Lower Layer.

In addition, it defines Software Component dependencies. Further, the Balloting Group/Sub-Group of the Working Group defines the testing method for the Software Component.

A Balloting Group/Sub-Group of the Working Group may define multiple Software Component Specifications, based on the same or different Draft, Working or Adopted Specification(s).

A Software Component Specification is accompanied by a Software Component Test Specification, defining the functionality tests and the test method for the Software Component. The Software Component Test Specification may re-use tests and/or test methodology, incl. test tools, already defined for the covered functionality. Both Software Component Specification as well as Software Component Test Specification could be parts of existing documents as opposed to documents of their own.

Only Adopted Specifications shall be used for certification purposes.

Next Higher Layer Software Component Interface: A set of functionalities exposed to the next higher layer by the Software Component. The Balloting Group/Sub-Group of the Working Group can choose to define the Interface in abstract terms or, for improved interoperability and App reusability, to prescribe their exact implementation. The Balloting Group/Sub-Group of the Working Group also defines whether the specified Next Higher Layer Component Interfaces are Simple Interfaces or Complex Interfaces. A component may also expose both a Simple Interface as well as a Complex Interface in which case the next higher layer Software Component shall clearly state which of the two interfaces is being made use of.

The Software Component vendor is required to provide a test application or test instructions on how to drive the Software Component via its next higher layer component interface in order to execute all test cases required for certification.

Simple Interface: A Next Higher Layer Software Component Interface resulting in execution of Software Component behavior with limited variability and complexity (e.g. triggering the sending of a payload-less “On” command). Typically, a Simple Interface has no or few parameters and no specific certification test requirements for the caller of those Simple Interfaces are expected. Because of its limited complexity, the Simple Interface can be used by the UIC without a need for compliance testing.
The Component Specification defines which of the Next Higher Layer Software Component Interfaces are Simple Interfaces. The interface shall be so simple that the UIC shall not be able to operate the Software Component in a non-compliant way.

**Complex Interface:** A Next Higher Layer Software Component Interface of a Software Component is considered complex when it provides to the next higher level (UIC or another Software Component) the ability to create network packets that may result in impacting the security, conformance or ability to operate on the network of commissioned devices. The Complex Interfaces would typically have specific certification test requirements for the caller of those Complex Interfaces. The Software Component Specification defines which of the Next Higher Layer Component Interfaces are Complex Interfaces.

**Lower Software Component Interface:** Set of functionalities expected by the Software Component to be exposed by the next lower layer. The Balloting Group/Sub-Group of the Working Group can choose to define the Interface in abstract terms or, for improved interoperability and component reusability, to prescribe their exact implementation. Alternatively, the Balloting Group/Sub-Group of the Working Group can choose to only define the lowest layer interface (e.g. messages going over the air) based on the Component including any dependent component and the SOE.

The Lower Software Component Interface may refer to APIs as exposed by a communication protocol/module, or by the next higher level interface of a dependent underlying Software Component. In some cases it may be defined in terms of over the air frames sent/received by such communication module, or rely on dependent certification programs (e.g. BLE, Wi-Fi) to define them.

**Exemplary Test Platform:** The particular platform used to perform compliance testing of a Software Component. It is a particular instance of hardware, making use of a Supported Operating Environment. The Exemplary Test Platform on which the compliance testing was performed does not bind the Software Component Certification applicability to that particular hardware. The Exemplary Test Platform is used as an exemplary instance of Supported Operating Environments that implement the dependencies required by the Software Component; the Software Component Certification, once granted, applies to all Supported Operating Environments with the same defined set of Component Dependencies. An example of an Exemplary Test Platform may be a Raspberry Pi platform with a particular OS version or a smartphone with a particular minor and major version of a particular OS.

**Component Dependencies:** Component Dependencies are to be defined by the Balloting Group/Sub-Group of the Working Group. Necessary conditions other than those specified by Next Lower Layer Component Interface, required for proper operation of the Component. Examples of common dependencies are libraries to handle crypto and network management; these could be libraries provided by a specific platform, or more generic ones like OpenSSL.

The Component Dependencies section of the Component Specification should address aspects like: Lowest supported version of the operating system, incl. major and minor version, and whether subsequent minor/major releases of the operating system will require component recertification; dependencies on additional software modules/libraries, if any; and hardware dependencies, if any; and which changes in the dependencies require Component recertification. The Balloting Group/Sub-Group of the Working Group may decide on additional conditions for Software Component Certification, such as how many versions of the component dependencies (for example, OS versions) are required for certification.

The certification program may define whether a Software Component can use another Certified Software Component to satisfy a dependency. Correct definition of the Component Dependencies shall allow for reuse of certified Software Components across matching platforms without recertification, while enabling proper operation of the Next Higher Layer, including the App. It is the responsibility of the WG defining the particular Software Component Certification Program to balance it.

10.2 Policy for Underlying Software Component Certification Program

The Software Component Certification Program is only available to Alliance Promoter, Participant and Adopter Members, i.e. only those Membership classes can certify a Software Component.

The only authority to grant Software Component Certification to an Underlying Software Component or UIC is Connectivity Standards Alliance. No test service provider or any other entity is authorized to grant or pursue Software Component Certification requests on behalf of Connectivity Standards Alliance.
The Software Component Certification Program does not waive or change the requirement for certifiers of Products to be Members of the Alliance, to follow the Alliance Trademark and Logo Usage Guidelines and Terms, or to comply with any policies of Connectivity Standards Alliance.

10.2.1 Underlying Software Component Testing

An Underlying Software Component must have successfully undergone full and complete compliance testing as defined in the respective Underlying Software Component Test Specification, running on an Exemplary Test Platform of the Underlying Software Component implementer’s choice.

The Exemplary Test Platform on which the compliance testing was performed does not bind the Underlying Software Component Certification applicability to that particular platform. The Exemplary Test Platform is used as an exemplary instance of Supported Operating Environments that implements the dependencies required by the Component; the Underlying Software Component Certification, once granted, applies to all Supported Operating Environments that can run the Software Component.

An Underlying Software Component successfully tested for compliance on an Exemplary Test Platform is certified for use on every other platform that fulfills all the same set of requirements on the Component Dependencies. Any modifications (by the end user) to the component will void the compliance promise of certification.

