FIDO Authenticator Certification Policy

Final Document, October 14, 2025

This version:
https://github.com/fido-alliance/certification/authtenticator-policy

Issue Tracking:
GitHub

Editor:
Certification Working Group (CWG) (FIDO Alliance)

Copyright © 2025 FIDO Alliance. All Rights Reserved.

Abstract

This document outlines the Policies and Procedures for the FIDO Authenticator Certification Program.

Table of Contents

1. Revision History§

Revision History

Date	Version	Description	Sunset Date
2017-04-20	1.0.0	Approved by CWG	2017-08-10
2017-08-10	1.0.1	Update to Confidentiality section to clarify that anonymized information must be approved by the Vendor prior to being shared outside of the Security Secretariat. Approved by CWG.	-
2017-11-02	1.1.0r01	First draft of 1.1.0 to add L4 and L5 to the Policy. Shared with CWG.	-
2018-04-23	1.1.1	Updated to reflect the approved level naming scheme and FIDO2 Certification.	-
2019-10-10	1.2.0	Updated to reflect the FIAR process for Derivative, Delta, and Recertification.	-
2020-11-12	1.3.0	Updates related mainly to the introduction of the new L3 companion program.	-
2021-10-22	1.4.0	Updated to reflect clarification to: • The L1+ program level description • The separate certification for Consumer and Enterprise profiles, as introduced in version 1.4.1 of the FIDO Authenticator Security Requirements • Defined process steps for Authenticator Maintenance section (Delta, Derivative, and Re-certification) • Remove VQ for L3/L3+ and replace with mapping table • dd profile change (i.e., consumer or enterprise) as a Delta	-
2025-10-14	1.4.1	Updated to reflect exception for version 1.5.1 FIDO Authenticator Security Requirements: A new companion program is allowed, which is based on a not-certified protection profile (GlobalPlatform FIDO2 SE [FIDO2SE-PP]).	-

2. 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, U2F, and FIDO2 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.

2.1. FIDO Certification Program§

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

2.2. FIDO Authenticator Certification§

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

2.3. FIDO Functional Certification Prerequisite§

FIDO Authenticator Certification is independent of **FIDO Functional Certification** (the process and policies described in FIDO Functional Certification Policy [Functional-CertificationPolicy]). 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-CertificationPolicy], before applying for FIDO Authenticator Certification.

2.4. Audience§

The primary audience of this document is the Certification Working Group, Security and Privacy Requirements Working Group, FIDO Administration, FIDO Board Certification Committee, and the full 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.

The FIDO Certification Webpage 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.

2.5. Instructions§

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

2.5.1. Support§

For help and support, visit the FIDO Certification Overview or contact the FIDO Certification Secretariat at certification@fidoalliance.org.

3. Roles & Responsibilities§

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

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

The **Certification Issue Resolution Team** is a Board level certification committee (Board Certification Committee (BCC)) that resolves certification issues that relate specifically to products currently or to be certified in the marketplace as they relate to specific Authenticator Certification Security and Privacy Requirements or other Authentication Certification program documents.

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

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.

Companion 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. Companion programs can be found within Security Level 3 and above.

4. Program Documents§

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

4.1. 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.

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 SPWG

4.2. Security and Privacy Requirements§

The term Security and Privacy 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 and Privacy Requirements are outlined in Certification Authenticator Documents Table.

For more information on how the Security and Privacy Requirements documents are updated, please see

Security Requirement Versioning.

Certification Authenticator Documents

Document Name	Description	Voting Requirement
Authenticator Security and Privacy Requirements	Security and Privacy Requirements by Level of FIDO Authenticator Certification. The Authenticator must meet the requirements listed in the Authenticator Security and Privacy Requirements of the Level they wish to be certified to.	Supermajority of the SPWG.
Authenticator Allowed Cryptography List	Part of the Common Security Requirements, outlines the allowed cryptographic algorithms for Authenticators.	Supermajority of the SPWG.
Authenticator Allowed Restricted Operating Environments List	Part of the Common Security Requirements, outlines the allowed restricted operating environments for Authenticators, necessary at L2 and higher.	Supermajority vote of the SPWG.
Authenticator Metadata Requirements	The fields in the Authenticator Metadata will be the primary method of communicating Authenticator Certification status and details about implementations to Relying Parties (RPs).	Supermajority vote of the SPWG.

4.3. Vendor Documents§

Vendor documents are additional program documents that must be completed by the Vendor. These documents are non-normative and the normative documents are the Security and Privacy Requirements listed above.

