Functional Certification Program Policy

November 2017

Version 1.3.3

Table of Contents

Figures

Tables

Revision History

Table 1-1: Revision History

Date	Version	Description
March 19, 2015	1.0.0	Public Release
September 3, 2015	1.1.0	Public Release
March 17, 2016	1.1.1	Approved Policy Updates: • Removed reference to FIDO Ready™ • Removed Non-Member Access Agreement and Fee • Added the FIDO Vendor Self-Assertion Checklist as a Certification Request requirement. • Added the algorithm for reducing the test matrix when there are too many attendees in the Interoperability Event Criteria. • Added maximum number of individuals per implementation at Interoperability Events. • Updated mds@fidoalliance and info@fidoalliance to submission via the FIDO website or certification@fidoalliance.org • Clarified that Certification submission requirements (including fees) are per implementation (not per company).
May 18, 2016	1.2.0	On Demand Program Launch Approved by FIDO BoD April 19, 2016.
July 28, 2016	1.2.1	Clarifications of Certification Policy: • FIDO Test Tools o Updated terms for confidential Vendor ID o Clarified Test Tools are “free and open for use by all participants” • Certification Requests and Issuance • U2F Interoperability Testing Procedure • Specification Version Retirement • Event Registration o Clarified that by participating in the interop participants are agreeing to “provide free and open access to [their] implementation for all event participants”. • (New) Specification Version Retirement • Pre-Interop Event Testing o Added more details about how pre-interop testing works.

Date	Version	Description
		• (New) Certification Version Maintenance Approved by CWG for Publication on July 28, 2016.
September 8, 2016	1.2.2	Updates: • Clarifications to add "Functional" Certification (so as not to be confused later with Security or Biometrics Certification). • Interoperability Event - Event Logistics: 90 Day Interop Policy changed due to On Demand. • On Demand Registration Calendar updated from example table to screen shot of actual calendar on the FIDO Website. • Derivative Test Plan requirements now include Conformance Self-Validation Testing. • Specification Version Retirement clarifications that Derivatives cannot be applied for against versions of the specification that are retired. Approved by CWG for Publication on September 8, 2016.
December 1, 2016	1.2.3	Updates: • Test Tools o Added clarification that test tool results (and for UAF authenticators, Vendor IDs) will be verified prior to Interoperability Testing registration. • Interoperability Testing o Added text to support third-party lab hosting of Interoperability Events. o Added requirements for U2F Authenticators to submit metadata • Certification Issuance o Clarifications on how all certification fees must be paid in full before a Certificate will be issued. o Added requirements for U2F Authenticators to submit metadata Approved by CWG for Publication on December 1, 2016.
February 7, 2017	1.2.4	Updates: • Derivate implementations are bound to the Functional Certification Policy in place at the time of the original (base) certification.

Date	Version	Description
		Approved by the Board Certification Committee on February 7, 2017.
March 9, 2017	1.2.5	Updates: • Transport Certification requirements updated from Mandatory to Optional. Approved by CWG on March 9, 2017.
May 10, 2017	1.3.0	Updates to support Authenticator Level 1 and Level 2 Certification: • Added Sunset Dates for Functional Certification Policy. • Removed Change Control section (replaced by Sunset Dates) • Added Authenticator Level 1 Certification Testing Procedures in the Testing Procedures section, including mapping table to Authenticator Security Requirements that are tested during Conformance Self-Validation and Interoperability Testing. • Included Vendor Questionnaire instructions to explain the process for L1 Authenticators to record the Authenticator Level 1 Test Procedures within the VQ. • Added Authenticator Certification to the Certification Issuance section. Authenticators complying to this version of the policy and later will not be issued a Functional Certificate, they must continue to the Authenticator Certification program to receive an Authenticator Certificate. • Added reference to the Authenticator Certification Policy. Approved by CWG on May 4, 2017. Approved by Board Certification Committee on May 10, 2017.
June 15, 2017	1.3.1	Addition of the option to list multiple Derivatives on one Certification Request as long as they are from the same Base Certificate. Addition of Revocation section within Certification Issuance. Removal of some L1 Interoperability Requirements as decided by SRWG. Approved by CWG on June 15, 2017.

Date	Version	Description
July 27, 2017	1.3.2	Added that Revocation of a Certification must be approved by the Board Certification Committee. Approved by CWG on July 27, 2017.
November 16, 2017	1.3.3	Modified the definition of the Certification Availability Date to be the date the first Interoperability Event can be held for the version. Sunset Dates were modified to be “at least” 6 months for Servers, and “at least” 18 months for Clients and Authenticators. Clarifications on the Sunset Dates for Specification Versions and Sunset Dates for Policy Versions section titles. Approved by CWG on November 16, 2017.

1 Introduction

This document gives an overview of the policies that govern functional certification as part of the FIDO Functional Certification Program for both the U2F [1-1] and UAF [1-2] specifications. These policies are the requirements and operational rules that guide the implementation, process and ongoing operation of the functional certification program and create an overall framework for the functional certification program to operate within.

The sections following this overview focus on functional areas of the FIDO Functional Certification Program, starting with the Functional Certification Policies (Chapter 2) and then following through each functional area of the certification program:

- Overall Functional Certification Policies (Section 2),
- Functional Certification Process Overview (Section 3),
- Conformance Self-Validation (Section 4),
- Interoperability Testing (Section 5),
- Certificate Issuance (Section 6),
- Derivative Certification (Section 7),
- Certification Mark Usage (Section 8), and
- Certification Administration (Section 9).

1.1 Audience

The intended audience of this document is the Certification Working Group (CWG), FIDO administration, and the FIDO Board of Directors.

The FIDO certification website [1-4] reflecting the information in this document is intended to help implementers understand the process for receiving functional certification and the policies surrounding the functional certification program.

2 Overall Functional Certification Policies

The functional certification program as a whole is the responsibility of the FIDO Certification Working Group (CWG), with necessary oversights and approvals from the FIDO Board of Directors and collaboration with other FIDO Working Groups where needed. The CWG may, at the discretion of its members, create subcommittees and delegate responsibilities for all or some portion of the CWG's functional certification program responsibilities to those subcommittees. The Certification Secretariat is responsible for implementing, operating, and managing the functional certification program defined by the CWG.

Implementations seeking functional certification may be submitted by FIDO member organizations or non-member organizations. This document governs all such requests for functional certification.

Functional certification applies to all FIDO implementations including UAF server, UAF client, UAF authenticator, U2F server and U2F authenticator. Each implementation of one of these five services must be certified completely regardless if multiple implementations exist in the same device or service. Functional certification is associated with a specific implementation and not with a specific SDK or with a specific company: each implementation must be certified, and the certification stays associated with that implementation so long as the implementation does not change its functionality.

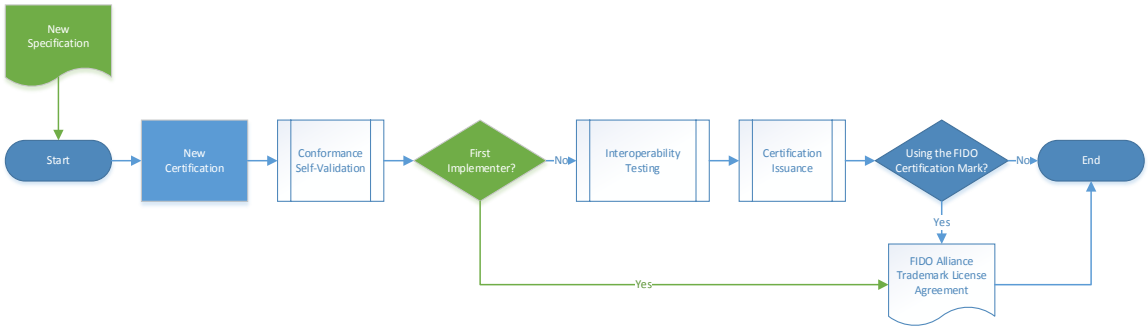
The following sections outline FIDO First Implementer, and Specification Version Retirement.

2.1 FIDO First Implementer

In the case of new versions of specifications, which may not have the minimum number of participants required for interoperability testing, a "First Implementer" program will be available. The program is designed for those companies that are the first to implement new specifications and wish to announce their conformance with those new specifications. First Implementer implementations will not be allowed to make the claim that they are "FIDO® Certified" but they may make the claim that they are a "First Implementer" if they meet the following criteria:

1. They have implemented the all mandatory portions of the specification for which they claim to be a first implementer.
2. They have passed Conformance Self-Validation testing with a test tool that minimally tests the mandatory features of the new specification.
3. The minimum number of required implementations are not available for a full matrix of Interoperability Testing (see Section 5.2.6).
4. They have executed a version of the FIDO Alliance Trademark Licensing Agreement [2-1] that allows them to make the claim of being a "First Implementer."

Figure 2-1: FIDO First Implementer Process



After the first FIDO Certifications are issued against a specification, and the required number of implementations to complete a full matrix of Interoperability Testing are available, it is no longer permissible to claim to be a "First Implementer". When this occurs, the Certification Secretariat will contact all "First Implementers" to notify the company that it must stop using the First Implementer branding, and if the implementation wishes to claim to be FIDO® Certified it must meet all the requirements of the certification program including passing interoperability testing with a full matrix of participants.

2.2 Specification Version Retirement (Sunset Dates for Specifications)

The FIDO Certification program upholds the latest standards developed by the FIDO Alliance.

When a new FIDO Specification version is approved as a Proposed Standard, and test tools are available for the new version, any implementations applying for FIDO Certification may implement the new version. A new version refers to a version within the same specification family, so for example, UAF 1.0 upgrading to UAF 1.1.

A specification version is considered Available for Certification (Certification Availability Date) when the first Interoperability Event can be held for the new version. In order for a valid, official, interoperability test there must be two of each implementation class, where each of the two implementations in each class must be from a different implementer company. See Interoperability Testing Event Criteria for more information.

The minimum time period between the Certification Availability Date of the new specification version and the Sunset Date of the previous specification version is:

- Servers: At least 6 months after the Certification Availability Date.
- Clients/Authenticators: At least 18 months after the Certification Availability Date.

After this deadline, the previous specification version will be Sunset (retired) from the Functional Certification Program and applications for implementations based on retired versions will no longer be accepted for Functional Certification. For more information on the latest Specification versions, please visit the U2F [1-1] and UAF [1-2] Specifications page.

2.3 Policy Version Retirement (Sunset Dates for Policy)

Unless a change is determined to be necessary to be implemented sooner by the CWG, changes will take effect according to the Functional Certification Policy Sunset Dates in the following sections.

When policies or testing procedures are changed, that change will be messaged to implementers through the appropriate email reflector.

