FIDO Certification Program Policy

Authenticator Certification

Version 1.0.0

April 2017

Revision History

Date	Version	Description
2017-04-20	1.0.0	Approved by CWG.

Contents

Table of Figures

Table of Tables

1 Introduction

This document defines the policies that govern FIDO Authenticator Certification. FIDO Alliance acts as the Certification entity for all approvals related to FIDO Certification Program.

FIDO Authenticator Certification is intended to certify the security characteristics of Authenticators conforming to FIDO Specifications (e.g. UAF and U2F Authenticators).

The policies contained herein are the requirements and operational rules that guide the implementation, process, and ongoing operation of FIDO Authenticator Certification and dictates the framework from within which the program will operate.

1.1 FIDO Certification Program

FIDO Certification Program refers to all certification schemes FIDO administers (e.g. FIDO Functional Certification, FIDO Authenticator Certification).

1.2 FIDO Authenticator Certification

FIDO Authenticator Certification refers to the process and policies described within this document.

1.3 FIDO Functional Certification Prerequisite

FIDO Authenticator Certification is independent of **FIDO Functional Certification** (the process and policies described in FIDO Functional Certification Policy [Functional]). However, an implementation must have successfully completed FIDO Functional Certification requirements for Authenticators, including Conformance Self-Validation and Interoperability Testing, as outlined in FIDO Functional Certification Policy [Functional], before applying for FIDO Authenticator Certification.

1.4 Audience

The primary audience of this document is the Certification Working Group, Security Requirements Working Group, FIDO Administration, and FIDO Board of Directors for the purpose of implementing FIDO Authenticator FIDO Certification Program.

The policies herein apply to Vendors and Laboratories that are undergoing or part of FIDO Authenticator Certification.

FIDO website [FIDO Cert] will reflect the information in this document, and is intended to help Vendors understand the process for receiving certification and the policies surrounding FIDO Authenticator Certification.

1.5 Instructions

All vendors shall follow the policy outlined in this document in order to gain FIDO Authenticator Certification for their implementations.

1.5.1 Support

For help and support, visit FIDO Website [FIDO Cert] or contact FIDO Certification Secretariat at certification@fidoalliance.org.

2 Roles & Responsibilities

FIDO Certification Program as a whole is the responsibility of FIDO **Certification Working Group (CWG)** in partnership with the **Security Requirements WG (SRWG)** for FIDO Authenticator Certification, with necessary oversights and approvals from FIDO Board of Directors, and collaboration with other FIDO Working Groups where needed.

The CWG and SRWG may, at the discretion of its chair and members, create subcommittees and delegate responsibilities for all or some portion of FIDO Certification Program responsibilities to those subcommittees.

The **Certification Working Group** is composed of FIDO member companies and oversees FIDO Certification Programs.

The **Security Requirements Working Group** is composed of FIDO member companies and defines the requirements for FIDO Authenticator Certification and acts as Security Experts for FIDO.

The **Certification Secretariat** is FIDO Staff responsible for implementing, operating, and managing all FIDO Certification Programs.

The **Security Secretariat** is FIDO Staff responsible for reviewing applications, questionnaires, monitoring security threats, and will act as an independent FIDO security expert for FIDO Certification Program. FIDO Staff that make up the Security Secretariat are: Technical Director, Security Certification Advisor, FIDO Certification Program Development, and individuals designated as Certification Secretariat.

The **Crisis Response Team** is composed of FIDO Staff, including the Executive Director, Marketing Director, Technical Director, Certification Secretariat, and Security Secretariat to respond to identified security vulnerabilities.

The **Certification Troubleshooting Team** is an ad-hoc CWG-appointed team consisting of FIDO staff and members common to all FIDO Certification Programs to diagnose, dispatch, and resolve policy and operational issues as they arise.

Accredited Security Laboratories are Security Testing Laboratories that have successfully completed FIDO Laboratory Accreditation [Lab Accreditation].

Accredited Security Laboratory Group is a closed FIDO group available only to Accredited Security Laboratory Approved Evaluators used to discuss Security Requirements and Security Threats.

Vendors seeking Certification may be FIDO member organizations or non-member organizations. This document governs all such requests for Certification.

Partner Programs are the independent FIDO Certification Programs with which FIDO relies on to offer joint FIDO Certification Programs to lessen the certification burden on Vendors. Partner programs can be found within Security Level 3 and above.

3 Program Documents

This section outlines and defines the documents that govern FIDO Authenticator Certification and their respective voting requirements.

3.1 Policy Documents

The Policy documents outline the program requirements for FIDO Authenticator Certification.

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

Table 1: FIDO Authenticator Certification Policy Documents

Document Name	Description	Voting Requirement
FIDO Authenticator Certification Policy	Policy and procedures for FIDO Authenticator Certification	Majority of CWG
Authenticator Metadata Requirements	Requirements for Metadata if submitted during FIDO Authenticator Certification	Majority of SRWG

3.2 Security Requirements

The term Security Requirements is used to refer to the set of documents which outline the requirements an Authenticator must meet to qualify for Certification. The documents that make up the Security Requirements are outlined in Table 2.

For more information on how the Security Requirements documents are updated, please see Section 10.3.

Table 2: Certification Authenticator Documents

Document Name	Description	Voting Requirement
Authenticator Security Requirements	Security Requirements by Level of FIDO Authenticator Certification.	Supermajority vote of the SRWG

	The Authenticator must meet the requirements listed in the Authenticator Security Requirements of the Level they wish to be certified to.	
Authenticator Allowed Cryptography List	Part of the Common Security Requirements, outlines the allowed cryptography for Authenticators	Supermajority vote of the SRWG
Authenticator Allowed Restricted Operating Environments List	Part of the Common Security Requirements, outlines the allowed restricted operating environments for Authenticators	Supermajority vote of the SRW

3.3 Vendor Documents

Vendor documents are additional program documents that must be completed by the Vendor.

Table 3: FIDO Authenticator Certification Vendor Documents

Document Name	Description	Voting Requirement
Vendor Questionnaire	A questionnaire to be completed by the Vendor that is a self-assertion of how the implementation meets the Security Requirements.	Majority vote of the SRWG
Impact Analysis Report	A document to be completed by the Vendor that outlines any changes in a Certified implementation for use in Delta Certification.	Majority vote of the SRWG

3.4 Accredited Security Laboratory Documents

Accredited Security Laboratory Documents are those used by the Accredited Security Laboratory during the Security Evaluation.

Table 4: Accredited Security Laboratory Documents

Document Name	Description	Voting Requirement
Security Test Procedures	The Test Procedures to be used by the Laboratory during the Security Evaluation.	Majority vote of the SRWG
Laboratory Report	The document to be completed by the Laboratory which outlines the results of the Security Evaluation.	Majority vote of the SRWG

4 FIDO Authenticator Certification Levels

FIDO Authenticator Certification Levels describe the level of defense the authenticator poses against various threats. The level categorizes the level of security of the device and Relying Parties (RPs) will know if they want to allow a device to connect to their services, given a device is certified to a security level and the verification is clear and trustworthy. The levels will solve a considerable portion of the gap between RPs and Device Vendors in terms of security related information of devices.

The levels supersede the previous level, so Level 2 will include all requirements for Level 1. Level 2 and above rely on existing certifications of underlying components defined by FIDO partners or technology organizations. If you are interested in FIDO supporting an additional Industry Technology as a partner program, please contact SRWG@lists.fidoalliance.org.

An implementation may complete FIDO Authenticator Certification for more than one Level. For each Level that FIDO Authenticator Certification is completed the implementation will be issued an Authenticator Certificate. There is no limit to the amount of Certifications possible for a single Authenticator implementation.

This section includes general examples of what is covered at each Certification Level. The formal definitions of each Certification Level and the specific differences between each Certification Level are defined within the Level-specific Security Requirements.

FIDO Authenticator Certification Levels are independent of (i.e. do not correspond to) partner and outside programs.

4.1.1 Level 1

Level 1 evaluates the Authenticator's implementation of security defenses.

The Level 1 Security Requirements will be tested and evaluated by FIDO Certification and Security Secretariats.

Examples of implementations that will NOT meet Level 1 Security Requirements:

- Authenticators that make their Active Server Pages (ASPs) readily available to other applications or users.

Level 1 Security Evaluations are completed by FIDO Security Secretariat.

4.1.2 Level 2

Level 2 evaluates the authenticator's defense against large scale software attacks.

Level 2 Authenticators are required to conform to a solution included in FIDO Allowed Restricted Operating Environment and Allowed Cryptography lists as part of the Security Requirements.

Examples of implementations that will NOT meet Level 2 Security Requirements:

1. Pure Rich OS software implementations of Authenticators that do not have a restricted operating environment.
2. Authenticators that do not support attestation.

Level 2 Security Evaluations are completed by a FIDO Accredited Security Laboratory.

4.1.3 Level 3

Level 3 tests the authenticator's defense against large scale software attacks, and provides greater assurance of defense compared to Level 2.

The Security Requirements for Level 3 depend on the technology and partner program used by the Authenticator.

Note: Level 3 is in active development in SRWG and it is not yet possible to certify to Level 3. This policy document will be updated when Level 3 is available for Certification.

4.1.4 Level 4 and Level 5

Level 4 and 5 rely on existing certifications of underlying components (e.g. Smart Card certifications - Common Criteria EAL 4+, or NIST Cryptographic Module Verification Program) defined by FIDO partners or technology organizations. The corresponding Security Requirements are based on the tamper-resistant technology used by the Authenticator.

Note: Levels 4 and 5 are in active development in SRWG and it is not yet possible to certify to Level 4 or Level 5. This policy document will be updated when they are available for Certification.

4.1.5 Level Upgrading and Downgrading

Upgrading (from Level 1 to Level 2, 3, 4, or 5) is only possible by completing FIDO Authenticator Certification for the new level, Conformance Self-Validation and Interoperability Testing is not required.

Downgrading a Security Level (for example, from Level 2 to Level 1) may be requested by the Vendor in cases where they can no longer meet the requirements of the higher level, or they no longer wish to have certification at the level originally requested, but can still meet the minimum requirements of the Level they are requesting a downgrade to. All requests for downgrading will be reviewed and approved by the Security Secretariat through the Delta Certification for Version Downgrade (7.2.3) process. If approved, the Authenticator Certificate will be updated to indicate the new Level but the date of certification will not be updated.

