FIDO Biometrics Requirements

Working Draft, August 30, 2018

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

Issue Tracking:
GitHub

Editors:
Stephanie Schuckers (Clarkson University)
Greg Cannon (Crossmatch)
Elham Tabassi (NIST)
Meagan Karlsson (FIDO)
Elaine Newton (formerly of NIST)

Abstract

This document contains the FIDO Biometric Certification Authenticator Requirements and Test Procedures.

Table of Contents

Special acknowledgement to Michael Schuckers, St. Lawrence University, for advice regarding statistics for biometric evaluation.

1. Revision History§

Line-by-line comparisons for Pull Requests can be viewed in the GitHub Repository by viewing thePull Requests and selecting the "Closed" Pull Requests, or by adding the PR number to the end of the URL, for example, https://github.com/fido-alliance/biometrics-requirements/pull/**9**.

Revision History

Date	Pull Request	Document version	Description
		0.1	Initial Draft
2017-01-05	#9	0.2	Population Section Edits
2017-02-02	#14, #17, #18, #19, #21, #23, #24, #34	0.3	Bootstrapping, ISO Terms, Number of Subjects, Test Visits, Genuine Verification Transaction, removed Test Environment, Report to Vendor, and editorial issues.
2017-03-02	#36	0.5	Minor editorial corrections from Feb 16 and March 2 calls.
2017-03-23	#38	0.6	Introduction to Bootstrapping and other editorial issues.
2017-03-29	#42	0.7	New Key Words, and Self-Attestation FAR Requirement (Optional), and Self-Attestation sections. Rule of 3 and Bootstrapping sections split into FAR and FRR.
2017-04-11	#44	0.8	Minor editorial corrections from March 30 call.
2017-			New Revision History. Expanded RFC 2119 Key Word explanation. New Target of Evaluation section. Reworded False Reject Rate, and False Accept Rate sections. Edits to Number of Subjects, Population, and Bootstrapping: FAR. New Template

04-14	#45	0.9	Adaptation and Enrollment sections. Added inline issues based on comments from Jonas Andersson. FRR requirement at 3%.
2017-04-27	#46	0.10	Removed "Active Impostor Attempt", replaced with "Zero-Effort Impostor Attempt". Added "Arithmetic Mean". Removed Personnel Terms that were not used in the document. In Bootstrapping: FAR section replaced confidence interval with FAR distribution curve. Changed SHOULD to SHALL in Test Reports section. For Genuine Verification Transactions, added "Test Subjects SHALL conduct 5 genuine verification transactions." Added inline issues.
2017-05-09	#47	0.11	Added notes about attempts.
2017-05-24	#48	0.12	Added Test Procedures for Presentation Attack Detection (PAD).
2017-06-08	#52	0.13	Clean up of Test Reports sections. Added editors.
2017-06-27	#55, #56	0.14	Added KaTeX formatting for the FRR and FAR formulas.
2017-08-03	#57	0.15	Additional PAD Requirements - Triage of Presentation Attacks.
2017-08-03	#53	0.16	Added Rate Limit Requirement and mapping to Authenticator Security Requirement 3.9.
2017-08-03	#54	0.17	Confidence Interval at 80%, Bootstrapping FAR Figure, Minimum number of subjects at 245, and minimum of 123 unique persons in the test crew.
2017-08-03	#58, #59, #60, #61	0.18	Editorial corrections.
2017-08-03	#63	0.19	Further updates for 80% confidence interval, failure to acquire will not be considered during off-line FAR testing.
2017-08-31	#64, #65	0.20	Offline testing of FAR updated from N(N-1)/2 to (N(N-a)/2, 4 fingers instead of two. Corrected usage of MUST and SHOULD to SHALL. Added details to Self-Attestation FAR, and Bootstrapping: FAR sections. Updated Report to Vendor to Report to FIDO, and added information that should NOT be included. Populated PAI Species for Fingerprint, and for Face sections.
2017-09-27	#77	0.21	Added additional rows to the Self-Attestation Number of Subjects table. Updated number of subjects for PAD from 4 to 10. Added text to PAI Species for Iris/Eye Section. Updates to the Impostor Presentation Attack Transactions and Imposter Presentation Attack Errors sections.
2017-10-12	#76, #75, #78	0.22	#76: Updates related to PAI species for IAPMR. Added biometric characteristic data as a requirement for the FIDO Reports. Added a requirement for Labs to get approval for the PAI species for modalities not covered in this requirements document prior to completing an evaluation. Other editorial corrections around transactions vs. attempts. #75: Added Rule of 3 Table to Rule of 3: FAR Section. #78: Clarifications to the FAR calculation. Rate limiting number of attempts shall be limited to 5. Removed the Pre-Verification section. Clarifications for stored verification transactions.
2017-10-26	#80	0.23	Added Self-Attestation for FRR (Optional) section.
2017-	#84, #85	0.24	Added PAI for Voice Section, clean up of open issues.

12-07			
2017-12-22	#87	0.25	PAI Species for Voice edits
2018-1-18	#98	0.26	Multiple edits, most editorial. Added requirement to PAD < 50% for all PAI species tested in addition to <20% for 5/6 Level A and 3/4 Level B.
2018-1-18	#100	0.27	Multiple edits, most editorial. Added requirement for multiple templates.

