FIDO Biometrics Certification Policy

Final Document, May 22, 2024

This version:

https://fidoalliance.org/specs/biometric/certificationpolicy/Biometric-Component-Certification-Policy-v1.5-fd-20240522.html

Issue Tracking:

GitHub

Editors:

Biometrics Working Group (FIDO Alliance)

Certification Working Group (CWG) (FIDO Alliance)

Abstract

This document outlines the Policies and Procedures for the FIDO Biometric Certification Programs.

Table of Contents

1. Revision History§

Revision History

Date	Pull Request	Version	Description
		0.1	Initial Draft
2017-10-17	#83	0.2	Added Process sections
2017-12-12		0.3	Added Biometric Subsystem Boundary, Allowed Integration Document, Post-Certification changes sections. Removed TMLA section.
2019-02-11		1.0	Added the pre-qualification step
2019-03-08		1.1	Improved wording by constantly using the term Component
2019-04-02		1.2	Minor correction of testing phase, fixed references

2020-05-06		1.3	Added section for sunsetting program documents.
2021-12-06		1.4	Updated Certification Request and Issuance to include IAPAR level, threshold, and test environment; add IAPAR to metadata.
2023-12-12		1.5	Updated Certification Policy to incorporate Face Verification for Remote Identity Verification (IdV - Face).

2. Introduction§

This document gives an overview of the policies that govern Biometrics Certification as part of two programs: -Biometric Component Certification (BCC) for certifying either a biometric sensor or for integrating a certified biometric sensor in a FIDO Authenticator. -Face Verification for Remote Identity Verification (IdV - Face) solutions.

These policies are the requirements and operational rules that guide the implementation, process, and ongoing operation of the Biometrics Certification programs and create an overall framework for FIDO Alliance biometric certification programming to operate within.

The policies in this document apply to both programs unless otherwise specified, where each section may include a subsection that is specific to each program.

2.1. Audience§

The intended audiences of this document are the Biometric Working Group (BWG), Certification Working Group (CWG), Identity Verification and Binding Working Group (IDWG), FIDO Administration, FIDO Board of Directors, and FIDO Accredited Laboratories.

The owner of this document is the Certification Working Group.

2.2. FIDO Roles§

Certification Working Group (CWG) (CWG)
: FIDO working group responsible for the approval of policy documents and ongoing maintenance of policy documents once a certification program is launched.

Biometrics Working Group (BWG)
: FIDO working group responsible for defining the Biometric Requirements and Test Procedures for the Biometric Certification Programs and to act as Subject Matter Expert (SME) following the launch of the program.

Identity Verification and Binding Working Group (IDWG)
: FIDO working group responsible for defining the Biometric Requirements and Test Procedures for the Remote Identity Verification (IdV) Certification Programs and to act as Subject Matter Expert (SME) following the launch of the program.

FIDO Biometric Secretariat
: FIDO Alliance Subject Matter Expert (SME) responsible for the coordination and final approval of evaluation reports from FIDO Accredited Biometric Laboratories. Also known as "secretariat".

FIDO Identity Verification Secretariat
: FIDO Alliance Subject Matter Expert (SME) responsible for the coordination and final approval of evaluation reports from FIDO Accredited Identity Verification Laboratories. Also known as "secretariat".

FIDO Certification Secretariat

FIDO Alliance certification expert responsible for administration of the FIDO Certification Programs, including finalizing certification requests, updating product listings, and issuing program certificates. For any questions

related to this document or FIDO Certification Programs, please contact the FIDO Certification Secretariat at certification@fidoalliance.org.

Vendor / Developer
Party seeking certification. Responsible for providing the testing harness to perform both online and offline testing that includes enrollment system (with data capture sensor) and verification software.

Original Equipment Manufacturer (OEM)
Company whose goods are used as components in the products of another company, which then sells the finished items to users.

Laboratory
Party performing testing. Testing will be performed by third-party test laboratories Accredited by FIDO Alliance to perform Biometric and/or Identity Verification Certification Testing. See also, FIDO Accredited Biometrics Laboratory and FIDO Accredited Identity Verification Laboratory.