The Underlying Software Component vendor shall declare which Dependencies (range) their Underlying Software Component is applicable to. (As example the Underlying Software Component vendor shall declare which version, or range of versions of an OS, the Underlying Software Component is intended to run on). The Underlying Software Component vendor shall also explain why the chosen Exemplary Test Platform is representative of the range of SOEs. The Balloting Group/Sub-Group of the Working Group shall determine which are the permitted Dependencies for an Underlying Software Component.

The certification documentation of the Underlying Software Component SHALL clearly list the platform configuration that was used during testing and provide sufficient traceability information to be able to repeat such tests in the future.

10.2.2 Certified Underlying Software Component Reuse

The purpose of certified Underlying Software Component reuse is to speed up time to market and minimize compliance testing effort, e.g. for different variants of hardware supported by the SOE which integrate the same certified Underlying Software Component.

A Software Component (including UIC and Underlying Software Component) references and consumes a set of Interfaces exposed by the Supported Operating Environment (and/or in case of the UIC, also the Underlying Software Component), which creates a well-defined Software Component/SOE relationship.

Underlying Software Component Certification may retain its validity for new or updated SOEs as long as towards the Alliance Director of Certifications it can be either proven by argument or backed by testing by the Underlying Software Component vendor that these new or updated SOEs do not break compliance. Especially, when there are no changes in the underlying APIs of a given SOE against which original certification was obtained, then certification may be inherited by newer versions of the SOE with the same APIs.

When there are no changes in any of the underlying interfaces that would affect protocol conformance, the Underlying Software Component certification SHALL carry over to newer version of the SOEs exposing the same interfaces (i.e. a Software Component is certified for use on all SOEs exposing the same interfaces and does not require certification with the Alliance for those other SOEs). The certified Software Component can be used on underlying hardware configurations supported by the SOE(s) without further certification.
Such an extension to an additional, new or updated SOE is only possible within 3 years of the original certifications. After this period new certification is required.

Additionally, the Balloting Group or Sub-Group of the Working Group which originally specified the Underlying Software Component may suggest to TCOC for approval of a fastpath method to deal with new or updated SOEs for the specific Underlying Software Component. If new or updated SOEs, or any underlying dependent Software
Components require changes to the Underlying Software Component itself, re-certification of the Underlying Software Component is required.

10.2.3 Underlying Software Component Recertification

If the previously certified Underlying Software Component changes, the Underlying Software Component implemener shall submit the Underlying Software Component for re-certification in accordance with the appropriate Certification Policy program rules.

The table below provides examples illustrating the application of the Software Component program. It lists exemplary change type, and the resulting need for Software Component recertification and compliance retesting. The table also applies for the case where there are multiple changes between two Software Component versions. If they require different certification paths, then the most demanding path is applicable.

If a change type is not explicitly listed in the table, please contact the Alliance certification team for further guidance.

If the illustrative example listed in the table conflicts with the normative text of the certification policy, the certification policy takes precedence.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Compliance retest needed?</th>
<th>Recertification needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Underlying Software Component adds new CSA-defined functionality, e.g. device type, role</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Underlying Software Component Bug and Security fixes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Underlying Software Component Dependency Changes (non SOE updates)</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>* assessment of Dependency change to be made to determine if re-test &amp; certification needed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-CSA-technology related Underlying Software Component change and UI changes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dependent Certified Underlying Software Component changes</td>
<td>No*</td>
<td>No*</td>
</tr>
<tr>
<td>*recertification requirement is lifted for “version of the same Certified Software Component or switching to a Certified Software Component with a matching set of Component Dependencies”; other changes to the Dependent Certified Underlying Software Component may require recertification and retesting and shall be consulted with Alliance certification team</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOE updates (other than SW component dependencies)</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Additionally, the Balloting Group or SubGroup of the Working Group which originally specified the Underlying Software Component may suggest to TCOC for approval a fast path method for the recertification of Underlying Software Component.

10.3 Policy for User Interface Component (UIC) Certification Program

The User Interface Component Certification Program is only available to Alliance Promoter, Participant, Adopter and Associate Members, i.e. only those Membership classes can certify a User Interface Component.

The UIC Certification Program does not waive or change the requirement for certifiers of UIC Software Components to be Members of the Alliance, to follow the Alliance Trademark and Logo Usage Guidelines and Terms, or to comply with any policies of Connectivity Standards Alliance. A UIC vendor of a certified UIC
Software Component is eligible to use CSA certified logo/language as specified in the applicable CSA Brand Guidelines document(s).

The only authority to grant UIC certification to an UIC is Connectivity Standards Alliance. No test service provider or any other entity is authorized to grant or pursue UIC Certification requests on behalf of Connectivity Standards Alliance.

A UIC intending to use the Alliance’s logo and trademark must seek UIC Certification for the implemented functionality as specified below, and follow the rules for Component recertification.

A UIC seeking certification must declare if it makes use of one or more Certified Underlying Software Component(s), referencing their Certification ID, and list all the Underlying Software Component functionality used by the UIC via Simple or Complex Interfaces.

The certification documentation of the Underlying Software Component SHALL clearly list the platform configuration that was used during testing and provide sufficient traceability information to be able to repeat such tests in the future.

The individual Balloting Group/Sub-Group of the Working Group may suggest to the TCOC for approval a fastpath certification for the following case: Updates to a UIC Software Component for which the UIC Component vendor declares that the nature of the update is not of relevance to the performance of the CSA certified functionality. The Alliance Director of Certifications reserves the right to require recertification for the updated version in case s/he considers the requirements for a fastpath certification as defined by the respective Balloting Group/Sub-Group of the Working Group and agreed by the TCOC as not being met.

10.3.1 UIC Type 2, making use of only Simple Interfaces of a Certified Underlying Software Component

If a UIC seeking certification makes use of one or more Certified Underlying Software Component(s) without change and only implements Simple Interfaces provided by the Certified Underlying Software Component, then the UIC does not require compliance testing. However, a UIC which only uses Simple Interfaces and wishes to use the certification logo MUST still certify.

Once granted, the certification of the UIC remains valid for subsequent releases of the UIC and does not require renewed certification application, as long as the UIC uses the same Certified Underlying Software Component and only Simple Interfaces, the same or modified set.

This could, for instance, include vendor specific functionality using the Certified Underlying Software Component.

