FIDO Biometrics Laboratory Accreditation Policy

Working Draft, August 30, 2018

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

Issue Tracking:
GitHub

Editor:
Meagan Karlsson (FIDO Alliance)

Abstract

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

Table of Contents

1. Revision History§

Revision History

Date	Pull Request	Version	Description
2017-05-02		0.1	Initial Draft
2017-08-03	#61	0.2	Updates to Third Party Accreditation Section
2017-08-08	#62	0.3	Third Party Accreditation: Removed Archived PPs, Technical Expertise: Added Live Subject Testing and PAD as requirements.
2017-12-13	#88	0.4	Updated Accepted Programs for ISO, Split Third Party Accreditation Requirements Section to add Biometric Testing Evidence section. Clarified Accreditation expiration handling.
2017-12-20	#91	0.5	Added intro to Third-Party Accreditation Requirements section.
2018-1-24	#101	0.6	Changed table in Third-Party Accreditation Requirements section to include only standards ISO 19795 and 30107 ([ISOIEC-19795-1], [ISO30107-1]), referenced in requirements document.

2. Introduction§

This document gives an overview of the policies that govern Laboratory Requirements for those seeking Biometric Laboratory Accreditation for the FIDO Certification Program.

This documentation also defines the relationship between FIDO and its Accredited Biometric Laboratories.

2.1. Audience§

This policy document is intended for Laboratories seeking or maintaining FIDO Laboratory Accreditation for the FIDO Certification Program.

The owner of this document is the Certification Working Group.

2.2. Support§

For help and support, contact the FIDO Certification Secretariat atcertification@fidoalliance.org or the FIDO Biometrics Secretariat at biomertics-secretariat@fidoalliance.org.

2.3. 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.

2.4. FIDO Terms§

FIDO Certified Authenticator
An Authenticator that has successfully completed FIDO Certification.

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.

2.5. 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].

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].

2.6. 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. Overview§

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.

This document covers the FIDO Biometric Laboratory Accreditation process and requirements for FIDO Certification. FIDO may issue other types of Laboratory Accreditation in the future, such Accreditation would be maintained as part of their own Accreditation Program and are outside the scope of this document.

Laboratories that have been Accredited by the FIDO Alliance via the process outlined herein will evaluate the Biometric Requirements of implementations according to the Biometric Certification Policy.

The FIDO Laboratory Accreditation process focuses on the necessary aspects of a Laboratory to evaluate an implementation through a combination of online and offline live subject testing. The approach that will be used is a Scenario Test, defined as: “evaluation in which the End To End system performance is determined in a prototype or simulated application” ([ISOIEC-19795-1], 4.4.2)

Testing shall be carried out on using samples captured with the real acquisition sensor in an environment that models the real world target application of interest and using a population with similar demographics characteristics to the end users.

All Laboratories shall follow the process outlined in this document in order to apply for and maintain their Active status as an Accredited Biometric Laboratory.

4. Roles & Responsibilities§

4.1. FIDO Alliance§

The FIDO (Fast IDentity Online) Alliance is a 501(c)6 nonprofit organization nominally formed in July 2012 to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance plans to change the nature of authentication by developing specifications that define open, scalable, and interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This new standard for security devices and browser plug-ins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security.

4.2. Certification Working Group (CWG)§

The Biometric Laboratory Accreditation program is a responsibility of the FIDO Certification Working Group (CWG) in partnership with 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 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.

4.3. Biometrics Assurance Subgroup§

The Biometrics Assurance Subgroup of the CWG is responsible for defining and maintaining the Biometric Requirements for Biometric Certification and acts as Biometric Experts for FIDO.

4.4. Certification Secretariat§

FIDO Staff responsible for implementing, operating, and managing FIDO Certification Programs.

4.5. Biometric Secretariat§

FIDO Staff responsible for providing unbiased assessments of the Lab Accreditation and Certification applications, and acting as an independent FIDO Biometrics expert for the FIDO Certification Program. The FIDO Staff that make up the Biometric Secretariat are: Technical Director, Biometric Certification Advisor, Certification Program Development, and individuals designated as Certification Secretariat.