FIDO Authenticator Certification Vendor Documents

Document Name	Description
Vendor Questionnaire	A questionnaire to be completed by the Vendor that is a self-assertion of how the implementation meets the Security and Privacy Requirements at Level 1, Level 1+, Level 2 and Level 2+.
Impact Analysis Report	A document to be completed by the Vendor that outlines any changes in a Certified implementation for use in Certification Maintenance.
Companion Program Mapping Table	A document prepared by SPWG to aid a Vendor completing L3 and L3+ Certification. The Table maps requirements from the Companion Program to the FIDO Security and Privacy Requirements.

4.4. Accredited Security Laboratory Documents§

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

Accredited Security Laboratory Documents

Document Name	Description	Voting Requirement
Security Laboratory Accreditation Policy	The policy governing the Security Laboratory Accreditation Program.	Majority vote of CWG
Security Test Procedures	The Test Procedures to be used by the Laboratory during the Security Evaluation.	Majority vote of the SPWG
FIDO Evaluation Report (FER)	The document to be completed by the Laboratory, which outlines the results of the Security Evaluation.	N/A

5. 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 Companion program, please contact the Security Secretariat at certification@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 number 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 and Privacy Requirements.

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

Level 3 and above rely on existing certifications of underlying components (e.g. Smart Card certifications - Common Criteria EAL 4+, or Global Platform TEE) defined by FIDO Companions or technology organizations. Certification without a Companion Program is not allowed as the effort is very high and the process is not established. It is thus recommended that Vendors completing Level 3 or above may have certification from one of the defined Companion Programs. Certification with a Companion Program with not-certified protection profile (i.e., GlobalPlatform FIDO2 SE) is allowed, with the use of the corresponding mapping table and a Security Target built on the PP by the Vendor.

5.1. Level 1§

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

The Level 1 Security and Privacy 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 Authenticator Security Parameters (ASPs) readily available to other applications or users.

Level 1 Security Evaluations are completed by FIDO Security Secretariat.

5.2. Level 1+§

Level 1+ tests the Authenticator's (SW implemented) defense against large scale software attacks and provides greater assurance of defense compared to Level 1.

The Security and Privacy Requirements for Level 1+ defends itself even if the device operating system is compromised. At L1+ white box cryptography and other software protection techniques are used rather than an AROE.

For L1+, FIDO has developed a methodology for evaluation of a software authenticator protected using software techniques such as white box cryptography. This method is based on a combination of other related industry

methods such as [CEMV3-1R5], [AttackPotentialSmartcards] and Annex A of [TEE-PP] but adapted to software specificities. This level does not have a companion program.

Level 1+ Security Evaluations is completed by a FIDO Accredited Security Laboratory, and includes penetration testing.

5.3. 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 and Privacy Requirements.

Examples of implementations that will NOT meet Level 2 Security and Privacy 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 documentation review by a FIDO Accredited Security Laboratory.

5.4. Level 2+§

Level 2+ tests the Authenticator's defense against substantial attacks and provides greater assurance of defense compared to Level 2.

> NOTE: Substantial attacks and L2+ still needs to be defined and agreed by the SPWG. It is expected to cover attacks that are conducted by attackers with limited skills and resources and that have known cybersecurity risks.

> NOTE: It is not yet possible to certify to Level 2+. This policy document will be updated when Level 2+ is available for Certification.

5.5. Level 3§

Companion Program Certification is available at Level 3. See the section(s) below for the currently supported Companion Programs for Level 3.

Level 3 Security Evaluations are completed by a FIDO Accredited Security Laboratory, and includes penetration testing.

5.5.1. TEE GlobalPlatform Companion Program§

At L3 the protection shall be strong enough to be protected against enhanced-basic effort software and hardware attacks as defined by AVA_VAN_.AP3 or higher equivalent vulnerability analysis. The attack potential tables for AVA_TEE.2 are as referenced in GlobalPlatform documentation.

5.5.2. Common Criteria Companion Program§

At L3 the protection shall be strong enough to be protected against enhanced-basic effort software and hardware attacks as defined by AVA_VAN 3 or higher equivalent vulnerability analysis. The attack potential tables for

AVA_VAN.3 are as referenced in smart card documentation.

As an example: a skilled amateur should be hindered to perform successful attacks on PCB-level (e.g. IC package not opened but pins are connected to attack equipment) with standard electronic lab equipment within hours to days.

5.5.3. FIDO2 SE GlobalPlatform Companion Program§

At L3 the protection shall be strong enough to be protected against enhanced-basic effort software and hardware attacks as defined by AVA_VAN 3 or higher equivalent vulnerability analysis. The attack potential tables for AVA_VAN.3 are as referenced in smart card documentation.