2.3. FIDO Terms§

FIDO Certified Authenticator
An Authenticator that has successfully completed FIDO Certification program and has been issued a FIDO Certificate.

FIDO Accredited Biometrics Laboratory
Laboratory that has been Accredited by the FIDO Alliance to perform FIDO Biometrics Testing for the Biometrics Certification Program.

FIDO Accredited Identity Verification Laboratory
Laboratory that has been Accredited by the FIDO Alliance to perform FIDO Remote Identity Verification and/or Biometrics Testing for the Remote Identity Verification Document Authenticity (DocAuth) and/or Face Verification Certification Programs.

FIDO Member
A company or organization that has joined the FIDO Alliance through the Membership process.

Certified Biometric Component
A Biometric Subcomponent that has completed the FIDO Biometric Component Certification program and has been issued a Biometric Component Certificate.

Certified Face Verification for Remote Identity Verification (IdV)
A face verification system for IdV that has completed the FIDO Biometric Certification Program and has been issued a Biometric IdV Face Verification Certificate.

2.4. Personnel Terms§

Test Subject
User whose biometric data is intended to be enrolled or compared as part of the evaluation. See Section 4.3.2 in [ISOIEC-19795-1].

> NOTE: For the purposes of this document, multiple fingers up to four fingers from one individual may be considered as different test subjects. Two eyes from one individual may be considered as different test subjects.

Test Crew
Set of test subjects gathered for an evaluation. See Section 4.3.3 in[ISOIEC-19795-1].

Target Population
Set of users of the application for which performance is being evaluated. See Section 4.3.4 in[ISOIEC-19795-1].

Test Operator
Individual with function in the actual system. See Section 4.3.6 in[ISOIEC-19795-1].

2.5. Key Words§

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

- SHALL indicates an absolute requirement, as does MUST.
- SHALL NOT indicates an absolute prohibition, as does MUST NOT.
- SHOULD indicates a recommendation.
- MAY indicates an option.

3. Overall Biometrics Certification Policies§

The Biometrics Certification program as a whole is the responsibility of the FIDOCertification Working Group (CWG), with the Biometrics Working Group and Identity Verification and Binding Working Group acting as the Subject Matter Experts (SME), with necessary oversights and approvals from the FIDO Board of Directors and collaboration with other FIDO Working Groups where needed.

The CWG may, at the discretion of its chair(s) and members, create subgroups and delegate responsibilities for all or some portion of the CWG’s certification program responsibilities to those subgroups. The Certification Secretariat is responsible for implementing, operating, and managing the certification program defined by the CWG.

Implementations seeking Biometrics Certification may be FIDO Members or non-member organizations.

3.1. Prerequisite Certifications§

FIDO Biometric Certification is independent of other FIDO Certification Programs. There are no FIDO Certification prerequisites to apply for Biometric Certification programs.

3.2. FIDO Authenticator Certification with a Certified Biometric Component - BCC Specific§

Once a Biometric Component is Certified (Certified Biometric Component), there are rules for how it can be integrated into an Authenticator seeking FIDO Authenticator Certification.

A Certified Biometric Component MUST be integrated according to the Allowed Integration Document defined by the Biometric Vendor during the Biometric Component Certification process.

The Authenticator implementation MUST complete FIDO Certified at Level 1 or higher. An Authenticator with only a Functional Certificate SHALL complete Authenticator Certification for Level 1 or higher to use a Certified Biometric.

Use of a Certified Biometric is OPTIONAL for Level 1 and Level 2. At Level 3 and higher an Authenticator MAY use a Certified Biometric Component, if a Biometric modality is used for authentication it MUST use a Certified Biometric Component.

3.3. Related FIDO Certification for Remote Identity Verification - IdV Face§

Automated remote identity verification solutions require multiple steps, some of which are in scope of this document and some of which will be covered by other documents.