The Functional Certification Policy Sunset Date is the last day a Vendor can submit an Application for Functional Certification against a version of the policy or test procedures. A Sunset Date is set from when a new version is published. The Sunset Date will be different depending on if the new version is a Major, Minor, or Patch version.

For the purpose of the Functional Certification Policy, the following definitions apply:

- Major: Includes incompatible changes. For example, an existing certification would no longer meet requirements.
- Minor: Added functionality in a backwards-compatible manner. For example, an existing certification still meets the requirements.
- Patch: Backwards compatible bug fixes. For example, editorial corrections that do not change any requirements.

The Functional Certification Policy and Interoperability Testing Procedures will be versioned Major.Minor.Patch.

For Major versions, Derivative Certifications will no longer be allowed against a version after the Sunset Date.

2.3.1 Functional Certification Policy Sunset Dates

Table 2: Sunset Dates - Functional Certification Policy

Version	Sunset Date		Derivative Certifications
Major	Servers	At least 6 months after Certification Availability Date	**No** Derivative Certifications allowed after Sunset Date.
	Clients Authenticators	At least 18 months after publication Certification Availability Date	
Minor	90 days after publication		Derivative Certifications allowed after Sunset Date.

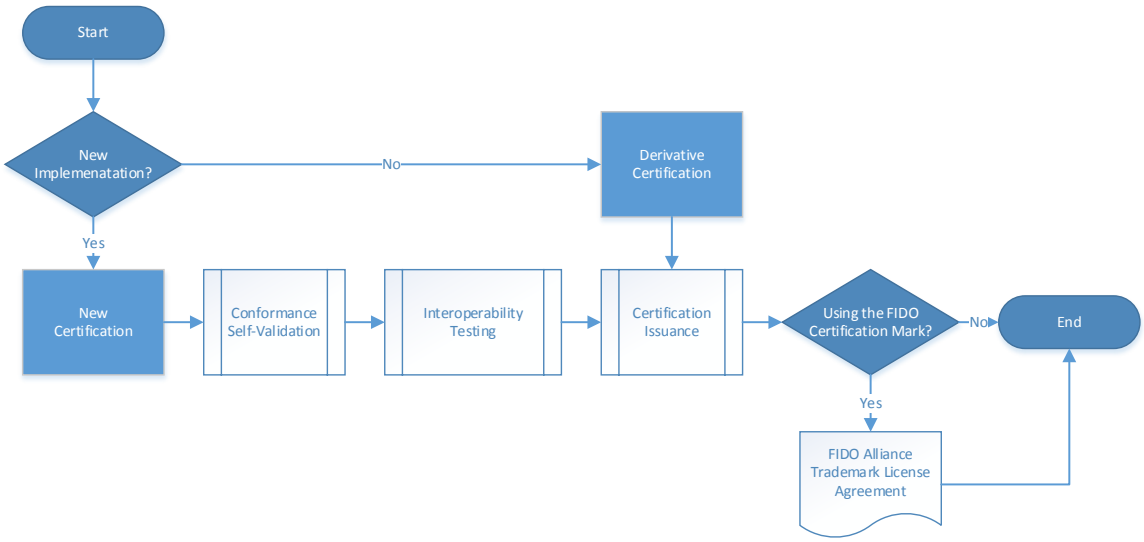
Version	Sunset Date	Derivative Certifications
Patch	No Sunset Date. Previous Version replaced immediately.	Derivative Certifications allowed after Sunset Date.

3 Functional Certification Process Overview

At the highest level, a FIDO implementation claiming to conform to either the UAF or U2F specifications must pass three steps in order to receive functional certification:

- Conformance Self-Validation: a FIDO implementation must be tested using the corresponding test tool to ensure that meets the tested aspects of the specification. Policies governing conformance self-validation are detailed in Section 3.
- Interoperability Testing: a FIDO implementation must participate in and demonstrate normative behavior during officially sanctioned interoperability testing. Policies governing interoperability testing are detailed in Section 5.
- Certificate Issuance: upon completing both conformance self-validation and interoperability testing, a FIDO implementation must submit the appropriate documentation and fees and receive notification of functional certification before claiming to be a certified FIDO implementation (See Section 6).

Figure 3-1: FIDO Certification Process



The steps above are required in order to receive functional certification. For a more detailed table outlining the certification steps see Table A-1.

Should a certified implementation be used in a new product or service, the resulting implementation will be deemed a Derivative Certification, which will be subject to fewer requirements for functional certification, see Section 7.

Any claim to functional certification or use of the Certification Mark by an uncertified product is prohibited. Please see Section 8 for more information.

In addition, should the specification change – either through a revised version of the specification or through published errata – there is no requirement for backwards compatibility. Implementations will not be required to re-certify should the standards, tools, or testing

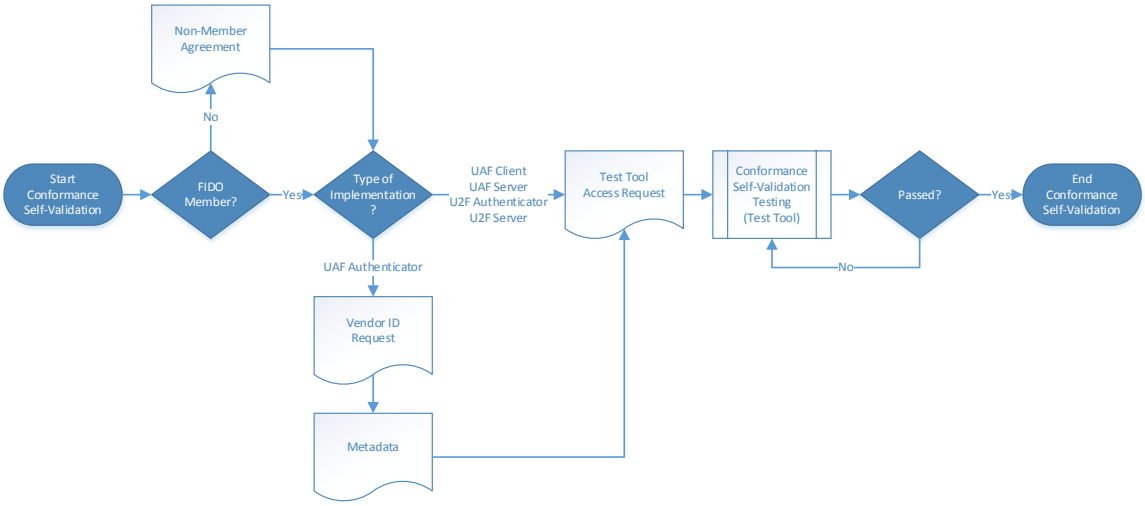
methodologies change. Functional certification is valid indefinitely and does not expire, regardless of the good-standing of membership.

4 Conformance Self-Validation

The guiding philosophy behind the Conformance Self-Validation is to "trust but verify" – trust that implementers are generally honest and want to create a market of compliant and interoperable implementations, but verify that Conformance Self-Validation was performed according to industry best practices.

It is the responsibility of the CWG to maintain the definition of Conformance Self-Validation. This is supported by the Certification Secretariat.

Figure 4-1: Conformance Self-Validation Process



4.1 FIDO Test Tools

The core of the Conformance Self-Validation process are the FIDO Test Tools. During the Conformance Self-Validation step, implementers must first request access to the Test Tool by completing a Test Tool Access Request [3-1].

UAF Authenticator implementers are required to register for a Vendor ID, by completing a Vendor ID Request [3-3] before completing a Test Tool Access Request. The Vendor ID serves as part of the AAID used in the UAF protocol. Only one Vendor ID will be allowed per company, with special exceptions being approved by the FIDO Executive Director. Unless otherwise requested through the Vendor ID Request Form, Vendor IDs will be publicly listed on the FIDO website as they are assigned. A confidential Vendor ID can be requested and the Vendor ID will remain confidential until the Functional Certification using the Vendor ID is made public. Any fees charged by FIDO for a Vendor ID will be applicable as a credit to any other certification program fees for the duration of 12 months. This includes any combination of certification, derivative, or other fees.

Implementers will be required to access the test tool corresponding to their implementation (e.g. U2F or UAF; client, server, or authenticator) and operate them according to the instructions provided by the test tools (UAF test tool [3-4], and the U2F test tool [3-5]). The test tools will create logs showing successful completion of the Conformance Self-Validation testing, which will

be required for both participation in Interoperability Testing as well as for submission to the Certification Secretariat for functional certification. The test tools will be hosted on a FIDO server. The test tools are free and open for use by all implementers. Implementers may use the test tools as frequently as required to validate their implementations.

Prior to performing an official Conformance Self-Validation test, an implementer must denote that the test that is about to be performed is an official test to be used as part of their implementation's functional certification. After passing an official test, the implementations may not change their configuration or implementation prior to the Interoperability Testing. In order to receive functional certification, the implementation must participate in an Interoperability Testing Event or schedule On Demand Testing within 90 days from the date of the successful Conformance Self-Validation test.

Conformance Self-Validation may be performed by the company that created the implementation, or may be outsourced to a third-party; however, in any event the implementer submitting for functional certification will be accountable for ensuring that Conformance Self-Validation was performed according to the policies, processes and standards required by the FIDO Functional Certification Program.

FIDO implementations must complete Conformance Self-Validation testing from start to finish without interruption or alteration in order to be considered a successful Conformance Self-Validation test. This prohibits rebooting (including crashing), reconfiguring, recompiling or otherwise changing the state of the implementation in ways that are not dictated by either the test tool or the test plan.

Conformance Self-Validation Test Results will be verified as complete before registration is allowed for Interoperability Testing. For UAF Authenticators, this includes a confirmation that the correct Vendor ID is used.

4.1.1 Test Tool Maintenance

From time to time, errors will be found in the test tools (e.g., crashing, bugs, non-compliance with specification) and vendors may be required to submit test tool change requests in order to have the test tool fixed. Test tool change requests will be subject to the dispute resolution process defined in Section 9.3. The Dispute Resolution Team is responsible for the management of test tool change requests.

4.2 Reference Implementations

The Certification Secretariat will maintain a list of reference implementations that can be used by organizations that are developing FIDO implementations and / or to be used in Confidential Certification. For servers, this will include the URL of the server and a point of contact for configuring access to the server. For clients and / or authenticators, this will include a list of commercially available FIDO Certified implementations, their model number or SKU, and a URL to an online retailer where the implementation can be purchased. FIDO will also have a Reference Implementation Library for the purpose of On Demand Testing, see section 5.3.2 for more information.

Implementers are not required to use reference implementations and they will be provided purely for the convenience of development and testing.