5.6. Level 3+§

Companion Program Certification is available at Level 3+. See the section(s) below for the currently supported Companion Programs for Level 3+.

Level 3+ Security Evaluations are completed by a FIDO Accredited Security Laboratory, and includes penetration testing.

5.6.1. Level 3+ – Common Criteria Companion Program§

At L3+ the protection shall be strong enough to be protected against moderate or high effort software and hardware attacks. A quantified example of such attacks is defined by AVA_VAN.4 or higher equivalent vulnerability analysis. The attack potential tables for AVA_VAN.4 are as referenced in smart card documentation.

As an example: a trained professional expert should be hindered to perform successful attacks on chip-level (e.g. IC package opened/decapsulated and attack equipment can act directly on the silicon).

5.6.2. Level 3+ – FIDO2 SE GlobalPlatform Companion Program§

At L3+ the protection shall be strong enough to be protected against moderate or high effort software and hardware attacks. A quantified example of such attacks is defined by AVA_VAN.4 or higher equivalent vulnerability analysis. The attack potential tables for AVA_VAN.4 are as referenced in smart card documentation.

5.7. Level Upgrading and Downgrading§

Upgrading (from Level 1 to Level 2, or 3) 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 Certification Maintenance for Level Downgrade 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.

6. 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-CertificationPolicy], before applying for FIDO Authenticator Certification.

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

6.1. 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.

- FIDO Authenticator Security and Privacy Requirements (By design)

  The authenticator implementation seeking Certification must first implement all applicable FIDO Authenticator Security and Privacy Requirements for a selected Level and prepare to pass the Security Test Procedures.

- Accredited Security Laboratory Selection (for Level 1+ and higher)

  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

- (First Evaluation) The vendor completes the Vendor Questionnaire for levels L1 and L2 for the implementation seeking Certification, which will be evaluated against the Authenticator Security and Privacy Requirements. The FIDO Evaluation Report will summarize the results of the security evaluation. For Level 1 this is completed by FIDO Security Secretariat. For Level 2 this is completed by the FIDO Accredited Security Laboratory and a FIDO Evaluation Report is submitted to FIDO for review and approval by the Security Secretariat. For the other higher levels, including Level 1+, it is completed by a FIDO Accredited Security Laboratory and a FIDO Evaluation Report of the penetration testing is submitted to FIDO for review and approval by the Security Secretariat.
- (Re-Evaluation) The Vendor completes the FIDO Impact Analysis Report [FIDO-FIAR] to highlight the changes with regards to a previously certified Authenticator. This will result into a Maintenance Certification.

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.

6.1.1. Step-by-Step Process§

FIDO Authenticator Certification Steps

Process Step	Responsible Party	Process Steps
Preparation	Vendor	Implements FIDO Specifications and Security and Privacy Requirements
	Vendor	For Level 1+ and above, hires a FIDO Accredited Security Laboratory to complete Security Evaluation.
	Accredited Security Laboratory	For Level 1+ and above, 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 Certification.
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 or the Maintenance Certification step for the applicable Level.
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.
		Reviews the FIDO Evaluation Report and

	FIDO Security Secretariat	• Approves, • Rejects, or • Requests Clarification
Level 1+, Level 3, and Level 3+: 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 for L1+. Completes the Mapping Table for Levels L3 and L3+ and sends to the Accredited Security Laboratory.
	Accredited Security Laboratory	Reviews the Mapping Table for Levels L3 and L3+, and resolves any questions directly with the Vendor. Completes Security Evaluation by performing the Security Test Procedures, including penetration testing. 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. 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.

6.2. Preparation§

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

1. FIDO Specifications (UAF, U2F, or FIDO2)
2. FIDO Functional Certification [Functional-CertificationPolicy] requirements for Authenticators
3. Authenticator Security and Privacy Requirements for the Security Level requested (e.g. Level 1)

4. Authenticator Allowed Cryptography List
5. Authenticator Allowed Restricted Operating Environments List
6. Authenticator Metadata Requirements

For Level 1+ and above, 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 Process*

6.3. 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-CertificationPolicy] for FIDO Functional Certification requirements.

Figure 2 *Step 2 - Functional Certification Process*

6.4. Application§

To begin FIDO Authenticator Certification, the Vendor completes the Certification Application on theImplementer Dashboard.

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 Process*

6.5. Security Evaluation§

The Security Evaluation step includes the Vendor's attestation of how the implementation meets the Security and Privacy 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.

6.5.1. Vendor Questionnaire§

Completing the Vendor Questionnaire includes actions from the Vendor, FIDO Security Secretariat, and the Accredited Security Laboratory. The Vendor Questionnaire is available on the Implementer Dashboard.