10.3.2 UIC Type 2, making use of Complex Interfaces of a Certified Underlying Software Component

If a UIC seeking certification makes use of one or more Certified Underlying Software Component(s) without change and only implements Interfaces as provided by the Certified Underlying Software Component without change, whereby any of those are Complex Interfaces, then the UIC requires compliance testing, the testing covering the usage of the Complex Interfaces.

Once granted, the certification of that UIC remains valid for subsequent releases of the UIC, as long as the UIC uses the same Certified Underlying Software Component, only uses Interfaces provided by the Certified Underlying Software Component, and an unmodified set of Complex Interfaces, and any set of Simple Interfaces, the same as originally certified or a modified set, with added/removed Simple Interfaces. Such Certified UIC does not require recertification.
10.3.3 UIC recertification: usage of Complex Interface of Certified Underlying Software Component

Addition of an Interface functionality not supported by the user Certified Underlying Software Component or addition of a new Complex Interface exposed by the Certified Underlying Software Component in a subsequent release of a Certified UIC requires recertification.

10.3.4 Change of Certified Underlying Software Component

A Certified UIC that was certified with a particular version of a Certified Underlying Software Component, does not require recertification upon integration of a subsequent version of the same Certified Underlying Software Component or switching to a Certified Underlying Software Component with a matching set of Component Dependencies within 3 years of its original certification.

10.3.5 Type 1 UIC (not making use of Certified Underlying Software Component)

If an UIC seeking Certification does not make use of any Certified Underlying Software Component, or implements parts of the functionality of an underlying Software Component (e.g. adding missing Interfaces or providing an improved implementation of an Interface functionality), that UIC requires certification of all the implemented functionality, and full re-certification of any subsequent releases.

The UIC vendor has to declare which Dependencies (range), incl. SOE, their UIC is applicable to. (For example, the UIC vendor shall declare which version, or range of version of an OS, the UIC is intended to run on.) The Balloting Group/Sub-Group of the Working Group shall determine which are the permitted Dependencies for a UIC.

10.4 Guidelines for Software Component Certification Program

The Software Component Specification will have defined Next Higher Layer/Lower Software Component Interface. This Interface may define specific function calls that can be passed in and out of the Software Component. In the Software Component Specification each function shall be categorized as either simple or complex depending on its variability and complexity, computational resources and/or other dependencies which the function has.

The definition of both Next Higher Layer/Lower Software Component Interfaces and the category of function shall be the responsibility of the respective Balloting Group/Sub-Group of the Working Group defining the Software Component.

The Balloting Group/Sub-Group of the Working Group is responsible for defining a complete test plan for the Software Component defined by that Balloting Group/Sub-Group of the Working Group, together with the method to test such a Software Component.
11 CERTIFICATION PROGRAMS

This Section describes existing Certification Programs, in terms of requirements and additions to the common process. Except where noted, each Product, Compliant Platform, or SW Component Certification Program uses the common rules and process described in the previous Sections. When there is a choice of options (i.e. Golden Units or no Golden Units), or dependencies (e.g. Platform vs. Product) then this is described here.

11.1 Compliant Platform: Zigbee PRO Stack

The Zigbee PRO Stack may be used under a number of Standards. Each Standard specifies the Stack revisions that it requires, or at least the minimum required.

11.1.1 Zigbee PRO Compliant Platform Certification Program

Platforms submitted for testing against the Zigbee PRO Compliant Platform Certification Program must be built on compliant IEEE 802.15.4 PHY/MAC layers. Compliance to IEEE 802.15.4 shall be determined by successful completion of the testing requirements described on document 14-0332 (Zigbee IEEE 802.15.4 Level Test Specification) at one of the CSA authorized test laboratories.

The Platform implementation SHALL conform to these Stack Specifications as appropriate to the declared PICS:

- 802.15.4-2011 or later as required by the Zigbee PRO Specification
- Zigbee PRO Specification
- Zigbee Green Power Proxy Basic and all other Zigbee Green Power components remain as optional features of the Zigbee PRO Specification.
  - Any Platform which implements any of the Zigbee Green Power features (including Proxy Basic) will be subject to ALL applicable testing.
  - Upon successful completion of the certification process, Platforms implementing any Zigbee Green Power feature will be identified as such in the Compliant Platform listing on the Alliance’s public website.
- Zigbee Direct functionalities remain as optional features of the Zigbee PRO Specification
  - Any Platform which implements any Zigbee Direct features will be subject to ALL applicable testing
  - Upon successful completion of the certification process, Platforms implementing these Zigbee Direct features will be identified as such in the Compliant Platform listing on the Alliance’s public website.

The program SHALL be defined by the following Sections, and specific Sections that pertain to a Compliant Platform (not a Certified Product):

1) Section 2 CSA Certified Program
2) Section 3 Testing
3) Section 4 Golden Unit
   a. In addition to the generic Golden Unit requirements defined in section 4, the Zigbee PRO Compliant Platform Golden Units SHALL also fulfill the following requirements:
      i. Shall be capable to act as a Zigbee Coordinator, Router and End Device;
      ii. Shall support all device operation (e.g., Zigbee Trust Centers, Network Managers, etc.)
4) Section 5.2 Revisions to Specifications
   a. The grace period SHALL be recommended by the Working Group as part of the 1.0 approval.
5) Section 6 Certification by Similarity, incl. Section 6.8 MAC/PHY Retest Requirements for Compliant Radios, with the additional rules for PHY spot checks:
   a. Full test (all test cases) of the first and last channel in the band (Channel 11 and 26 for 2.4 GHz)
   b. Spot check for the rest of the channels (2 channels per test case)
11.1.2 Zigbee Stack Software Component Certification

A software component implementing the Zigbee PRO stack, as defined in the Zigbee Direct Specification [R9], Section C.4.

In case the implementation under test is based on an implementation that has previously achieved ZCP certification and the resulting Zigbee Stack Software Component fulfills all of the following requirements:

- the Zigbee Stack Software Component is based on a Certified Zigbee PRO Compliant Platform implementation, unmodified with the exception of modifications required for porting to a new SoE;
- The Unmodified Certified Zigbee PRO Compliant Platform implementation that the Zigbee Stack Software Component is based on is NOT older than three years;
- The Zigbee Stack Software Component implements the Zigbee Stack Software Component Specification [R9], Section C.4;

then only a subset of testing as defined for a Zigbee Stack Software Component (ZDSC-I) in the Zigbee Direct Test Specification [R8] is required to prove compliance.