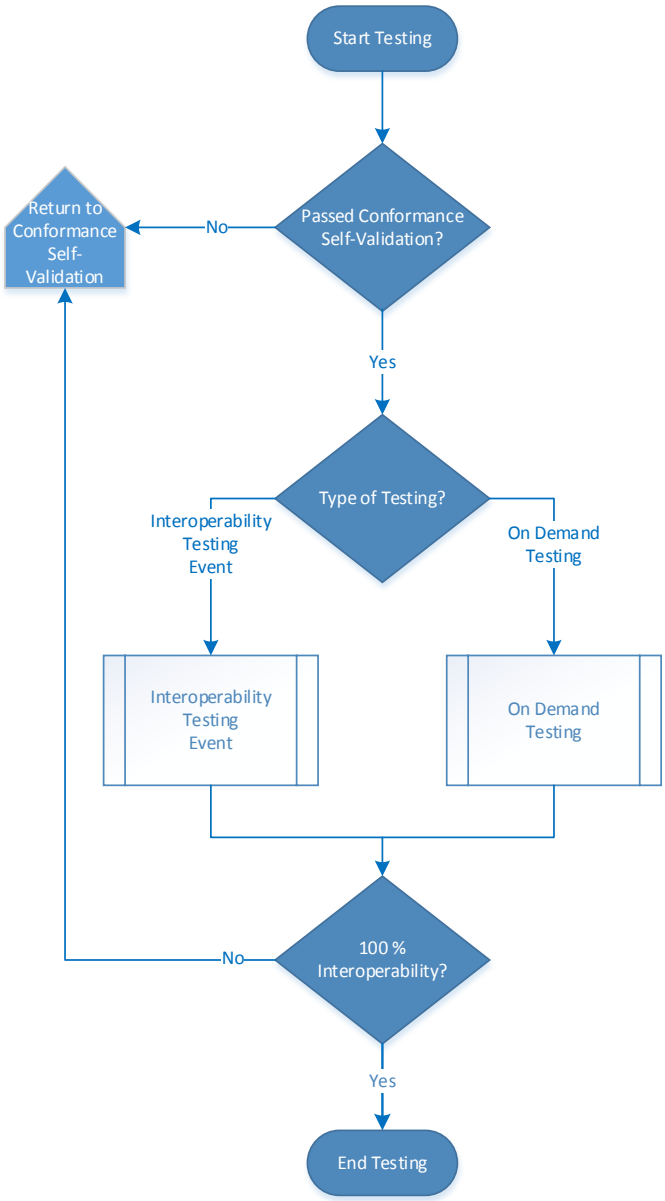
5 Interoperability Testing

Interoperability Testing is the responsibility of the CWG and is implemented and supported by the Certification Secretariat. Interoperability Testing is a required step in the Functional Certification process.

The following types of Interoperability Testing are supported for Functional Certification:

- Interoperability Testing Event (section 5.2)
- On Demand Testing (section 5.3)

Figure 5-1: Interoperability Testing Overview



5.1 Informal (Non-Certification) Testing

Other, informal (i.e. not certification eligible), interoperability testing opportunities will be made available to those interested in performing matrix testing for purposes of development and validation of implementations. These testing sessions are optional and do not count towards functional certification requirements. However, they are a good opportunity to work through bugs and prepare for functional certification. Informal Testing can include both new and existing technologies.

During the development of new specifications ("New Technology"), the FIDO Technology Working Groups typically hold informal interoperability testing events to test implementations of the specifications. Functional certification Interoperability Testing Events occur only after the specifications are published. Companies interested in getting involved with specification development and testing before specifications are released should get involved in a FIDO working group [4-9].

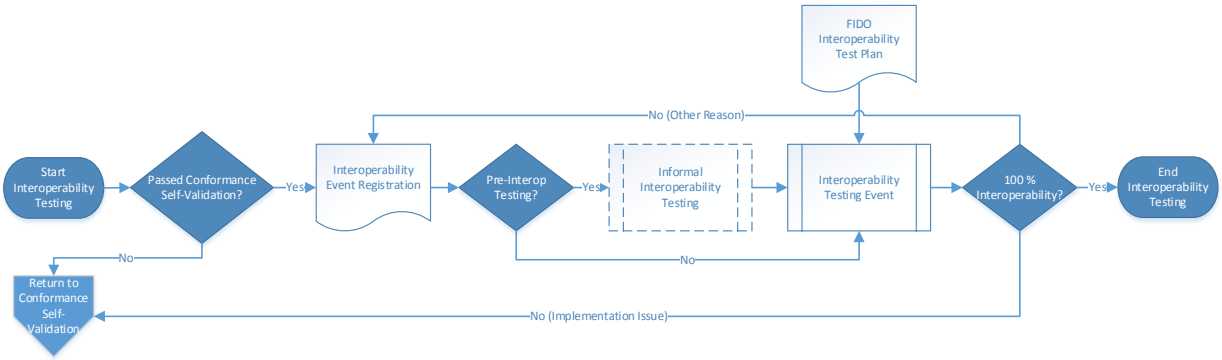
FIDO may utilize existing or develop new liaison relationships with other standards / certification bodies to have informal interoperability testing alongside other events FIDO members may already be attending. These informal interoperability testing events will be announced to the general membership when available and will also be published on the FIDO Upcoming Events page [4-10].

5.2 Interoperability Testing Events

Prior to attending an Interoperability Testing Event, an implementation must pass Conformance Self-Validation Testing, as described in Section 3.

Interoperability Events may be hosted by FIDO or by third-party Laboratories that have been approved and trained by FIDO.

Figure 5-2: Interoperability Testing Process



The following sections describe the logistics, registration, testing criteria, and testing procedures associated with FIDO Interoperability Testing Events.

5.2.1 Remote Interoperability Testing

To any extent possible, implementers are encouraged to attend Interoperability Testing Events in person, but remote accommodations may be provided for the benefit of implementers that cannot travel large distances to attend the events. Implementers are encouraged to volunteer their facilities for Interoperability Testing Events to facilitate multiple implementers being in the same place at the same time during Interoperability Testing Events. Due to the remote nature of testing, implementers are required to provide screen-sharing when remote as well as a webcam showing the client-side implementations (client or authenticator) being tested.

All remote testing requests must be approved at least 14 days prior to the event start date.

5.2.2 Event Logistics

The Certification Secretariat will be responsible for coordinating logistics for interoperability events, including scheduling, implementer communications, screen-sharing and webcam software, dial-ins, test matrices, and any other aspects required for an interoperability test.

For Specifications not supported by On Demand Testing (see section 5.3), Interoperability Testing Events will happen no less than once every 90 days, and may occur more frequently based on the direction of the CWG. For Specifications where On Demand Testing is available, Interoperability Events may be scheduled less frequently at the discretion of CWG.

Notification of upcoming events will be communicated to implementers, both through email, through the FIDO Alliance website, and through the Member's Calendar [4-1].

5.2.3 Event Registration

Implementers must register for interoperability events, and event registration will be closed 14 days prior to the event. To register, implementers must complete the interoperability event registration [4-2].

A non-disclosure agreement [4-3] is required to protect all test participants' confidential information.

Results from the Conformance Self-Validation step must be submitted through the FIDO test tool used to complete self-validation testing. These results must be confirmed by the Certification Secretariat at least 7 days before attending an interoperability event to ensure that the implementations are at least minimally complaint to the specifications.

Participants will be required to submit the names of every individual participating in the interoperability event, as well as the names and technical details of all of the implementations that will be participating. Individuals or implementations that are not declared prior to the event may be declined participation at the discretion of the Certification Secretariat. Due to space limitations in testing rooms we can guarantee space for only two individuals per implementation. Requests to bring more individuals will be entertained only if a request is made to the Certification Secretariat (certification@fidoalliance.org) at least two weeks in advance of the event, and if there is adequate space remaining. Vendors will be notified after the close of registration if their request has been accepted.

By registering for an interoperability testing event you are agreeing to participate and attend the entirety of the scheduled event and to provide free and open access to your implementation for all event participants. If individuals registered do not show up for the first half-day of testing (by 12 noon local time to the event), or if when they arrive late more than 50% of the test matrix has been completed, the implementation forfeits their eligibility for the event and the implementation will be removed from the test matrix.

5.2.3.1 Confidential Certification

A company may wish to pass Functional Certification with an implementation that is extremely secretive, or that may have extreme financial impact to an organization if it or details about it become known to the public or to its competition. In these circumstances, at the discretion of the FIDO Executive Director, an implementation may qualify for Confidential Certification.

The requirements for an implementation to pass Confidential Certification are the same as for any other FIDO Certified implementation. However, due to the sensitivity of an implementation attending an interoperability test, the Certification Secretariat will arrange for a group of companies to participate in interoperability testing that is mutually agreeable to both FIDO and the organization performing Confidential Certification; or the Certification Secretariat may arrange for FIDO Certified implementations that are commercially available to perform all the steps of interoperability testing without holding an Interoperability Event.

5.2.4 Pre-Interop Event Testing

Pre-Interop Testing is an opportunity to work through issues prior to the Interoperability Event with other event participants. During event registration, the option will be provided to participate in Pre-Interop Event Testing.

The Certification Secretariat will distribute the Pre-Interop Testing matrix within 3 business days after event registration closes. Implementers that opt-in to pre-interop testing will receive contact information for the other pre-interop participants so that they can coordinate their own informal testing prior to the event. Implementers are responsible for providing all necessary URLs, software, metadata, or other information required directly to the other Pre-Interop Testing participants.

Given the relatively short duration of Interoperability Testing Events, implementers are strongly encouraged to take advantage of Pre-Interop Event Testing. This program has shown to significantly increase an implementation's chances of passing interoperability testing during the interoperability event.

5.2.5 Re-Testing

It is desirable to have previously certified implementations return to future interoperability events to continually test the interoperability between old and new implementations. In addition to the reference device program, a short-term financial incentive is also provided: Any organization that returns to an interoperability event with its previously certified implementation(s) will be given a 50% credit against the certification fees for a future certification. This financial incentive policy requires approval by the FIDO Board of Directors for each Interoperability Event.

5.2.6 Interoperability Testing Event Criteria

In order for a valid, official interoperability test there must be two of each implementation class (server and authenticator; and client in the case of UAF) where each of the two implementations in each implementation class must be from a different implementer company.

In the event that there aren't two of each implementation for an interoperability event, the Certification Secretariat may cancel the event by giving notification 12 days before the event to the companies that have registered; or, the Certification Secretariat may provide reference implementations, if available, that the Certification Secretariat will operate during the event.

The interoperability test will consist of each implementation being tested with every other implementation in order to ensure that each implementation is compatible with every other implementation for 100% interoperability between all participating implementations. Reference implementations will be included in the test matrix if they are available.