The Authenticator Boundary needs to be defined by the Vendor during the Vendor Questionnaire in line with the Security and Privacy Requirement. 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 Certification Maintenance must 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*

6.5.2. 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 [FIDOAuthenticatorSecurityRequirements].

The Security Secretariat will complete a FIDO Evaluation Report (FER) and return it to the Vendor.

6.5.3. Level 1+ and Above Laboratory Evaluation§

For Level 1+ and above, the Vendor will choose and hire a FIDO Accredited Security Laboratory to perform Security Evaluation:

- by reviewing the Vendor Questionnaire and performing the Security Test Procedures [FIDOAuthenticatorSecurityRequirements] at Level 2
- by performing penetration testing at level L1+
- by reviewing the Mapping Table (and Security Target) and performing penetration testing at levels L3 and L3+

The Laboratory will complete a FIDO Evaluation Report (FER) and return it to the Vendor and FIDO Security Secretariat.

Figure 5 *Step 5 - Security Evaluation Process*

6.5.4. 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 1+ and above, only the FIDO Evaluation Report must be submitted to FIDO.

Figure 6 *Step 6 - FIDO Evaluation Report Process*

6.6. Certification Issuance§

6.6.1. Requests§

When submitting for FIDO Authenticator Certification, Vendors must:

1. Have passed testing requirements at an Interoperability Event, see FIDO Functional Certification Program Policy [Functional-CertificationPolicy].
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 on the FIDO Implementer Dashboard
2. Approved Vendor Questionnaire or Mapping Table, depending on Security Level
3. Completed FIDO Evaluation Report
4. Certification Fees

Figure 7 *Step 7 - Certification Issuance Process*

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:

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).
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.

6.6.2. 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
- Profile type (Consumer and Enterprise)
- Feature support (Complete Feature Support)
- The date that FIDO Evaluation Report was approved
- The Security Level
- The Companion 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 Companion Program, for example, GlobalPlatform will be abbreviated to GP.

        > NOTE: For Level 1, Level 1+ and Level 2 “FA” will indicate FIDO Alliance as there are no Companion programs for these levels.

    - DDDDDDDD is the date of issuance (year, month, day)
    - NNN is the sequential number of certifications issued that day

FIDO Certified Products will be viewable and searchable by FIDO membership and the public-at-large, with the exception of certifications that are confidential.

7. Certification Maintenance and Updates§

Over time changes to the authenticator can occur that affect the FIDO Authenticator Security and Privacy Requirements. These changes can be categorized as non-interfering, minor, and major. Depending on how these changes are classified will determine whether the product requires a Derivative, Delta, or Re-certification.

The FIDO Authenticator Certification Program allows to process efficient certification maintenance and updates for products or services that rely upon existing Certified implementations. The intent is to reduce the burden for receiving certification for implementations that presents non-interfering or minor differences with regards to previously certified implementation.

7.1. FIDO Impact Analysis Report (FIAR)§

In order to make a determination of the magnitude of changes, the vendor will need to complete the FIDO Impact Analysis Report process. The vendor will complete the form describing all the changes in order to determine their impact on the FIDO Security and Privacy Requirements.

7.1.1. FIDO Impact Analysis Report Review Process§

The FIAR review process is composed of three steps:

1. Submission: The vendor submits the complete FIAR document based on the FIAR Template and submit to the FIDO Security Secretariat.
2. Review: The FIDO Security Secretariat reviews the submitted FIAR for completeness and analyzes the changes to determine their impact on the FIDO Authenticator Security and Privacy Requirements.
3. Conclusion: The FIDO Security Secretariat will provide judgement based on the characteristics of the changes made to the Certified Authenticator. The conclusion will indicate that the changes are either: NON-INTERFERING, MINOR, or MAJOR.

7.2. Derivative Certification (NON-INTERFERING)§

A NON-INTERFERING change has NO impacts on the FIDO Security and Privacy Requirements coverage. Typical changes could be features outside of the Authenticator Boundary or bug fixes related to functional features, performance optimization or an updated name or look.

A Derivative Certification process is conducted on an Authenticator that has been already certified in earlier versions. In the case where the Security Secretariat concluded that changes reflected in the IAR have NON-INTERFERING impacts on FIDO Security and Privacy Requirements coverage after reviewing the FIAR provided by the Vendor, then an addendum to the existing certificate is created. It is made publicly available by the end of this process.