2. Introduction§

This document provides implementation requirements for Vendors and Test Procedures which FIDO Accredited Biometric Laboratories can use for evaluating the biometric component of a FIDO Authenticator. The biometric component of the authenticator can be certified either as a component of the authenticator or as a separate biometric subsytem where the biometric certification can be used as input to a FIDO authenticator certification which includes the biometric subsystem. The test will focus on the passing requirements for biometric performance for the following metrics.

- False Accept Rate (FAR)
- False Reject Rate (FRR)
- Impostor Attack Presentation Match Rate (IAPMR)

The output of this test is provided to the FIDO certification program and will be used as a component to FIDO Certified products. The data will also be incorporated in the FIDO Metadata Service (MDS).

Associated documents to this document include: FIDO Biometrics Laboratory Accreditation Policy FIDO Biometrics Certification Policy

2.1. Reference Documents§

The following ISO standards are normative references to this certification program:

ISO/IEC 19795-1: Information technology-Biometric performance testing and reporting-Part 1: Principles and framework. ISO/IEC, Editor (2006). ([ISOIEC-19795-1])

ISO/IEC 19795-2:2007 Information technology -- Biometric performance testing and reporting -- Part 2: Testing methodologies for technology and scenario evaluation, ISO/IEC, Editor (2007) ([ISOIEC-19795-2])

ISO/IEC 30107-1:2016 Information technology -- Biometric presentation attack detection -- Part 1: Framework,ISO/IEC, Editor, 2016 [ISO30107-1]

ISO/IEC 30107-3:2017 Information technology -- Biometric presentation attack detection -- Part 3: Testing and reporting, ISO/IEC, Editor, 2017 [ISO30107-3]

2.2. Audience§

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

The owner of this document is the Biometrics Assurance Subgroup.

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, and has an valid 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.

2.5. Biometric Data and Evaluation Terms§

False Accept Rate (FAR)
The proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed. See Section 4.6.6 in [ISOIEC-19795-1].

False Reject Rate (FRR)
The proportion of verification transactions with truthful claims of identity that are incorrectly denied. See Section 4.6.5 in [ISOIEC-19795-1].

Failure-to-Aquire Rate (FTA)
Proportion of verification or identification attempts for which the system fails to capture or locate an image or signal of sufficient quality. See Section 4.6.2 in [ISOIEC-19795-1].

Failure-to-Enrol Rate (FTE)
proportion of the population for whom the system fails to complete the enrolment process See Section 4.6.1 in [ISOIEC-19795-1].

Impostor Attack Presentation Match Rate (IAPMR)
Proportion of presentation attacks in which the target reference is matched. See[ISO30107-3].

Sample
User's biometric measures as output by the data capture subsystem. See Section 4.1.1 in [ISOIEC-19795-1].

Template
User's stored reference measure based on features extracted from enrollment samples. See Section 4.1.3 in [ISOIEC-19795-1].

Target of Evaluation (TOE)
The product or system that is the subject of the evaluation. See theTOE section in this document.

Presentation

Submission of a single biometric sample on the part of a user. See Section 4.2.1 in [ISOIEC-19795-1].

Attempt
Submission of one (or a sequence of) biometric samples to the system. See Section 4.2.2 in [ISOIEC-19795-1].

Transaction
Sequence of attempts on the part of a user for the purposes of an enrollment, verification, or identification. See Section 4.2.3 in [ISOIEC-19795-1].

Genuine Attempt
Single good-faith attempt by a user to match their own stored template. See Section 4.2.4 in [ISOIEC-19795-1].

Zero-Effort Impostor Attempt
Attempt in which an individual submits his/her own biometric characteristics as if he/she were attempting successful verification against his/her own template, but the comparison is made against the template of another user See Section 4.2.5 in [ISOIEC-19795-1].

Online
Pertaining to execution of enrollment and matching at the time of image or signal submission. See Section 4.4.4 in [ISOIEC-19795-1].

Offline
Pertaining to execution of enrollment and matching separately from image or signal submission. See Section 4.4.5 in [ISOIEC-19795-1].

Verification
Application in which the user makes a positive claim to an identity, features derived from the submitted sample biometric measure are compared to the enrolled template for the claimed identity, and accept or reject decision regarding the identity claim is returned. See Section 4.5.1 in [ISOIEC-19795-1].

Stored Verification Transaction
A set of acquired biometric verification sample(s) from an on-line verification transaction, which is stored for use in off-line verification.

Presentation attack instrument (PAI)
Biometric characteristic or object used in a presentation attack, in [ISO30107-1].

PAI species
Class of presentation attack instruments created using a common production method and based on different biometric characteristics, in [ISO30107-3].

2.6. Statistical Terms§

Arithmetic Mean
The average of a set of numerical values, calculated by adding them together and dividing by the number of terms in the set.

Variance
V. Measure of the spread of a statistical distribution. See Section 4.7.3 in [ISOIEC-19795-1].

Confidence Interval
A lower estimate *L* and an upper estimate *U* for a parameter such as *x* such that the probability of the true value of *x* being between *L* and *U* is the stated value (e.g. 80%). See Section 4.8.2 in [ISOIEC-19795-1].

2.7. 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].

2.8. 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.

2.9. Document Structure§

This document outlines the Requirements and Test Procedures for the FIDO Biometrics Certification Program.

2.10. Target of Evaluation§

The Target of Evaluation (TOE) for the purpose of the FIDO Biometric Certification Program SHALL include all functionality required for biometrics: the Biometric Data Capture, Signal Processing, Comparison, and Decision functionality, whether implemented in hardware or software.