An implementation will never be automatically upgraded or downgraded from a Security Level for any reason.

5 Authenticator Certification Process

An implementation must have successfully completed FIDO Functional Certification requirements for Authenticators, including Conformance Self-Validation and Interoperability Testing, as outlined in FIDO Functional Certification Policy [Functional], before applying for FIDO Authenticator Certification.

The following sections provide a high-level overview of FIDO Authenticator Certification process and types of Certification.

5.1 Process Overview

A FIDO Implementation seeking FIDO Authenticator Certification must pass the following in order to receive FIDO Authenticator Certification:

Preparation

- FIDO Interoperability Requirements
  An implementation seeking FIDO Certification must first have successfully completed FIDO Functional Certification requirements for Authenticators, including Conformance Self-Validation and Interoperability Testing.
- Implementation Requirements
  The authenticator implementation seeking Certification must first implement all FIDO Security Requirements for a Level and prepare to pass the Security Test Procedures.
- Accredited Security Laboratory Selection
  The vendor should begin conversations with a FIDO Accredited Security Laboratory to prepare for FIDO Authenticator Certification.

Application

- The vendor completes the application to start FIDO Authenticator Certification process.

Security Evaluation

- The vendor completes the Vendor Questionnaire for the implementation seeking Certification, and the implementation must be evaluated against the Authenticator Security Requirements using FIDO Evaluation Report. For Level 1 this is completed by FIDO Security Secretariat, and for Level 2 it is completed by a FIDO Accredited Security Laboratory and a FIDO Evaluation Report is submitted to FIDO for review and approval by the Security Secretariat.

Certification Issuance

- Authenticator Certificates are issued once all Security Requirements for a Level are met, and evaluated by the Certification Secretariat.

Trademark Licensing Agreement (Optional)

- The Vendor signs the TMLA if they wish to use the Certification Mark or FIDO Logo.

Metadata Submission to MDS (Optional)

- The Vendor optionally uploads Metadata to MDS.

5.1.1 Step-by-Step Process

Table 5: FIDO Authenticator Certification Steps

Process Step	Responsible Party	Process Steps
Preparation	Vendor	Implements FIDO Specifications and Security Requirements.
	Vendor	For Level 2, Chooses a FIDO Accredited Security Laboratory to complete Security Evaluation.
	Accredited Security Laboratory	For Level 2, Proposes a contract to the Vendor pending Certification Application approval.
Functional	Vendor	Completes FIDO Functional Certification requirements for Authenticators, including Conformance Self-Validation and Interoperability Testing. See [Functional].
Application	Vendor	Submits FIDO Authenticator Certification Application to FIDO Certification Secretariat. Completes the Authenticator Vendor NDA and submits to FIDO.
	FIDO Certification Secretariat	Reviews the Application for completeness, communicates with the Vendor as needed to clarify any questions. Approves the Application when it meets all requirements and returns to Vendor. Signs FIDO portion of the Authenticator Vendor NDA, and returns to the Vendor.
Security Evaluation	Vendor	The Vendor must complete the Security Evaluation step for Level 1 OR Level 2.
Level 1: Security Evaluation	Vendor	Completes the Vendor Questionnaire and sends to FIDO Security Secretariat.
	FIDO Security Secretariat	Reviews the Vendor Questionnaire, and resolves any questions directly with the Vendor. Completes Security Evaluation by performing the Security Test Procedures.

		Completes FIDO Evaluation Report and submits to Vendor along with a decision to: • Approve, • Reject, or • Requests Clarification
Level 2: Security Evaluation	Vendor	Notifies the selected FIDO Accredited Security Laboratory that the Application meets FIDO's criteria and enters a contract with the Laboratory.
	Vendor	Completes the Vendor Questionnaire and sends to the Accredited Security Laboratory.
	Accredited Security Laboratory	Reviews the Vendor Questionnaire, and resolves any questions directly with the Vendor. Completes Security Evaluation by performing the Security Test Procedures. Completes FIDO Evaluation Report and submits to Vendor and FIDO Security Secretariat.
	FIDO Security Secretariat	Reviews the FIDO Evaluation Report and • Approves, • Rejects, or • Requests Clarification When a decision is made, returns the FIDO Evaluation Report to the Accredited Security Laboratory and the Vendor.
Certification Issuance	Vendor	When Laboratory Report is Approved, Completes a Certification Request, including: • Approved Vendor Questionnaire (for L1 only) • Approved FIDO Evaluation Report
	FIDO Certification Secretariat	Reviews the Certification Request, and if complete, issues an Authenticator Certificate.
	Vendor	Optionally signs FIDO Trade Mark License Agreement (TMLA) and/or a Certification Announcement with FIDO Marketing. Optionally uploads Metadata to MDS.

	FIDO Certification Secretariat	Updates Certified Products on FIDO website to reflect the Certification.

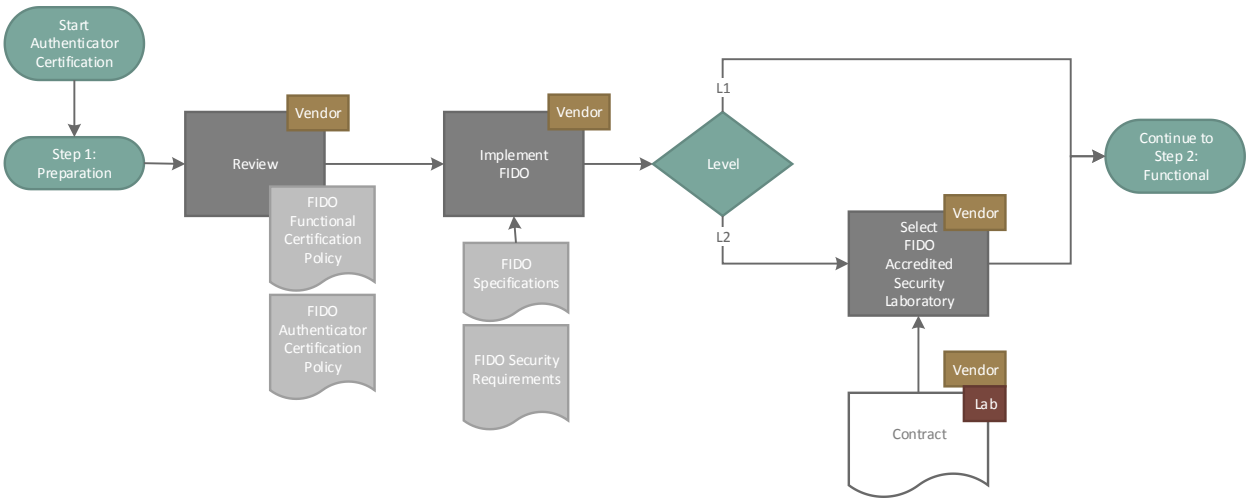
5.2 Preparation

Implementations seeking FIDO Certification must fulfill the requirements specified in the following documents:

1. FIDO Specifications (UAF or U2F)
2. FIDO Functional Certification [Functional] requirements for Authenticators
3. Authenticator Security Requirements for the Security Level requested (e.g. Level 2)
4. Authenticator Allowed Cryptography List
5. Authenticator Allowed Restricted Operating Environments List
6. Authenticator Metadata Requirements

For Level 2, it is recommended for the Vendor should contact a FIDO Accredited Security Laboratory early in order to work out contract and NDA details so the Vendor and the Lab are ready for the Security Evaluation process, and so the Lab can be listed as part of the Application step.

Figure 1: Step 1 - Preparation



5.3 Functional

Vendors must complete FIDO Functional Certification requirements for Authenticators, including the Conformance Self-Validation and Interoperability Testing, prior to submitting an application for FIDO Authenticator Certification. See [Functional] for FIDO Functional Certification requirements.

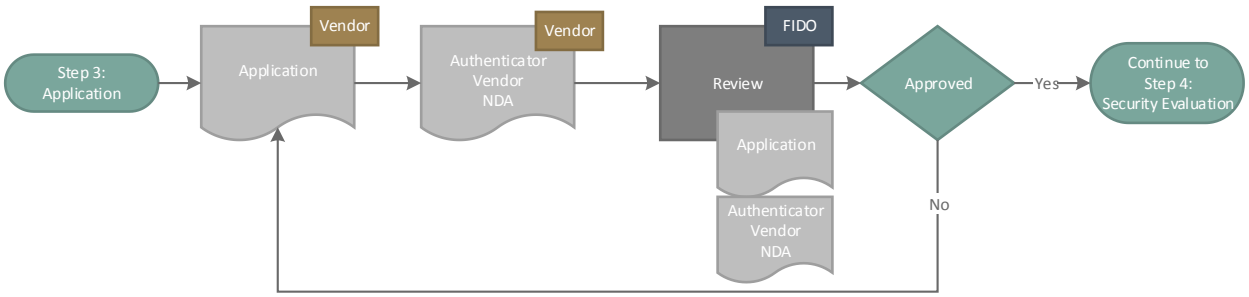
Figure 2: Step 2 - Functional

5.4 Application

To begin FIDO Authenticator Certification, the Vendor completes the Certification Application [Application].

FIDO Certification Secretariat is responsible for reviewing and approving the Certification Application and, if approved as complete, returning it to the Vendor.