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

The following are required as part of the Derivative FIDO Certification submission:

- A completed FIAR report (evaluated by the Security Secretariat to determine Derivative)
- Completed Self-Conformance Test Results
- Certification Request Form (Indicating Derivative on request)

7.3. Delta Certification (MINOR Change)§

A MINOR change has an impact that is sufficiently minimal to not affect the security assurance level provided by test procedures and calibration requirements to the extent that the Authenticator needs to be re-certified. Changes to the FIDO Security and Privacy Requirements that DO NOT require Calibration falls typically into this scope, but this is not a restricted case. Typical changes could be bug fixes indirectly related to a security feature or the ASPs, an additional feature interacting with the Authenticator boundary or a security strength optimization.

A Delta Certification is conducted on an Authenticator that has been already certified in earlier versions. In the case where the Security Secretariat concluded that changes reflected in the FIAR have MINOR impacts to the FIDO Authenticator Security and Privacy Requirements coverage, then the following must apply:

- For L1: FIDO Security Secretariat will review only the updates made to the VQ and approves it, then an addendum to the existing certificate is created and made publicly available by the end of the process.
- For L1+ and above: The Accredited Lab will review only the updates made to the VQ, conduct the delta tests and updates the relevant FER to reflect the new version. Then, an addendum to the existing certificate is created by FIDO Security Secretariat and made public by the end of the process

A certification based on a particular profile (e.g. Consumer Profile) will benefit from derivative certification for another profile (e.g. Enterprise Profile). As of current version of the specifications, only Consumer and Enterprise Profiles are available.

The following are required as part of the Delta FIDO Certification submission:

- A completed FIAR report (evaluated by the Security Secretariat to determine Delta)
- Completed Self-Conformance Test Results
- Interoperability Testing (On Demand options are available)
- Certification Request Form (Indicating Delta on request)

7.4. Re-Certification (MAJOR Change)§

A **MAJOR** change has a potential impact on the security assurance level. Changes to the FIDO Security and Privacy Requirements that DO require Calibration falls typically into this category. Typical changes could be the addition/remove/replacement of an ASP or a cryptographic algorithm, an implementation of a new countermeasure or a change to the Authenticator boundary security architecture. Note that in some cases, an update including several minor changes could lead to a major impact on security, in that case, the Security Secretariat might consider it as a major change.

A Re-Certification is conducted on an Authenticator that has been already certified in earlier versions. In the case where the Security Secretariat concluded that changes reflected in the FIAR have MAJOR impacts to the FIDO Authenticator Security and Privacy Requirements coverage, then the following must apply:

- For L1: FIDO Security Secretariat will review completely the VQ while reusing previous certification results to the maximum extent possible to minimize duplication of effort. Then approves it and issue a new certificate, which will replace the existing one. This new certificate will be made publicly available by the end of the process.
- For L1+ and above: The Accredited Lab will review completely the VQ (for L1 and L2) or the Mapping Table (for L3 and L3+) and re-conduct testing while reusing previous certification results to the maximum extent possible to minimize duplication of effort. Then updates the FER to reflect the new results before submitting it to FIDO Security Secretariat. That latter will validate the FER and issue a new certificate which will replace the existing one. This new certificate will be made publicly available by the end of the process.

The following are required as part of the Re-certification FIDO Certification submission:

- A completed FIAR report (evaluated by the Security Secretariat to determine Re-certification)
- Completed Self-Conformance Test Results
- Interoperability testing (OnDemand options are available)
- Completion of VQ with reuse of previous certification results were applicable
- Certification Request Form (Indicating Full Certification on request)

7.5. Types of Certification Maintenance§

7.5.1. Certification Maintenance for Product Upgrades§

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

7.5.2. Certification Maintenance for Version Upgrade§

Security Requirements and Security Test Procedures will be maintained and versioned by the SPWG. A Vendor is allowed to upgrade to an Active Version of the Security and Privacy Requirements or Test Procedure (see Security Requirement Versioning) 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 and Privacy Requirements.

7.5.3. Certification Maintenance for Level Downgrade

A Vendor may request a Level 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.

7.5.4. Certification Maintenance 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).

A Certification Maintenance for Security Vulnerability requires the Vendor to provide FIDO with an Action Plan that outlines the Vendor's roll out plan once the Certification Maintenance process is processed. 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.

7.5.5. Certification Maintenance after Suspension

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

7.5.5.1. Policy Suspension

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

7.5.5.2. 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. The Certification Maintenance 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 SPWG. 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:
    - Failure to respond to and address Security Vulnerability identified in a Certified product.
    - Failure to report changes made to a Security Certified implementation. To remain Security Certified after changes, a Vendor must follow the Delta Certification process.
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 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 SPWG 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 SPWG 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 SPWG 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 8 *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 29147:2018, Information technology - Security techniques - Vulnerability disclosure [ISO-29147-2018].