A TOE SHALL be provided for each Allowed Integration, e.g. different thickness of glass.

The Integration Manual is provided for reference to the Laboratory, it SHALL be coherent with the configuration and operation of the Test Harness.

Relevant product identification which can be referenced by both Biometrics supplier and OEM. The test results will be announced for the uniquely identified product.

The TOE SHALL be provided to the Laboratory from the Vendor in the form of a Common Test Harness which is set up to offer practical possibility for the Laboratory to perform the testing efficiently and identify the components of the Test Harness as being of the TOE.

3. Requirements§

Currently, only one Certification Level exists for the biometric requirements (Certification Level 1). Therefore, all requirements in this chapter apply to this level.

3.1. FIDO Biometric Performance Levels§

The FIDO Biometric Certification Program uses False Reject Rate (FRR) and False Accept Rate (FAR) to measure Biometric Performance.

3.1.1. False Reject Rate (FRR)§

Requirement

False Reject Rate SHALL meet the requirement of less than 3:100 for the upper bound of a 80% confidence interval. FRR is measured at the transaction level.

The actual achieved FRR SHALL be documented by the laboratory. Requirememts on reporting can be found in section .

§5.1.7 Reporting Requirements

The threshold, or operational point, SHALL be fixed during testing. It is set by the Vendor and SHALL correspond to the claimed False Accept Rate (FAR) value to be tested.

FRR SHALL be estimated by the equation given in[ISOIEC-19795-1], 8.3.2.

Limitation

For the purposes of this test, no more than five attempts will be allowed per verification transaction. The calculation of FRR SHALL be based on:

$$FRR\ (\%) = \frac{Number\ of\ Genuine\ Transactions\ for\ which\ decision\ is\ reject\ or\ FTA\ happens\ for\ all\ Attempts}{Total\ Number\ of\ Genuine\ Transactions\ Conducted} * 100$$

All errors encountered during the testing, specifically FTA, SHALL be recorded according to[ISOIEC-19795-2], 7.3.

3.1.2. False Accept Rate (FAR)§

Requirement

False Accept Rate SHALL meet the requirement of less than 1:10,000 for the upper bound of a 80% confidence interval. FAR is measured at the transaction level.

FAR SHALL be estimated as follows (see also[ISOIEC-19795-1], 8.3.3.)

> The false accept rate is the expected proportion of zero-effort non-genuine transactions that will be incorrectly accepted. A transaction may consist of one or more non-genuine attempts depending on the decision policy.
>
> The false accept rate SHALL be estimated as the proportion (or weighted proportion) of recorded zero-effort impostor transactions that were incorrectly accepted.

Note: Please note that for the weighted proportion of recorded zero-effort impostor transactions the weights will be equal for each user as there will always be 5 impostor transactions per enrolled user.

> The false accept rate will depend on the decision policy, the matching decision threshold, and any threshold for sample quality. The false accept rate SHALL be reported with these details, alongside the estimated false reject rate at the same values, (or plotted against the false reject rate at the same threshold(s) in an ROC or DET curve).

FAR is computed through offline testing based on enrollment templates and verification samples collected during online testing.

The vendor provides an SDK which inputs an enrollment template and a stored verification transaction and which returns the decision to “accept” or “reject”. Each decision used in computing the FAR is based on an inter-person (between person) combinations of an enrollment template and samples stored during verification.

The actual achieved FAR SHALL be documented by the laboratory, together with all other information about the test as per [ISOIEC-19795-1] and [ISOIEC-19795-2].

The threshold, or operational point, SHALL be fixed during testing. It is set by the Vendor. The threshold SHALL be the same as the threshold used for FRR.

The number of attempts allowed per verification transaction SHALL be fixed during testing. It is set by the Vendor.

Limitation

For the purposes of this test, the same number of attempts as used in false reject rate on-line testing (e.g. five) shall be used for each off-line verification transaction. The calculation of FAR SHALL be based on the following equation:

$$FAR\ (\%) = \frac{Number\ of\ zero-effort impostertransactions\ Transactions\ for\ which\ decision\ is\ Accept}{Total\ Number\ of\ zero-effort impostertransactions\ Transactions\ Conducted} * 100$$

A false accept error SHALL be declared if any attempts in the stored verification transaction results in a match decision. Since FAR is calculated off-line based on previously stored attempts, Failure to Acquire SHALL NOT be considered in computation of FAR.

Option

A Vendor MAY at their choice claim lower FAR than the 1:10,000 requirement set by FIDO. The procedures for submitted test data SHALL follow methods described in Self-Attestation FAR (Optional).

> Note: The transaction FAR can be used as a worst case value for an attempt FAR and thus can be used for attempt level probability calculations in FIDO Security Requirements. In FIDO certification, the transaction FAR is computed such that if at least one attempt is a match for stored verification transaction (when compared to an enrollment template for a different individual), then a FAR error is declared for that transaction. For computing an attempt FAR, in order to ensure than no single combination of individuals impacts the attempt FAR more than another, attempts would need to be randomly sampled such that there is an equal number attempts per combination of individuals. Since attempt level FAR is not computed, this criteria is not required for this test.

> Note: As a further note, the FAR is an error that is related to so called zero-effort-impostor-attempts. In these attempts, the attacker will spend no effort all in order to get recognised as a different individual but simply use their own biometric characteristic. This metric does not provide any information on how the TOE would behave in cases where an attacker starts with dedicated attacks.