In case the Zigbee Stack Software Component implementation under test fails to meet any of the requirements above the Zigbee Stack Software Component SHALL comply with these points instead:

- The Zigbee Stack component Specification
- All test cases defined for a Zigbee Stack Component (ZDSC-N) in the Zigbee Direct Test Specification [R8] are required to prove compliance.

11.2 Certified Product based on Zigbee PRO Compliant Platform

11.2.1 Legacy Profile Product Certification Program

A legacy Profile Standard is built upon the Zigbee PRO Stack. A Product implementation SHALL be built upon a Zigbee PRO Compliant Platform and conform to the Zigbee PRO Stack Specification revision as required by the Profile Standard:

The Product implementation SHALL conform to these Standard Specifications as appropriate to the declared PICS:

- Zigbee Cluster Library
- A legacy Profile Standard, such as ZHA, ZSE, ZLL, ZBA, etc.

The program SHALL be defined by the following Sections that pertain to a Certified Product (not a Compliant Platform):

1) Section 2 CSA Certified Program
2) Section 3 Testing
3) Section 4 Golden Unit
4) Section 5.2 Revisions to Specifications
   a. The grace period SHALL be recommended by the Working Group as part of the 1.0 approval.

Note: After the grace period following the release of Zigbee 3.0 Standard, there will only be a Legacy Profile Product Certification Program for Zigbee Smart Energy (ZSE).
11.2.2 Zigbee 3.0 Product Certification Program

The Zigbee 3.0 Standard is built upon the Zigbee PRO Stack. A Product implementation SHALL be built upon a Zigbee PRO Compliant Platform and conform to the Zigbee PRO Stack revision as required by the Zigbee 3.0 Standard:

The Product implementation SHALL conform to these Standard Specifications as appropriate to the declared PICS:

- Application Architecture
- Base Device Behavior Specification
- Green Power Specification requirements for a Zigbee Router (Green Power Basic Proxy)

  a. Zigbee Green Power Proxy Basic is a mandatory feature for all Zigbee 3.0 routing capable devices. However,

     i. If the Zigbee 3.0 routing capable Product was built using a Zigbee Pro Compliant Platform which implements (and was properly certified for) the Zigbee Green Power Proxy Basic feature and it has not been modified, the Zigbee 3 Product will only be subject to a SINGLE Zigbee Green Power Proxy Basic test case as follows:

        1. Test Case 5.3.1.4 if the Compliant Platform used was certified before August 1, 2017
        2. Test Case 5.4.1.23 if the Compliant Platform used was certified on or after August 1, 2017

     ii. If the Zigbee 3 routing capable Product was built on a Zigbee PRO Compliant Platforms which DOES NOT implement the Zigbee Green Power Proxy Basic feature or HAS NOT been properly certified for it (or it has been modified), then the Product is subject to ALL applicable Zigbee Green Power Proxy Basic test cases.

- Zigbee Direct Specification requirements for a Zigbee routing capable Products implementing Zigbee Direct Device (ZDD) functionality

  a. In case the Zigbee routing capable Products additionally supports some or all of the features of a Zigbee Direct Device (ZDD), all test cases outlined for such a device in the Zigbee Direct Test Specification [R8] apply. However,

     i. If the Zigbee 3.0 routing capable Product was built using a Zigbee Pro Compliant Platform which implements (and was properly certified for) all mandatory and any optional ZDD features that the Zigbee Pro Compliant Platform implements AND the Product uses, and the ZDD functionality implementation has not been modified, the Zigbee 3.0 Product making use of all these ZDD features, or a subset of the optional and all mandatory features will only be subject to a SINGLE ZDD testcase from [R8] as follows:

        ZDD-CS-TC-02 (Verify the DUT ZDD can form a centralized security network with no TLV parameters)

     ii. If the Zigbee 3 routing capable Product was built on a Zigbee PRO Compliant Platforms which DOES NOT implement the ZDD feature or HAS NOT been properly certified for it (or it has been modified), then the Product is subject to ALL applicable ZDD test cases

- Zigbee Cluster Library
- One or more application device Specifications

The program SHALL be defined by the following Sections that pertain to a Certified Product (not a Platform):

1) Section 2 CSA Certified Program
2) Section 3 Testing
   a. Including Section 3.3.1 Connectivity Standards Alliance Test Harness
3) Section 5.2 Revisions to Specifications
   b. The grace period SHALL be recommended by the Working Group as part of the 1.0 approval.
11.3 Certified Product: Green Power Device

The Green Power Device Stack supports a single Green Power Device Standard. There is no Complaint Platform Program.

11.3.1 Green Power Device Product Certification Program

The Product implementation SHALL conform to these Standard Specifications as appropriate to the declared PICS:

- 802.15.4 2011 or later as required by the Green Power Specification
- Green Power Specification requirements for a Green Power Device

The program SHALL be defined by the following Sections that pertain to a Certified Product (not a Platform):

1) Section 2 CSA Certified Program
2) Section 3 Testing
   a. Including Section 3.3.1 Connectivity Standards Alliance Test Harness.
3) Section 5.2 Revisions to Specifications
   b. The grace period SHALL be recommended by the Working Group as part of the 1.0 approval.

11.4 RF4CE

The RF4CE Stack supports a single Remote Control Standard.

11.4.1 RF4CE Compliant Platform Program

The Platform implementation SHALL conform to these Stack Specifications as appropriate to the declared PICS:

- 802.15.4 2006 or later as specified by RF4CE Specification
- RF4CE Specification

11.4.2 Remote Control Product Certification Program

The Remote Control Standard is built upon the RF4CE Stack. A Product implementation SHALL be built upon a Zigbee RF4CE Compliant Platform and conform to the RF4CE Standard revision as required by the Remote Control Standard.

The Product implementation SHALL conform to the Standard Specifications as appropriate to the declared PICS:

- ZRC Specification

The program SHALL be defined by the following Sections that pertain to a Certified Product (not a Platform):

1) Section 2 CSA Certified Program
2) Section 3 Testing
3) Section 4 Golden Unit
4) Section 5.2 Revisions to Specifications
   a. The grace period SHALL be recommended by the Working Group as part of 1.0 approval.

11.5 Matter

Two types of solutions may be granted Matter Certification:
1. Matter Hardware Solution (Section 11.5.1)
   - A Matter Hardware Solution is a purpose-built piece of hardware that provides capabilities of Matter device type(s) and role(s).