Figure 3: Step 3 - Application



5.5 Security Evaluation

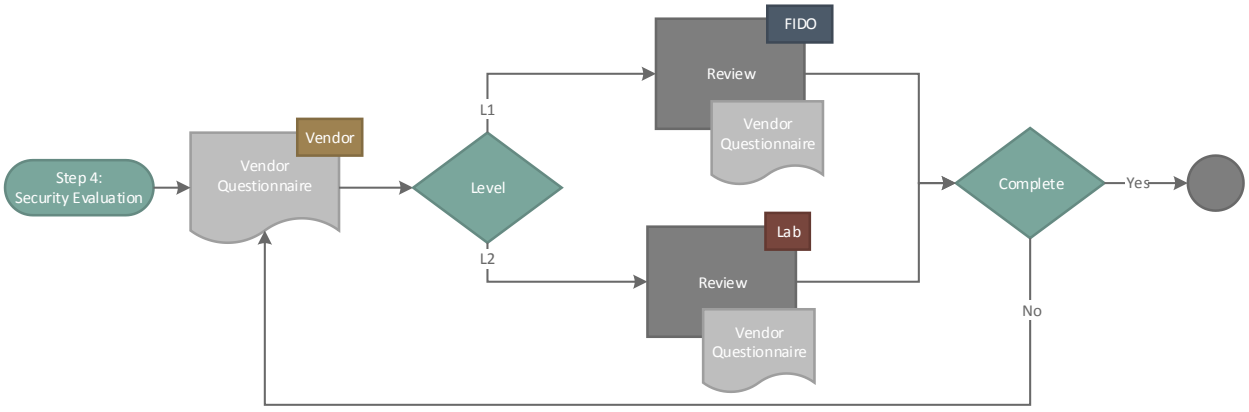
The Security Evaluation step includes the Vendor's attestation of how the implementation meets the Security Requirements and the Security Evaluation performed by FIDO Security Secretariat or a FIDO Accredited Security Laboratory to review the Vendor Questionnaire and complete the Test Procedures.

5.5.1 Vendor Questionnaire

Completing the Vendor Questionnaire [Questionnaire] includes actions from the Vendor, FIDO Security Secretariat, and the Accredited Security Laboratory.

The Authenticator Boundary needs to be defined by the Vendor during the Vendor Questionnaire in line with the Security Requirement 1.1 [Requirements]. After receiving an Authenticator Certificate, an implementation may not make any changes within the Authenticator Boundary and still claim to be FIDO Certified. If changes are made, a Delta Certification (Section 6) may be performed to verify that the changes do not impact the Security Requirements, and FIDO Certified status may be maintained.

Figure 4: Step 4 - Vendor Questionnaire Process



5.5.2 Level 1 Security Secretariat Evaluation

For Level 1, the Security Evaluation will be performed by the Security Secretariat by reviewing the Vendor Questionnaire and performing the Security Test Procedures [Test Procedures].

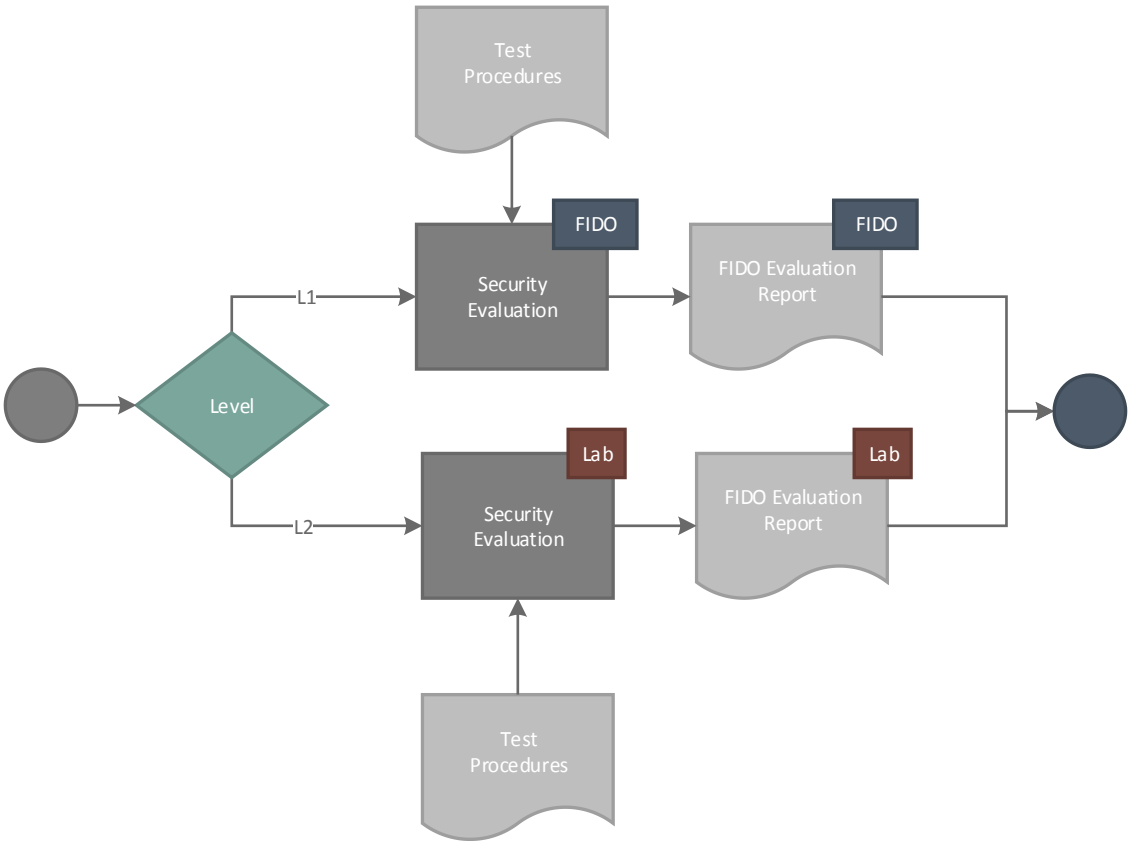
The Security Secretariat will complete a FIDO Evaluation Report [Evaluation Report] and return it to the Vendor.

5.5.3 Level 2 Laboratory Evaluation

For Level 2, the Vendor will choose a FIDO Accredited Security Laboratory to perform Security Evaluation by reviewing the Vendor Questionnaire and performing the Security Test Procedures [Test Procedures].

The Laboratory will complete a FIDO Evaluation Report [Evaluation Report] and return it to the Vendor and FIDO Security Secretariat.

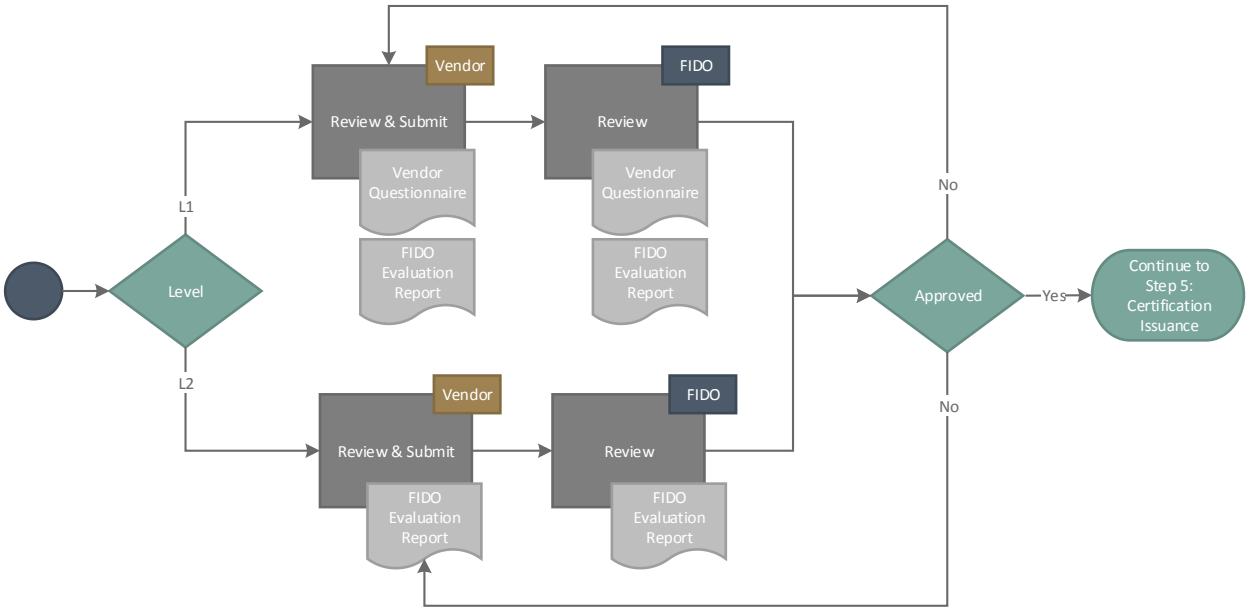
Figure 5: Step 4 - Security Evaluation Process



5.5.4 FIDO Evaluation Report Review

Once complete, the Vendor reviews the FIDO Evaluation Report prepared by the Laboratory or FIDO Security Secretariat and submits to FIDO. For Level 1, the approved Vendor Questionnaire and FIDO Evaluation Report must be submitted to FIDO. For Level 2, only the FIDO Evaluation Report must be submitted to FIDO.

Figure 6: FIDO Evaluation Report Process



5.6 Certification Issuance

5.6.1 Requests

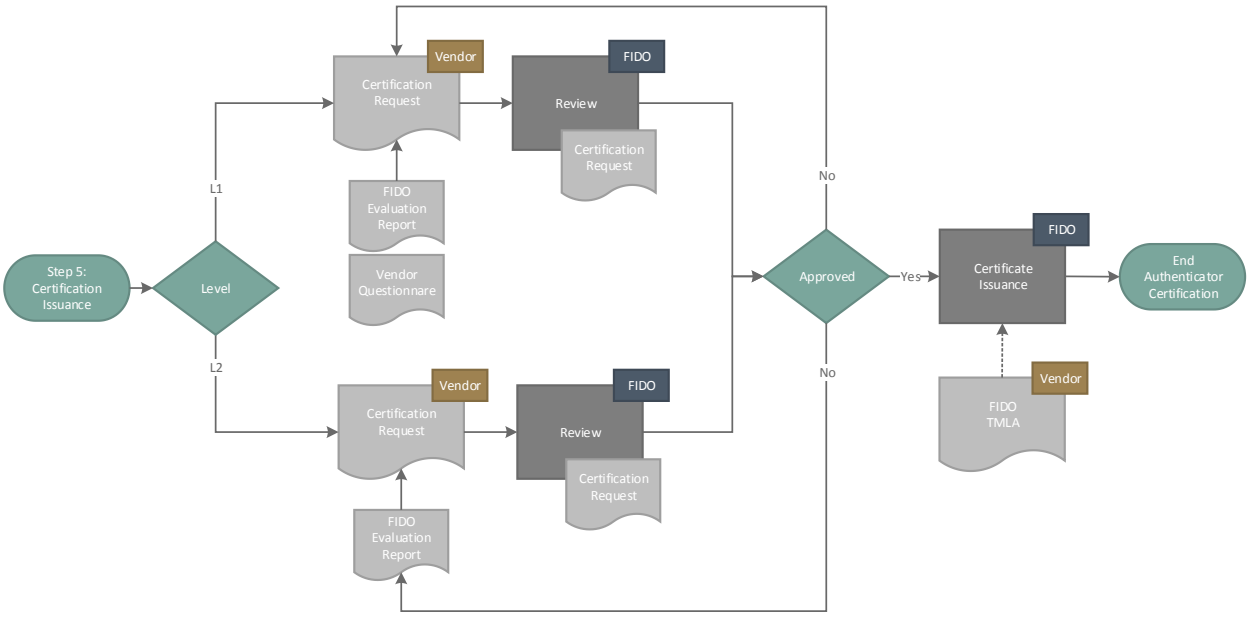
When submitting for FIDO Authenticator Certification, Vendors must:

1. Have passed testing requirements at an Interoperability Event, see FIDO Functional FIDO Certification Program Policy [Functional].
2. If a member of FIDO, be in good standing with all dues and invoices paid in full.
3. Be willing to adhere to all policies.