In scope for IdV - Face:

- Matching - Comparison of a photo/video of a subject with a reference face image from an identity document

- Presentation attack detection - automated discrimination between bona-fide subjects and presentation attacks

Out of scope for IdV - Face (covered in FIDO Document Authenticity Certification for Remote Identity Verification Requirements (IdV - DocAuth) [DocAuth]):

- Automatically verifying identity document authenticity

3.3.1. Biometric Recognition Boundary§

The boundary of the Biometric Recognition to be certified (also called TOE, or Target of Evaluation) is defined by the Vendor. All functionality required for biometrics must be included within the boundary, this includes the Data Capture, Signal Processing, Data Storage, Comparison, and Decision functionality.

3.4. Biometric Certification Process§

1. **Application**
2. **Qualification**
3. **Biometric Testing**
4. **Laboratory Report**
5. **Certification Request**
6. **Certification Issuance**

3.4.1. Application§

Vendor applies for FIDO Biometric Certification by submitting an Application. Vendor enters a contract with a FIDO Accredited Biometric or Identity Verification Laboratory.

Biometric or Identity Verification Secretariat reviews the Application and notifies the Vendor that it is approved or requires clarification.

3.4.2. Qualification§

After the developer officially applied for certification, they SHALL provide the following to the laboratory:

- The TOE and test harness, along with its required descriptions on use
- The TOE Description Document
- The Test Plan Document
- The Allowed Integration Document (if applicable)
- any other test plans about tests performed by the developer (if available)
- any other information deemed necessary by the developer

The laboratory SHALL review the TOE, the test harness, and the provided documents and ensure they are complete. The laboratory SHALL specifically ensure and perform:

- that the TOE and the test harness can be used on the basis of the instructions provided by the developer,
- that the TOE Description, Test Plan, and other test documentation provided by the developer is a complete and comprehensive

- that the test documentation looks auspicious (it should, however, be evident that the laboratory cannot perform a complete review of the test documentation at this point),
- that any test plans about tests performed by the developer (if any) are complete and comprehensive descriptions of the tests that the developer has performed,
- the laboratory SHOULD perform a pre-test to ensure that the TOE can be integrated into the test environment of the laboratory. The pre-test should at least contain one transaction for performance testing and one attempt for PAD testing. Pre-testing should also ensure that the test infrastructure of the laboratory (e.g. for offline testing or logging) can interact with the TOE. The pre-test may be skipped if the positive integration of the test harness into the infrastructure can be shown differently (e.g. as the TOE has been certified before by the same laboratory),
- the laboratory SHALL perform a first review of the TOE concerning the FIDO criteria for certification. While it is certain that the laboratory cannot perform the whole test up to this point, the laboratory shall ensure that all existing criteria are taken into account for planning of further tests (this can e.g. be easily achieved by the use of a checklist).

The laboratory SHALL submit all reviewed and complete test documentation to the FIDO Biometric or Identity Verification Secretariat. All parties SHALL agree that the TOE envisions a positive perspective to finish the certification. While this agreement cannot (and does not) mean that the decision on certification will be taken, it rather be reached so that no obvious obstacles are visible that would be in the way of a certification. The secretariat will notify the laboratory that all test documentation is approved or requires clarification.

Upon test documentation approval, the laboratory, developer, and FIDO Certification Secretariat SHALL then work to reach an agreement on:

- the schedule for the certification,
- the required contract (if any) for finishing the certification (if this has not yet been done in the first place),

The FIDO qualification stage for biometric certification does not confirm self-attested biometric performance numbers that may be provided by the vendor, e.g., false accept rate (FAR), false reject rate (FRR), or presentation attack detection performance (PAD).

The agreement is summarized by the laboratory in written form. This can be part of the test plan for the rest of the certification or in the form of a separate document.

After this agreement has been reached, the developer is considered to have reached the qualification of the certification.

3.4.3. Biometric Testing§

The FIDO Accredited Biometric or Identity Verification Laboratory will be responsible for testing against the requirements through a combination of online and offline live subject testing. Testing will be completed according to the FIDO Biometrics Requirements ([FIDOBiometricsRequirements]).

Labs seeking FIDO Accreditation shall follow the FIDO Biometric and/or Identity Verification Laboratory Accreditation Policy [FIDOBiometricsLaboratoryAccreditationPolicy]. A list of FIDO Accredited Biometric and Identity Verification Laboratories will be available on the [FIDO Website](https://fidoalliance.org). Prior to testing, the FIDO Accredited Biometric and Identity Verification Laboratories shall prepare a test plan and submit this test plan to FIDO for approval.