3.1.3. Self-Attestation FAR (Optional)§

Self-attestation for FAR is optional. If the vendor chooses self-attestation for FAR, the following requirement applies. The vendor SHALL attest to an FAR of [1:25,000 or 1:50,000 or 1:75,000 or 1:100,000] at an FRR of 3% or less. This claim SHALL be supported by test data as described in Self Attestation (Optional) and documented through a report submitted from the Vendor to the Laboratory. The Laboratory SHALL validate the report follows FIDO requirements described in Self Attestation (Optional) and supports the claim. The laboratory SHALL compare the FAR bootstrap distribution generated as a result of the independent testing and determine if it is consistent with the self-attestation value. The arithmetic mean of the bootstrap distribution SHALL be less than or equal to the self-attestation value. If this is not met, the self-attestation value SHALL NOT be added to the meta-data.

3.1.4. Self-Attestation FRR (Optional)§

Self-attestation for FRR is optional. If the vendor chooses self-attestation for FRR, the following requirement applies. The vendor SHALL attest to an FRR at no greated than 3% as measured when determining the self-attested FAR. In other words, self attestation for FRR is only possible when self attesting for FAR. This claim SHALL be supported by test data as described in Self-Attestation (Optional) and documented through a report submitted from the Vendor to the Laboratory. The Laboratory SHALL validate the report follows FIDO requirements described in Self-Attestation (Optional) and supports the claim. The laboratory SHALL compare the FRR measured as a result of the independent testing and determine if it is consistent with the self-attestation value. The FRR measurement SHALL be less than or equal to the self-attestation value. If this is not met, the self-attestation value SHALL NOT be added to the meta-data.

3.1.5. Maximum Number of Templates from Multiple Fingers (OPTIONAL)§

Requirement

If a subject enrolls multiple fingers (e.g. index and thumb) and uses them interchangeably (i.e. one OR another), the FAR increases where the FAR for two fingers enrolled is approximately twice the FAR for one finger enrolled. This section describes the process such that a biometric system can be certified to operate with two or more enrolled fingers. Other biometric modalities where this may apply are described in notes below.

The vendor SHALL declare the maximum number of different fingers which can be enrolled. The FAR associated with Multiple Templates (FAR_{MT}) SHALL be calculated according to the following and SHALL not be greater than 1:10,000.

FAR_{MT} =1 - ((1-FAR_{MT})^B)

B=Max # Templates FAR_{SA}=Self-attested FAR verified by FIDO according to SectionSelf-Attestation FAR (Optional).

At the time of FIDO authenticator certification, the maximum number of templates which meet the FAR requirement MAY be be stored in the meta-data and SHALL NOT be greater than maximum number verified during biometric certification, according to above. If this analysis is not performed, the maximum number of templates SHALL default to one. Self-attested FAR in the meta-data SHALL be based on the single template FAR.

> Note: Some iris systems may enroll each eye separately and allow successful verification even if only one eye is presented. Eyes can be considered in place of fingers for this section, if applicable to the TOE.

> Note: The same process may be used for other modalities which have a similar property, i.e., where multiple parts of the body can be used interchangeably, e.g. palm veins for right and left hand. The vendor SHALL submit how this property may apply the modality of the TOE. The FIDO lab SHALL use the same process to assess maximum number of templates.

3.2. FIDO Presentation Attack Detection Criteria§

3.2.1. Impostor Attack Presentation Match Rate (IAPMR)§

Requirement

Five of the six selected Level A PAI species SHALL achieve an IAPMR of less than 20%. In addition, all selected Level A PAI species SHALL achieve an IAPMR of less than 50%. Three of the four selected Level B PAI species SHALL achieve an IAPMR of less than 20%. In addition, all selected Level B PAI species SHALL achieve an IAPMR of less than 50%. Levels A and B are defined in Test Procedures for Presentation Attack Detection (PAD)

The actual achieved IAPMR for each PAI species SHALL be documented by the laboratory, together with all other information about the test.

The threshold, or operational point, SHALL be fixed during testing. It is set by the Vendor and SHALL correspond to the claimed False Accept Rate (FAR) value to be tested.

Limitation

No more than five attempts SHALL be allowed per impostor presentation attack transaction. The PAI SHALL be presented the maximum number of attempts allowed for a transaction OR until it matches (which results in an error).

$$IAPMR\ (\%) = \frac{Number\ of\ Transaction\ for\ which\ decision\ is\ Accept}{Total\ Number\ of\ Impostor\ Presentation\ Attack\ Transaction\ Conducted} * 100$$

IAPMR SHALL be calculated for each PAI Species. All errors encountered during the testing SHALL be recorded according to [ISOIEC-19795-2], 7.3.

> Note: A failure to acquire for an impostor presentation attack transaction does not count as an error, as some systems may produce a failure to acquire in response to a detected presentation attack.

3.2.2. Rate Limits§

Additional requirements in the FIDO Authenticator Security Requirements may impact the biometric TOE under evaluation herein. Those are tested as part of FIDO Authenticator Certification. As part of these requirements, FIDO Authenticators are required to rate-limit user verification attempts according to FIDO Authenticator Security Requirements, Requirement 3.9. For the purposes of biometric certification testing, rate limiting SHOULD be turned off and the test laboratory SHALL limit the number of attempts per transaction to five.