4.6. Accredited Laboratory§

FIDO Laboratory Accreditation is available to public and private testing laboratories, including commercial laboratories; universal laboratories; and federal, state, and local government laboratories.

4.6.1. Authorized Representative§

Laboratory-appointed Representative to act as the main point of contact for FIDO.

4.6.2. Approved Evaluators§

Accredited Biometric Laboratory personnel that have participated in FIDO Training and satisfactorily completed the Knowledge Test.

5. Laboratory Requirements§

Accreditation is granted following the successful completion of the Accreditation process, which includes submission of an application, payment of fees, assessments, FIDO Training, and Knowledge Tests.

Laboratories are accredited for a specific site location. Laboratories will be assessed based on the criteria listed in this section, and criteria may be different based on the requested Scope of Accreditation.

Laboratories are required to maintain their Accreditation status through participation in the FIDO Alliance Accredited Biometrics Laboratory Group, and complete FIDO Training and Knowledge Tests as new requirements or specification versions are released.

Accreditation must be renewed with proof of continuous support of the latest standards and practices every 3 years.

There will be a public list of FIDO Accredited Biometric Laboratories on the FIDO Website.

FIDO Accredited Biometric Laboratories must meet all the requirements included in the following sections.

5.1. Third-Party Accreditation Requirements§

The Third-Party Accreditation Requirements are intended to lessen the burden on the FIDO Laboratory Accreditation process by accepting common Accreditations as proof of meeting a subset of the Laboratory Requirements, and therefore not requiring rework that has already been completed as part of one of these Third-Party Accreditations.

Laboratories are required to have, at the time of application, and to maintain Third-Party Accreditations throughout their time as an Accredited Laboratory as outlined in this section. If a required Third-Party Accreditation expires within the validity period of the Laboratory Accreditation Certificate, a Laboratory must

submit the updated Accreditation Certificates from the Third-Party to the Biometric Secretariat. The Laboratory is not required to complete the Accreditation Renewal process to update Third-Party Accreditations within the validity period (before expiration) of the Accreditation Certificate.

5.1.1. ISO Third Party Accreditation§

Compliance to ISO 17025 is a prerequisite requirement for all laboratories and can be shown through a third party accreditation program.

The Laboratory is responsible for maintaining the Third Party Accreditation listed in their Application, or obtaining a new Third Party Accreditation from the list above to maintain their Accredited status. The Biometric Secretariat will track the expiration date of the Third Party Accreditations, the Laboratory will be sent a notice by FIDO when the Third Party Accreditation is close to expiring if updated information has not been provided by the Laboratory. Updating Accreditation Requirements does not require a new Accreditation.

If a Laboratory fails to maintain their Accreditation to meet the Third Party Accreditation Requirements (or any other requirements within this Policy), the Biometric Secretariat will begin the Accreditation Revocation process.

5.1.2. Biometric Testing Evidence Requirements§

In addition to the required compliance to ISO/IEC 17025 the laboratory shall also be able to perform testing in accordance with the following standards:

ISO Accredidation - Accepted Programs

Scope	Program	Area of Accredidation
ISO/IEC 19795-1:2006 ([ISOIEC-19795-1])	Information technologyg	Biometric performance testing and reporting-Part 1: Principles and framework
30107-3:2017 ([ISO30107-3])	Information technologyg	Biometric presentation attack detection -- Part 3: Testing and reportin

The following Lab Accreditations are recognized as fulfilling FIDO Lab Accreditation Requirements for Biometric Accreditation Biometric Testing Evidence Requirements and can be used as evidence during the Accreditation Application.

To meet the evidence requirements, the laboratory must have Accreditation from at least one of these Accepted Programs, OR document their ability to perform Biometric Testing to an equivalent of one of these Accepted Programs. The Biometric Secretariat will be responsible for reviewing the evidence provided in the Application.