3.4.3.1. Allowed Integration Document - BCC Specific§

An Allowed Integration Document is used to document the changes that may be necessary to accommodate integration into an Authenticator or other form factor, including a subsystem being form factor agnostic. The Allowed Integration Document MUST be drafted by the Vendor and provided to the Accredited Biometrics

Laboratory. The Allowed Integration Document MUST include an explanation of software and hardware changes.

3.4.3.2. Biometric Data

Biometric data captured from Test Subjects SHALL be maintained in a secure manner by the Laboratory. Biometric data MAY be provided to Vendor under an agreement between the Vendor and Laboratory, pursuant to laws of the jurisdiction(s) of the parties. Aside from the Vendor, the Accredited Biometrics or Identity Verification Laboratory SHALL NOT provide the biometric data to any other third parties or FIDO, except as needed for purposes of an audit of the Laboratory by FIDO.

> NOTE: Additional logical security requirements are provided in Section 5.3.2. Logical Security of the FIDO Biometric Laboratory Accreditation Policy.

3.4.4. Laboratory Evaluation Report

Accredited Laboratory performs testing and returns Laboratory Evaluation Report to Vendor and FIDO secretariat. The Laboratory Evaluation Report MUST include:

- biometric testing results for all requirements
- the review of the Allowed Integration Document (if applicable), and the laboratory MUST validate that the changes will not impact performance.
- self-attestated results by the developer (if applicable). Please note that requirements that address questions of self-attestation SHALL be understood as checklist items. This specifically means that the Laboratory is not meant to perform any comprehensive analysis with respect to the information on self-attestation received by the developer.

FIDO secretariat reviews the Laboratory Evaluation Report and makes a decision to Approve, Reject, or ask for clarification.

3.4.5. Certification Request and Issuance

3.5. Request - BCC Specific

When submitting for FIDO Biometric Component Certification, Vendors MUST:

- Submit a completed Laboratory Evaluation Report indicating the evaluated operating points and passed Biometric Evaluation,
- If a FIDO Member, be in good standing with all membership dues and certification invoices paid in full,
- MUST adhere to all applicable policies.

FIDO Biometric Component Fees will be assessed per evaluated operating point. Multiple operating points can be defined within the evaluated TOE. All certification fees are available at https://fidoalliance.org/certification/certification-fees/. To receive FIDO Biometric Component Certification, Vendors MUST complete payment of certification fees.

When submitting for FIDO Authenticator Certification, Vendors must:

- Have passed Biometric Evaluation
- If a FIDO Member, be in good standing with all membership dues and certification invoices paid in full,
- MUST adhere to all applicable policies.

3.6. Related FIDO Certification for Remote Identity Verification - IdV Face

When submitting for FIDO Remote Identity Verification - IdV Face Certification, Vendors MUST:

- Submit a completed Laboratory Evaluation Report indicating the evaluated operating points and passed Biometric Evaluation,
- If a FIDO Member, be in good standing with all membership dues and certification invoices paid in full,
- MUST adhere to all applicable policies.

FIDO Biometric Component Fees will be assessed per evaluated operating point. Multiple operating points can be defined within the evaluated TOE. All certification fees are available at https://fidoalliance.org/certification/certification-fees/. To receive FIDO Remote Identity Verification - IdV Face Certification, Vendors MUST complete payment of certification fees.