2. Matter Software Component Solution (Section 11.5.2)
   - A Matter Software Component Solution is a piece of software that runs within a context of an SOE that supports, at minimum, all the mandatory requirements for a Matter Software Component.

For cases where a Matter solution supports both a Matter Hardware Solution and a Software Component Solution running on an SOE, the Matter solution may be certified independently as a Matter Hardware Solution and a Matter Software Component Solution, or the device may be certified for all functionality as a Matter Hardware Solution.

### 11.5.1 Matter Hardware Solution

Matter Hardware Solutions submitted for testing are complete solutions. A compliant Matter Hardware Solution shall conform to the Matter Standard Specification (for interoperability) including the cluster(s) from the cluster library and device type(s) supported by the solution.

#### 11.5.1.1 Matter Dependent Certification Programs

Matter does not certify network and application layer solutions separately; the Matter Hardware Solution certification relies on dependent certification by Dependent Certification Programs (DCP).

Dependent certification provides a mechanism for a Matter Hardware Solution developer to attest to the certification of their products connectivity capabilities (hardware and software) certification to the minimum
Matter requirements for each of the different possible connectivity capability options. This allows for certification to be done by the IC device manufacturer, a module or platform manufacturer or the actual Matter Hardware Solution manufacturer and from a Matter certification perspective is inherited if or when it is used in instantiations that incorporate that externally certified dependent portion.

The following are the current DCP supported by Matter:

- Bluetooth SIG: Bluetooth LE v4.0 or later for an end product type as defined by Bluetooth
- Ethernet Compliance: Showing evidence of successfully passing self-defined and self-testing of IEEE PMA (Physical Media Attachment). See IEEE 802.3-2015 or later (Clause 40 for 1000Base-T, Clause 22/38 for 100BASE-T, and Clause 14 for 10Base-T) or later for a description of PMA.
- Wi-Fi Alliance Certification Program: Wi-Fi 4 (802.11n) or later
- Thread Group Certification Program: Thread 1.3.0 or later

Compliance to the dependent certifications for each of the Matter Hardware Solutions supported connectivity capabilities is verified via questions regarding Matter Certification Attestation when filling out the Declaration of Conformity and SHALL be answered along with other product and certification related questions when seeking CSA certification of a new or revised/updated Matter solution.

11.5.1.2 Matter Recertification for SDK Releases

The Matter SDK is expected to be released in a scheduled cadence or upon some urgency due to a major security fix, Specification modification, or maintenance release with bug fixes even if the spec is not modified and there are no security fixes. Since SDK software updating indicates a change in a previously certified device, by Matter recertification policy, the SDK updated device needs to go through the recertification process. Depending on the scope of the device change, the CSA recertification policy requires either document submission or testing verification by an Authorized Test Laboratory. Depending on the scope of changes, either spot testing or full testing can be conducted. The policy details are described in the following context with respect to testing requirement categorization. If a vendor is not certain of which recertification testing method to apply, a vendor may seek advice from the Alliance Director of Certifications before recertification submission. The policy prescribed here is only applicable to Matter Hardware Solution recertification. Matter Software Component Solution recertification policy can be found in Section 11.5.2.

The following diagram represents the overall device recertification process for recertification testing of SDK release device updates.
11.5.1.2.1 SDK release update requiring SDK recertification testing by an Authorized Test Laboratory

If new PICS items are added compared to the previously certified Matter device, a device needs to go through recertification testing via an Authorized Test Laboratory in case of

- Addition of new mandatory features
- Addition of new optional features if implemented by the previously certified device
- Modification of existing mandatory and optional features
- Security/Bug fixes

11.5.1.2.2 SDK release updates requiring no SDK recertification testing

The following device changes incurred during SDK release update can be exempted from SDK recertification testing

- Modification related to compilation and integration of SDK into the device
- Removing Matter optional features not implemented by the device
- Disabling or removing features subsequently declared to be provisional
- Vendor specific extension implementation not defined in the Matter Specification
- Diagnostic interface addition/removal
- Renaming a bundle change

11.5.2 Matter Software Component Solution

This section covers the Matter Working Group defined policies for Software Components Certification. Matter Software components include both User Interface Components (UIC) e.g. Applications, and Underlying Software Components e.g. OS-specific library. Refer to Section 10 Software Component Certification for policies that are not explicitly covered.

A Matter Software Component is an implementation of the Matter Specifications. To qualify for the Matter Software Component Certification program, a Software Component shall meet the following requirements:

1. Should run within the context of a SOE
2. Should not itself be an attestable/commissionable Matter Hardware Solution (see exceptions in Section 11.5.2.1)
3. Support only certifiable functionality within scope of the Certified Software Component (Section 11.5.2.1)

11.5.2.1 Certifiable Matter Software Component Functionality

Only the following functionality, along with application & utility cluster(s) required to support these, are certifiable under the Matter Software Component program:

- Commissioner (Matter Specification Section 5 and 6)
- Controller (Matter Specification Section 1.3)
- OTA Provider (Matter Device Library Section 2.4)
- Media Device Types:
  - Casting video player (Matter Device Library Section 10.3)
  - Content App (Matter Device Library Section 10.5)
  - Casting Video client (Matter Device Library Section 10.6)
  - Video remote control (Matter Device Library Section 10.7)
The list of certifiable Matter Software Component functionality may be revised in future Certification Policy revisions. In the case where a Software Component vendor requests additional certifiable functionality added to Matter Software Component policy, the Matter Steering Committee may propose revisions to the TCOC to approve proposed revisions.

Scope of testing for the Software Component will be based on capability declared in the PICS thus reflecting the certification of the declared Software Component functionality. All test cases applicable for the functionality shall be run.

Matter Software Components shall use the Software Component PICS identifier to indicate it is a Software Component Solution and not a Hardware Solution.

11.5.2.2 Matter Software Component Certification Categories

The Matter software component certification program is structured around the following categories:

1. Matter capable UIC making use of Certified Component
2. Matter SW Component

The following flow chart will help determine which certification category the Matter Software component falls under:

For cases where a Matter device supports both a Matter Hardware Solution and a Software Component Solution running on an SOE, there are two options for certification:

- either, Matter device shall be certified independently for the Matter Hardware Solution and for the Matter Software Component Solution functionality.
- or, the device shall be certified for all functionality as a Matter Hardware Solution.
11.5.2.2.1 Matter capable UIC making use of Certified Component

A Matter capable User Interface Component (MUIC) is an Application using a certified Matter Software Component and does not implement any protocol functionality defined in the Matter Specifications. The MUIC relies completely on the Matter functionality provided by one or more unmodified certified Software Components running on a SOE.