In order to receive FIDO Authenticator Certification, Vendors must submit the following for each implementation being certified:

1. Security Certification Request [Application]
2. Approved Vendor Questionnaire
3. Completed FIDO Evaluation Report
4. Certification Fees

Figure 7: Step 5 - Certification Issuance



If it is found that reports 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 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 or 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 Vendor's submission of final documentation to FIDO. There are four possible outcomes to certification:

Table 6: Authenticator Certificate Request Actions

Outcome	Description

Approval	The Vendor's Certification request is approved and the implementation is certified. Approval will only be granted if the implementation has all the required documentation. Upon approval, the certified implementation will be registered in the certification database and the Vendor will be notified by email. Notification will include a certification number for future reference.
Rejection	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 Vendor will be notified by email with the corresponding reason(s) for rejection and will have the opportunity to resubmit. 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.
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 10.6.1).
Failure	The request was rejected because the request was inappropriate or impossible and it would be inappropriate to resubmit.

Should a certification request be rejected, delayed, or failed, the submitting Vendor will have the right to submit a Dispute Resolution Request, which will follow the Dispute Resolution Process described in Section 10.6.1.

5.6.2 Issuance

When an Authenticator 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
- If UAF Authenticator, Vendor ID (also called AAID).
- FIDO Certification Program Policy version against which the implementation has been certified
- The date that the Vendor Questionnaire was approved
- The date that FIDO Evaluation Report was approved
- The security level
- The partner program (if Level 3 or above, FIDO if Level 1-2)
- Any dependent certifications (TEE, CC, etc.)

- The Accredited Security Laboratory that performed the evaluation
- FIDO Evaluation Report number
- A certification number of the format SSSVVVV-SSSSTTTT-LL-PP-DDDDDDDDNNN where:
    - SSS is FIDO Specification
    - VVVV is the version of FIDO specification
    - SSSS is the version of the Security Requirements
    - TTTT is the version of the Test Procedures
    - LL is to indicate that the numbered Level
    - PP is to indicate and abbreviated Partner Program, for example, GlobalPlatform will be abbreviated to GP.
        - Note: For Level 1 and Level 2 "FA" will indicate FIDO Alliance as there are no partner programs for Level 1-2.
    - DDDDDDDD is the date of issuance (year, month, day)
    - NNN is the sequential number of certifications issued that day

FIDO® Certified products [Certified] will be viewable and searchable by FIDO membership and the public-at-large, with the exception of certifications that are confidential (see Section 10.2.1.1).

6 Derivative Certification

Derivative Certification is for products or services that rely upon existing Certified implementations for conformance with 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 FIDO Functional Certification Policy in place at the time of the original (base) Certification.

The process for Derivative Certification for an Authenticator is described in the Functional Policy [Functional].

7 Delta Certification

Delta Certification is testing to verify the implementation still meets requirements in the following cases:

- after changes are made to a Security Certified implementation (see Delta Certification for Product Upgrades),
- when changes are made to the Security Test Procedures (see Delta Certification for Version Upgrade), or
- to remove a Suspension (see Delta Certification after Suspension).

Changes that do not meet the Delta Certification definition as outlined below require full testing (i.e. new Certification).

The Delta Certification Process applies to all Delta Certifications, specific differences for each type are listed in the Types of Delta Certification section below.

7.1 Delta Certification Process

Delta Certification should be pursued by Certified implementations that have made a change within the authenticator boundary or that are upgrading their implementation to an Active version of FIDO Specification, Security Requirements, or Test Procedures (for versioning see 3 and 10.5).

7.1.1 Impact Analysis Report

The vendor is required to submit their original Vendor Questionnaire with the respective changes to the original certification explained - this document is referred to as the Impact Analysis Report. The Impact Analysis Report must indicate all changes since the original certification, and include the type of Delta Certification they are requesting. The Security Secretariat reviews and approves the Impact Analysis Report.

7.1.2 FIDO Security Secretariat Review

All Impact Analysis Reports will be reviewed by the Security Secretariat.

7.1.3 Delta Security Review

Delta Certification requires a Delta Security Review for the areas identified in the Impact Analysis Report. This Delta Security Review will be completed by an Accredited Security Laboratory unless determined to be Laboratory Exempt by the Security Secretariat. For Level 1, all Delta Certifications are Laboratory Exempt.

7.1.3.1 Laboratory Review

Changes made inside the authenticator boundary are reviewed by a FIDO Accredited Security Laboratory to determine if any changes are relevant to the functionality used by the Authenticator to meet FIDO requirements.

- If changes **are not** relevant, the lab issues a letter to FIDO Security Secretariat requesting that the existing certification be extended to include the new version of hardware and/or firmware.
- If the changes **are** relevant to functionality used to meet FIDO Security Requirements, then the lab conducts all testing that is relevant to the impacted functionality. A letter with the results is then drafted by the lab and sent to FIDO Security Secretariat requesting that the certification be extended. In the event that the testing shows non-compliance, the results are reported to the developer to support remediation.

7.1.3.2 Laboratory Exempt

When following the Delta Certification process, an implementation may be found to have made changes that will be considered "Laboratory Exempt" by the Security Secretariat during review of the Impact Analysis Report.

Laboratory Exempt is used to describe the decision that the Security Secretariat has ruled the changes made to the implementation are exempt from requiring evaluation by a FIDO Accredited Security Laboratory. The Impact Analysis Report will still be evaluated by the Security Secretariat and the Lab Evaluation step is the only portion of the Delta Certification process that is skipped for Exempt Delta Certification.

Examples of Laboratory Exempt reasoning:

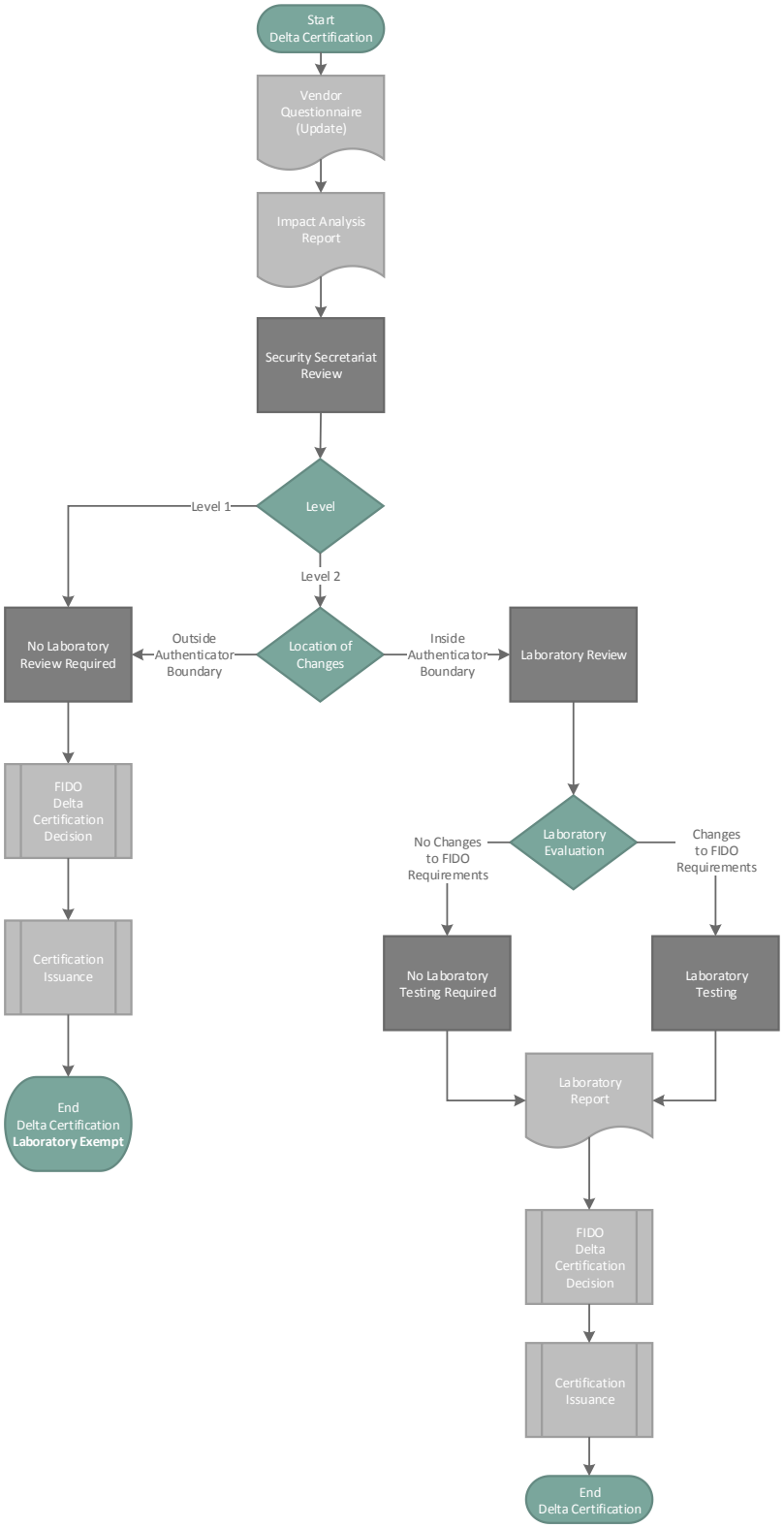
- Level 1
    - All Level 1 Delta Certifications will be "Laboratory Exempt".
- Product Upgrades
    - The change(s) were made outside of the Authenticator Boundary of the Security Certified Implementation and shows clearly no impact on the security of the Authenticator.
    - The change(s) were reviewed by FIDO Security Secretariat and determined to not impact the ability of the implementation to meet the Security Requirements or Test Procedures originally certified against.
- Security Test Procedures Version Upgrades
    - The Laboratory Report from the original certification demonstrates that the implementation meets the requirements of the latest version.
    - The changes included in the new version do not apply to the Security Certified implementation.