3.6.1. Certificate Issuance

3.7. Issuance - BCC Specific

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

- The name of the organization that has been certified
- The name and version of the implementation that has been certified
- Biometric Program
- The modality(s) that was / were certified
- Test Environment
- Certification Level achieved and corresponding IAPAR threshold
- FIDO Certification Program policy version against which the implementation has been certified
- The FIDO Biometric Requirements version against which the implementation was certified against
- The Laboratory evaluation date
- The data that the FIDO Evaluation Report was approved
- A certification number of the format RRRVVVVPPPDDDDDDDDNNN where:
    - RRR is the FIDO Requirements
    - VVVV is the version of the FIDO Requirements
    - PPP is the Biometrics Program (BCC)
    - DDDDDDDD is the date of issuance (year, month, day)
    - NNN is the sequential number of certifications issued that day

3.8. Related FIDO Certification for Remote Identity Verification - IdV Face

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

- The name of the organization that has been certified
- The name and version of the implementation that has been certified
- Biometric Program
- The modality(s) that was / were certified
- Test Environment

- Certification Level achieved and corresponding IAPAR threshold
- FIDO Certification Program policy version against which the implementation has been certified
- The FIDO Biometric Requirements version against which the implementation was certified against
- The Laboratory evaluation date
- The data that the FIDO Evaluation Report was approved
- The certification expiration date (3 years from the date of certification issuance)
- A certification number of the format RRRVVVVPPPDDDDDDDDNNN where:
    - RRR is the FIDO Requirements
    - VVVV is the version of the FIDO Requirements
    - PPP is the Biometrics Program (IdV)
    - DDDDDDDD is the date of issuance (year, month, day)
    - NNN is the sequential number of certifications issued that day

[FIDO® Certified products](https://fidoalliance.org/certification/fido-certified-products/) will be viewable and searchable by FIDO members and the public at large, with the exception of certifications that are confidential.

3.8.1. FIDO Metadata Service - BCC Specific§

FIDO provides information to Relying Parties regarding FIDO Authenticators through the FIDO Metadata Service. This information could be used by Relying Parties for purposes such as determining whether it accepts the authenticator or enables certain privileges (e.g., checking an account balance vs. transferring funds).

The biometric-related information that the FIDO Metadata service provides includes the following:

- Biometric Component Certification Level
- Self-Attested False Accept Rate (FAR)
- Self-Attested False Reject Rate (FRR)
- IAPAR certified rate

Submitting Metadata to the FIDO Metadata Service is OPTIONAL. However, Metadata MUST be submitted during the Biometric Component Certification process and will be verified for accuracy and completeness during the Laboratory Evaluation.

3.9. Post-Certification Changes§

3.10. Post-Certification - BCC Specific§

Changes documented and defined by the Vendor in the Allowed Integration Document will provide the specifications for how a sensor can change during integration into an Authenticator implementation or other form factor. Changes documented in the Allowed Integration Document do not require Delta or New Certification.

Any unanticipated changes at the time of the Biometric Certification (i.e., changes not included in the Allowed Integration Document) are not allowed without first completing a Delta Certification to update the Allowed Integration Document.

Post Certification Changes	Process
	Delta Certification.

Minor changes in **Hardware** that do not impact biometric performance. This includes updates/additions to the Allowed Integration Document).	Justification of changes provided by the Vendor (Impact Analysis Report) and Vendor Self-Test Data Reviewed by the Accredited Laboratory. Validation of any additions to the Allowed Integration Document by the Accredited Laboratory.
Major changes in **Hardware** that do not impact biometric performance.	New Certification
Any change in **Hardware** that impacts biometric performance.	New Certification
Minor changes in **Software** that do not impact matching performance (e.g. compiled on a new platform).	Delta Certification Justification of changes provided by the Vendor (Impact Analysis Report).
Major changes in **Software** that impact matching performance if underlying sensor does not change.	Delta Certification Retest with Accredited Laboratory using data collected in previous testing, as long as biometric data has not been given to vendor
Any change in **Software** if underlying sensor is changed.	New Certification

3.10.1. Delta Certification§

Delta Certification is when the Vendor has made changes to the original certified implementation, and the Vendor wishes for that implementation to remain certified.

- If the changes are not within an Allowed Integration Document, a Delta Certification MUST be completed. If a Delta Certification is not completed, the certification has reason to be revoked.
- When a Delta Certification is complete, the original Certificate is updated/replaced to include the Delta information.

> NOTE: Delta Certification was introduced for the Authenticator Certification but does not exist for Functional Certification.

3.10.2. Derivative Certification§

Derivative Certification is when a new implementation has been created based on a Certified implementation, and the Vendor wishes to re-use the original Certification for this new implementation because there have been **no changes** to the Certified functionality. The intent of Derivative Certification is to reduce the burden for receiving certification for implementations that are substantially the same.