Third Party Accreditation - Accepted Programs

Program	Accreditation	Scope	URL
NIST NVLAP	Biometrics Testing LAP	• 30/BTA Biometrics Testing and Analysis • 30/ST Scenario Testing - Human Crew (Laboratory) • 30/SLT System Level Testing (Enrollment/Verification) • 30/CPST Conformance to Performance Specifications Testing	https://www.nist.gov/national-voluntary-laboratory-accreditation-program-nvlap/biometrics-testing-lap

Common Criteria	Common Criteria Licensed Lab	Must have evaluated an implementation against at least one of the Protection Profiles listed below	https://www.commoncriteriaportal.org/labs

5.1.3. Common Criteria Protection Profiles§

In order for a Laboratory to claim Common Criteria (CC) Accreditation as evidence for the Accreditation Application the Laboratory must have performed an evaluation against at least one of the following Protection Profiles, OR provide evidence of using [CAFVM] or [BEAT].

Common Criteria - Biometric Protection Profiles

Protection Profile	Version	Date	CC Version	URL
Biometric Verification Mechanisms Protection Profile	1.3	7 August 2008	3.1 Revision 2	https://www.commoncriteriaportal.org/files/ppfiles/pp0043b.pdf
Fingerprint Spoof Detection Protection Profile	1.7	27 November 2009	3.1 Revision 2	https://www.commoncriteriaportal.org/files/ppfiles/pp0062b_pdf.pdf
Fingerprint Spoof Detection Protection Profile	1.8	25 January 2010	3.1 Revision 3	https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0063.htn

5.2. Business Requirements§

This section describes the overall business requirements which a Laboratory must meet.

5.2.1. Legal§

The Laboratory must be recognized as a legal entity and must be (or must be a part of) an organization that is registered as a tax-paying business or as having a tax exempt status or as a legal entity in some form with a national body.

The Laboratory must be able to sign and abide by all FIDO legal agreements for Accredited Biometric Laboratories, including the FIDO Laboratory Evaluation Agreement.

5.2.2. Public Communications§

The Laboratory agrees to abide by FIDO's policy that evaluation and/or testing performed at any FIDO Accredited Biometric Laboratory is acceptable for Biometric Certification, and must make no claims to the contrary in its marketing material.

A Laboratory must not, under any circumstances, communicate nor disclose to any third party, including to the Vendor or other entity submitting an application for evaluation, that an implementation has or has not been Certified by FIDO. FIDO, not the Laboratory, shall be the final party to determine whether a particular implementation conforms to the FIDO Specifications or FIDO Certification Program Policies.

5.2.3. Independence§

The Laboratory must be able to demonstrate independence in test case analysis methodology and testing process from the party involved in the design or manufacturing of the implementation Vendor without prior agreement from FIDO.

- The Laboratory must not be owned by an implementation Vendor without prior agreement from FIDO.
- The Laboratory must not evaluate an implementation that the Laboratory has been involved in designing except that they may provide quality assurance testing (debug sessions) prior to the Vendor submitting the product for official FIDO evaluation.

5.3. Security Requirements§

This section describes the Security Requirements that a laboratory must meet.

5.3.1. Physical Layout§

The Laboratory must have sufficient security measures to prevent unauthorized people from entering the building. If the Laboratory is part of a shared building or complex, there must be sufficient security measures to prevent unauthorized people from entering the Laboratory offices.

5.3.1.1. Evaluation Areas§

Areas in the Laboratory facilities in which products, components, or data are tested or stored must be restricted to authorized personnel. Authorized personnel are defined by the Laboratory as part of [ISO 17025].

5.3.1.2. Storage§

Within the Laboratory there must be sufficient (according to [ISO 17025]) secure storage space to provide adequate protection for all ongoing work. Secure storage must be provided for all materials retained by the Laboratory after the FIDO Evaluation has been completed.

5.3.2. Logical Security§

The Laboratory must maintain and comply with a logical security policy that includes, at a minimum, the following requirements.

5.3.2.1. Classified Materials and Information§

Test samples and documents must be handled with care and the materials must be controlled and stored securely whether in electronic or paper format.