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 {#VulnerabilityMonitoring}§

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

- Cybersecurity & Infrastructure Security Agency
- NIST National Vulnerability Database
- MITRE Common Vulnerabilities and Exposures

9.1.3. Ad Hoc Security Updates§

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

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, SPWG 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.

In the case that information must be shared outside of the FIDO Security Secretariat, the information must be anonymized. Any anonymized information must be approved by the Vendor prior to being shared.

Anonymized information on the vulnerability may be provided to SPWG or other technical working groups (as defined in the Triage Action) for expert opinions on the vulnerability. The vendor can designate if confidentiality can be removed for SPWG 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 CISA Traffic Light Protocol.

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 theVulnerability Triage Protocol Table. 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.

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 to 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 SPWG 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 the Calculation of Attack Potential Table.

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 the Calculation of Attack Potential Table.

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

9.3.1. Attack Potential Calculation – Level 1 and Level 2§

For Level 1 and Level 2, 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 5 [CEMV3-1R5]. 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 [CEMV3-1R5].

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.

The Calculation Of Attack Potential 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.

The Rating of Attack Potential 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.

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.

9.3.1.1. Attack Potential Calculation - Level 1+

For Level 1+, the assigned Attack Potential will be calculated based on the potential to exploit the vulnerability as defined in [L1plus-Eval]. 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 in the following section, but the full version is included in [AttackPotentialSmartcards].

Attack Potential to L1+

Factor	**Value for Identification Phase**	**Value for Exploitation Phase**
Elapsed Time		
<= one hour	0	0
<= one day	1	2
<= one week	2	4
<= one month	3	6
> one month	5	8
Expertise		
Layman	0	0
Proficient	2	3
Expert	5	5
Multiple Experts	7	7
Knowledge of TOE		
Public	0	0
Restricted	2	2
Sensitive	4	4
Critical	6	6
Window of Opportunity		
Unlimited Access	0	0
Easy	1	1
Moderate	2	3

Difficult	4	5
Equipment		
Standard	0	0
Specialized	1	3
Bespoke	2	5
Replicability		
Easy	N/A	0
Moderate	N/A	3
Difficult	N/A	6

The Attack Potential Calculation Tables for L1 and L2 and L1+ are used to assign values to what factors are required to exploit the Vulnerability; Elapsed Time, Expertise, Knowledge of the Target of Evaluation (TOE), Windows of opportunity, Equipment, and Replicability. The sum of value of each area is then used to determine the rating of the vulnerability.

The Rating of Vulnerabilities Table shows the value ranges for each Attack Potential category.

Rating of Vulnerabilities

Range of Values*	**TOE Resistant to Attackers with the Attack Potential of**
0-11	No Rating
12-25	Basic
26-32	Moderate
>32	High

* Final Attack Potential = Identification + Exploitation

9.3.1.2. Attack Potential Calculation - Level 3

9.3.1.2.1. GlobalPlatform Companion Program

For Level 3, the assigned Attack Potential will be calculated based on the potential to exploit the vulnerability as defined in Application of Attack Potential to TEE. Potential vulnerabilities are prioritized based on an estimate of time, expertise, knowledge, access, and equipment.

More details on the attack potential calculation could be found in [TEE-PP].

9.3.1.2.2. Common Criteria Companion Program

For Level 3, the assigned Attack Potential will be calculated based on the potential to exploit the vulnerability as defined in Application of Attack Potential to Smartcards [AttackPotentialSmartcards]. 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 in the following section, but the full version is included in [Attack Potential Smartcards].

9.3.1.3. Attack Potential Calculation – Level 3+

For Level 3+, the assigned Attack Potential will be calculated based on the potential to exploit the vulnerability as defined in Application of Attack Potential to Smartcards [AttackPotentialSmartcards]. 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 [AttackPotential Smartcards].

Attack Potential to Smartcards

Factor	Identification	Exploitation
Elapsed Time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Experts	7	6
Knowledge of TOE (Target of Evaluation)		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very Critical Hardware Design	9	N/A
Access to TOE		
< 10 Samples	0	0
< 30 Samples	1	2
< 100 Samples	2	4
> 100 Samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized(1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open Samples (Rated According to Access to Open Samples)		
Public	0	N/A
Reserved	2	N/A
Sensitive	4	N/A
Critical	6	N/A

(1) If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this shall be rated as bespoke. Test benches for side-channel and fault attacks are normally considered to be too similar and not different enough.

The Attack Potential to Smartcards Table is used to assign values to what factors are required to exploit the Vulnerability; Elapsed Time, Expertise, Knowledge of the Target of Evaluation (TOE), Access to TOE, Equipment, and Open Samples. The sum of value of each area is then used to determine the rating of the vulnerability.