A Derivative implementation may not modify, expand, or remove functionality tested in the Biometric Certification Program. Derivative Biometric Component is bound to the Biometrics Certification Policy at the time of the original (base) certification.

Derivatives gain their own Certificate and can be listed as a separate product.

3.10.2.1. Derivative Certification Process

Derivative Certification requires an assertion from the Vendor that the Certified Biometric (base) and the Subcomponent implementation (Derivative of base) does not modify, expand, or remove functionality that was tested during the base certification. This assertion is reviewed and approved by the Biometric Secretariat.

3.11. Certification States

A list of Certified Implementations will be maintained by the Biometric Secretariat, and a public list will be available on the FIDO website. Certification may be in one of the following states: Active, Certified, Suspended, or Revoked.

3.11.1. Active

Once an application is submitted to the FIDO Secretariat, the Certification state becomes “Active”. The Accreditation remains in an “Active” during the Certification process.

This state is not shared outside of the FIDO Biometric Secretariat and Accredited Laboratory chosen by the Vendor.

3.11.2. Certified

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

3.11.3. Suspended

A Biometric Certificate may be suspended, for more information on the Suspension process, seeSuspension.

3.11.4. Revoked

An Authenticator Certificate may be revoked, for more information on Revocation, seeRevocation.

3.12. Related FIDO Certification for Remote Identity Verification - IdV Face

New Certification is required three (3) years following the date of initial certificate issuance. A six (6) month grace period is provisioned following certificate expiration for a vendor and laboratory to complete a new certification.

Certificate expiration notices SHALL be completed by the FIDO secretariat six (6) months, three (3) months, and one (1) month prior to certificate expiration or until new certification activity is initiated by the Vendor. Likewise, such notices SHALL continue to be issued by the FIDO secretariat six (6) months and three (3) months prior to the end of a grace period or until new certification activity is initiated by the Vendor. Certificate expiration notices SHALL not continue past the grace period.

However, if changes to hardware or underlying sensor are completed to a FIDO Certified product during the three (3) year certification then an Impact Analysis Report SHALL be completed by the Vendor and submitted to the Laboratory and FIDO Secretariat to determine if Delta or New Certification is required. Similarly, if a software vulnerability is identified or a significant update to the software is completed during the three (3) year certification then an Impact Analysis Report SHALL be completed by the Vendor and first submitted to the FIDO Secretariat to determine if the impact is Non-Interfering, Delta or New Certification. Next, if the FIDO Secretariat requires a Delta or New Certification then the Vendor is asked to follow up with the Laboratory.

Post Certification Changes	Process
Minor changes in **Hardware** that do not impact biometric performance.	Delta Certification. Justification of changes provided by the Vendor (Impact Analysis Report) and Vendor Self-Test Data Reviewed by the Laboratory and FIDO Secretariat.
Major changes in **Hardware** that do not impact biometric performance.	New Certification
Any change in **Hardware** that impacts biometric performance.	New Certification
Any change in **Software** if underlying sensor is changed.	New Certification

3.12.1. Delta Certification§

Delta Certification is when the Vendor has made changes to the original certified implementation hardware or underlying sensor and the Vendor wishes for that implementation to remain certified.

- If a Delta Certification is not completed, the certification has reason to be revoked.
- When a Delta Certification is complete, the original Certificate is updated/replaced to include the Delta information and the initial date of certificate expiration remains unchanged.

3.12.2. Derivative Certification§

Derivative Certification is when a new implementation has been created based on a Certified implementation and the Vendor wishes to re-use the original Certification for this new implementation because there have been **no changes** to the Certified functionality. The intent of Derivative Certification is to reduce the burden for receiving certification for implementations that are substantially the same.

A Derivative implementation may not modify, expand, or remove functionality tested in the Biometric Certification Program. Derivative IdV Face Certifications are bound to the Biometrics Certification Policy.

Derivatives gain their own new certificate and can be listed as a separate product.