4. Common Test Harness§

For each operating point to be evaluated, the Vendor SHALL provide a biometric system component of the FIDO authenticator which has at a minimum:

A. Configurable Enrollment system which:
   1. Selects the operating point(s) to be evaluated.
   2. Has enrollment hardware / software as will be executed by the FIDO authenticator.
   3. Includes a biometric data capture sensor and enrollment software.
   4. Can clear an enrollment.
   5. Can store an enrollment from acquired biometric sample(s) for use in on-line verification evaluation.
   6. Can provide enrollment templates from acquired biometric sample(s) defined as “user’s store reference measure based on features extracted from enrollment samples” for use in off-line verification evaluation.
   7. Indicates a failure to enroll ([ISOIEC-19795-1], 4.6.1)

B. Configurable Verification on-line system which:
   1. Selects the operating point(s) to be evaluated.
   2. Has verification hardware / software as will be executed by the FIDO authenticator.
   3. Includes a biometric data capture sensor, a biometric matcher, and a decision module.
   4. Captures features from an acquired biometric sample to be compared against an enrollment template.
   5. Makes accept/reject decision at a specific operating point.
   6. Indicates an on-line failure to acquire ([ISOIEC-19795-1], 4.6.2).

7. Indicates an on-line decision(accept or reject).
8. Provides a set of acquired biometric sample(s) from an on-line verification transaction (this is called a stored verification transaction). This will be used for off-line verification.

C. Configurable Verification off-line software, which:
1. Selects the operating point(s) to be evaluated.
2. Has verification software as will be executed by the FIDO authenticator.
3. Accepts an enrollment template and the stored verification transaction and performs matching in off-line batch mode.
4. Provides a decision (accept or reject).

D. logging capabilities, which:
1. Record every interaction with the TOE.
2. Allow the tester to manually addd interactions (e.g. the fact that a tester just cleaned the sensor device)

> Note: For Enrollment, some vendors MAY use multiple samples per test subject (e.g. multiple impressions for a single finger). A enrollment template can be based on multiple stored samples. This SHOULD be opaque to the tester.

> Note: For a Stored Verification Transaction, the Test Harness SHALL store all attempts in a transaction. This will be used for off-line verification testing.

4.1. Security Guidelines§

For security purposes, provided enrollment templates and verification transactions should be confidentiality and data authentication protected using cryptographic algorithms listed within the FIDO Authenticator Allowed Cryptography List. The lab SHALL report to FIDO the process used to help assure TOE consistency and security.

> Note: For example, only the vendor and FIDO Accredited Laboratory should have the ability to decrypt this information. To help assure TOE consistency, the vendor could use different keys to protect/authenticate the data collected from each tested allowed integration. The test result data specific to particular combinations of operating points and integrations could include that configuration information within the authentication.

5. Test Procedures for FAR/FRR§

Biometric Performance Testing SHALL be completed by using the Scenario Test approach, an evaluation in which the end-to-end system performance is determined in a prototype or simulated application. See Section 4.4.2 in ([ISOIEC-19795-1]).

Testing shall be perfomed using the Common Test Harness defined inCommon Test Harness.

5.1. Test Crew§

The Test Crew is the Test Subjects gathered for evaluation.

5.1.1. Number of Subjects§

The minimum number of subjects for a test SHALL be 245, based on [ISOIEC-19795-1] and associated analysis in the Statistics and Test Size section of this document.

For fingerprint, up to four different fingers from a single person can be considered as different test subjects. For the fingerprint biometrics, these fingerprints SHALL be constrained to the index, thumb, or middle fingers, and SHALL be the same as was used for enrollment. A minimum of 123 unique persons SHALL be in the test crew.

For eye-based biometrics, both the left and right eye can be considered as two different test subjects. A minimum of 123 unique persons SHALL be in the test crew.

> Note: Two eyes cannot be considered as different test subjects if both eyes are enrolled at one time.

In the event there is an enrollment failure according to Enrollment Transaction Failures, an additional Subject SHALL be enrolled for each enrollment failure.

5.1.2. Population

The population SHALL be experienced with the TOE in general and SHALL be given a possibility to try and acquaint themselves with the TOE before starting to enroll and prior to performing verification transactions. The population SHALL be motivated to succeed in their interaction with the TOE and they SHALL perform a large number of interactions with the TOE during a short period of time.

The population SHOULD be representative of the target market in relationship to age and gender. Age and gender recommendations are taken from [ISOIEC-19795-5] for access control applications (Section 5.5.1.2 and 5.5.1.3). The following targets SHOULD be used for age and gender:

5.1.2.1. Age

Age Distribution Requirements

Age	Distribution
< 18	0%
18-30	25-40%
31-50	25-40%
51-70	25-40%
> 70	0%

5.1.2.2. Gender

Gender Distribution Requirements

Gender	Distribution
Male	40-60%
Female	40-60%

Note: As indicated in [ISOIEC-19795-1], ideally, the test subjects SHOULD be chosen at random from a population that is representative of the people who will use the system in the real application environment. In some cases, however, the test subjects do not accurately represent the real-world users. If the test crew comes from the vendor's employee population, they MAY differ significantly from the target users in terms of educational level, cultural background, and other factors that can influence the performance with the chosen biometric system.

5.1.3. Statistics and Test Size§

The following sections describe the statistical analysis of the data which results from both on-line tests for assessment of FRR and off-line tests for assessment of FAR. Testing will result in a matrix of accepts and rejects for each verification transaction. This data can be used to calculate the upper-bound of the confidence interval through the bootstrapping method described in this section which are used in determining if TOE meets the Requirements set in Section Requirements..