Example: Downloadable application (which displays Matter Logo & Branding) supporting Matter Commissioning & Controller functionality running on an SOE, that only uses APIs provided by a certified Matter Software Component residing in the SOE for Matter functionality.

Matter Software Components that use the Matter SDK only expose Simple Interfaces, and, if a MUIC uses such a certified Software Component, Matter compliance testing is not required for certification of the MUIC.

However, necessary documentation is required to be submitted to the CSA for approval for Certification of the MUIC. This is equivalent to Section 10.3.1 UIC Type 2, making use of only Simple Interfaces of a Certified Component.

A Matter Software Component may choose to expose Complex Interface(s) that is not part of the Matter SDK, and, if a MUIC uses such a Complex Interface, Matter compliance testing would be required for certification of the MUIC, as described in the following sections:

- Section 10.3.2 UIC Type 2, making use of Complex Interfaces of a Certified Component
- Section 10.3.3 UIC recertification: usage of Complex Interface of Certified Component

11.5.2.3 Certification of Matter Software Component

A vendor may build an Underlying Software Component or UIC (Application) that implements CSA-defined protocol functionality, but does not use a certified Software Component, or extends the functionality provided by a certified Software Component. The vendor may certify the Software Component under the Matter Software Component category. Vendors shall submit their Software Component to an Authorized Test Laboratory for qualification testing.

This is equivalent to Section 10.3.5 Type 1 UIC (not making use of Certified Component). All Matter Software Component implementations shall be required to submit to an Authorized Test Laboratory for certification.

Examples of implementation of Underlying Software Component include:

- Software Component that implements CSA-defined protocol functionality
- UIC that implements CSA-defined protocol functionality

Once a Software Component is certified, it can be referenced by any MUIC for certification purposes using the Matter capable UIC making use of a Certified Component category (Section 11.5.2.2.1)

Vendor specific proprietary extensions outside the scope of the Matter protocol Specifications are not certifiable and hence should not be considered when evaluating for the Custom implementation category.

Recertification of Matter Software Component implementation should follow same policy as Section 10.2.3 Underlying Software Component recertification

11.5.3 Matter Security

11.5.3.1 Security Requirements

Matter Security Requirements are of two different natures:
1. Functional Security Requirements are specific to Matter secured protocol and interoperability (Security by design requirements). Those requirements are spread all over the Matter Specification [R11]; with the most important of them being explicitly described in Sections 13.2 to 13.5.


11.5.3.2 Functional Security Requirements Validation

The Functional Security Requirements will be validated as part of the Matter Test Plan, like the other requirements in the Matter Specification [R11].

11.5.3.3 Robustness Security Requirements Validation

The Robustness Security Requirements cannot be tested using an automated test suite as the implementation can vary by vendor. The Matter Certification Attestation questions contained in the Declaration of Conformity list the requirements in Section 13.6 “Security Best Practices” of the Matter Specification [R11]. The applicant indicates compliance and justification for each item and submits the form to the Alliance Director of Certifications as part of the certification documentation. The Alliance Director of Certifications will then review and determine if the form should be approved, rejected, or if changes are needed to complete the review. The following rules will apply:

- The Matter Certification Attestation questions contained in the Declaration of Conformity SHALL be completed by the applicant and this is mandatory to obtain CSA Certification (whatever its content - see hereafter).
- For Matter 1.0, most Robustness Security Requirements are optional best practice requirements tagged as “SHOULD” or “MAY” (see Matter Specification [R11] Section 13.6 “Security Best Practices”). So partial compliance or non-compliance to those “SHOULD” requirements will not block the certification. Note that this tolerance may become stricter in the future releases of Matter Specification where some “SHOULD” requirements could become “SHALL” or some new requirements could be introduced.
  - As an exception to the above, a few requirements of Matter Specification [R11] Section 13.6 are tagged as “SHALL”. For those requirements, non-compliance is not permitted and will block the certification.
- For each requirement a Yes/Partial/No/NA answer is mandatory, and further explanation may be provided by the applicant to describe how the requirement is fulfilled, why it is not fulfilled, or why it is not applicable.
- For confidentiality reasons, the filled forms are not public. The forms will remain exclusively in the hands of the Alliance Director of Certifications. For the same reasons, the level of details in the explanations may be adapted to protect applicant IP.
- The applicant may rely on inherited 3rd party security certification(s) of the product or its components (microcontroller, OS, Platform, Software Component or application) to corroborate the explanations. In that case, the inherited 3rd party security certification information SHOULD be reported in the Matter Certification Attestation questions contained in the Declaration of Conformity.


11.5.3.4 Certification Revocation

During the certification validity period, security vulnerabilities may be found in the product implementation. Security vulnerabilities may lead to the revocation of the certification.

Security incidents and security vulnerabilities are handled according to the Security Incident Response Plan document [R14].
11.5.3.5 Security Requirements when applying for Certification by Similarity

A product submitted for Certification by Similarity may or may not inherit the Security Requirements Referential of its parent. In addition to the Certification by Similarity Testing Exemption questions the Matter Certification Attestation questions contained in the Declaration of Conformity SHALL also be answered when applying for Certification by Similarity.

11.5.3.6 Security Requirements when applying for Certification Transfer

A product submitted for Certification Transfer will inherit the Security Requirements Referential of its parent.

11.5.3.7 Security Requirements when applying for Product Family Certification

For Product Family Certification, all the members of the Family may or may not be attributed the same Security Requirements Referential of the Family. The Matter Certification Attestation questions contained in the Declaration of Conformity SHALL be answered for the entire Family and will apply to all the members of the Family. The questions asked in the Declaration of Conformity are shown in APPENDIX B. It is recognized that some of the Matter Certification Attestation questions contained in the Declaration of Conformity may not apply identically to all members of the Family.

11.5.4 Matter Certification Attestation

Matter Certification Attestation questions are included in the Declaration of Conformity. A product developer applying for any type of Matter Certification (standard Certification, Certification by Similarity, or Product Family Certification) SHALL answer the Matter Certification Attestation questions.