Classified material must be stored in secure containers, where unauthorized access is prevented by appropriate measures (e.g. alarms, surveillance, and sufficient mechanical protection).

Disclosure of FIDO or vendor data and documents to third parties must be authorized in writing by an officer of the company that owns the data or documents to be released. Classified documents must be stored according to their classification level. When a vendor grants permission to the Laboratory to release classified information concerning the vendor's implementation to FIDO, this information may be released only to FIDO. The FIDO Biometric or Certification Secretariat will release the information to appropriate working group members within FIDO.

5.3.2.2. Test Operating Points§

Vendor-provided testing platforms need to choose one or more specific operating point to be tested. The laboratory must check that an implementation that claims certification shall operate at these same points.

5.3.2.3. Evaluation Reports§

All Evaluation Reports must be stored securely.

The Laboratory must store samples and all reports and logs the test sessions (whether paper or electronic) for a period of three years from the date the FIDO Evaluation Report was submitted to FIDO.

When submitting electronic Evaluation Reports to FIDO, the report must, be PGP encrypted and securely uploaded using the FIDO Evaluation Report Submission Form. All FIDO Certification forms and Evaluation Reports 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 Biometric Secretariat and the Laboratory, all evaluation reports sent via email will not be reviewed and will be deleted.

5.4. Administrative Requirements§

This section describes the administrative requirements that a Laboratory must meet.

5.4.1. Quality Assurance§

The Laboratory must have a quality system based upon ISO requirements, providing documented procedures defining processes to ensure a high quality of testing and test reproducibility. A Laboratory is required to comply with ISO 17025, and must also comply with the requirements stated elsewhere in this document.

5.4.2. Personnel§

The Laboratory must maintain a list of FIDO-qualified test personnel (Approved Evaluators) consisting of a description of their role in the organization, their qualifications, and their experience. The Laboratory must have procedures in place to ensure a match between staff training and and roles in the performance of FIDO activities.

The individual(s) performing the evaluation must be included on the Evaluation Reports submitted to FIDO. These Approved Evaluators will be required to maintain knowledge of FIDO Specifications and FIDO Certification Program Policies.

5.5. Technical Requirements§

5.5.1. Technical Expertise§

Prior experience with FIDO Specifications is strongly recommended as Laboratory employees that wish to be Approved Evaluators are required to pass a Knowledge Test in order to receive Accreditation.

The Laboratory must have at least two years of experience of testing in the domain for which it is seeking Accreditation. Including, but not limited to:

- Live Subject Testing

Additionally, the Laboratory must have experience of testing in:

- Presentation Attack Detection

5.5.1.1. Live Subject Testing

The Laboratory must have at least two years experience with Live Subject Testing.

> Note: Ideally, the Laboratory should have experience with Live Subject Testing of at least 123 unique individuals, as required in the Biometric Requirements for the Biometrics Certification Program.

5.5.1.2. Presentation Attack Detection

The Laboratory must have previous experience with Presentation Attack Detection, and Presentation Attack Instruments (PAI) for Imposter Presentation Attack Transactions.

If the Laboratory has followed [CAFVM] methodology for evaluations they can use that as evidence for this requirement.

6. Laboratory Accreditation Process

The following diagram illustrates the steps in the New Accreditation Process.

Figure 1 *New Accreditation Process*

The following table outlines the process steps in detail.

New Accreditation Process

Step	**Responsible Party**	**Process Requirement**
FIDO Accreditation Application	Laboratory	Completes the Laboratory Accreditation Application
	FIDO Biometric Secretariat	Completes review of Laboratory Accreditation Application. Informs Laboratory if the Application meets FIDO requirements, by providing an Accreditation Assessment Report to the Laboratory, notifying the Laboratory if it may proceed with the Accreditation process. Provides the Laboratory with the FIDO Laboratory Evaluation Agreement.
Legal Agreements	Laboratory	Schedules an appointment with the FIDO Biometric Secretariat and makes the financial and legal arrangements with the Biometric Secretariat to complete the Accreditation Assessment. Signs Laboratory portion of the FIDO Laboratory Evaluation Agreement.
FIDO Accreditation Training	Laboratory	On Boarding Call with FIDO Biometric Secretariat. FIDO Training and Knowledge Test.
Accreditation Issuance	Laboratory	Pays Accreditation Fees.
		If the Accreditation Assessment and Knowledge Test meets all requirements:

