FIDO Biometrics Certification Policy

Working Draft, August 30, 2018

This version:
https://github.com/fido-alliance/biometrics-cert-policy

Issue Tracking:
GitHub
Inline In Spec

Editor:
Meagan Karlsson (FIDO Alliance)

Abstract

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

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.

2. Introduction§

This document gives an overview of the policies that govern Biometrics Certification as part of the FIDO Biometrics Certification Program.

These policies are the requirements and operational rules that guide the implementation, process, and ongoing operation of the Biometrics Certification program and create an overall framework for the Biometrics Certification Program to operate within.

2.1. Audience§

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

The owner of this document is the Certification Working Group.

2.2. FIDO Roles§

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

Biometrics Assurance Subgroup

FIDO subgroup of the CWG responsible for defining the Biometric Requirements and Test Procedures to develop the Biometrics Certification program and to act as an SME following the launch of the program.

Vendor
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 to perform Biometric Certification Testing. See also, FIDO Accredited Biometrics 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 Member
A company or organization that has joined the FIDO Alliance through the Membership process.

Certified Biometric Subsystem
A Biometric Subcomponent that has completed the FIDO Biometric Certification program and has been issued a Biometric Subsystem 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), specifically the Biometrics Assurance Subgroup, 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 and members, create subcommittees and delegate responsibilities for all or some portion of the CWG's certification program responsibilities to those subcommittees. The Certification Secretariat is responsible for implementing, operating, and managing the certification program defined by the CWG.

Implementations seeking Biometrics Certification may beFIDO 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 for a subsystem.

3.2. FIDO Authenticator Certification with a Certified Biometric Subsystem§

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

A Certified Biometric Subsystem MUST be integrated according to the Allowed Integration Document defined by the Biometric Vendor during the Biometric 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+ an Authenticator MAY use a Certified Biometric Subsystem, if a Biometric modality is used for authentication it MUST use a Certified Biometric Subsystem.

3.2.1. Biometric Subsystem Boundary§

The boundary of the Biometric Subsystem 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.

3.3. Biometric Certification Process§

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

3.3.1. Application

Vendor applies for FIDO Biometric Certification. Vendor enters a contract with a FIDO Accredited Biometric Laboratory.

Biometric Secretariat review the Application, notifies the Vendor that it is Approved, Rejected, or requires clarification.

3.3.2. Biometric Testing

Vendor submits Biometric Authenticator to a FIDO Accredited Biometric Laboratory. Vendor indicates desired testing. Approximate time / cost provided is by Accredited Laboratory.

The FIDO Accredited Biometric 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 [add reference].

Labs seeking FIDO Accreditation shall follow the FIDO Biometric Laboratory Accreditation Policy [add reference]. A list of FIDO Accredited Biometric Laboratories will be available on the FIDO Website [add reference].

3.3.2.1. Allowed Integration Document

An Allowed Integration Document is used to document the changes that may be necessary to accommodate integration into an Authenticator. 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.

3.3.2.2. Biometric Data

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

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

3.3.3. Laboratory Report

Accredited Laboratory performs testing and returns Laboratory Report to Vendor and FIDO Biometric Secretariat. The Laboratory Report must include the review of the Allowed Integration Document, the Laboratory MUST validate that the changes will not impact performance.

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

3.3.4. Certification Request

If Laboratory Report is Approved, Vendor completes a Certification Request, including Metadata to be added to the Metadata Service to describe the Certified Biometric Subsystem (see FIDO Metadata Service).

3.3.4.1. FIDO Metadata Service

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 Certification Level
- Self-Attested False Accept Rate (FAR)
- Self-Attested False Reject Rate (FRR)

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

> ISSUE 1 To be updated according to decision in Biometrics Subgroup. Discussion still ongoing.

3.3.5. Certification Issuance

FIDO Reviews and, if complete, Approves the Certification Request and issues a Biometric Subsystem Certificate.

3.4. Post-Certification Changes

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. Changes documented in the Allowed Integration Document do not require Delta or New Certification.

Any changes that were unanticipated at the time of the Biometric Subsystem 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
Minor changes in **Hardware** that do not impact biometric performance. This includes updates/additions to the Allowed Integration Document).	Delta Certification. 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).
	Delta Certification

Major changes in **Software** that impact matching performance if underlying sensor does not change.	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

3.4.1. 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.

3.4.2. Derivative Certification§

Derivative Certification is when a new implementation has been created based off of 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 Subsystems are 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.

3.4.2.1. Derivative Certification Process§

Derivative Certification requires an assertion from the Vendor that the Certified Biometric Subsystem (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.

3.5. 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.

3.5.1. 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.

3.5.2. Certified§

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

3.5.3. Suspended§

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

3.5.4. Revoked§

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

3.6. Certification Suspension§

A Certificate may be suspended by the FIDO Biometric Secretariat.

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

The Biometric Secretariat may decide that:

- no further action is required and the Certification remains Active, OR
- a Delta Certification is required to verify the Biometric Subcomponent still meets Certification 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 Biometric Certified list on the FIDO Website while the Certificate status is Suspended.

3.7. Certification Revocation§

A Certificate may be revoked by the FIDO Biometric Secretariat.

In the event that the Biometric Secretariat becomes aware of a revocation event, the Biometric Secretariat 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.

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

The Biometric 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 Biometric Certified list on the FIDO Website.

3.8. Dispute Resolution Process

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

Upon receipt of a Dispute Request, the FIDO Biometric 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 Biometric Secretariat will notify the Vendor seeking Certification.

3.9. Program Administration

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

3.9.1. Sensitive Information

3.9.1.1. Data Protection

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

When submitting electronic documentation to the Biometric 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 Biometric Secretariat, and will not be shared.

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

3.9.1.2. 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.

3.9.1.3. Operational Reports

The Biometric 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.

Index§

Terms defined by this specification§

References§

Normative References§

[ISOIEC-19795-1]
ISO/IEC 19795-1:2006 Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework. 2006. URL: https://www.iso.org/standard/41447.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

Issues Index§

ISSUE 1 To be updated according to decision in Biometrics Subgroup. Discussion still ongoing.↵

↑

→