3.12.2.1. Derivative Certification Process§

Derivative Certification requires an assertion from the Vendor that the Certified Biometric (base), and the Subcomponent implementation (Derivative of base) does not modify, expand, or remove functionality that was tested during the base certification. This assertion is reviewed and approved by the Biometric Secretariat.

3.13. Certification States§

A list of Certified Implementations will be maintained by the FIDO secretariat and a public list will be available on the FIDO website. Certification may be in one of the following states: Active, Certified, Suspended, or Revoked.

3.13.1. Active§

Once an Application is submitted to the FIDO secretariat, the Certification state becomes “Active”. The Application remains “Active” during the Certification process.

This state is not shared outside of the FIDO secretariat and laboratory chosen by the Vendor.

3.13.2. Certified§

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

3.13.3. Suspended§

A Biometric Certificate may be suspended, for more information on the Suspension process, seeSuspension.

3.13.4. Revoked§

A Biometric Certificate may be revoked, for more information on Revocation, seeRevocation.

3.14. Certification Suspension§

A Certificate may be suspended by the FIDO secretariat.

In the event that the FIDO secretariat becomes aware of a suspension event, the secretariat will investigate the claim to determine if the event is cause for Suspension.

The FIDO secretariat may decide that:

- no further action is required, and the Certification remains Active, OR
- a Delta Certification is required to verify the Biometric still meets Requirements.

Vendors will be given at least 30-day notice prior to updating the Certificate status to Suspended, along with the necessary steps to remove the Suspension.

Suspension is an indication that the Certification must undergo a Delta Certification to reactive the Certified status.

The Suspended status will not be publicly shared, but the Implementation will be removed from the Certified list on the FIDO Website while the Certificate status is Suspended.

3.15. Certification Revocation§

A Certificate may be revoked by the FIDO secretariat.

In the event that the secretariat becomes aware of a revocation event, they will investigate the claim to determine if the event is cause for Revocation.

Revocation events include:

1. Certificate expiration, or
2. Remaining in a Suspended status for more than 180 days, whichever occurs first.

Revocation is an indication that the Certificate is no longer certified and must undergo a New Certification to be certified.

The secretariat will provide 30-day notice prior to updating the Certificate status to Revoked.

If not done so already due to a Suspension, any Revoked Certificates will be removed from the Certified list on the FIDO Website.

3.16. Dispute Resolution Process

In the event a Vendor disputes the results of decisions made by the FIDO secretariat, a Dispute Request may be submitted to the secretariat via a form on the FIDO Website.

Upon receipt of a Dispute Request, the FIDO secretariat forwards the Dispute Request to the Dispute Resolution Team. The Dispute Resolution Team is responsible for determining the validity of the request and the appropriate routing of the request. The Vendor can indicate in the request if they would like to remain anonymous (the default behavior), or if their company name and implementation name may be shared with the Dispute Resolution Team.

If the certification has outstanding disputes or other issues, the certification may be delayed. Should the certification be delayed, the FIDO secretariat will notify the Vendor seeking Certification.

3.17. Program Administration

The Certification Working Group will be responsible for maintaining these policies.

3.17.1. Sensitive Information

3.17.1.1. Data Protection

The secretariat is responsible for protecting sensitive information during transit and storage.

When submitting electronic documentation to the secretariat, it must be uploaded using forms on the FIDO website.

All Biometric Certification forms and their attachments will be stored within an encrypted database only accessible by the FIDO secretariat, and will not be shared.

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

3.17.1.2. Certification Status

No Vendor, Accredited Laboratory, nor other third-party may refer to a product, service, or facility as FIDO approved, accredited, certified, nor otherwise state or imply that FIDO (or any agent of FIDO) has in whole or part approved, accredited, or certified a Vendor, Laboratory, or other third-party or its products, services, or facilities, except to the extent and subject to the terms, conditions, and restrictions expressly set forth within in an Accreditation Certification or Biometric Certificate issued by FIDO.

3.17.1.3. Operational Reports

The FIDO secretariat will provide Operations Reports as requested by FIDO or FIDO Working Groups.

Any reporting performed by the Biometric Secretariat will be performed at the aggregate level to preserve confidentiality, and will not include the specific name or details of any Vendor or Implementation.