In the event that there are too many implementations registered for an interoperability event, FIDO may extend the event by adding additional days, or by reducing the test matrix. If the test matrix is reduced the following algorithm will be used to create the test matrix:

- Every implementation must test with every other compatible implementation at least once
- Every implementation in the same implementation class (authenticator, client, server) must have the same number of tests +/- 1
- No client or authenticator implementation should have to perform more than 90 tests per testing day
- The overall test matrix cannot be more than 120 tests per facilitator, per day

Interoperability Testing will be run according to a test plan (test matrix) with the oversight of a facilitator. The facilitator may be part of the Certification Secretariat or FIDO staff. In the event that the interoperability event has too many attendees to be facilitated by the Certification Secretariat or FIDO staff, implementer companies may volunteer to facilitate provided that they do not facilitate for the Interoperability Testing of their own implementations. The facilitator will be the unbiased referee in the testing and document the results. If implementers don't agree with the results and the facilitator is from an implementer company or a FIDO staff member, the disputing parties will have the opportunity to request that the Certification Secretariat intervene. Should the implementers not agree with the assessment of the Certification Secretariat, the implementers will have the right to submit a Dispute Report [4-4] that will be managed by the Dispute Resolution Process, see Section 9.3.

During Interoperability Testing Events, implementations will be allowed to change their code, state or configuration; however, after making changes they must re-perform all their designated tests as well as Conformance Self-Validation Testing.

Interoperability Testing will only be considered successful if: 1) the implementation interoperates with all other implementations according to the test plan without any errors (including crashing); and 2) there is a matrix of implementations that includes two of each implementation class

where all implementations in that matrix are interoperable with each other and must include successful interoperability with any reference implementations, should any exist.

In order to determine which implementations pass Interoperability Testing, the following algorithm will be used:

1. Remove any implementations from the testing matrix which did not pass any interoperability tests
2. Any implementation that passes its testing with every other implementation in the matrix is considered to pass
3. For each failed test, identify the root cause and which implementation is not conformant with the specifications. The implementations that are conformant with the specifications will be considered passing and the implementation that is not conformant will not pass
4. If a root cause cannot be identified or compliance with the specification is indeterminate, the issue will be sent to the Certification Troubleshooting Team along with any supporting evidence gathered from the interoperability test.
5. If the Certification Troubleshooting Team cannot make a determination or if the results are disputed, the issue will enter the Dispute Resolution Process.

The goal of the Interoperability Event is 100% interoperability between implementations and demonstrably passing all test cases. The results of the Interoperability Event are final and no re-testing will be permitted or facilitated after the event.

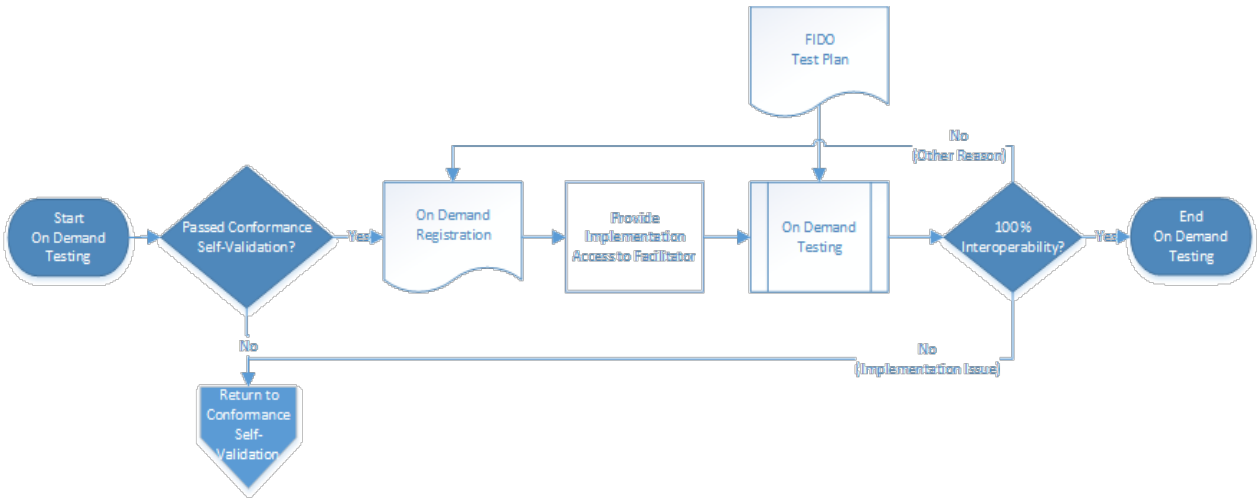
5.3 On Demand Testing

Prior to beginning the On Demand Testing process, an implementation must pass Conformance Self-Validation Testing, as described in Section 3.

On Demand Testing will only be made available if there are a minimum number of reference implementations within the FIDO Certified Reference Implementation Library [4-6]. The Certification Secretariat will announce to FIDO membership when On Demand Certification is available.

The vendor submitting for On Demand Certification is responsible for providing access to their implementation to the On Demand facilitator. The vendor will also supply any implementation-specific operating instructions as part of the On Demand registration (section 5.3.4).

Figure 5-3: On Demand Testing Process



5.3.1 New Technology

FIDO continues to update and release technical specifications, and vendors continue to deliver new products based on these updated FIDO specifications. The Functional Certification program will be continue to be updated as needed to support the "New Technology" defined in the FIDO specifications. Because no certified reference implementations will exist when New Technology is first introduced, On Demand testing will not be an option for the first functional certifications of new technology. Therefore, new technology must continue to participate in Interoperability Test Events (see section 5.1).

Once the minimum number of certified reference implementations as outlined in the On Demand Testing Criteria (section 5.3.7) are available within the FIDO Certified Implementation Reference Library [4-6], the technology will no longer be considered "New Technology" and it will then be eligible for On Demand Testing.

5.3.2 Reference Implementation Library

The Reference Implementation Library will be composed only of FIDO Certified implementations.

The Reference Implementation Library will be publically available on the FIDO website [4-6].

For servers, this will include the URL of the server and a form to request the information for a point of contact for configuring access to the server. For clients and / or authenticators, this will include a list of commercially available FIDO Certified implementations, their model number or SKU, and a URL to an online retailer where the implementation can be purchased.

5.3.2.1 Donating Implementations

FIDO members with certified implementations can donate their implementations to the FIDO Reference Implementation Library. By doing so, members agree to allow their implementation to be used in On Demand Testing and to be listed on the public Reference Implementation Library page.

If you are interested in donating, please fill out the Reference Implementation Donation Form [4-7].

5.3.2.2 Reference Implementation Library Management

The Reference Implementation Library will be continuously evaluated to ensure that all specifications eligible for On Demand testing have enough Reference Implementations to meet the minimum requirements. When there is not enough reference implementations to fulfill minimum requirements, a specification will no longer be eligible for On Demand certification and the company must instead participate in an Interoperability Event.

A Reference Implementation will remain as part of the Reference Implementation Library so long as the device is functional and interoperable to functional certification standards. In the case that a donated reference implementation is no longer fully functional, it will be returned to the company.

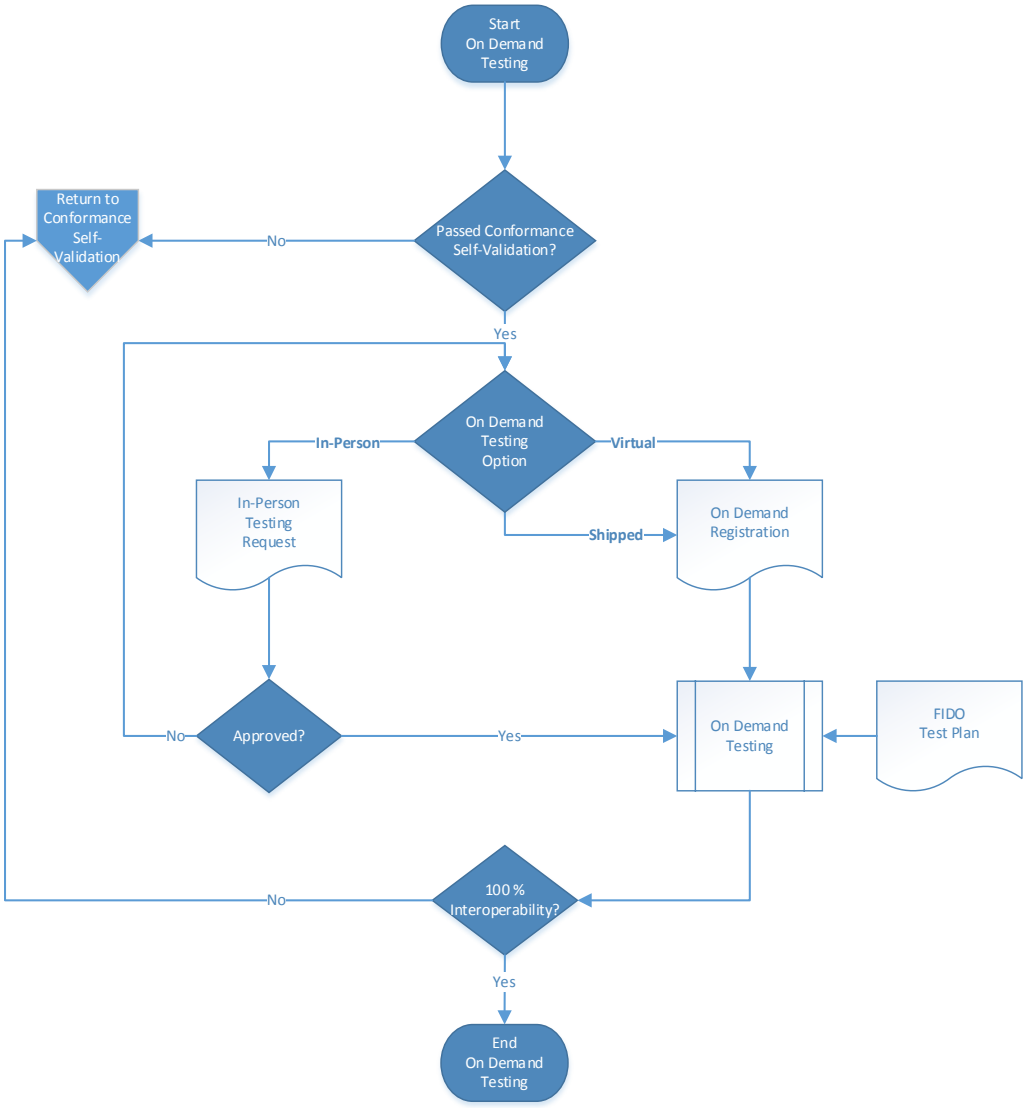
If a specification is deprecated or new requirements are added through errata a notification will be sent to all companies with Reference Implementations in the Library notifying them of the updated specification requirements. Any Reference Implementation that fails to comply with the current Functional Certification requirements will not be used in the On Demand matrix and will be considered out-of-date. Donated Reference Implementations that remain in an out-of-date state for a period of more than 90 days will be removed from the library and send back to the company.