The questions are to be answered to attest compliance to:
- Robustness Security Requirements as specified in Matter Specification [R11] Section 13.6 as they apply to Hardware Solutions and Software Component Solutions and
- Dependent Certifications on which the Matter Specification relies (e.g., Bluetooth SIG, Ethernet, Thread Group, Wi-Fi Alliance) as specified in Matter Dependent Certification Programs (see 11.5.1.1).

Questions used to support Matter Certification Attestation fall into three areas as described hereafter.

Product Identification:

Matter product information is included in the Declaration of Conformity, thereby allowing all relevant parties to associate the attestation with the product that is pursuing certification.

Robustness Security Requirements Attestation:

This section contains questions that allow product developers to declare compliance to the Robustness Security Requirements as specified in Matter Specification [R11] Section 13.6 “Security Best Practices”.

Note: Requirements 13.6.9.b and 13.6.9.e are not included in the questionnaire as they do not concern product design nor vendor process.

To answer these questions, the developer SHALL, for each security requirement question,

- State Yes/Partial/No/NA compliance
- Optionally supports compliance declaration with a brief explanation (For 3rd party security certification, the Certificate reference SHOULD be provided)

The security related questions apply to Hardware Solutions as well as Software Component Solutions. Some of the requirements may not fit well to both types of products. The vendor can use the “NA” selection for such requirements and support the claim with an explanation.
Dependent Certifications Attestation:

Where an underlying certification/compliance regimen requires its own certification (e.g., Bluetooth SIG, Ethernet, Thread Group, Wi-Fi Alliance), a Matter product developer SHALL provide proof (Certification Attestation) of having passed this certification at the time of applying for Matter certification. Please refer to Matter Dependent Certification Programs in Section 11.5.1.1 for more details.

The Certification Attestation should preferably be a Certificate number delivered by the scheme issuing the certification (where applicable) and allowing online verification of the certified product.

The applicant shall provide any information needed to unambiguously link the Certification Attestation with the Matter product.
APPENDIX A: CERTIFICATION BY SIMILARITY TESTING EXEMPTION REQUEST QUESTIONS

<table>
<thead>
<tr>
<th>Product Developer Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name:</td>
</tr>
<tr>
<td>Contact Name: (First, Last)</td>
</tr>
<tr>
<td>Contact Email:</td>
</tr>
<tr>
<td>Work Phone:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Original Certified Product Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
</tr>
<tr>
<td>Software Revision:</td>
</tr>
<tr>
<td>Hardware Revision:</td>
</tr>
<tr>
<td>CSA Certificate ID</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Submitted for Testing Exemption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
</tr>
<tr>
<td>CSA Specification(s) Rev.#(s) and any Errata at Time of Request</td>
</tr>
<tr>
<td>Software Revision:</td>
</tr>
<tr>
<td>Hardware Revision:</td>
</tr>
</tbody>
</table>

Note: Revision number is the number used to distinguish this specific build of the Product from a subsequent or prior one.
<table>
<thead>
<tr>
<th>Detailed Differences:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: Please explain in detail the differences between the Product currently on the Integrators List / Approved List and the item you are submitting for certification by similarity. (Please do not use terms that only your company or your specific industry understands.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Has the schematic changed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes: ☐ No: ☑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>If YES, Please Explain:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Have any components changed (including RF hardware):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes: ☐ No: ☑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>If YES, Please Explain:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
Has the CSA Component Enclosure Changed? (Structural, Material or Density)

| Yes: ☐ No: ☐ |

If YES, Please Explain:

| Does the change expose new functionality? |

| Yes: ☐ No: ☐ |

If YES, Please Explain:
<table>
<thead>
<tr>
<th>Has the firmware changed?</th>
<th>Yes: ☐ No: ☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>If YES, Please Explain:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Has the Product driver changed (if applicable)?</th>
<th>Yes: ☐ No: ☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>If YES, Please Explain:</td>
<td></td>
</tr>
</tbody>
</table>

Signature: _________________________________________________________________


## APPENDIX B: MATTER CERTIFICATION ATTESTATION QUESTIONS

Product Identification Questions

<table>
<thead>
<tr>
<th>Product Developer Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name:</td>
<td></td>
</tr>
<tr>
<td>Contact Name: (First, Last)</td>
<td></td>
</tr>
<tr>
<td>Contact Email:</td>
<td></td>
</tr>
<tr>
<td>Work Phone:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Submitted for Matter Certification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td></td>
</tr>
<tr>
<td>CSA Specification(s) Rev.#(s) and any Errata at Time of Request</td>
<td></td>
</tr>
<tr>
<td>Software Component Revision:</td>
<td></td>
</tr>
<tr>
<td>Hardware Revision:</td>
<td></td>
</tr>
<tr>
<td>Firmware Revision:</td>
<td></td>
</tr>
</tbody>
</table>
Robustness Security Requirements Attestation Questions

To fill-in the below questionnaire, the developer must, for each security requirement,

- State Yes/Partial/No/NA compliance
- (Optional) Justify compliance with a brief explanation (For 3rd party security certification, the Certificate reference should be provided)

