Certification Program Policy
3/19/2014

Table of Contents

TABLE OF CONTENTS 2

1 OVERVIEW 3

2 OVERALL CERTIFICATION POLICIES 4

3 CONFORMANCE SELF-VALIDATION 6

4 INTEROPERABILITY TESTING 8

5 CERTIFICATION SECRETARIAT AND CERTIFICATION ISSUANCE 10

6 CERTIFICATION MARK USAGE 13

7 DERIVATIVE CERTIFICATION 14

7.1 DERIVATIVE SERVER REQUIREMENTS 14
7.2 DERIVATIVE CLIENT / AUTHENTICATOR REQUIREMENTS 15

8 CHANGE CONTROL 16

1 Overview

This document gives an overview of the policies that govern functional certification as part of the FIDO Certification Program for both U2F and UAF specifications. These policies are the requirements and operational rules that guide the implementation, process and ongoing operation of the certification program and create an overall framework for the certification program to operate within. The policies cover all aspects of the certification program: self-test, interoperability testing, timelines, roles, responsibilities, certification mark usage, certification submission, issuance and retrieval.

The certification policies in this document supersede all previous policies governing FIDO Certification, including the policies and processes governing the issuing of "FIDO Ready" certification. No further FIDO Ready interoperability events will be performed and any existing FIDO Ready certifications will remain valid only for the duration of their corresponding Trademark Licensing Agreements (TMLAs).

The intended audience of this document is the Certification Working Group (CWG), FIDO administration, and the FIDO board of directors. During the implementation phase of the program, a version of this document will be created for implementers to help them understand the process for receiving certification and the policies surrounding the certification program.

The sections following this overview focus on functional areas of certification program, starting with the overall policies governing certification and then following through each functional area of the certification program: self-test, interoperability testing, certification issuance, certification mark, Certification Secretariat / administration.

2 Overall Certification Policies

The certification program as a whole is the responsibility of the 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 certification program responsibilities to those subcommittees. The Certification Secretariat is responsible for implementing, operating, and managing the certification defined by the CWG.

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

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. 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.

At the highest level, a FIDO implementation claiming to conform to either the UAF or U2F specifications must pass three stages in order to receive 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 4.
- **Interoperability Testing**: a FIDO implementation must participate in and demonstrate normative behavior during an 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 certification before claiming to be a certified FIDO implementation.

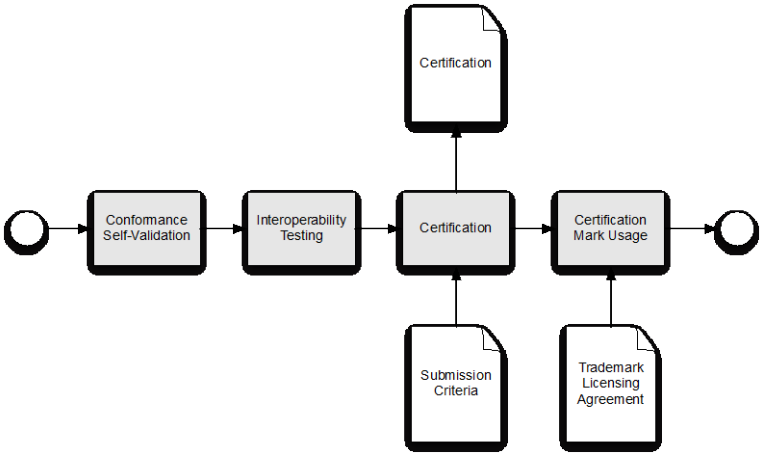

Figure 1 – A process overview of the major certification steps and process artifacts.

The steps above are required in order to receive certification. Any claim to certification or use of the certification mark by an uncertified product is prohibited. 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. Certification is valid indefinitely and does not expire, regardless of the good-standing of membership.

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 certification.

Prior to certification, UAF Authenticators will be required to register for a Vendor ID, which 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 Executive Director.

3 Conformance Self-Validation

Conformance self-validation definition is the responsibility of the CWG and is implemented and supported by the Certification Secretariat. 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.

The core of the conformance self-validation process is the test-tool, which has been acquired and / or created by the FIDO Alliance prior to the drafting of this policy document. Implementers will be required to access the test tools corresponding to their implementation (e.g. – U2F or UAF; client, server, or authenticator) and operate them according to the provided instructions. The test tools will create logs showing successful completion of the conformance self-validation testing will be required for both participation in interoperability testing as well as for submission to the Certification Secretariat for certification. The test tools will be hosted on a FIDO server, and implementers may use the test tools as frequently as required to validate their implementations. Prior to performing an official conformance self-validation test, a 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 certification. After passing an official test, the implementations may not change their configuration or implementation prior to the interoperability testing. In order to receive certification, the implementation must participate in an interoperability-testing event 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 the certification will be accountable for ensuring that conformance self-validation was performed according to the policies, processes and standards required by the FIDO 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. 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.

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 the FIDO Certification Process document.

In addition to test tools, the FIDO Alliance may – at its discretion – make available reference implementations to implementers to support their testing and certification initiatives. At this time there are no mandatory requirements around the use of any potential reference implementations.

4 Interoperability Testing

Interoperability testing is the responsibility of the CWG and is implemented and supported by the Certification Secretariat. Interoperability testing is a required portion of certification. Prior to attending interoperability testing, an implementation must pass conformance self-validation testing, as described in Section 3.

To any extent possible, implementers are encouraged to attend interoperability testing events in person, but remote accommodations will 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 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 web-cam showing the client-side implementations (client or authenticator) being tested.