	FIDO Certification Secretariat	• Signs the FIDO portion of the FIDO Laboratory Evaluation Agreement. • Issues a Laboratory Accreditation Certificate. • Adds the Laboratory to the list of Accredited Biometric Laboratories on the FIDO website.

7. FIDO Accreditation Application§

To officially start the accreditation process the Laboratory must complete the Accreditation Application by providing documentation for the following areas.

7.1. Proposed Scope of Accreditation§

Proposed scope within those Programs for which the Laboratory is applying for Accreditation. For the biometric requirements, the term scope hereby refers to the biometric modalities (e.g. fingerprint) that the laboratory will be allowed to test. FIDO is seeking laboratories to cover all modalities (fingerprint, face, voice, iris), if possible, but will consider applications for a subset of those modalities.

Scope of Accreditation can be changed later following the Accreditation Scope Change process.

7.2. Authorized Representative§

An applicant Laboratory must designate an Authorized Representative that will act as the main contact for FIDO.

7.3. Business Practices§

The Laboratory shall provide evidence of business practices in the form of a written report describing:

- Services of the organization
- Structure of the organization, demonstrating the isolation between the Laboratory and other areas of the organization (e.g. design area).
- Percentage of revenue received from each of the Laboratory's top ten vendor customers relative to the total revenue of the Laboratory.
- Certificate of ownership and/or tax identification number.

7.4. Physical & Logical Security§

The Laboratory shall provide evidence of physical and logical security. This must be provided to FIDO either within the Laboratory procedures and documentation or a written report describing:

- Laboratory security policy with particular focus on the physical and logical network security measures.
- Personnel background check security policies.
- Confidential data protection practices.
- Vendor-provided testing platforms check

7.5. Administrative Conformance§

The Laboratory shall provide evidence of administrative conformance in the form of a written report describing:

- Description of the Laboratory's quality assurance system.
- Overview of the Laboratory personnel and the qualifications of Laboratory personnel involved in the performance of any testing or administrative duties connected with this Accreditation.
- Overview of the Laboratory equipment and techniques.
- Description of the Laboratory security policy with particular focus on the procedures for identification and recording of test samples.
- Overview of Laboratory asset management system for documentation and equipment.

7.6. Technical Expertise§

Technical expertise summary describing:

- Experience with FIDO Specifications.
- List of and evidence of other Formal Accreditations held by the Laboratory relevant to the proposed Scope of Accreditation.

7.7. Application Review§

The Biometric Secretariat will review the Laboratory Accreditation Application and will assess the Laboratory's fulfillment of all applicable requirements within the proposed Scope of Accreditation. The Biometric Secretariat will inform Laboratory if the Application meets FIDO requirements, by providing an Accreditation Assessment Report to the Laboratory, notifying the Laboratory if it may proceed with the Accreditation process.

8. Legal Agreements§

8.1. Laboratory Evaluation Agreement§

The Authorized Representative must sign the Laboratory Evaluation Agreement.

8.2. Confidentiality§

No vendor, Laboratory, nor other third party may refer to a product, service, or facility as FIDO approved or accredited, nor otherwise state or imply that FIDO (or any agent of FIDO) has in whole or part approved, accredited, or certified a vendor, Laboratory, implementation, 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 Certificate of Accreditation issued by FIDO.

8.3. Consistent Business Practices§

It is mandatory that any evaluation and/or test results from any FIDO Accredited Biometric Laboratory be recognized by all other FIDO Accredited Biometric Laboratories or FIDO Accredited Security Laboratories without any further investigation.