5.1.3.1. Bootstrapping: FAR§

Bootstrapping is a method of sampling with replacement for the estimation of the FAR distribution curve. Bootstrap calculations will be conducted according to [ISOIEC-19795-1]), Appendix B.4.2, where v(i) is a specific test subject, where i = 1 to n, where n is the total number of test subjects:

1. Sample n test subjects with replacement v(1),...,v(n).
2. For each v(i), sample with replacement (n-1) non-self templates.
3. For each v(i), sample with replacement m attempts made by that test subject.
4. This results in one bootstrap sample of the original data (i.e. a new set of data which has been sampled according to 1-3). Intra-person SHALL be avoided if more than one finger or eye is used for each subject.

A false accept rate is obtained for each bootstrap sample. The steps above are repeated many times. At least 1,000 bootstrap samples SHALL be used, giving a false accept rate (FAR) for each. The distribution of the bootstrap samples for the false accept rate is used to approximate that of the observed false accept rate.

1. One-sided upper 100(1-α)% confidence limit is computed from the resulting distribution, where the upper bound is set at 80%
2. If the upper limit is below the FAR threshold (e.g. 1:10,000), there is reasonable confidence that the standard is met.

Note: Simulations of the bootstrapping process were performed using settings required by FIDO in order to determine the mean FAR associated with Upper Bound of the Confidence interval. The following settings were used: 245 Subjects (n), 1 enrollment per subject, 5 verification transactions(m), 298,900 total impostor comparisons from $N = nm(n–1)$, Errors were randomly distributed across the 298900 comparison, 5000 bootstraps created using ISO method.

Note: (continued) When the Upper Bound (UB) of the Confidence Interval of the bootstrap distribution is set to 1:10,000, the mean FAR is necessarily below 1:10,000. Table below provides the mean FAR associated with 68%, 80%, and 95 UB Confidence Intervals when the UB is set to 1:10,000. For example to achieve an 80% upper bound, in this simulation, the mean FAR is 1:13,000.

Table: Mean of Bootstrapping Distribution Associated Different Upper Bounds of Confidence Interval set to 1:10,000

Upper Bound (UB) of Confidence Interval Set to 1:10,000	**Number of Errors to Achieve UB**	**Mean of FAR Bootstrap Distribution Associated with UB**

68%	27 (out of 298,900)	1/11,000
80%	23 (out of 298,900)	1/13,000
95%	17 (out of 298,900)	1/18,000

Figure 1 provides a schematic of the bootstrap distribution and FAR requirement. A biometric sub-system passes biometric certification if the upper bound of the 80% one-sided confidence interval derived from the bootstrap distribution is less than 1:10,000.

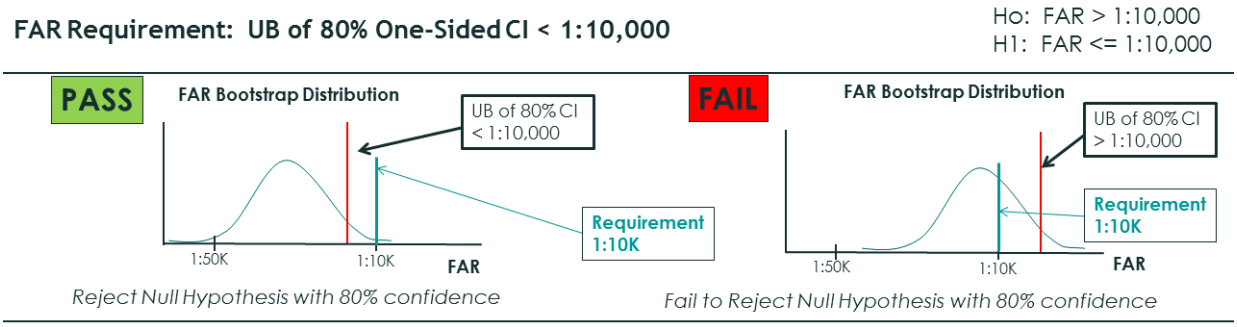

Figure 1 *Bootstrapping FAR Schematic*

5.1.3.2. Bootstrapping: FRR

Bootstrapping is a method of sampling with replacement for the estimation of the FRR distribution curve. Bootstrap calculations will be conducted according to [ISOIEC-19795-1], Appendix B.4.2, where v(i) is a specific test subject, where i = 1 to n, where n is the total number of test subjects:

1. Sample n test subjects with replacement v(1),...,v(n).
2. For each v(i), sample with replacement m attempts made by that test subject.
3. This results in one bootstrap sample of the original data (i.e. a new set of data which has been sampled according to 1-3).

A false reject rate is obtained for each bootstrap sample. The steps above are repeated many times. At least 1,000 bootstrap samples SHALL be used, giving a false reject rate (FRR) for each. The distribution of the bootstrap values for the false reject rate is used to approximate that of the observed false reject rate.

1. One-sided upper 100(1-α)% confidence limit is computed from the resulting distribution, where the upper bound is set at 80%
2. If the upper limit is below the FRR threshold (e.g. 3 in 100), there is reasonable confidence that the standard is met.

5.1.3.3. Rule of 3: FAR

In the event that there are zero errors in the set of zero-effort imposter comparisons, the TOE meets the FAR requirement on the basis of the "Rule of 3".