Operational reports will include:

- the number of certification requests,

- the number of certifications granted,
- disputes and their resolutions,
- process updates,
- certification mark or TMLA violations,
- any other notable events or operational metrics.

3.17.2. Biometric Requirement Versioning§

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

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

3.17.2.1. Biometric Requirements§

Biometric Requirements refers to the document that outlines the requirements for FIDO Biometric Certification. This document includes:

1. Biometric Requirements,
2. Biometrics Test Procedures,

3.17.2.2. Active Version(s)§

The Active Version(s) of Biometric Requirements refers to a version or versions that are currently published and will be accepted for Certification. A new version of the Biometric Requirements 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 Biometric Requirements 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 Biometric Requirements Version 2.0 has an Evaluation Availability date of July 1, 2020. The Sunset Date for Version 1.0 is then assigned to be one year from that date. A vendor wishing to complete Certification between July 1, 2020 and December 31, 2020 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 January 1, 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 Biometric Requirements for any new or Delta Certifications.

Table of Example Active and Sunset Dates

Biometric Requirements Version	**Evaluation Availability Date**	**Sunset Date**
1.0	January 1, 2017	December 31, 2020
2.0	July 1, 2020	

3.17.2.2.1. Evaluation Availability Date§

Biometric Requirements will be assigned an Evaluation Availability Release Date that is equivalent to the first day

the version is available for Biometric Evaluation. The Evaluation Availability Date is the date at which the version becomes an Active Version.

Biometric Requirements will include a Version Release Statement to document the Biometric Requirements that have changed from the previous version.

3.17.2.2.2. Transition Period§

Biometric Certification is associated with a particular version of Biometric Requirements. When a new version of the Biometric Requirements 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.

3.17.2.2.3. Sunset Date§

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

The Sunset Date is not an indication that the biometric subcomponent becomes untrustworthy on this date. It only means that Biometric Requirements have been updated, and the Active version(s) is required for Certification. Biometric Requirements are updated when new requirements or test procedures may have entered the ecosystem. Biometric Requirements may also be updated to improve testing techniques.

When changes are made to the Biometric Requirements it must be determined how quickly these should be implemented for all evaluations. The scope and type of changes within the Biometric Requirements 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 Requirements and/or Test Procedure(s). Major changes will be assigned a Sunset Date of 6 months to the previous version of the Biometric Requirements.

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, but which don’t impact the Biometric functionality. Minor changes will be assigned a Sunset Date of 6 months to the previous version of the Biometric Requirements.

Emergency changes would generally be only done under extreme circumstances such as a widespread threat that has an immediate impact on FIDO clients. When such a scenario occurs that requires changes to the Biometric Requirements, 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 Biometric subcomponents of the FIDO client meet the defined emergency; no other changes are allowed to be included.

3.17.2.2.4. Sunset Dates and Products Already Under Evaluation§

It is important to note that any implementation with an application that has been approved by the Biometric 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.

3.17.2.2.5. Sunset Date Voting§

The Sunset Date for a Biometric Requirements version will be recommended by the Biometric Secretariat and approved by a majority vote of the CWG. The Sunset Date is assigned when a new version of the Requirements becomes Active.

Index§

Terms defined by this specification§

References§

Normative References§

[FIDOBiometricsLaboratoryAccreditationPolicy]
Meagan Karlsson. *Biometrics Laboratory Accreditation Policy*. May 2019. URL: https://fidoalliance.org/specs/biometric/labaccreditationpolicy/Biometric-Lab-Accreditation-Policy-v1.0-fd-20190530.html

[FIDOBiometricsRequirements]
Stephanie Schuckers; et al. *FIDO Biometrics Requirements*. October 2020. URL: https://fidoalliance.org/specs/biometric/requirements/Biometrics-Requirements-v2.0-fd-20201006.html

[ISOIEC-19795-1]
ISO/IEC 19795-1:2021 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. 2021. URL: https://www.iso.org/standard/73515.html

[RFC2119]
S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels* March 1997. Best Current Practice. URL: https://tools.ietf.org/html/rfc2119