If the changes made are determined by the Security Secretariat to be Laboratory Exempt, the Vendor will be notified by the Security Secretariat and the Review by an Accredited Security Laboratory will not be required. The Security Secretariat will complete the Review of the Impact Analysis Report and if approved, will notify the Vendor that they may then apply for a Delta Certificate.

7.1.4 Delta Certification Issuance

If any changes made during the Delta Certification process impact the original Certificate (see Issuance) a new Certificate will be issued by the Certification Secretariat. This includes the Certification Level or the Version of FIDO Specification, Security Requirements, or Test Procedures.

Figure 8: Delta Certification Process



7.2 Types of Delta Certification

7.2.1 Delta Certification for Product Upgrades

Delta Certification for Product Upgrades should be used when a vendor makes changes to their Security Certified implementation or its environment after initial FIDO Authenticator Certification.

7.2.2 Delta Certification for Version Upgrade

Security Requirements and Security Test Procedures will be maintained and versioned by the SRWG. A Vendor is allowed to upgrade to an Active Version of the Security Requirements or Test Procedure (see Section 10.5) using the Delta Certification process.

A new Authenticator Certificate will be issued for a Delta Certification for Version Upgrade to reflect the Version of the Security Requirements.

7.2.3 Delta Certification for Level Downgrade

A Vendor may request a Version Downgrade (e.g. Level 2 to Level 1).

A new Authenticator Certificate will be issued to indicate the new Level but the date of certification will be the same as the original Certificate.

7.2.4 Delta Certification for Security Vulnerability

If an Authenticator Certificate has been suspended due to a Security Vulnerability, the implementation must make changes to resolve the identified security vulnerability with the Vendor Deadline for Corrective Action (see Security Vulnerability Assessment, section 9).

A Delta Certification for Security Vulnerability requires the Vendor to provide FIDO with an Action Plan that outlines the Vendor's roll out plan once the Delta Certification is issued. The Action Plan can be defined by the Vendor, but should include at the minimum a statement of intent to release the implementation and a timeline for such a release. FIDO will not monitor or enforce Action Plans, but will use them to understand the current market risk for FIDO implementations.

7.2.5 Delta Certification after Suspension

If a certification has been suspended (Section 10.2.3), a vendor is allowed to reactivate a suspended certification using the Delta Certification process.

7.2.5.1 Policy Suspension

If an implementation is found to not be in compliance with FIDO Authenticator Certification Policy, including the ability to meet the Security Requirements as originally certified, the implementation may be suspended by the Security Secretariat. See section 10.2.3.

7.2.5.2 Security Vulnerability Suspension

If an Authenticator Certificate has been suspended due to the failure to respond to FIDO by the Deadline or to complete a Corrective Action, the Vendor must complete one of the Vendor Action Options that correspond to the Attack Potential of the Vulnerability to remove the suspension.

If an Authenticator Certificate has been suspended due to a Security Vulnerability, the implementation must make changes to resolve the identified Security Vulnerability (Section 9). The Delta Certification process must be used to certify changes to an implementation made as a result of a Security Vulnerability.

An approved Delta Certification after Suspension will reactivate a Suspended Certification and remove the suspended status, but will not update the original certification date.

If an Authenticator Certificate is in the Suspended state for 180 days due to a Security Vulnerability the Certificate will be escalated to “Revoked”.

8 FIDO Authenticator Certification Revocation

An Authenticator Certificate can be revoked by the Security Secretariat with recommendations from SRWG. Revocation is an indication that the Authenticator is no longer certified and will never return to good standing.

Revocation events include:

1. Failure to follow FIDO Authenticator FIDO Certification Program Policy (this document), including:
    a. Failure to respond to and address Security Vulnerabilities (Section 9) identified in a Security Certified product.
    b. Failure to report changes made to a Security Certified implementation. To remain Security Certified after changes, a Vendor must follow the Delta Certification process (Section 7).
2. False statements on any FIDO form.
3. Violation of FIDO Trademark & Licensing Agreement, if signed.
4. Remaining in a “Suspended” state for more than 180 days.

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 (unless it is a Security Vulnerability, which would be handled as outlined in Section 9) 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.

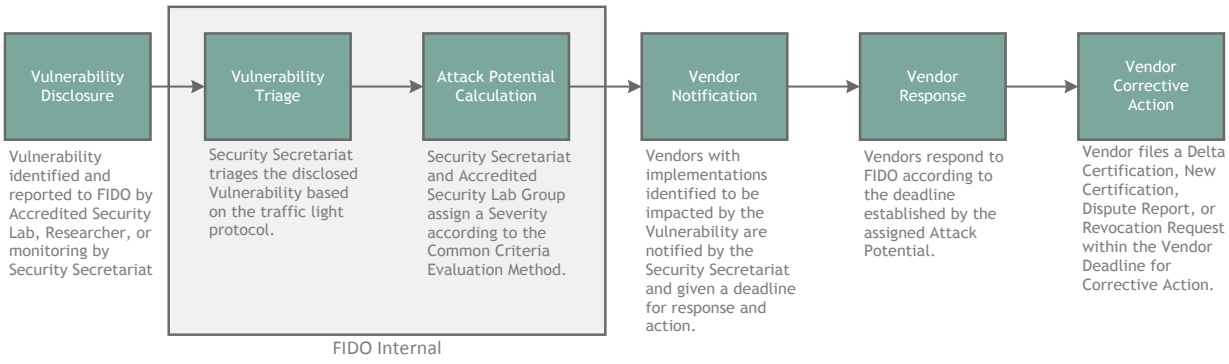
If the Vendor submitted Metadata Statements, the Table of Contents (TOC) for the certificate will be updated via a status update by the Certification Secretariat to reflect the updated certification state.

9 Security Vulnerability Assessment

In recognition that security is a process and the landscape of threats is constantly evolving, the Security Secretariat will be responsible for identifying and evaluating new threats as they arise, and recommending to SRWG how to appropriately update Security Test Procedures, or FIDO Authenticator Certification Policy. The assessment of threats occurs as both a periodic requirements review and as an ad hoc process.

The Security Secretariat will work with third-parties such as vendors, researchers, and labs to identify new threats and attacks and will follow the Security Vulnerability Assessment process described below. The SRWG may form a subcommittee specifically dedicated to analyzing and addressing these threats.
The Security Vulnerability Assessment process will be reviewed every six months by the SRWG to evaluate if the categories and processes are meeting the needs of FIDO Certification. The Security Vulnerability Assessment will be updated as necessary to reflect FIDO Security landscape.

Figure 9: Security Vulnerability Assessment Process



9.1 Vulnerability Disclosure

A vulnerability is a weakness of software, hardware, or online service that can be exploited. The following proposed process is based on the international standard for disclosing a vulnerability as outlined in ISO/IEC 29147:2014, *Information technology - Security techniques - Vulnerability disclosure* [ISO/IEC 29147:2014].

9.1.1 Means for Contact

FIDO Contact page will have a referring link to the Vulnerability Disclosure form. All contact between FIDO and the Vendor will be secure.

9.1.2 Active Monitoring

The Security Secretariat will monitor, at a minimum, the following sources for security alerts:

- US-CERT [US-CERT]
- NIST National Vulnerability Database [NIST NVD]
- MITRE Common Vulnerabilities and Exposures [MITRE]

9.1.3 Ad Hoc Security Updates

Ad Hoc Security Updates are notifications from FIDO Security Secretariat, security labs, partner programs, or researchers to SRWG.

9.1.4 Bulletins and Alerts

Based on the analysis of identified threats, FIDO Security Secretariat may issue monthly bulletins or ad hoc alerts to impacted Vendors of FIDO Security Certified implementations and FIDO Approved Laboratories.

9.1.5 Periodic Security Review

No less than once every 12 months from the date of last publication, SRWG will review, and if needed, update and vote to approve modifications to the Security Requirements.

9.1.6 Confidentiality

Company- or Implementation-specific concerns will be addressed privately by the Security Secretariat. The company, product, vendor model, or information on how to replicate the vulnerability will never be disclosed to other FIDO Staff, FIDO Members, or FIDO Working Groups.

Anonymized information on the vulnerability may be provided to SRWG or other technical working groups (as defined in the Triage Action of Table 7) for expert opinions on the vulnerability. The vendor can designate if confidentiality can be removed for SRWG or other groups on a case-by-case basis.

9.2 Vulnerability Triage

Should the Security Secretariat be notified of or identify a threat the Security Secretariat will triage the severity of the vulnerability and send notifications based on the US-CERT Traffic Light Protocol (https://www.us-cert.gov/tlp).

The Vulnerability Triage step is the first step of the Vulnerability Assessment process and is used as internal pre-selection criteria to help determine which groups should be notified and how quickly the vulnerability needs to be assigned a severity.

The Vulnerability Triage Protocol is defined in Table 7. Once a Vulnerability has been assigned a Triage Level (Red, Amber, Green, or White) the Security Secretariat will kick off the Triage Action. The Triage

Action for each Triage Level has a deadline, and from that deadline there is an Attack Potential Calculation Deadline. For example, if a vulnerability is triaged as **Amber** the Security Secretariat must hold a call with the Security Lab Group and Crisis Response team within 3 business days of Vulnerability Disclosure, and within 5 business days of that call the Attack Potential Calculation must be complete. The total elapsed time from Vulnerability Disclosure to Attack Potential Calculation for an Amber vulnerability must not exceed 8 business days.