9. FIDO Accreditation Training§

9.1. On Boarding Call§

An introduction to FIDO Specifications and FIDO Certification Programs will be given by the FIDO Biometric Secretariat.

9.2. FIDO Training§

FIDO Training will be conducted by FIDO for the Laboratory Personnel requesting recognition as Approved Evaluators. A minimum of one Approved Evaluator is required for Laboratory Accreditation. This training will prepare individuals to pass the Knowledge Test.

9.3. Knowledge Test§

To become an Approved Evaluator, the Laboratory Personnel must pass a Knowledge Test on FIDO Specifications, Biometric Requirements, Biometric Test Procedures, and Program Policies.

10. Accreditation Issuance§

10.1. Fees§

Laboratories must pay all Accreditation fees before a Laboratory Accreditation Certificate will be issued.

10.2. Laboratory Accreditation Certificate§

Once at least one individual from the Laboratory has satisfactorily completed the Knowledge Test, the Authorized Representative can file an Accreditation Certificate Application.

The Certification Secretariat will be responsible for verifying all submitted documentation and issuing Laboratory Accreditation Certificates.

Turn-around time for Accreditation Certificates will be as soon as reasonably possible and no more than 30 days from the submission of the Application. When the Laboratory Accreditation Certificate is issued, it will contain the following information:

- The Company name of the Laboratory that has been Accredited
- The address of the Laboratory
- The Scope of Accreditation (BA for Biometric Assurance)
- The version of the Biometric Laboratory Accreditation Policy at the time of Accreditation
- The Expiration Date of the Accreditation
- Any restrictions, as necessary
- The Issuance Date of the Accreditation
- The Certificate Number in the format LAPPPPPPYYYYMMDDNNN, where:
    - LA = Lab Accreditation
    - PPPPPP = Policy Version in the format MMNNRR where:
        - MM = Major Number,
        - NN = Minor Number,
        - RR = Revision Number
    - YYYY = Year Issued
    - MM = Month issued
    - DD = Day issued
    - NNN = Sequential Number of Certificates issued that day

The Laboratory's Accreditation is valid for 3 years after the issuance date.

10.3. Decision Appeals§

If FIDO decides that a Laboratory is initially denied Accreditation, FIDO shall notify the Laboratory of the decision and will provide the reasons for not granting Accreditation. If the Laboratory disagrees with the reasons given for not granting Accreditation, it may appeal the decision. Appeal actions shall be initiated within 30 days of the notification of the decision not to grant Accreditation.

11. Accreditation Maintenance§

11.1. Group Participation§

Laboratories are required to participate in the Accredited Biometrics Laboratory Group and maintain voting rights.

If a Laboratory loses its voting rights it will be issued a written warning by FIDO, and the Laboratory will be given the opportunity to regain voting rights. If the Laboratory fails to regain voting rights within the timeline specified in the written warning the Laboratory will be suspended.

11.2. Requirement Version Maintenance§

The Laboratory will be required to maintain support of all active versions of the Biometric Requirements. For new versions, Laboratories will be required to support the version 90 days after the public release of the version.

11.3. Transparency of Testing Practices and Results§

Records of testing shall include, at a minimum, the Reference Devices used and the test configurations. All other information regarding testing shall be included as required in the FIDO Evaluation Report. FIDO may request more information on how testing was performed or reported, and detailed records shall be kept for a minimum of three years from the date the FIDO Evaluation Report was submitted to FIDO.

11.4. Knowledge Tests§

Training sessions and knowledge tests will be required as new requirements or specification versions are released. The knowledge test must be satisfactorily completed by at least one Approved Evaluator before completing an evaluation against the new version, or within 90 days of publication, whichever comes first.

In order to maintain Accreditation, Approved Evaluators are required to satisfactorily complete Knowledge Tests every three years as part of the renewal process.

11.5. Disclosure of Security Vulnerabilities§

If at any time the Accredited Biometric Laboratory encounters a Security Vulnerability within the Authenticator Boundary the Laboratory shall make the best effort to notify the FIDO Security Secretariat, FIDO Biometric Secretariat, and the Vendor within 48 hours.