> Note: The "Rule of 3" method is utilized to establish an upper bound if there are zero errors in the test, according to [ISOIEC-19795-1], Appendix B.1.1. As long as the laboratory utilizes at least n=245 subjects, this results in n(n-1)/2 or 29890 combinations (N). Rule of 3 states the upper bound of the 95% confidence interval is 3/N, or 0.0100%. For an 80% upper bound, the upper bound is 1.61/N or 0.00535%, which meets the FIDO FAR requirement of 0.01%. The following table provides number of subjects needed to meet Rule of 3 for lower FAR and when two (a=2) instances (fingers or eyes) are used.

Table: Rule of 3 for FAR

Rule of 3 ([ISOIEC-19795-1])	**FAR**				
	0.0100%	0.0040%	0.0020%	0.0013%	0.0010%
	1:10,000	1:25,000	1:50,000	1:75,000	1:100,000
One unique sample per person (e.g., one finger or one eye)					
# of people needed (n)	245	390	550	675	775
# Combinations-C = n(n-1)/2	29890	75855	150975	227475	299925
Claimed error = 3/C (when zero errors in C combinations)	0.0100%	0.0040%	0.0020%	0.0013%	0.0010%
Two unique sample per person (e.g., two fingers or two eyes)					
# people needed (n)	123	195	275	335	388
# unique samples (a)	2	2	2	2	2
# Combinations-C = (a^2)*n*(n-1)/2	30012	75660	150700	223780	300312
Claimed error = 3/C (when zero errors in C combinations)	0.0100%	0.0040%	0.0020%	0.0013%	0.0010%

5.1.3.4. Rule of 3: FRR

In the event that there are zero errors in the set of geniune comparisons, the TOE meets the FRR requirement on the basis of the Rule of 3.

> Note: The "Rule of 3" method can be utilized to establish an upper bound if there are zero errors in the test, according to [ISOIEC-19795-1], Appendix B.1.1. As long as the laboratory utilizes at least 245 people, this results in 245 genuine comparisons. Rule of 3 states the upper bound of the 95% confidence interval is 3/N (3/245) or 1.22%. For an 80% upper bound, the upper bound is 1.61/N or 0.65%, which is meets FIDO FRR requirement of 3%.

5.1.4. Test Visits

As this test is focused on False Accept Rate, collection from test subjects MAY occur in one visit.

5.1.5. Template Adaptation

Some systems perform template updates, that is, the enrollment template is adapted after successful verification transactions.

Vendor SHALL inform the Laboratory whether template adaptation is employed and SHALL give instructions on what number of correct matches SHOULD be performed in order to have the TOE adequately trained

before the testing. For the purposes of testing, the Template Adaptation SHALL be turned off, after the TOE has been fully trained on correct templates.

> Note: Template adaptation which requires an extensive amount of time may incur increased cost of the laboratory test.

The offline software SHALL utilize enrollment templates in the same way as the online software.

5.1.6. Enrollment§

Enrollment procedures SHALL be provided in writing to the Laboratory by the Vendor. These procedures SHALL be followed by the Test Crew. Instructions MAY be provided in any form, including interactive on screen guidance to the Test Subject. The Administrator SHALL record any FTE, if appropriate, with any divergence from enrollment instructions that MAY have caused the failure.

5.1.7. Reporting Requirements§

5.1.7.1. Logging of test activities§

In addition to the reports, the laboratory SHALL maintain a log file in which each interaction (including all attempts from performance testing and all attempts from PAD testing) with the TOE is recorded. The log SHALL include all test attempts, all preprative attempts, management attempts (e.g. setting a threshold) and maintenance activities (e.g. cleaning a sensor). The log SHALL at least contain the following information for each entry:

- Timestamp
- Identity of the tester
- Type of attempt
- Expected outcome
- Actual outcome

The log SHOULD be written automatically by the TOE (cf.requirements for logging for test harness) whenever possible but will be to be augmented by manual entries that are not known to the TOE. The manual augmentation of the log file is necessary as the TOE does not have the required information to log for some events (e.g. the actual user who performed an impostor attempt under a wrong identity) or will even not be aware of some events (e.g. the fact that a sensor has been cleaned).

The log MUST neither be submitted to FIDO nor the vendor but remain with the laboratory. It may be used to answer questions that arise in the context of the certification procedure and is accessible by FIDO upon request.

5.1.8. Report to the FIDO§

The following SHALL be included in a report to the FIDO, following [ISOIEC-19795-1], 10.5:

- Summary of the FIDO Biometric Certification and Requirements
- Number of individuals tested
- Distribution of Age
- Distribution of Gender
- Description of the Test Environment
- Description of the Test Platform

- Distribution of the time lapsed between Enrollment and Acquisition
- Number of enrollment transactions
- Number of genuine verification transactions
- Number of impostor verification transactions
- Failure to Enroll Rate
- Failure to Acquire Rate
- False Reject Rate
- False Accept Rate
- Distribution of Genuine Verification Transaction Time
- Bootstrap Distribution

Other items of value MAY include:

- Distribution of ethnicity/race
- Additional information as agreed upon between the lab and vendor

The lab SHALL NOT include the identity and other personal information of the participants.

A copy of the report SHALL be provided to vendor prior to being provided to FIDO.

5.1.8.1. FIDO Reports

FIDO will verify the biometric-related metadata according to the FIDO Metadata Statement ([FIDOMetadataStatement]) and FIDO Metadata Service ([FIDOMetadataService]).

5.2. Test Methods

Testing will be performed through a combination of Online and Offline Testing ([ISOIEC-19795-1]).