Table 7: Vulnerability Triage Protocol

Triage Level	Triage Reasoning	Triage Action	FIDO Attack Potential Calculation Deadline (from Triage Action)
RED	Attack in progress OR At-scale attacks exist that can be performed with readily available tools and limited skill.	Schedule a call within 72 hours of Vulnerability Disclosure with the Accredited Security Lab Group and Crisis Response Team to share information about the vulnerability.	3 business days
AMBER	Vulnerability that is likely lead to a scalable attack.	Share information and documents with the Accredited Security Lab Group and the Crisis Response Team within 3 business days.	5 business days
GREEN	Vulnerability where attack unlikely, or not scalable.	Share information and documents with entire Accredited Security Lab Group and SRWG within 5 business days.	14 business days
WHITE	Vulnerability that is outside the scope of FIDO specifications.	Share information in a monthly bulletin.	N/A End Vulnerability Assessment Process.

Severity Examples

- **White** — Out of scope of Certification or the Authenticator security boundary.
- **Green** – Researcher finds a theoretical flaw that requires special / new tools to carry out the attack.
- **Amber**— Software to exploit the vulnerability is available.
- **Red** — Actual attacks against this authenticator have been carried out.

Attack Potential Calculation Deadlines are shown in Table 7.

9.3 Attack Potential Calculation

The Attack Potential Calculation process is used to quickly notify the proper groups of a Security Vulnerability.

Each Vulnerability triaged as Red, Amber, or Green during the Vulnerability Triage stage requires the notification group to meet to calculate and assign a formal Attack Potential using the Rating of Vulnerabilities summarized in
Table 9.

A Vulnerability triaged as White will not continue the Vulnerability Assessment process.

The assigned Attack Potential will be calculated based on the potential to exploit the vulnerability as defined in Appendix B.4 of the Common Criteria Evaluation Methodology (CEM) version 3.1 revision 4 (https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf). Potential vulnerabilities are prioritized based on an estimate of time, expertise, knowledge, access, and equipment.

An excerpt of the calculation of attack potential is included here, but the full version is included in CEM.

Table 8: Calculation of Attack Potential

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple Experts	8
Knowledge of TOE (Target of Evaluation)	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / Unlimited Access	0

Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialized	4(3)
Bespoke	7
Multiple Bespoke	9

(1) When several proficient persons are required to complete the attack path, the resulting level of expertise still remains "proficient" (which leads to a 3 rating).

(2) Indicates that the attack path is not exploitable due to other measures in the intended operation environment of the TOE.

(3) If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke.

Table 8 is used to assign values to what factors are required to exploit the Vulnerability; Elapsed Time, Expertise, Knowledge of the Target of Evaluation (TOE), Window of Opportunity, and Equipment. The sum of value of each area is then used to assign an Attack Potential category.

Table 9 shows the value ranges for each Attack Potential category. Vulnerabilities calculated with a total value between 0-9 are considered to have Basic attack potential. For example, a value of 0 means a layman attacker with standard equipment and using public knowledge of the TOE with unlimited access could exploit the vulnerability in less than one day. Enhanced-Basic with a range of 10-13 could be that same scenario, but change the elapsed time to 3 or 4 months. Another example of Enhanced-Basic is the same scenario as above but maybe it requires an expert and specialized equipment but still with public knowledge and unlimited access the vulnerability could be exploited in less than a day, giving a value of 10.

Table 9: Rating of Attack Potential

Values	Attack Potential
0-9	Basic
10-13	Enhanced-Basic
14-19	Moderate
20-24	High
=>25	Beyond High

Note: As FIDO Certification Program evolves, the Accredited Security Laboratory Group will be responsible for defining FIDO-specific scoring criteria that can be used to augment CEM to better align with the technology and environments of FIDO Authenticators.

9.4 Vendor Notification

Once a Vulnerability has been assigned an Attack Potential the Security Secretariat will review the impact on existing Certifications. If a Security Certified implementation is found to have a security vulnerability,

the Vendor will be given notice of the type and calculated attack potential of the vulnerability by the Security Secretariat. The Vendors or Products impacted by a Security Vulnerability will never be shared outside of the Security Secretariat.

Attack Potential Calculations will be reevaluated more than once during the life-cycle of a vulnerability. In the case that the Attack Potential is updated (for example, from Enhanced-Basic to Basic) a new Notice will be sent to the Vendor with the new Attack Potential. When a Notice is distributed it voids any previous notices and restarts the Vendor Response and Corrective Action step.

9.5 Vendor Response and Corrective Action

Note: The following process is only relevant to Level 1 and Level 2 Certification as per this version of the document. Future versions addressing higher levels of certifications may impact the deadlines, the attack potential and required actions.

9.5.1 Vendor Response

Upon receiving notice from FIDO Security Secretariat, the Vendor will be required to respond to FIDO Security Secretariat within the Vendor Deadline for Response to FIDO for the Assigned Severity, and include their intent to take Corrective Action within the deadline within the Vendor Deadline for Corrective Action in Table 10 and Table 11.

Note: At the time of the response to FIDO the Vendor may not know what Corrective Action they will pursue, the response deadline is just to acknowledge to FIDO that the Vendor received the notice of the vulnerability and agrees to take Corrective Action within the deadline.

9.5.2 Vendor Corrective Action

Within the Vendor Deadline for Corrective Action in Table 10 and Table 11 the Vendor has the option to correct the implementation and show their intent to remain Security Certified by filing an application for a Delta or New Certification. If the Vendor chooses not to make any corrections to their implementation the vendor may request Revocation by filing a Revocation Request. If the Vendor does not agree with the assigned Attack Potential of the vulnerability, the Vendor may file a Dispute Report with the Security Secretariat.

“Corrective Action” in Table 10 and Table 11 is defined as one of the following:

- Filing an Application for a New Certification, and filing a Revocation Request for the Certification with the Vulnerability.
- Filing an Application for a Delta Certification.
    - If the Vendor is filing for a Delta Certification due to corrections made to the implementation, an Action Plan is required to be provided to FIDO that outlines the Vendor’s roll out plan once the Delta Certification is issued. See section 7.2.4, Delta Certification for Security Vulnerability.
- Filing a Revocation Request for the Certification with the Vulnerability.

- Filing a Dispute Report with the Security Secretariat.

Note: Filing the Application, Request, or Dispute is the beginning of the respective processes and all that is required to fulfill the Corrective Action requirements. Corrective Action means that the process to protect the Certification against the Security Vulnerability has been started, but completing the entire process is not required within the Deadline for Corrective Action.

For an explanation of the consequences of not meeting the Deadlines listed in Table 10 and Table 11, see FIDO Deadline Enforcement.

Level 1 and Level 2 have different Vendor Action Deadlines and Corrective Action Requirements, Level 1 is outlined in and Level 2 is outlined in.

9.5.2.1 Level 1 Vendor Action Deadlines

Table 10: Vendor Action Deadlines – Level 1

If the Attack Potential is:	Vendor Deadline for Response to FIDO	Corrective Action Required?	Vendor Deadline for Corrective Action
Basic	5 business days from Notice	Yes	90 days from Notice
Enhanced-Basic	15 business days from Notice	No	No Corrective Action Required.
Moderate	30 business days from Notice	No	No Corrective Action Required.
High	60 business days from Notice	No	No Corrective Action Required.
Beyond High	No Response Required.	No	No Corrective Action Required.

9.5.2.2 Level 2 Vendor Action Deadlines

Table 11: Vendor Action Deadlines – Level 2

If the Attack Potential is:	Vendor Deadline for Response to FIDO	Corrective Action Required?	Vendor Deadline for Corrective Action
Basic	5 business days from Notice	Yes	90 days from Notice
Enhanced-Basic	15 business days from Notice	Yes	150 days from Notice
Moderate	30 business days from Notice	Yes	365 days from Notice
High	60 business days from Notice	No	No Corrective Action Required.
Beyond High	No Response Required.	No	No Corrective Action Required.

9.5.3 FIDO Deadline Enforcement

FIDO will enforce the Vendor Deadline for Response to FIDO and Vendor Deadline for Corrective Action by either suspending or revoking certifications, as shown in Table 13.

For all changes to the certification state, if the Vendor submitted Metadata Statements to MDS, the Table of Contents (TOC) for the Certificate will be updated via a status update by the Security Secretariat to reflect the updated certification state.

9.5.3.1 Vendor Deadline for Response to FIDO

If the Vendor does not notify FIDO within the Deadline for Response to FIDO indicated in the notice the certification state will be updated to "Suspended".

If no response is received by the Vendor within 180 days of the Vendor Deadline for Response to FIDO (where required), the certification state will be changed to "Revoked" (see Section 10.2.4).

For a failure to respond, a Certificate may be returned from the "Suspended" state back to the "Certified" state by responding to FIDO. The Vendor Deadline for Corrective Action will remain the same, regardless of when the Vendor responds.

9.5.3.2 Vendor Deadline for Corrective Action

If the Vendor does not take Corrective Action by the date specified in the Deadline for Corrective Action, the certification state will be updated to "Suspended".

An Authenticator Certificate may be returned from the "Suspended" state back to the "Certified" state by performing one of the Vendor Corrective Action Options for the Attack Potential. See Delta Certification after Suspension.

If no Corrective Action is received by the Vendor within 180 days of the Vendor Deadline for Corrective Action (where required), the certification state will be changed to "Revoked" (see Section 10.2.4).

9.5.3.3 Level 1 Deadlines

Table 12: FIDO Deadline Enforcement – Level 1

If the Attack Potential is:	Vendor Deadline for Response to FIDO (Suspension Date)	Vendor Deadline for Response to FIDO (Revocation Date)	Vendor Deadline for Corrective Action (Suspension Date)	Vendor Deadline for Corrective Action (Revocation Date)
Basic	5 business days from Notice	185 days from Notice	90 days from Notice	270 days from Notice
Enhanced-Basic	15 business days from Notice	195 days from Notice	N/A	N/A
Moderate	30 business days from Notice	210 days from Notice	N/A	N/A
High	60 business days from Notice	240 days from Notice	N/A	N/A
Beyond High	N/A FIDO will not Suspend or Revoke Certifications with Beyond High Attack Potential.			