5.3.3 On Demand Testing Options

There are three different options available for On Demand Testing:

1. Virtual
2. Shipped
3. In-Person

Figure 5-4: On Demand Testing Options



5.3.3.1 Virtual

Virtual On Demand Certification requires the vendor submitting for On Demand Testing to provide the Certification Secretariat access to, and instructions for, the operation of their implementation. The Certification Secretariat will facilitate the On Demand Interoperability Testing Process (see section 5.3.6). Contact information for a representative from the vendor company must be provided, and the representative must be available during their testing slot if any questions or issues come up during testing. The company will be notified of the result when complete. Once complete, the company may revoke the Certification Secretariat's access to their implementation.

5.3.3.2 Shipped

Shipped On Demand Certification requires the vendor submitting for On Demand testing to ship the implementation, and operating instructions, to our Certification Secretariat P.O. Box in the

United States. The Certification Secretariat will facilitate the On Demand Interoperability Testing Process (see section 5.3.6). A company representative should be available if any questions or issues come up during testing. The company will be notified of the result when complete. Once complete, the Certification Secretariat will ship the implementation back to the company. The FIDO Alliance/Certification Secretariat will be responsible for ensuring that confidentiality of the submitted implementation is maintained.

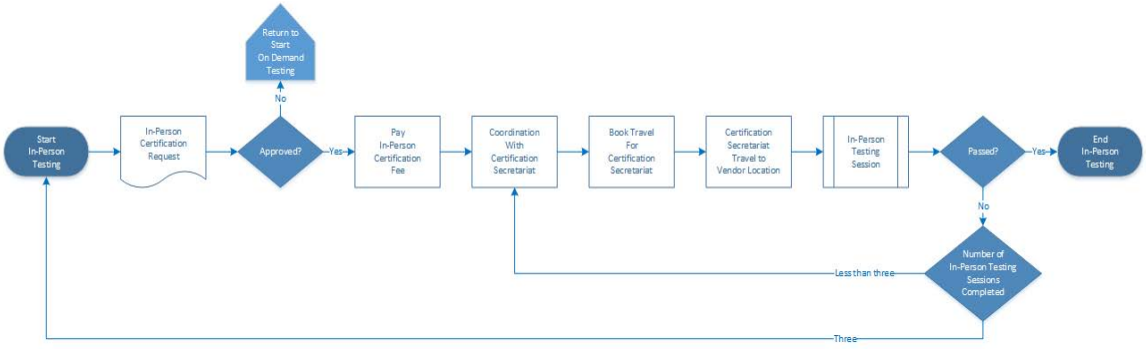
The company is responsible for all shipping arrangements and associated costs. During registration, desired return shipping methods can be stated. Standard return shipping costs will be included as part of functional certification fees. Any shipping and insurance requirements for the return of implementations beyond the standard will need to be organized and funded by the company and relayed to the Certification Secretariat. The Certification Secretariat will do their best to ensure all return shipping needs are met.

5.3.3.3 In-Person

In-Person On Demand testing requires a company representative to be present during the testing procedure. In order to apply for In-Person Testing, the vendor submitting for On Demand Testing must complete an In-Person Testing Request [4-5] for each implementation. Requests received will be evaluated on a case-by-case basis by the Certification Secretariat. In-Person testing has an additional $10,000 USD fee per implementation, and the company is responsible for all travel and expenses associated with In-Person testing.

If the In-Person Certification Request is approved, the vendor will need to coordinate directly with the Certification Secretariat to establish an itinerary for travel and testing. The Certification Secretariat will travel to the vendor's desired located to perform testing. Each approved In-Person Certification Request entitles the vendor to up to three testing sessions, each lasting a maximum of three days, for a total of nine days. Completing In-Person testing in less than three sessions is possible if the implementation passes all certification requirements. If the implementation does not pass within the three allowed testing sessions the vendor is required to restart the In-Person testing process, including submission of the In-Person Certification Request and fees.

Figure 5-5: In-Person Testing Option



If the In-Person Certification Request is rejected, the company should reassess the feasibility of completing On Demand Certification through either participation in a scheduled Interoperability

Event, or by On Demand Certification through a Virtual or Shipped option. Appeals for rejected In-Person Certification Requests can be made to the Certification Review Team in the form of a Dispute Report.

An In-Person Certification Request may be rejected for the following reasons:

1. An Interoperability Test Event is scheduled, and is less than 30 days away. The company will be encouraged to attend the Interoperability Testing Event rather than use the In-Person testing option.
2. There are insufficient certified reference implementations available within the FIDO Reference Implementation Library to complete On Demand Testing.

5.3.4 Registration

Results from the Conformance Self-Validation step (see Chapter 3) must be submitted through the FIDO test tool used to complete Self-Validation testing. These results must be confirmed by the Certification Secretariat before On Demand Testing will take place to ensure that the implementations are at least minimally complaint to the specifications.

Implementers must register for On Demand Testing. To register, companies must complete the On Demand Testing Registration [4-8]. If requesting In-Person testing, companies must complete an In-Person Testing Request [4-5]. Participants will be required to submit the information for a primary contact who can explain, if necessary, how to operate the implementation, and who will be available to respond to questions or issues should any arise during testing. Participants must also provide the names and technical details of the implementation(s) seeking On Demand Testing.

5.3.4.1 Book a Testing Slot

As part of Registration, companies will select the time slot for testing with the facilitator using the On Demand Registration Calendar [4-8].

The company contact indicated during registration must be available for any questions during the slot that is booked, in the case where a facilitator has any questions. If the vendor is unavailable in the case that a facilitator attempts to contact, the testing session will be immediately terminated and the vendor must reschedule their testing slot using the On Demand Registration Calendar [4-8]. If the implementation fails testing, the vendor must fix the issues in their implementation and reschedule a testing slot when they believe the implementation will pass. Testing slots should not be used as debug sessions, a testing slot should be scheduled when the vendor has confidence the implementation is ready for certification testing.

The Certification Secretariat reserves the right to notify vendors of a testing slot cancellation 72 hours in advance. Vendors will have the ability to schedule a new testing slot using the On Demand Registration Calendar [4-8].

Table 5-1: Example - On Demand Registration Calendar

SEPTEMBER 2016

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
28	29	30	31	1	2	3
4	5	6 U2F - 7 am PT [Register Now!]	7	8	9	10
11	12	13 U2F - 7 am PT [Register Now!]	14	15	16	17
18	19 U2F - 4 pm PT [Register Now!]	20 U2F - 7 am PT [Register Now!]	21	22	23	24
25	26 U2F - 4 pm PT [Register Now!]	27 U2F - 7 am PT [Register Now!]	28	29	30	1

5.3.5 Pre-Testing

Once On Demand registration is complete and a testing slot has been booked, it is recommended that vendors complete pre-testing prior to their testing slot.

Vendors can use the Reference Implementation Library as a reference for certified implementations. Vendors can request access to pre-test against Servers in the Reference Implementation Library, by completing a Pre-testing Request available on the Reference Implementation Library page. Commercially available Authenticators can be purchased directly from the implementer company.

Reference Implementations that are available to pre-testing will be limited to those that can be hosted virtually. FIDO does not guarantee availability of any reference implementations for pre-testing.

5.3.6 Test Facilitation

On Demand Testing will be run by a facilitator according to the testing criteria outlined below. The facilitator may be part of the Certification Secretariat or FIDO staff.

5.3.6.1 On Demand Testing Process

For On Demand testing to be fair to all participants a test matrix of reference implementations will be selected by the following algorithm:

1. All Reference Implementations compliant to the specification under Functional Certification are initially eligible.
2. In order for a valid, official On Demand test, there must be a minimum of three reference implementations of each implementation class where each of the three implementations

must be from a different member company. A maximum of six implementations will be supported.

3. The matrix will then be generated to meet the following requirements:
    a. 50% of the minimum required reference implementations, if possible, will be composed of market leaders. If 50% cannot be achieved, all possible market leader implementations will be used. Market leaders will be determined by the estimated number of implementations in the market at the time of testing, it is the responsibility of the facilitator to make their best assessment of the market leaders within the library to fulfill this requirement.
    b. The remaining number of reference implementations needed will be randomly selected from the remaining reference implementations within the library.
        i. As needed, the facilitator may include variations of features in the matrix to ensure complete testing. Some examples include types of authentication, like pin entry or biometric scans.

Logs will be kept by the facilitator of all testing sessions, in the case where an implementation fails and needs re-testing, the same test matrix containing the same reference implementations as the previous testing session will be used.

Vendors cannot select or request the reference implementations used during their On Demand Testing Session. All Reference Implementations used are confidential until completion of the testing session for On Demand Certification. Upon completion, the test results will be presented to the vendor and will include the reference implementations.

5.3.7 On Demand Testing Criteria

5.3.7.1 Pass Criteria

On Demand Testing will only be considered successful if:

1. The implementation interoperates according to the test plan without any errors (including crashing); and
2. There is a matrix of implementations that includes two of each implementation class where all implementations in that matrix are interoperable with each other and must include successful interoperability with any reference implementations, should any exist.

Table 5-2: Example - U2F Testing Matrix

	Reference Implementation 2	Reference Implementation 3	Reference Implementation 4
	Authenticator	Authenticator	Authenticator

		Register	Authenticate	Register	Authenticate	Register	Authenticate
Implementation Under Test	Server						
Reference Implementation 1	Server						
Reference Implementation 2	Server	N/A	N/A				

In the example testing matrix above ("Test Plan"), the implementation under test is the implementation that is requesting certification. The implementation under test is a server, and in order to fulfill the testing requirements, the implementation under test is tested against authenticator Reference Implementation 2, 3, and 4 for the Register and Authenticate tests.

In order to determine which implementations pass On Demand Testing, the following algorithm will be used:

1. Remove any implementations from the testing matrix which did not pass any interoperability tests.
2. Any implementation that passes its testing with every other implementation in the matrix is considered to pass.
3. For each failed test, identify the root cause. If the implementation is not conformant with the specifications, the test will be considered a fail.
4. If a root cause cannot be identified or compliance with the specification is indeterminate, the issue will be sent to the Certification Troubleshooting Team along with any supporting evidence gathered from the On Demand test.
5. If the Certification Troubleshooting Team cannot make a determination or if the results are disputed, the issue will enter the Dispute Resolution Process.

The goal of On Demand Testing is 100% demonstrably passing all test cases. The results of the On Demand testing are final.

5.3.7.2 Fail Criteria

An implementation is considered to fail On Demand Testing if the implementation does not pass all required tests as outlined in the test plan.