The vulnerability will be triaged and handled according to the Security Vulnerability Assessment process outlined in the Authenticator Certification Policy.

11.6. Proficiency Assessments§

At any time, at the discretion of FIDO, a Proficiency Assessment may be required.

FIDO will inform the Laboratory that the Proficiency Evaluation must be performed, the requirements of the assessment, and the date by which the assessment must be completed. The scope of the Proficiency

Assessment will include a Laboratory's capabilities and compliance with the Security Test Procedures.

If an Accredited Biometric Laboratory does not complete the assessment to the satisfaction of FIDO by the date required, FIDO will suspend or revoke its Accreditation.

A Proficiency Assessment follows the process outlined in the Renewal Assessment, but instead is initiated by FIDO.

12. Accreditation Renewal§

A Laboratory must be validated through a Renewal Assessment every 3 years to maintain FIDO Accreditation.

12.1. Renewal Assessment§

The Renewal Assessment must be completed before the expiration date of the Laboratory's Accreditation. It is the responsibility of the Laboratory to renew its Accreditation before it expires. If a Laboratory does not renew its Accreditation, FIDO may revoke its Accreditation.

The following table outlines the process steps in detail.

Renewal Assessment Process

Responsible Party	**Process Steps**
Laboratory	Completes FIDO Renewal Request
FIDO Biometric Secretariat	Completes assessment of the Renewal Request. Informs Laboratory if the Renewal Request meets FIDO requirements and if it may proceed with the Renewal process. Identifies the Renewal Assessment requirements and informs the Laboratory.
Laboratory	Schedules an appointment with a FIDO Biometric Secretariat and makes the arrangements with the Security Secretariat for the Renewal Assessment Training. Satisfactory completion of the Knowledge Test by at least one Approved Evaluator.
FIDO Biometric Secretariat	Completes the Renewal Assessment Report and provides the document with the Approved or Rejected decision to the Laboratory.
Laboratory	Pays Renewal Assessment Fees.
FIDO Certification Secretariat	If the Renewal Assessment Report is Approved by FIDO: • Issues an updated Laboratory Accreditation Certificate. • Updates the Laboratory information on the FIDO Website, if necessary.

13. Modification or Termination of Accreditation§

A Laboratory's Accreditation may be modified or terminated.

The following sections outline reasons for modification or termination of Accreditation.

13.1. Laboratory Change in Testing Services Offered§

At any time, a Laboratory may decide to change the testing services it offers. If this occurs, the Laboratory is required to notify FIDO.

If a Laboratory decides to cease offering one or more of many FIDO testing services, the Laboratory must send a notice to FIDO using the Accreditation Change Request Form. Upon receipt of such a request, FIDO will modify the Laboratory's Scope of Accreditation accordingly, re-issue a Certificate of Accreditation (without changing the expiration date), and update the details in the list of Accredited Biometric Laboratories on the FIDO website.

If the Laboratory decides to cease offering their only FIDO testing service, FIDO Laboratory Accreditation will be Revoked.

13.2. Laboratory Change - Other§

The Laboratory must notify FIDO immediately of any changes in personnel (including Approved Evaluators), ownership, legal status, location or other change that may impact the Accreditation. The Laboratory shall use the FIDO Change Request to notify FIDO of these changes.

13.3. Accreditation Scope Change§

In the case where a Laboratory requests to add a new type of Accreditation evaluation and/or testing (i.e. add to the Scope of Accreditation), an Accreditation Scope Assessment is required. The existing renewal date for the Laboratory's Accreditation does not change.

The requirements for an Accreditation Scope Assessment are determined by FIDO at the time of the Assessment. The scope of the Assessment is a whole or subset of the Accreditation Assessment.

The Accreditation Scope Change process follows the Accreditation Assessment process, but instead starts by completing a Change Request.

13.4. Laboratory Termination of Accreditation§

At any time, a Laboratory may request termination of its Evaluation Agreement with FIDO.