9.5.3.4 Level 2 Deadlines

Table 13: FIDO Deadline Enforcement – Level 2

If the Attack Potential is:	Vendor Deadline for Response to FIDO (Suspension Date)	Vendor Deadline for Response to FIDO (Revocation Date)	Vendor Deadline for Corrective Action (Suspension Date)	Vendor Deadline for Corrective Action (Revocation Date)
Basic	5 business days from Notice	185 days from Notice	90 days from Notice	270 days from Notice
Enhanced-Basic	15 business days from Notice	195 days from Notice	150 days from Notice	330 days from Notice
Moderate	30 business days from Notice	210 days from Notice	365 days from Notice	545 days from Notice
High	60 business days from Notice	240 days from Notice	N/A	N/A
Beyond High	N/A. FIDO will not Suspend or Revoke Certifications with Beyond High Attack Potential.			

10 Program 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 FIDO Alliance; or that the statement of work be amended as appropriate.

10.1 Sensitive Information

The FIDO Security Secretariat and FIDO Certification Secretariat are responsible for protecting sensitive information during transit and storage.

When submitting electronic documentation to FIDO, it must be PGP encrypted and securely uploaded using forms on the FIDO website. All FIDO Certification forms and Evaluation Reports and their attachments will be stored within an encrypted database only accessible by the FIDO Certification Secretariat and Security Secretariat, and will not be shared.

Unless a previous agreement has been made between the FIDO Certification Secretariat or the FIDO Security Secretariat and the Vendor or Laboratory, all documents sent via email will not be reviewed and will be deleted.

10.2 Certification States

A list of Certified Authenticators will be maintained by the Certification Secretariat and a public list will be available on FIDO Website [Certified]. Certification may be in the following states: Active, Confidential, Certified, Suspended, or Revoked.

10.2.1 Active

Once an application is submitted to FIDO, the Certification state becomes “Active”. Active applies to initial Certification and Delta Certification.

This state is not shared outside of FIDO Staff.

10.2.1.1 Confidential

Confidential Certification is allowed for companies that wish to complete FIDO Certification process confidentially. Vendors can request their certification remain confidential when applying for Certification.

During a Confidential Certification, only FIDO Certification Secretariat and FIDO Security Secretariat and FIDO Executive Director have any knowledge of the existence or details of the product. Any Accredited Security Laboratory involved in certification will also have knowledge of the product. FIDO Working Groups and FIDO Board of Directors will not have knowledge of the product until Confidentiality is

withdrawn. The Certificate will not be announced and will not appear on FIDO Website until Confidentiality is withdrawn.

Confidentiality may be withdrawn at the request of the Vendor by submitting a written request to the Certification Secretariat with the corresponding certification number. The Certification Secretariat will contact Vendors of confidential certifications once every three months to verify that certifications should retain the confidential status.

The requirements for an implementation to pass Confidential Certification are the same as for any other FIDO Certified implementation.

10.2.2 Certified

An implementation with a “Certified” status is one that has been issued an Authenticator Certificate and is in good standing.

10.2.3 Suspended

An Authenticator Certificate may be suspended, for more information on the Suspension process, see Section 9.4.

10.2.4 Revoked

An Authenticator Certificate may be revoked, for more information on Revocation, see Section 0.

10.3 Publication and Disclosure of Certification Status

This section outlines how and what a Vendor can say about their FIDO Certified product.

10.3.1 Metadata

During the Security Evaluation the Metadata Statement will be verified for accuracy and completeness. The required fields for FIDO Authenticator Certification are outlined in the Authenticator Metadata Requirements [Authenticator MDS Req]. Implementations seeking Certification must register Metadata Statements with FIDO Security Secretariat during the Certification Request.

The Vendor has the option to submit Metadata to FIDO MDS. FIDO Metadata Service [MDS] will allow FIDO Authenticators to describe their security-relevant characteristics to Relying Parties (RP). The Metadata Statement is optional to submit to MDS, however it is strongly encouraged to provide information to RPs.

10.3.2 Trademark and Licensing Agreements

10.3.2.1 Usage

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

FIDO Certification Mark(s) may only be used in conjunction with implementations that have the approved corresponding certification, and where the Vendor has executed FIDO Alliance Trademark License Agreement [TMLA]. 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 FIDO Certification mark(s) if they agree to FIDO Trademark and Service Mark Usage Agreement for Websites [Web TMLA].

10.3.2.2 Violation Reporting

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

10.3.2.3 Enforcement

The Certification Secretariat will be responsible for a monthly review of certification mark usage and usage of 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 outside of policy or the TMLA. 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 FIDO Certification Program Policy or FIDO Authenticator Certification Policy, they will have the right to submit a Dispute Report [Dispute] that will follow the Dispute Resolution Process (Section 10.6.1).

10.4 Product Documentation

Only implementations that have a FIDO Authenticator Certificate can claim to be a FIDO® Certified Authenticator. This includes, but is not limited to, within data sheets, marketing materials, websites, and product packaging.

10.4.1 Guidelines

All documentation referencing FIDO Authenticator Certification should include:

- Level of FIDO Authenticator Certification
- Partner Program, if Level 3 or above (e.g. GlobalPlatform TEE)
- Date of Functional Certificate Issuance
- Date of Authenticator Certificate Issuance
- Version of Security Test Procedures used for FIDO Authenticator Certification

10.4.2 Violation Reporting

In the event that a reference to FIDO® Certified or FIDO® Certified Authenticator is being misused, a report can be filed by contacting FIDO Certification Secretariat.

10.4.3 Enforcement

The Certification Secretariat will be responsible for a monthly review of the usage of FIDO® Certified terminology to ensure that usage is compliant with these guidelines.

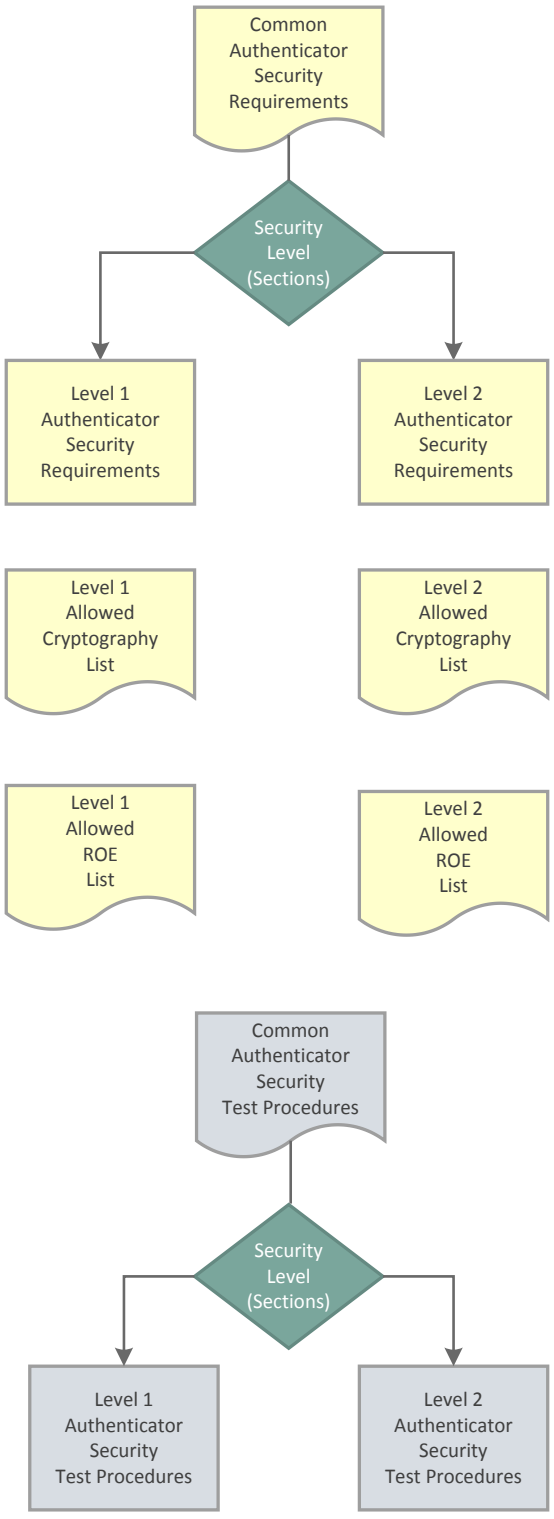
Reasonable attempts will be made to contact any party that is using the certification terminology in an unapproved fashion. If the party contacted is a FIDO member and they disagree with the assessment that the certification mark is being used in a way that FIDO Certification Program Policy violates policy, they will have the right to submit a Dispute Report [Dispute] that will follow the Dispute Resolution Process (Section 10.6.1). Should a violation be found, and no action is taken after reasonable attempts to contact the vendor, it will be referred to the Board of Directors.

10.5 Security Requirement Versioning

Every certification issued by FIDO Alliance must be against an Active Version of the Security Test Procedures. Version history, including the Active Version(s) and their descriptions, will be maintained on FIDO Website.

The Document Hierarchy dictates that Security Test Procedures, as the lowest level, will always be updated and it is therefore the revision of the Security Test Procedures that will trigger the following versioning process.

Figure 10: Authenticator Document Hierarchy



10.5.1 Security Requirements

Security Requirements refers to the document set outlining the requirements for FIDO Authenticator Certification. This includes:

1. Level- or Partner-Specific Authenticator Security Requirements,
2. Authenticator Allowed Cryptography List,
3. Authenticator Allowed Restricted Operating Environments List, and
4. Authenticator Metadata Requirements.

10.5.1.1 Conditions

The individual documents that make up the Authenticator Security Requirements may be updated independently of one another.

10.5.2 Level- or Partner-Specific Security Requirements

Level- or Partner-Specific Security Requirements are the Security Requirements applicable to each level or partner program are required in addition to the Common Authenticator Security Requirements.