In the case of a fail, the implementation will be notified via email by the Certification Secretariat. Implementations will be allowed to change their code, state or configuration; however, after making changes they must re-perform all their designated tests as well as Conformance Self-Validation Testing.

Should the implementers not agree with the assessment of the Certification Secretariat, the implementers will have the right to submit a Dispute Report that will be managed by the Dispute Resolution Process (see section 9.3).

5.4 Interoperability Testing Procedures

The testing procedures apply to all types of Interoperability Testing.

5.4.1 UAF Interoperability Testing Procedures

Following the policies above, UAF testing will iterate through the prescribed combination of Authenticators / ASMs, Clients and Servers. This will require the following configuration for each set of tests:

- The Client, Authenticator and Server's Relying Party Application (RP App) will be loaded on to a single implementation
- The Server will install the metadata for the Authenticator with corresponding policies and permissions
    a. The facilitator will confirm that the metadata for the Authenticator has been registered with the FIDO Alliance.

For each prescribed combination, the following tests will be performed in front of a facilitator:

1. Register: perform valid registration with the server.
2. Authenticate: perform valid authentication with the server.
3. Transaction: perform a transaction with the server. The test must show a text or image indicator of the transaction that is being performed and confirmation that the transaction was successful.
4. De-Register: remove the registration from the device. Confirm that de-registration was successful by attempting an authentication with the server and confirming that it fails.

Other policies for UAF testing include:

- In order to fully exercise the implementations in each test case, authentication caching should be disabled.
- Performing these tests on an emulator is permitted as long as it is the same target OS and configuration.
- Using an "OK button" or "PIN" for the matcher is permissible, provided that the ASM and Authenticator will not be modified in the final product claiming to be FIDO Certified.

Note that due to the time required for configuration of each test and the potential number of combinations for UAF Interoperability Testing Events, each test event will span a maximum of three days. Implementers are expected to attend each day, even if their implementations have already passed all of their designated tests, to facilitate any necessary re-testing. If it is determined that fewer days of testing are required for the interoperability test, the Certification Secretariat will notify participants 7 days prior to the event or as soon as reasonably possible.

5.4.2 U2F Interoperability Testing Procedures

Following the policies above, U2F testing will iterate through the prescribed combination of Authenticators and Server. Interoperability Testing is performed with the Chrome browser as the U2F Client. Testing is performed with the native U2F functionality of the browser and the U2F Chrome Extension will not be allowed in testing. This policy may be changed when other U2F Clients become available.

This will require the following configuration for each set of tests:

- The Server will install the metadata for the Authenticator with corresponding policies and permissions
    a. The facilitator will confirm that the metadata for the Authenticator has been registered with the FIDO Alliance.

Each combination of Authenticator and Server will be required to perform the following tests for a facilitator:

1. Register: The U2F Authenticator will be required to register itself with the U2F Server.
2. Authenticate: The U2F Authenticator, after being registered with the server, will be required to demonstrate that it can authenticate with the server.

Per the specifications, human interaction is required for each of these steps, such as the touch of a button; the insertion or removal of a device; etc. If the insertion of a device is being used as the form of human interaction, it should require being re-inserted each time a test step is performed.

Servers must be prepared to perform the following test steps:

1. Negative Register: Register with an invalid certificate in a way that should be rejected by the server.
2. Negative Authentication: After valid registration, authenticate with invalid credentials in a way that may be rejected by the server.

These steps are optional for a client to implement, since some implementations may have difficulty implementing invalid certificates or the other mechanisms required for performing these test steps. However, when a client does support these steps, servers are required to pass Interoperability Testing for Negative Register and Negative Authentication.

5.4.3 Level 1 Authenticator Certification Testing Procedures

For Authenticators seeking Level 1 Authenticator Certification, Authenticator Security Requirements below in Table 3 must be verified during Conformance Self-Validation or Interoperability Testing.

Requirements and the Vendor Questionnaire are defined in the Authenticator Security Requirements [5-4].

Note: Authenticators completing L2+ are not required to demonstrate the Requirements during Conformance Self-Validation or Interoperability Testing, the Authenticator Security Requirements

are evaluated by an Accredited Security Laboratory during the Security Evaluation step of Authenticator Certification.

Evaluation Methods include Conformance Self-Validation and Interoperability Testing:

- For **Conformance Self-Validation**, the Requirement is verified automatically during registration or testing.
- For **Interoperability Testing**, the Vendor shall demonstrate to the Test Proctor how the Authenticator meets the Requirement during Interoperability Testing.

Reasonable effort will be taken by the Test Proctor to isolate the testing of the requirements in Table 3 from other Vendors at Interoperability Events.

Table 3: L1 Interoperability Requirements Mapping

Specification(s)	Requirement	Evaluation Method
UAF	1.4	Interoperability Testing
UAF	1.9	Interoperability Testing
UAF & U2F	3.1	Interoperability Testing
U2F	3.3	Interoperability Testing
UAF	3.4	Interoperability Testing
UAF	3.5	Interoperability Testing
UAF & U2F	3.9	Interoperability Testing
UAF	4.4	Interoperability Testing
UAF & U2F	6.2	Interoperability Testing
UAF & U2F	6.3	Interoperability Testing

5.4.3.1 Vendor Questionnaire Instructions

The Vendor Questionnaire or any supporting documentation that may contain confidential information is not required to be submitted or presented for verification during Interoperability Testing. For the Requirements listed in Table 3, it is sufficient to demonstrate the fulfillment of the Requirement to the Test Proctor. The Test Proctor will record the Pass / Fail of each Requirement in the Interoperability Test Results for each Authenticator.

During the Vendor Questionnaire portion of Authenticator Certification [5-5], Vendors can indicate in the Vendor Questionnaire that the Requirement was verified during Conformance

Self-Validation or Interoperability Testing by providing the Interoperability Test Results as evidence, and are not required to provide additional documentation for that Requirement.

6 Certification Issuance

Certification Issuance is the final required step of the FIDO Certification Process, and can only be entered after successful completion of the Conformance Self-Validation and Interoperability Testing steps.

6.1 Authenticator Certification

Authenticators will not be issued a Functional Certificate and instead must continue on to the Authenticator Certification Policy [5-5] and at the successful completion of the Authenticator Certification process will be issued an Authenticator Certificate.

Therefore, Authenticators shall skip the Certification Issuance step outlined in this section.

6.2 Certification Secretariat

The Certification Secretariat is responsible for communication with implementers, operations of the certification process, and the issuance and administration of certificates. Due to the sensitivity of some certification information – such as the status of certification or confidential implementations – distribution of information about the certification status of specific implementations will be limited to the Certification Secretariat and FIDO staff members. This pertains to the status and workflow of specific certification requests, and after an implementation has been granted or rejected certification the policies governing disclosing certification information will apply.

When filing requests in previous steps of the certification process the Certification Secretariat will respond via email within three business days. Please allow up to 10 business days for processing all submissions related to the Certification Issuance step, unless otherwise stated.

6.3 Certification Requests and Issuance

When submitting for certification, implementers must:

1. If a member company of FIDO, be in good standing
2. Have all certification invoices paid in full
3. Be willing to adhere to all policies
4. Be submitting a product intended for commercial use

In order to receive certification, implementers must submit the following for each implementation being certified:

1. Certification Request [5-1], including a description of the implementation and implementation type being certified
2. Conformance Self-Validation Testing Results
3. Interoperability Testing Results and event documentation, including the date of the event
4. A signed and completed copy of the FIDO Vendor Self-Assertion Checklist [5-3].
5. Certification Fees

In addition, UAF ASM / Authenticators must:

1. Have a Vendor ID
2. Have registered metadata with certification@fidoalliance.org
3. Provide information about the authenticator model and version, to be used in potential Derivative Certification(s)

In addition, for each transport supported, U2F Authenticators must:

1. Have registered metadata with certification@fidoalliance.org

An implementer may also optionally submit:

1. A signed Implementation Conformance Statement stating that the implementation meets all the aspects of the FIDO specifications that may not be directly testable.
2. Provide proof that the transport is certified by the corresponding transport technology's industry certification process (if certification is available).

If it is found that Conformance Self-Validation results or other documentation has been falsified; if implementations have been modified, or if any other policy is violated, intentionally or unintentionally, the violations are subject to review by the FIDO Board of Directors. The Board of Directors may choose a suitable recourse, ranging from requiring that an implementation go through the Certification Process again to become certified to revoking FIDO membership and / or previous certifications, depending on the severity of the transgression.

The Certification Secretariat will be responsible for verifying all submitted documentation as well as:

1. Ensuring that all disputes have been resolved and that the resolutions do not prevent the certification of the implementation
2. Noting any changes in specifications, errata, test tools, Conformance Self-Validation process or Interoperability Testing process that would impact the ability to certify the implementation

Turn-around time for functional certification will be as soon as reasonably possible and no more than 30 days from the implementer's submission of documentation. There are four possible outcomes to certification:

1. Approval: The implementer's certification request is approved and the implementation is certified.
2. Rejection: The request was rejected because of a technical error that is correctable, and the implementer will have the opportunity to correct the error and resubmit through the resubmission process.
3. Delay: The request has been delayed beyond the typical 30 day certification window because of pending events (e.g. a dispute that is still pending resolution, see Section 9.3).
4. Failure: The request was rejected because the request was inappropriate or impossible and it would be inappropriate to resubmit.

Approval will only be granted if the implementation has all of the required documentation and it is reasonably sufficient to document compliance with the corresponding specification(s). Upon approval, the certified implementation will be registered in the functional certification database

and the implementer will be notified by email. Notification will include a functional certification number for future reference.

Rejection may occur if any document is missing or invalid; or if any other condition exists that would prevent functional certification. If a certification request is rejected, the implementer will be notified by email with the corresponding reason(s) for rejection and will have the opportunity to resubmit through the resubmission process. The Certification Secretariat will make every reasonable attempt to ensure that all errors in a submission are identified so that they can be addressed in parallel, rather than sequentially. An implementation may be resubmitted three times before it is considered a failed functional certification attempt, and the implementation would need to be resubmitted and functional certification fees paid again.

Should a certification request be rejected, delayed or failed, the submitting implementer will have the right to submit a Dispute Resolution Request, which will follow the Dispute Resolution Process described in Section 9.3.

When a certificate is issued, it will contain the following information:

- The name of the organization that has been certified
- The name of the implementation that has been certified
- The implementation class (Server, Authenticator, Client) of the implementation
    - If Authenticator, the Vendor ID
- The FIDO Specification and version for which the implementation has been certified
- The FIDO Functional Certification Program Policy version against which the implementation has been certified
- The date that Conformance Self-Validation test was passed
- The date that Interoperability Testing was passed
    - Including the type of Interoperability Testing:
        - Interoperability Event
        - On Demand, Virtual
        - On Demand, Shipped
        - On Demand, In-Person
- A certification number of the format SSSVVVVDDDDDDDDNNN where SSS is the FIDO Specification, VVVV is the version of the FIDO specification
    - DDDDDDDD is the date of issuance, and NNN is the sequential number of the certification issued that day

FIDO® Certified products [5-2] will be viewable and searchable by FIDO membership and the public-at-large, with the exception of certifications that are confidential.