The Rating of Vulnerabilities for CC v3 Table shows the value ranges for each Attack Potential category.

Rating of Vulnerabilities for CC v3

Range of Values*	**TOE Resistant to Attackers with Attack Potential of**
0-15	No Rating
16-20	Basic
21-24	Enhanced Basic
25-30	Moderate
31 and above	High

* Final Attack Potential = Identification + Exploitation

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 the Corrective Action Deadline tables for Level 1, Level 1+, Level 2, Level 3, and Level 3+.

> 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 the Tables forLevel 1, Level 1+, Level 2, Level 3, and Level 3+ 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 the Tables Level 1, Level 1+, Level 2, Level 3, and Level 3+ 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 Certification Maintenance 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 the Tables Level 1, Level 1+, Level 2, Level 3, and Level 3+, see FIDO Deadline Enforcement.

Vendor Action Deadlines and Corrective Action Requirements correspond to the certification Level.

9.5.2.1. Level 1 Vendor Action Deadlines

Vendor Action Deadline - 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 1+ Vendor Action Deadlines

Vendor Action Deadline - 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
Moderate	30 business days from Notice	No	No Corrective Action Required.
High	60 business days from Notice	No	No Corrective Action Required.

9.5.2.3. Level 2 Vendor Action Deadlines

Vendor Action Deadline - 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	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.

9.5.2.4. Level 3 Vendor Action Deadlines

Vendor Action Deadline - Level 3

If the Attack Potential is:	**Vendor Deadline for Response to FIDO**	**Corrective Action Required?**	**Vendor Deadline for Corrective Action**
No Rating	5 business days from Notice	Yes	90 days from Notice
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.

9.5.2.5. Level 3+ Vendor Action Deadlines

Vendor Action Deadline - Level 3+

If the Attack Potential is:	**Vendor Deadline for Response to FIDO**	**Corrective Action Required?**	**Vendor Deadline for Corrective Action**
No Rating	5 business days from Notice	Yes	90 days from Notice
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	Yes	365 days from Notice
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 the Deadline Enforcement Tables Level 1, Level 1+, Level 2, Level 3, and Level 3+.

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”.

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 Certification Maintenance 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”.

9.5.3.3. Level 1 Deadlines

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 1+ Deadlines

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
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

9.5.3.5. Level 2 Deadlines

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	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.			

9.5.3.6. Level 3 Deadlines

FIDO Deadline Enforcement - Level 3

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)**
No Rating	5 business days from Notice	185 days from Notice	90 days from Notice	270 days from Notice
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.			

9.5.3.7. Level 3+ Deadlines

FIDO Deadline Enforcement - Level 3+

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)**
No Rating	5 business days from Notice	185 days from Notice	90 days from Notice	270 days from Notice
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	365 days from Notice	545 days from Notice
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. 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.

10.2.4. Revoked§

An Authenticator Certificate may be revoked.

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 [FIDOMetadataRequirements1-1]. 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[FIDOMetadataService] 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 [FIDO-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.

10.3.2.2. Violation Reporting§

In the event that FIDO® Certified mark is being misused, a report can be filed by completing theFIDO Certification Logo Violation Form 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 FIDO Dispute Report that will follow the Dispute Resolution Process.

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
- Companion Program, if Level 3 or above (e.g. Common Criteria or 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 FIDO Dispute Report that will follow the Dispute Resolution Process (Section 9.6.1). 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 9 *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 Companion-Specific Authenticator Security and Privacy 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 Companion-Specific Security Requirements§

Level- or Companion-Specific Security and Privacy Requirements are the Security and Privacy Requirements applicable to each level or Companion program are required in addition to the Common Authenticator Security and Privacy Requirements.

10.5.2.1. Conditions§

When a new revision of the Level or Companion-Specific Security and Privacy Requirements is developed, all supporting documents are required to be updated in accordance with the Level- or Companion-Specific Security and Privacy 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 and Privacy Requirements. Security Test Procedures include tests to meet the common, level- and Companion-specific Security and Privacy Requirements.

10.5.3.1. Conditions§

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

The Security Test Procedures will always be updated if the Common, or corresponding Level- or Companion-Specific Security and Privacy Requirements are updated. As new Security and Privacy Requirements are

created, the Security Test Procedures will require an update to support testing of those requirements.

The SPWG 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.

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 SPWG. 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 (Certification Maintenance for Version Upgrade), or they may choose to completely restart the Certification process.