The Certification Secretariat will be responsible for coordinating logistics for interoperability events, including scheduling, implementer communications, screen-sharing and web-cam software, dial-ins, test matrices, and any other aspects required for a well executed interoperability test. Interoperability testing will happen no less than once every three months, and may occur more frequently based on the direction of the CWG. Notification of upcoming events will be communicated to implementers, both through email, through the FIDO Alliance website, and through the member's calendar at https://confluence.fidoalliance.org/calendar/mycalendar.action. Implementers must register for interoperability events no less than 14 days before the event occurs.

In order for a valid, official interoperability test there must be three of each implementation class (server and authenticator; and client in the case of UAF) where each of the three implementations in each implementation class must be from a different implementer company. The interoperability test will consist of each implementation being tested with every other implementation.

Interoperability testing will be run according to a test plan 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 implementers of 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 a 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 request that will be managed by the dispute resolution process.

During interoperability testing, implementations will not be allowed to change their state or configuration. Rebooting or restarting implementations should be avoided to any extent possible and recompiling or reconfiguring implementations is prohibited.

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 three 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.

5 Certification Secretariat and Certification Issuance

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.

FIDO will establish a Certification Troubleshooting Team, which will be a group of no more than 5 people to quickly diagnose, dispatch and resolve technical and operational issues as they arise.

When submitting for certification, implementers must:

1. Be in good standing with all dues paid in full
2. Submit a form indicating willingness to adhere to all policies
3. Be submitting a product intended for commercial use
4. Have a vendor ID

In order to receive certification, implementers must submit:

1. Certification forms, including a description of the implementation and implementation type being certified
2. Interoperability event documentation, including the date of the event

A 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

If conformance self-validation results or other documentation that has been falsified; if implementations have been modified, or if any other policy is violated, intentionally or unintentionally, the violations be subject to review by the FIDO board of directors. The board of directors may choose a suitable recourse, ranging from requiring that an implementation be certified again 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 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).
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 certification database and the implementer will be notified by email. Notification will include a certification number for future reference.

Rejection may occur if any document is missing or invalid; or if any other condition exists that would prevent 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 certification attempt, and the implementation would need to be resubmitted and 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.

The certification database will be viewable by FIDO membership and the public-at-large, with the exception of certifications that are confidential. Certification information will include the name of the company, the name of the implementation, the class of the implementation, any optional functionality supported, date of conformance self-validation, and the date of interoperability testing.

Confidential certification may be requested at the time that a certification request is submitted and will prevent the certification from being visible to membership or to

the general public. 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.

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 by the Certification Secretariat; however other Working Groups will continue to be coordinated in their current manner.

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.

6 Certification Mark Usage

The definition of the Certification Mark is the responsibility of the 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.

The FIDO certification mark(s) may only be used in conjunction with implementations that have the approved corresponding certification, and where the implementer company has executed the Certification Mark Agreement. 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.

The Certification Secretariat will be responsible for a monthly review of certification mark usage to ensure that usage is compliant with agreements. 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 request that will follow the dispute resolution process.

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. To that end, a derivative implementation may not modify, expand or remove FIDO functionality from the certified implementation on which it is based.

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.

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. For that reason, trademark licensing and certification for derivative server implementations the sole requirement that in order for the derivative implementation to use the FIDO certification mark in conjunction with their product or service, it must abide by an agreement that will be laid out on the FIDO Alliance web site. The intent is to follow a model similar to node.js[1].

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

7.2 Derivative Client / Authenticator Requirements

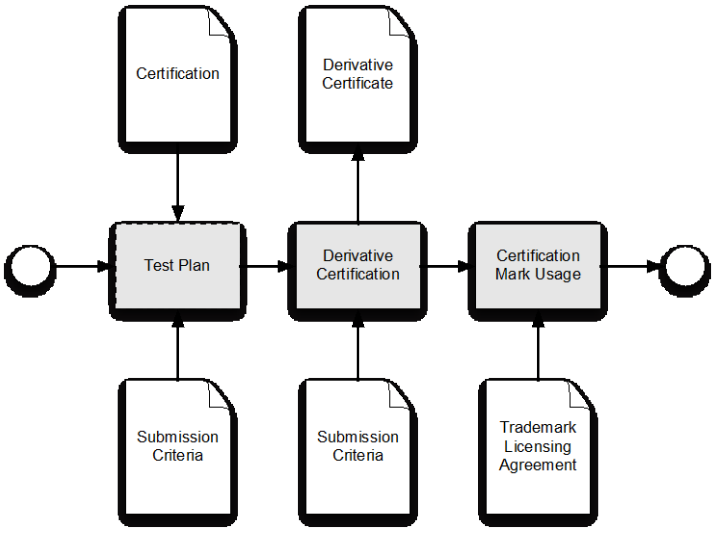

Figure 2 – An overview of the derivative certification process for clients and authenticators, to be contrasted against Figure 1

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 implementation it must:

1. Follow test plan provided by the FIDO Alliance to ensure that the derivative implementation is functional and has not broken the initial certified implementation
2. Request Derivative Certification from the Certification Secretariat by submitting a Derivative Certification Request and the corresponding documentation

Client and authenticator derivative implementations are not required to undergo Conformance Self-Validation or Interoperability testing, and test plan provided by the FIDO Alliance is a substitute for these steps. The process for submitting for certification laid out in Section 5 will remain the same.

In order to use the FIDO Certification Mark, the derivative implementation must execute a Trademark Licensing Agreement (TMLA).

8 Change Control

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. 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.

When the policies are changed, that change will be messaged to implementers through the appropriate email reflector. Unless a change is determined to be necessarily implemented immediately, changes will take effect 90 days after the approval vote order to give enough time to communicate the changes and change any operational procedures.