Confidential certification may be requested at the time that a certification request is submitted and will prevent the Certificate from being visible to membership or to the general public. Note that confidential certification may be requested either as part of the confidential certification process or independently from it – the two are independent of each other. Confidentiality may be withdrawn at the request of the implementer by submitting a written request to the Certification Secretariat with the corresponding certification number. Implementations that have been granted confidential certification may not use the certification mark until their confidentiality has been withdrawn. The Certification Secretariat will contact implementers of confidential

certifications once every three months to verify that certifications should retain the confidential status. For more information on Confidential Certification see Section 5.2.3.1.

6.4 Revocation

A Certificate can be revoked by the Certification Secretariat. Revocation is an indication that the implementation is no longer certified and will never return to good standing.

Revocation events include:

- Failure to follow FIDO Authenticator FIDO Functional Policy (this document), including, but not limited to:
    - Changes made to the FIDO portion of a Certified implementation after Certification.
    - False statements on any FIDO form.
    - Violation of the FIDO Trademark & Licensing Agreement (TMLA), if signed.
    - Failure to pay Certification Fee invoices.
    - If Metadata Statements submitted to MDS, Violation of MDS terms.

Reasonable attempts will be made by the Certification Secretariat to contact the Vendor and report the revocation event. The Vendor will be given a minimum of 30 days and maximum of 180 days from first contact to resolve any of the revocation events.

If the Certification Secretariat considers the event to be resolved within the deadline the Certificate will not be revoked and will remain in a “Certified” state.

If the revocation events are not resolved within the allocated time, the Certification Secretariat will recommend revocation to the Board Certification Committee. The Board Certification Committee will have the final decision to revoke a Certification.

If the Certificate is revoked, TMLAs will be revoked, and the implementation listing will be removed from the FIDO Certified webpage.

For Authenticators, if the Certification is revoked and if the Vendor submitted Metadata Statements, the Table of Contents (TOC) for the certificate will be updated via a status update by the Certification Secretariat to reflect the updated certification state.

6.5 Certification Program Management

In order to provide continuity of operations between the Certification Secretariat and the FIDO Alliance, the Certification Secretariat will attend CWG meetings and any joint meetings or other meeting where topics around certification are on the agenda. The Certification Secretariat will not have voting rights, but may participate in conversation and deliberations. Meeting notes, scheduling, logistics and other aspects of FIDO CWG meetings will be arranged in the same manner as other Working Groups and not by the Certification Secretariat.

In order to provide transparency and ensure appropriate managerial oversight, the Certification Secretariat will report to the CWG and / or the Board of Directors at each plenary meeting or as requested. Operational reports will include:

- the number of certification requests,
- the number of certifications granted,
- a breakdown of the implementation types that have been certified,
- a report of any disputes and their resolutions,
- a report of any interoperability events that have taken place,
- an update on the test tools,
- any process updates,
- certification mark violations,
- any other notable events or operational metrics

Any reporting performed by the Certification Secretariat will be performed at the aggregate level to preserve confidentiality, and will not include the specific name or details of any implementation or small set of implementations.

7 Derivative Certification

Derivative Certification is for products or services that rely upon existing certified implementations for conformance with the FIDO specifications. The intent of derivative certifications is to reduce the burden for receiving certification for implementations that are substantially the same.

A derivative implementation may not modify, expand or remove FIDO functionality from the certified implementation on which it is based. Derivate implementations are bound to the Functional Certification Policy in place at the time of the original (base) certification.

The certified implementation for a derivative may be from the same company (e.g. certify one model of a mobile phone and then create derivative implementations for similar products); or may be a certified implementation from a third-party (e.g. a certified SDK that is used in a finished product).

In order to drive adoption, client/authenticator derivative certifications and server derivative certifications have different requirements for Derivative Certification.

The following scenarios outlined in Table 7-1 are designed to help determine whether an implementation qualifies for a Derivative Certification.

Table 7-1: Certification Scenarios

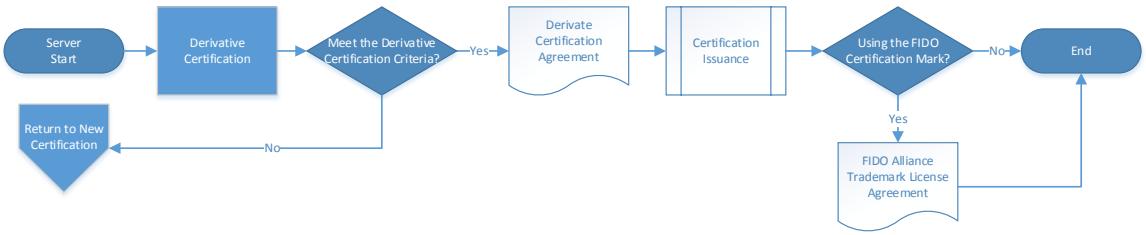
Implementation	Derivative?
Company B Using a FIDO Certified SDK from Company A	Yes
Company B Using a FIDO certified hardware module with FIDO software burned into it from Company A	Yes
Mobile Phone that is FIDO Certified releases a new model	Yes
Mobile Phone that is FIDO Certified has several variations (e.g. different colors, 32GB, 64 GB)	No. Variations that do not alter the implementation are covered under original certification.
Website using a FIDO enabled authentication based on a FIDO Certified server component licensed from another company	Yes
Company with FIDO Certified implementation [New Product 1.0] introduces a new product [New Product 1.0.1] that is the same as the previous implementation, except that is fixes some typos, fixes some bugs, and applies new security patches	No. Product is functionally the same and does not require new certification or derivative certification.

Implementation	Derivative?
Company with FIDO Certified implementation [New Product 1.0.1] introduces new product [New Product 1.1] that adds some features unrelated to FIDO	No. Product is functionally the same and does not require new certification or derivative certification.
Company with FIDO Certified implementation [New Product 1.1] introduces new product [New Product 2.0] that is different from New Product 1.1, but the FIDO components have remained unchanged	Yes
Company with FIDO Certified implementation [New Product 2.0] introduces New Product 3.0 that adds/removes/modified FIDO functionality	No. Product must undergo the full certification process and receive a new certificate.

7.1 Derivative Server Requirements

In anticipation of millions of websites / relying parties using FIDO specifications and potentially using the FIDO certification mark in conjunction with their services, the overhead for Derivative Certification for these websites / relying parties must be extremely low. Therefore, the sole requirement for a derivative Server implementation to use the FIDO certification mark in conjunction with their product or service is that it must abide by the FIDO Alliance Trademark and Service Usage Agreement for Websites [6-1]. The intent is to follow a model similar to node.js[1].

Figure 7-1: Derivative Server Certification Process



7.2 Derivative Client / Authenticator Requirements

Client and authenticator implementations that are based on certified implementations may also receive derivative certification; however, they have different requirements. For a client or authenticator derivative implementation to receive derivative certification it must:

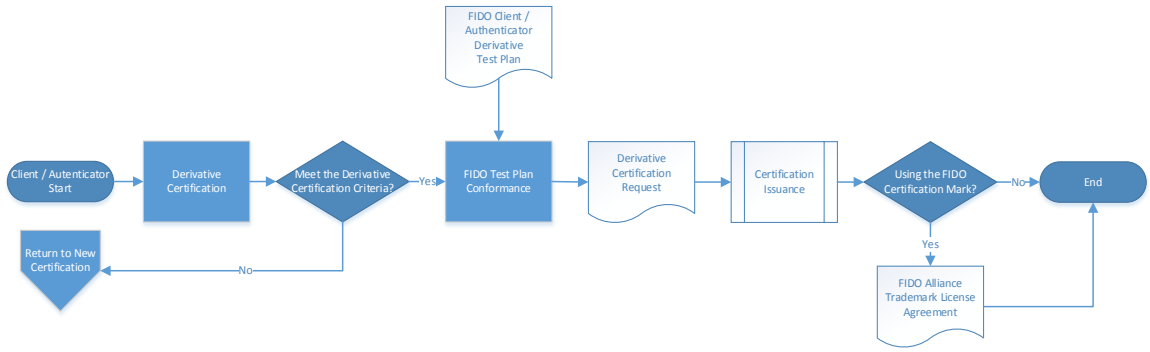
1. Follow the Derivative Test Plan provided by the FIDO Alliance to ensure that the derivative implementation is functional and has not broken the initial certified implementation.

[1] http://nodejs.org/images/trademark-policy.pdf

2. Request Derivative Certification from the Certification Secretariat by submitting a Certification Request [5-1] that indicates the certification is derivative along with the corresponding documentation.

Client and authenticator derivative implementations are not required to undergo Interoperability Testing. Conformance Self-Validation Testing is required as outlined in the Derivative Test Plan. The process for submitting for certification laid out in Section 6 will remain the same.

Figure 7-2: Client / Authenticator Derivative Certification Process



The Derivative Test Plan will not be required for implementations that have passed Conformance Self-Validation and Interoperability Testing. This is expected to be a rare scenario, since one of the major goals of the derivative requirements is to remove the heavier requirements around Interoperability Testing.

Derivative Test Plan results [6-2] are to be submitted along with the Certification Request for those implementations that used a Derivative Test Plan.

In order to use the FIDO Certification Mark, the derivative implementation must execute a FIDO Alliance Trademark Licensing Agreement [2-1].

7.3 Certification Request for Derivatives

Vendors may choose to process many Derivative certifications at one time, or multiple times within one year.

For each Certification Request:

- All Derivatives must be from the same Base Certification.

At least one Derivative per Certification Request must complete the Derivative Test Plan (including passing Conformance Self-Validation Testing). For the other Derivatives, the Vendor must self-attest that the Derivative does not change FIDO functionality and could meet the requirements of the Derivative Test Plan.

8 Certification Mark Usage

The definition of the Certification Mark is the responsibility of the Marketing Working Group (MWG) and the implementation of the Certification Mark is the responsibility of the CWG. All operational aspects of the Certification Mark, including enforcement, management of Trademark Licensing Agreements (TMLAs) and so forth, are to be carried out by the Certification Secretariat.

8.1 Usage

Certified implementations are invited and encouraged to use the FIDO® Certified mark and logo to promote their implementation's conformance with the FIDO specifications. These certification marks are reserved for FIDO Certified implementations to enable quick identification of implementations that are exemplars of the FIDO values: stronger, simpler, authentication.