10.5.6. Exception for the GlobalPlatform FIDO2 SE Companion Program§

Any product implementing CTAP version 2.1, compliant with Security and Privacy requirements version 1.5.1, and asking for certification at level L3 or L3+ can benefit from the GlobalPlatform FIDO2 SE Companion

Program, without sunset dates.

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-29147-2018] includes recommendations on how to resolve such conflicts in the context of an organization's published Vulnerability Disclosure 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 FIDO Dispute Report.

10.6.1. Dispute Resolution Process§

In the event a vendor disputes the results of the Security Secretariat, a FIDO Dispute Report 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.

Appendix A: Program Documents§

Program Documents

Title	**Location**
FIDO Authenticator Certification Application	FIDO Implementer Dashboard
FIDO Certified Products	FIDO Certified Products Webpage
Authenticator Dispute Report	FIDO Implementer Dashboard
FIDO Evaluation Report (FER)	FIDO Implementer Dashboard
FIDO Certification Website	FIDO Certification Getting Started Page
FIDO Functional Certification Policy	FIDO Certification Getting Started Page
Impact Analysis Report (IAR)	FIDO Implementer Dashboard
FIDO Certified Logo Violation Form	Certified Logo Violation Form
FIDO Alliance Trademark License Agreement	TMLA
FIDO Trademark and Service Mark Usage Agreement for Websites	Web TMLA

Appendix B: Terms & Abbreviations§

Terms & Abbreviations

Term / Abbreviation	**Definition**
ASP	Authenticator Security Parameters
Authenticator Boundary	A vendor-defined boundary according to Security Requirement 1.1.
CWG	Certification Working Group
FER	FIDO Evaluation Report
HSV	Handset Vendor
MDS	Metadata Service
MNO	Mobile Network Operator
RP	Relying Party
SPWG	Security Requirements Working Group

References§

Normative References§

[FIDO2SE-PP]
Protection Profile for FIDO2 SE v1.0 | GPC_SPE_210 March 2025. URL: https://globalplatform.org/specs-library/fido2-se-protection-profile/#collapse-

[FIDOAuthenticatorSecurityRequirements]
Rolf Lindemann; Dr. Joshua E. Hill; Douglas Biggs. *FIDO Authenticator Security Requirements*. November 2020. Final Draft. URL: https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-security-requirements-v1.4-fd-20201102.html

[ISO-29147-2018]
ISO/IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure October 2018. URL: https://www.iso.org/standard/72311.html

Informative References§

[AttackPotentialSmartcards]
Application of Attack Potential to Smartcards January 2019. URL: https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3.2.pdf

[CEMV3-1R5]
CCMB-2017-04-004 Common Methodology for Information Technology Security Evaluation - Evaluation Methodology. April 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[FIDO-FIAR]
Certification Working Group (CWG); Security and Privacy Requirements Working Group (SPWG). *FIDO Impact Analysis Report (FIAR)*. April 2018. URL: https://media.fidoalliance.org/wp-content/uploads/2019/03/FIDO_IAR_v1.0_RELEASE.docx

[FIDO-TMLA]
FIDO Alliance. *FIDO Alliance Specification Trademark License Agreement v3.7*. July 2020. URL: https://media.fidoalliance.org/wp-content/uploads/2020/07/FIDO-Trademark-License-Agreement-v3.7_English.pdf

[FIDOLabPolicy]
CWG. *FIDO Certification Program - Security Laboratory Accreditation Policy* May 2017. Published. URL: https://media.fidoalliance.org/wp-content/uploads/SecurityLaboratoryAccreditationPolicy_v1.1_20170526.pdf

[FIDOMetadataRequirements1-1]
Meagan Karlsson. *FIDO Authenticator Metadata Requirements v1.1*. 29 June 2018. URL: https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-metadata-requirements-v1.1-fd-20180629.html

[FIDOMetadataService]
B. Jack; R. Lindemann; Y. Ackermann. *FIDO Metadata Service*. 21 May 2025. Proposed Standard. URL: https://fidoalliance.org/specs/mds/fido-metadata-service-v3.1-ps-20250521.html

[Functional-CertificationPolicy]
Certification Working Group (CWG). *FIDO Functional Certification Program Policy*. Proposed Standard. URL: https://media.fidoalliance.org/wp-content/uploads/2021/10/Functional_Certification_Program_Policy_v1.3.9_FINAL.pdf

[L1plus-Eval]
TBD. *Application of attack potential to FIDO L1+ (AAP)* May 2019. URL: https://members.fidoalliance.org/wg/SPWG/document/10636

[TEE-PP]
GPD_SPE_021 TEE Protection Profile version 1.3 September 2020. URL: https://globalplatform.org/specs-library/tee-protection-profile-v1-3/