The Laboratory shall complete an Accreditation Change Request to notify FIDO. Upon receipt of such request, FIDO will confirm termination of the Accreditation and Evaluation Agreement and remove the Laboratory's name from the FIDO website.

13.5. Non-conformance§

Non-conformance refers to an Accredited Biometric Laboratory's failure to conform to the policies or requirements listed herein.

If FIDO finds a Laboratory to be in non-conformance the Laboratory will be contacted and given a deadline to provide further information or correct the non-conformance. If the Laboratory fails to respond to FIDO or does not adequately correct the non-conformance the Accreditation will be suspended for further investigation or to allow the Laboratory to correct their non-conformance. Accreditation will be revoked if the non-conformance is not resolved. If the Laboratory disagrees with a non-conformance decision the Laboratory has the option to file a formal appeal or complaint to Certification Secretariat to be reviewed by the Crisis Response Team.

14. Accreditation Status§

14.1. Pending§

Laboratory that has started the Accreditation process but has not yet received an Accreditation Certificate or notice of a decision not to Accredit the Laboratory.

14.2. Active§

Accredited Biometric Laboratory in good standing with FIDO.

14.3. Inactive§

Inactive status is given to a Laboratory that has voluntarily requested in writing that their Accreditation be placed on hold due to unforeseen or unavoidable circumstances that temporarily prevent the Laboratory from adhering to the FIDO Laboratory Accreditation policy.

Inactive Laboratories will not be listed on the FIDO Website.

A Laboratory may have an Inactive status for no longer than one year.

If the Laboratory does not become Active after one year the Laboratory Accreditation shall beSuspended.

14.4. Suspended§

At any time, at FIDO's discretion, FIDO may suspend a Laboratory's Accreditation:

- Based on the results of an Assessment
- Due to a Laboratory's Non-conformance
- If a Laboratory fails to complete a Proficiency Assessment

If the Laboratory is suspended:

- The Laboratory will receive written notice of the suspension along with the actions required to return to Active status.
- The Laboratory will be removed from the FIDO Website.
- FIDO will set the requirements and date by which a Proficiency Assessment must be completed. If the Laboratory remains in a suspended state for a period of 180 days the Laboratory Accreditation will be Revoked. 90, 60, and 30 days prior to this deadline notices will be sent to the Suspended Laboratory.

14.5. Revoked§

At any time, at FIDO's discretion, FIDO may revoke a Laboratory's accreditation:

- Based on the results of an Assessment
- Due to a Laboratory's Non-conformance
- If a Laboratory fails to renew its Accreditation before the expiration date.
- If a Laboratory has not performed testing on FIDO products within the last 3 years.

If the Laboratory is revoked:

- The Laboratory will receive written notice of the Revocation.
- The Laboratory will be removed from the FIDO Website.
- The Laboratory Evaluation Agreement will be terminated.

- The Laboratory must make available to FIDO all evaluation reports for implementations already certified by FIDO or currently in testing for Certification within 30 days of the notice of revocation.
- The Laboratory must promptly return to FIDO all FIDO property and all confidential information. Alternatively, if so directed by FIDO, the Laboratory must destroy all confidential information, and all copies thereof, in the Laboratory's possession or control, and must provide a certificate signed by the Authorized Representative of the Laboratory that certifies such destruction in detail acceptable to FIDO.

Index§

Terms defined by this specification§

References§

Normative References§

[BEAT]
N. Tekampe; et al. BEAT: Towards the Common Criteria evaluations of biometric systems URL: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

[CAFVM]
CCDB-2008-09-002 Characterizing Attacks to Fingerprint Verification Mechanisms. 2011. published. URL: https://www.commoncriteriaportal.org/files/supdocs/CCDB-2008-09-002.pdf

[ISO30107-1]
ISO/IEC JTC 1/SC 37 Information Technology - Biometrics - Presentation attack detection - Part 1: Framework. URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=53227

[ISO30107-3]
ISO/IEC 30107-3:2017 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. 2017. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en

[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

↑

→