10.5.2.1 Conditions

When a new revision of the Level or Partner-Specific Security Requirements is developed, all supporting documents are required to be updated in accordance with the Level- or Partner-Specific Security Requirements.

10.5.3 Security Test Procedures

The Security Test Procedures outlines the specific tests required to be administered by the Accredited Security Laboratory to verify the implementation meets the Authenticator Security Requirements. Security Test Procedures include tests to meet the common, level- and partner-specific Security Requirements.

10.5.3.1 Conditions

Security Test Procedures can be updated independently of the Common, or Level- or Partner-Specific Security Requirements. If it is found that the Security Test Procedures do not satisfactorily test the Authenticator Security Requirements (e.g. due to discovered vulnerabilities or threats) new test procedures may be added without changes to any Security Requirements.

The Security Test Procedures will always be updated if the Common, or corresponding Level- or Partner-Specific Security Requirements are updated. As new Security Requirements are created, the Security Test Procedures will require an update to support testing of those requirements.

The SRWG together with the Security Secretariat represent the interests of FIDO Authenticator FIDO Certification Program, including Certified Authenticators. The Security Test Procedures will be updated only as determined to be necessary to protect and maintain the security of these interests.

10.5.4 Active Version(s)

The Active Version(s) of Security Test Procedures refers to a version or versions that are currently published and will be accepted for Certification. A new version of the Security Requirements or Security Test Procedures is published and available for certification on an Evaluation Availability Date specific to that version. After this date the version becomes Active, and there will be a Transition Period (described below) where the previous Security Test Procedures are being phased out to a Sunset Date (described below). A version is no longer considered Active once the Sunset Date has passed.

The example below is a scenario for a Version 2.0 release. In this scenario, the Level 2 Security Test Procedures Version 2.0 has an Evaluation Availability date of June 1, 2020. The Sunset Date for Version 1.0 is then assigned to be one year from that date. A vendor wishing to complete Level 2 Certification between June 1, 2020 and June 1, 2021 has the option to apply for Certification against the two Test Procedure versions that are active, 1.0 and 2.0. This is considered the transition period for Version 1.0. On June 2, 2021 the only Active Version will be 2.0. Since the Sunset Date for Version 1.0 has passed, and the vendor must comply with the Version 2.0 Security Test Procedures for any new or Delta Certifications.

Table 14: Example Active and Sunset Date

Certification Level	Security Requirements Version	Security Test Procedures Version	Evaluation Availability Date	Sunset Date
1	1.0	1.0	January 1, 2017	-
2	1.0	1.0	January 1, 2017	June 1, 2021
2	1.0	2.0	June 1, 2020	-

10.5.4.1 Evaluation Availability Date

Security Test Procedures will be assigned an Evaluation Availability Release Date that is equivalent to the first day the version is available for Security Evaluation. The Evaluation Availability Date is the date at which the version becomes an Active Version.

Security Test Procedures will include a Version Release Statement to document the Security Test Procedures that have changed from the previous version.

10.5.4.2 Transition Period

Security Certification is associated with a particular version of Security Test Procedures. When a new version of the Security Test Procedures is available for evaluation (i.e., is an Active Version), the previous version will enter a Transition Period where it is available for Certification only up to an assigned Sunset Date.

10.5.4.3 Sunset Date

A Sunset Date is the date at which a version of Security Test Procedures is no longer an Active Version accepted for Certification. New and Delta Certifications can only be made against an Active Version of Security Test Procedures.

The Sunset Date is not an indication that the authenticator becomes untrustworthy on this date. It only means that Security Test Procedures have been updated, and the Active version(s) is required for Certification. Security Test Procedures are updated when new attack or defense techniques may have entered the ecosystem. Security Test Procedures may also be updated to improve testing techniques.

When changes are made to the Security Test Procedures it must be determined how quickly these should be implemented for all evaluations. The scope and type of changes within the Security Test Procedures are used to determine the Sunset Date for previous versions.

There are three classifications of changes which allow to gauge the time period which should be assigned for the Sunset Date: Major changes, Minor changes, and Emergency changes.

Major changes would generally be noted by a change in the major version number for the Procedures. The expectation of a major change version would include a change to Test Procedure(s). Major changes will be assigned a Sunset Date of 1 year to the previous version of the Security Test Procedures.

Minor changes would generally be noted by a change in the minor version number for the Procedures. The expectation of a minor change would be clarifications to the procedures, or for example the inclusion of additional supported algorithms (that have been approved by the appropriate TWG), but which don't impact the security functionality. Minor changes will be assigned a Sunset Date of 6 months to the previous version of the Security Test Procedures.

Emergency changes would generally be only done under extreme circumstances such as a widespread flaw (such as Heartbleed or similar) that has an immediate impact on FIDO clients. When such a scenario occurs that requires changes to the Security Test Procedures, an immediate Sunset Date for previous versions would be assigned. Due to the extreme nature of the Sunset Date, changes required through an Emergency Sunset must be limited specifically to those needed to ensure the security of FIDO client to meet the defined emergency; no other changes are allowed to be included.

10.5.4.3.1 Sunset Dates and Products Already Under Evaluation

It is important to note that any implementation with an application that has been approved by the Security Secretariat prior to the Sunset Date will be allowed to complete the evaluation, for Major or Minor Sunset Dates. For Emergency Sunset Dates, even products under evaluation will be required to comply with the changes included in the new version with the Emergency Sunset Date.

10.5.4.3.2 Sunset Date Voting

The Sunset Date for a Security Test Procedure version will be recommended by the Security Secretariat

and approved by a majority vote of the SRWG. The Sunset Date is assigned when a new version of the Test Procedures becomes Active.

10.5.5 Version Upgrades

Implementations that would like to upgrade to a newer version of Security Test Procedures must go back to a FIDO Accredited Security Laboratory for evaluation of what has changed (Delta Certification for Version Upgrade), or they may choose to completely restart the Certification process.

10.6 Resolving Conflict

There may be cases where a vendor disagrees with a decision or results from the certification process. The Organization for Internet Safety guidelines [ISO/IEC 29147:2014] includes recommendations on how to resolve such conflicts in the context of an organization's published vulnerability disclosure (Section 9.1) process.

In summary:

- Leave the process only after exhausting reasonable efforts to resolve the disagreement;
- Leave the process only after providing notice to the other party;
- Resume the process once the disagreement is resolved.

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

10.6.1 Dispute Resolution Process

In the event a vendor disputes the results of the Security Secretariat, a Dispute Report [Dispute] is submitted to the Certification Secretariat via FIDO website. Upon receipt of a Dispute Report, the Certification Secretariat forwards the Dispute Report to the Certification Troubleshooting Team. The Certification Troubleshooting 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 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 Vendor must be notified.

10.7 Program Management

In order to provide continuity of operations between the Certification Secretariat and 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.

11 Liability

FIDO performs Certification on a best-effort basis and does not guarantee or provide any warranties for any product provider's products, and the Certification process does not relieve vendors from the need to make their own investigations to ensure the security or fitness or purpose of any products.

FIDO Alliance will NOT take any liability or enter into any contract with a Relying Party where it takes legal or financial responsibility for losses due to a successful attack on a certified authenticator. This is true for all types of and levels of certification that FIDO Alliance issues.

12 Appendix A: Program Documents

Reference	Title	URL
[Allowed Crypto]	Authenticator Allowed Cryptography List	TBD Source: https://github.com/fido-alliance/security-requirements/blob/master/fido-authenticator-allowed-cryptography-list.html
[Allowed ROE]	Authenticator Allowed Restricted Operating Environments List	TBD Source: https://github.com/fido-alliance/security-requirements/blob/master/fido-authenticator-allowed-restricted-operating-environments-list.html
[Authenticator MDS Req]	Authenticator Metadata Requirements	TBD Source: https://github.com/fido-alliance/security-requirements/blob/master/fido-authenticator-metadata-requirements.html
[TMLA]	FIDO Alliance Trademark License Agreement	https://fidoalliance.org/wp-content/uploads/FIDO-Trademark-License-Agreement-v-3.1.1-.pdf
[Logo]	FIDO Certified Logo Violation Form	http://fidoalliance.org/certified-logo-violation/
[Certified]	FIDO Certified products	https://fidoalliance.org/certification/fido-certified/
[Functional]	FIDO Functional Certification Policy	https://fidoalliance.org/wp-content/uploads/Certification_Program_Policy.pdf
[Web TMLA]	FIDO Trademark and Service Mark Usage Agreement for Websites	https://fidoalliance.org/fido-trademark-and-service-mark-usage-agreement-for-websites/

[IAR]	Impact Analysis Report	TBD
[Dispute]	Authenticator Dispute Report	TBD
[Application]	FIDO Authenticator Certification Application	TBD
[Questionnaire]	Vendor Questionnaire	TBD
[Evaluation Report]	FIDO Evaluation Report	TBD
[Requirements]	Security Requirements	TBD
[Test Procedures]	Security Test Procedures	TBD
[Lab Accreditation]	FIDO Security Laboratory Accreditation Program	
[FIDO Cert]	FIDO Certification Website	https://fidoalliance.org/certification/

13 Appendix B: References

Reference	Title	URL
[MDS]	FIDO UAF Authenticator Metadata Service v1.0	https://fidoalliance.org/specs/fido-uaf-metadata-service-v1.0-rd-20141008.pdf
[ISO/IEC 29147:2014]	ISO/IEC 29147:2014, *Information technology - Security techniques - Vulnerability disclosure*	http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip
[MDS Terms]	Metadata Service Terms	https://fidoalliance.org/metadata-service-terms/
[MITRE]	MITRE Common Vulnerabilities and Exposures	https://cve.mitre.org/
[NIST NVD]	NIST National Vulnerability Database	https://nvd.nist.gov/
[US-CERT]	US-CERT, United States Computer Emergency Readiness Team	https://www.us-cert.gov/

14 Appendix C: Terms & Abbreviations

Term / Abbreviation	Definition
Authenticator Boundary	A vendor-defined boundary according to Security Requirement 1.1.
ASP	Active Server Page
CWG	Certification Working Group
HSV	Handset Vendor
MDS	Metadata Service
MNO	Mobile Network Operator
RP	Relying Party
SRWG	Security Requirements Working Group