The FIDO Certification Mark(s) may only be used in conjunction with implementations that have the approved corresponding functional certification, and where the implementer company has executed the FIDO Alliance Trademark License Agreement [2-1]. As mentioned previously, the certification mark cannot be used in conjunction with an implementation that is certified under Confidential Certification until after the confidential certification has been withdrawn.

Relying parties and companies operating websites, applications, or other Servers that may be running a FIDO Certified server may use the FIDO certification mark if they agree to the FIDO Trademark and Service Mark Usage Agreement for Websites [6-1].

8.2 Violations

In the event that the FIDO® Certified mark is being misused, a report can be filed by completing the Certified Logo Violation form [7-1] and submitting a URL and a photo of the misuse of the FIDO Certified logo.

8.3 Enforcement

The Certification Secretariat will be responsible for a monthly review of certification mark usage and usage of the FIDO® Certified terminology to ensure that usage is compliant with the TMLA. This review will use online search engines or other methods to find usage of certification marks, whence the Certification Secretariat will ensure that the mark usage is appropriate and that the corresponding implementation has indeed been certified for the claimed functionality. Should a certification mark violation be found, it will be referred to the Board of Directors.

Reasonable attempts will be made to contact any party that is using the certification mark in an unapproved fashion. If the party contacted is a FIDO member and they disagree with the assessment that the certification mark is being used in a way that violates policy, they will have the right to submit a Dispute Report [4-4] that will follow the Dispute Resolution Process.

9 Certification Administration

The CWG will be responsible for maintaining these policies and will have the authority to change them as they see fit. The CWG should take care, to any extent possible, to ensure that any revisions to these policies fall within the current statement of work between the Certification Secretariat and the FIDO Alliance; or that the statement of work be amended as appropriate.

9.1 Voting

Voting to modify these policies or any aspect of the FIDO Certification Program will be subject to standard Working Group voting procedures and require a simple majority vote.

9.2 Certification Troubleshooting Team

FIDO has established a Certification Troubleshooting Team, which is a group of no more than five people to quickly diagnose, dispatch and resolve technical and operational issues as they arise.

9.3 Dispute Resolution Process

During the certification process, disputes may arise. If this occurs, a Dispute Report [4-4] is submitted to the Certification Secretariat via the website. Upon receipt of a Dispute Report, the CS forwards the Dispute Report to the Certification Review Team (CRT). The Certification Review Team is responsible for determining the validity of the request and the appropriate routing of the request. The Certification Secretariat notifies the Certification Working Group (CWG) of all Dispute Reports and their resolution.

If the certification has outstanding disputes or other issues, the certification may be delayed. Should the certification be delayed, the implementer must be notified.

If the certification is rejected, failed or delayed, the implementer will have the option of submitting a Dispute Report.

Appendix A

Certification Process Actions

Table A-1 is to be used as a reference for the actions involved with the functional certification process.

Not all actions are mandatory for all implementations. For more information refer to the section referenced in the step column.

Table A-1: Certification Process Actions

Step	Action	Submission	Fee?	Processing Time
Conformance Self-Validation	Register for Test Tool Access Request [3-1].	FIDO Website	No	3 business days
Conformance Self-Validation	If UAF Authenticator, complete a Vendor ID Request [3-3]. One per company.	FIDO Website	Yes	3 business days
Conformance Self-Validation	If Authenticator, submit Metadata.	certification@fidoalliance.org	No	
Conformance Self-Validation	Complete Conformance Self-Validation Testing using the Test Tool	Online via Test Tool UAF [3-4] U2F [3-5]	No	
Interoperability Testing Events	Register for an Interoperability Testing Event [4-2]. Dates can be found on the website [4-1].	FIDO Website	No	Must be completed 14 days prior to the Event
Interoperability Testing Events	Complete the Interoperability Non-Disclosure Agreement [4-3].	FIDO Website	No	
Interoperability Testing Events	Complete Interoperability Testing	At Interoperability Event	No	
(Optional)	Complete an In-Person Testing Request	FIDO Website	Yes, if approved.	10 business days

Step	Action	Submission	Fee?	Processing Time
On Demand Testing				
(Optional) On Demand Testing	Complete Pre-Testing	FIDO Website	No	3 business days
On Demand Testing	Register for an On Demand Testing Slot using the On Demand Testing Calendar [4-8]	FIDO Website	No	
Certification Issuance	Complete a Certification Request [5-1].	FIDO Website	Yes	10 business days
Certification Issuance	Submit Conformance Self-Validation Testing Results	FIDO Website	No	10 business days
Certification Issuance	Submit Interoperability Testing Results	FIDO Website	No	10 business days
Certification Issuance	Pay Certification Fees	FIDO Website	Yes	
Derivative Certification	Complete a Certification Request [5-1] with Derivative Certification selected.	FIDO Website	No	10 business days
Derivative Certification	Submit Derivative Test Plan Results [6-2].	FIDO Website	No	10 business days
Derivative Certification	Pay Certification Fee	FIDO Website	Yes	10 business days
Certification Mark Usage	Consent to the Trademark License Agreement [2-1].	FIDO Website	No	
Certification Mark Usage	Consent to the Trademark and Service Mark Usage Agreement for Websites [6-1].	FIDO Website	No	
(Optional)	Complete a Dispute Report [4-4].	FIDO Website	No	

Step	Action	Submission	Fee?	Processing Time
Dispute Resolution Process				
(Optional) Reference Implementation Library	Donate a certified Implementation to the Reference Implementation Library [4-7]	FIDO Website Implementation by Mail	No	

Appendix B

References

Table B-1: References

Standard / Document	URL	Ref
Authenticator Certification Policy	TBD Approved Draft: https://workspace.fidoalliance.org/kws/groups/fido-cwg/download/6024/latest	[5-5]
Authenticator Security Requirements	TBD Approved Draft: https://workspace.fidoalliance.org/kws/groups/fido-cwg/download/6093/latest	[5-4]
Certification Request	https://fidoalliance.org/certification-request/	[5-1]
Certification Website	https://fidoalliance.org/certification/	[1-4]
Certified Logo Violation Form	http://fidoalliance.org/certified-logo-violation/	[7-1]
Derivative Test Plan Results	https://fidoalliance.org/wp-content/uploads/Derivative-Test-Plan-20150326.pdf	[6-2]
Dispute Report	https://fidoalliance.org/dispute-report/	[4-4]
FIDO Alliance Trademark Licensing Agreement	https://fidoalliance.org/wp-content/uploads/FIDO_Trademark_License_Agreement_v_3.1.pdf	[2-1]
FIDO® Certified Products	https://fidoalliance.org/certification/fido-certified/	[5-2]
FIDO Upcoming Events	https://fidoalliance.org/upcoming-events/	[4-10]

Standard / Document	URL	Ref
FIDO Working Groups	https://fidoalliance.org/working-groups/	[4-9]
In-Person Testing Request	https://fidoalliance.org/in-person-testing-request/	[4-5]
Interop Registration	https://fidoalliance.org/interop-registration/	[4-2]
Interoperability Non-Disclosure Agreement	https://fidoalliance.org/wp-content/uploads/FIDO-Interoperability-NDA.pdf	[4-3]
Member Calendar	https://confluence.fidoalliance.org/calendar/mycalendar.action	[4-1]
On Demand Testing Calendar	https://fidoalliance.org/on-demand-registration-calendar/	[4-8]
Reference Implementation Donation Form	https://fidoalliance.org/reference-implementation-donation-form/	[4-7]
Reference Implementation Library	https://fidoalliance.org/reference-implementation-library/	[4-6]
Test Tool Access Request	https://fidoalliance.org/test-tool-access-request/	[3-1]
Trademark and Service Mark Usage Agreement for Websites	https://fidoalliance.org/fido-trademark-and-service-mark-usage-agreement-for-websites/	[6-1]
U2F Conformance Test Tool	http://u2fconformance.fidoalliance.org/	[3-5]
U2F Specification	https://fidoalliance.org/specs/fido-u2f-v1.0-nfc-bt-amendment-20150514.zip	[1-1]
UAF Conformance Test Tool	https://conformance.fidoalliance.org/	[3-4]
UAF Specification	http://fidoalliance.org/wp-content/uploads/2014/12/fido-uaf-v1.0-ps-20141208.zip	[1-2]
Vendor ID Request	https://fidoalliance.org/vendor-id-request/	[3-3]

Standard / Document	URL	Ref
Vendor Self-Assertion Checklist	https://fidoalliance.org/wp-content/uploads/FIDO-Certification-Checklist.pdf	[5-3]

Terminology and Definitions

Table B-2: Terminology and Definitions

Term	Definition
FIDO Authenticator	A FIDO Authenticator is responsible for user verification, and maintaining the cryptographic material required for the relying party authentication.
Certification	The FIDO Certification program allows members and non-members to measure and claim compliance with FIDO specifications and use the corresponding certification marks.
Certification Secretariat	The Certification Secretariat is responsible for implementing, operating, and managing the certification program as defined by the CWG.
FIDO Client	The software entity processing the UAF or U2F protocol messages on the FIDO User Device. FIDO Clients may take one of two forms: 1. A software component implemented in a user agent (web browser or native application). 2. A standalone piece of software shared by several user agents. (web browsers or native application).
Confidential Certification	A certified implementation that is not visible to membership or to the general public.
Derivative Certification	Certification for products or services that rely upon existing certified implementations for conformance with the FIDO specifications.
Dispute Resolution Process	During the certification process, disputes may arise between implementers or between interpretations of a specification. If this occurs, a Dispute Report is submitted to the Certification Secretariat.
FIDO Certification Mark	The FIDO Certification Mark(s) is the trademarked graphic and / or text indicating that a product or service has been certified to be conformant with the FIDO specifications.
FIDO Functional Certification Program	The programs and policies required for FIDO Functional Certification, described in this document.
FIDO Ready	“FIDO Ready™ is the testing program put in place before the FIDO 1.0 specifications were finalized. It is now obsolete.
FIDO Server	Server software typically deployed in the relying party’s infrastructure that meets UAF or U2F protocol server requirements.

Certification Troubleshooting Team	A team established to quickly diagnose, dispatch and resolve technical and operational issues as they arise. Also referred to as the Certification Review Team.
Vendor ID	A unique identifier assigned by FIDO to each company implementing a UAF authenticator.

Abbreviations and Notations

Table B-3: Abbreviations and Notations

Abbreviation/Notation	Meaning
AAID	Authenticator Attestation ID. Also known as the FIDO Vendor ID Number
ASM	Authenticator Specific Module
CWG	Certification Working Group
MWG	Marketing Working Group
RP App	Relaying Party Application
SDK	Software Development Kit
TMLA	Trademark Licensing Agreement
UAF	Universal Authentication Framework
U2F	Universal Second Factor Protocol