<table>
<thead>
<tr>
<th>Cryptography (§13.6.1)</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.6.1.a Devices and Nodes SHOULD include protection against remote attacks that can be used to extract or infer cryptographic key material.</td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
<tr>
<td>13.6.1.b Devices SHOULD protect the confidentiality of attestation (DAC) private keys. The level and nature of protection for these keys may vary depending on the nature of the Device.</td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
<tr>
<td>13.6.1.c Nodes SHOULD protect the confidentiality of Node Operational Private Keys. The level and nature of protection for these keys may vary depending on the nature of the Nodes.</td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
<tr>
<td>13.6.1.d Cryptographic keys SHALL be randomly chosen using a cryptographically secure random number generator in accordance with algorithms defined in Section 3.1, “Deterministic Random Bit Generator (DRBG)”</td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
<tr>
<td>13.6.1.e Devices SHALL use non-repeating initialization vectors for a given session key.</td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Commissioning (§13.6.2)</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.6.2.a Manufacturers SHOULD control the number of DACs issued under their vendor ID.</td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
<tr>
<td>13.6.2.b Where practical, the setup code SHOULD NOT be photograph-able or visible when installed (e.g., QR code hidden with a flap).</td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>13.6.2.c</td>
<td>Uncommissioned Devices SHOULD only be available to be commissioned with some form of physical proximity user interaction (e.g. power cycle or button press).</td>
</tr>
<tr>
<td>13.6.2.d</td>
<td>For Devices subject to physical tampering (e.g. doorbell, camera, door lock, devices designed for outdoor use cases), the physical interaction to initiate commissioning and/or the setup code (QR code, NFC Tag or Manual code) SHOULD NOT be accessible to a physical attacker. E.g. setup code is removable or not on the device, the button used to initiate commissioning for the lock is inside the house.</td>
</tr>
<tr>
<td>13.6.2.e</td>
<td>A Commissioner or Administrator SHOULD only add Root Certificates that it trusts to a Node.</td>
</tr>
<tr>
<td>13.6.2.f</td>
<td>A device manufacturer SHOULD implement Basic Commissioning Method only for devices that adequately secure the Passcode.</td>
</tr>
<tr>
<td>Firmware (§13.6.3)</td>
<td>Compliance</td>
</tr>
<tr>
<td>13.6.3.a</td>
<td>Vendors of Matter implementations (including their suppliers of Matter functionality) SHOULD have a public vulnerability reporting mechanism and policy and actively monitor, identify and rectify in a timely manner security vulnerabilities throughout the publicly stated security lifecycle policy of the product. Typical responsible disclosure guidelines allow vendors from 60 to 120 days to patch a vulnerability, but the implementation of such a program is at each vendor’s discretion.</td>
</tr>
<tr>
<td>13.6.3.b</td>
<td>Devices SHOULD have a verified boot based in an immutable root of trust to verify the authenticity of firmware. Commissioners SHOULD only be loaded on a computing platform that has such a verified boot. If devices cannot support verified boot, devices SHOULD perform verification on any firmware update before applying the new firmware.</td>
</tr>
<tr>
<td>Section</td>
<td>Compliance</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Manufacturing (§13.6.4)</strong></td>
<td>Yes/Partial/No/NA</td>
</tr>
<tr>
<td><strong>13.6.4.a</strong></td>
<td>Fusing of Devices in production SHOULD be done to limit unintended access to hardware components. For example, vendors may disable debug interfaces, and program trust anchors for secure boot. There are multiple options to secure fusing on the factory floor (e.g., physically securing the fusing station, pre-fusing the silicon, etc).</td>
</tr>
<tr>
<td>Justification:</td>
<td></td>
</tr>
</tbody>
</table>

| **Resiliency (§13.6.5)** | Yes/Partial/No/NA |
| **13.6.5.a** | Matter implementations SHOULD implement resiliency features (e.g., responding to secure boot failures with recovery or error signaling mode) to detect and handle compromise. |
| Justification: | |

| **Battery Powered Devices (§13.6.6)** | Yes/Partial/No/NA |
| **13.6.6.a** | Battery powered Devices SHOULD respond to excessive queries by rate limiting (even limiting the rate to zero if desired). |
| Justification: | |

| **Tamper Resistance (§13.6.7)** | Yes/Partial/No/NA |
| **13.6.7.a** | Protection against physical attacks (especially those that impact cybersecurity) MAY be needed for some devices, as determined by the manufacturer. |
| Justification: | |

| **Distributed Compliance Ledger (§13.6.9)** | Yes/Partial/No/NA |
| **13.6.9.a** | Vendors SHOULD avail themselves of the DCL store-and-forward functionality so that they can control posting of data about their products to the DCL. |
| Justification: | |

| **13.6.9.c** | Vendors SHOULD run and use their own Observer Nodes and restrict access to it to make sure that it stays available to the vendors' DCL clients. |
| Justification: | |

| **13.6.9.d** | Vendors SHOULD protect DCL private keys in Hardware Security Module (HSM) equipped servers. |
| Justification: | |
Dependent Certification Requirements Attestation Questions

<table>
<thead>
<tr>
<th>Bluetooth Certification</th>
<th>Is Bluetooth utilized?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Matter products utilizing Bluetooth, Matter requires certification to Bluetooth LE v4.0 or later to support Matter commissioning.</td>
<td></td>
</tr>
<tr>
<td>If this device is Bluetooth based, proof of Bluetooth LE v4.0 or later certification is required. Please provide supporting details below:</td>
<td></td>
</tr>
<tr>
<td>If the above QDID has been obtained by Bluetooth Qualification Process with “No Required Testing” (inheritance) please give details about the original component/design (reference, whether it is a SW or HW IP, how it has been integrated and used):</td>
<td></td>
</tr>
<tr>
<td>Yes/No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethernet Certification</th>
<th>Is Ethernet utilized?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Matter products utilizing Ethernet, Matter requires IEEE PMA Compliance Attestation. See IEEE 802.3-2015 or later (Clause 40 for 1000Base-T, Clause 22/38 for 100BASE-T, and Clause 14 for 10Base-T) or later for a description of PMA.</td>
<td></td>
</tr>
<tr>
<td>If this device is Ethernet based, proof of IEEE PMA Compliance Attestation is required. Please provide supporting details below:</td>
<td></td>
</tr>
<tr>
<td>Self-test report to be provided with the registration file:</td>
<td></td>
</tr>
<tr>
<td>Yes/No</td>
<td></td>
</tr>
</tbody>
</table>
**Wi-Fi Certification**

<table>
<thead>
<tr>
<th>Is Wi-Fi utilized?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes/No</td>
</tr>
</tbody>
</table>

For Matter products utilizing Wi-Fi, Matter requires certification to Wi-Fi 4 (802.11n) or later.

If this device is Wi-Fi based, proof of Wi-Fi 4 (802.11n) or later certification is required. Please provide supporting details below:

If the above Certification ID has been obtained by the Wi-Fi certification option “QuickTrack” or “Derivative” (inheritance) please give information about the original component/design (reference, whether it is a SW or HW IP, how it has been integrated and used):

---

**Thread Certification**

<table>
<thead>
<tr>
<th>Is Thread utilized?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes/No</td>
</tr>
</tbody>
</table>

For Matter products utilizing Thread, Matter requires certification to Thread 1.3.0 or later.

If this device is Thread based, proof of Thread 1.3.0 or later certification is required. Please provide supporting details below:

If the above Certification Attestation has been obtained through Thread Certification Inheritance for Derivative Products, Modules, or End Products, please give information about the original component/design (reference, whether it is a SW or HW IP, how it has been integrated and used):