5.2.1. Pre-Testing Activities

Pre-test activities SHALL be performed according to [ISOIEC-19795-2]:

- Section 6.1.8 Pre-test procedures
- Section 6.1.8.1 Installation and validation of correct operation

5.2.2. Online Testing

This section will focus on Online Testing.

To facilitate estimation of false accept rate, all enrollment templates and all captured biometric samples from all verification transactions are stored to allow for offline computation of the FAR.

5.2.2.1. Online: Enrollment

Enrollment SHALL be performed according to [ISOIEC-19795-1], 7.3.

5.2.2.1.1. Pre-Enrollment

Before enrollment test subjects MAY perform practice transactions.

5.2.2.1.2. Enrollment Transactions§

Enrollment transactions SHALL be conducted without test operator guidance. Any kind of guidance SHALL be provided by the biometric authentication system/capture sensor in a similar way to the final application.

The enrollment process will be different depending on the biometric authentication system. This process MAY allow enrollment after one attempt, or MAY require multiple presentations and attempts. For testing, this process SHALL be similar to the final application.

5.2.2.1.3. Enrollment Transaction Failures§

A failure to enroll SHALL be declared when the biometric authentication system is not able to generate a template for the test subjects after executing three enrollment transactions.

5.2.2.2. Online: Genuine Verification Transaction§

Genuine verification transactions SHALL be performed according to[ISOIEC-19795-1], 7.4. This means that the following requirements SHALL be met:

Genuine transaction data shall be collected in an environment, including noise, that closely approximates the target application. This test environment shall be consistent throughout the collection process. The motivation of test subjects, and their level of training and familiarity with the system, should also mirror that of the target application.

The collection process should ensure that presentation and channel effects are either uniform across all users or randomly varying across users. If the effects are held uniform across users, then the same presentation and channel controls in place during enrolment should be in place for the collection of the test data. Systematic variation of presentation and channel effects between enrolment and test data will lead to results distorted by these factors. If the presentation and channel effects are allowed to vary randomly across test subjects, there shall be no correlation in these effects between enrolment and test sessions across all users.

In the ideal case, between enrolment and the collection of test data, test subjects should use the system with the same frequency as the target application. However, this may not be a cost-effective use of the test crew. It may be better to forego any interim use, but allow re-familiarization attempts immediately prior to test data collection.

For systems that may adapt the template after successful verification, some interim use between enrolment and collection of genuine attempt and transaction data may be appropriate. The amount of such use should be determined prior to data collection, and should be reported with results.

The sampling plan shall ensure that the data collected are not dominated by a small group of excessively frequent, but unrepresentative users.

Great care shall be taken to prevent data entry errors and to document any unusual circumstances surrounding the collection. Keystroke entry on the part of both test subjects and test administrators should be minimized. Data could be corrupted by impostors or genuine users who intentionally misuse the system. Every effort shall be made by test personnel to discourage these activities; however, data shall not be removed from the corpus unless external validation of the misuse of the system is available.

Users are sometimes unable to give a usable sample to the system as determined by either the test administrator or the quality control module. Test personnel should record information on failure-to-acquire attempts where these would otherwise not be logged. The failure-to-acquire rate measures the proportion of such attempts, and is quality threshold dependent. As with enrolment, quality thresholds should be set in accordance with vendor advice.

Test data shall be added to the corpus regardless of whether or not it matches an enrolled template. Some vendor software does not record a measure from an enrolled user unless it matches the enrolled template. Data collection under such conditions would be severely biased in the direction of underestimating false non-match error rates. If this is the case, non-match errors shall be recorded by hand. Data shall be excluded only for predetermined causes independent of comparison scores.

All attempts, including failures-to-acquire, shall be recorded. In addition to recording the raw image data if practical, details shall be kept of the quality measures for each sample if available and, in the case of online testing, the matching score or scores.

5.2.2.2.1. Pre-Verification§

Before genuine verification transactions test subjects MAY perform practice transactions.

5.2.2.2.2. Genuine Verification Transaction§

Test Subjects SHALL conduct 5 genuine verification transactions. Genuine verification transactions SHALL be conducted without test operator guidance. Any kind of guidance SHALL be provided by the biometric authentication system / capture sensor in a similar manner to the final application.

The verification process MAY be different depending on the biometric authentication system. This process MAY require multiple presentations. For testing purposes, this process SHALL NOT have more than five attempts for each transaction. A transaction SHOULD NOT exceed 30 seconds.

The authenticator vendor SHALL describe to the Accredited Biometric Laboratory what constitutes the start and end of a verification transaction.

All attempts used for the online genuine verification transaction SHALL be stored for offline testing.

> Note: If it only two attempts for a verification transaction to succeed, only two attempts would be stored.

5.2.2.2.3. Genuine Verification Errors§

A failure to acquire SHALL be declared when the biometric authentication system is not able to capture and / or generate biometric features during a verification attempt (an FTA MAY happen per attempt). The on-line verification test harness SHALL indicate to the laboratory when a failure to acquire has occurred.

> Note: A failure to acquire will not be considered during off-line FAR testing.

A false rejection error SHALL be declared when the biometric authentication fails to authenticate the test subjects after executing the complete verification transaction (which includes no more than five attempts).

The manner in which the laboratory records failure to acquire, false rejects, and true accepts are left to the laboratory, but SHALL be done automatically to avoid introducing human error.

5.2.2.2.4. FRR§

False reject rate SHALL be calculated according to requirements in FRR and statistical analysis in Statistics and Test Size.

5.2.3. Offline Testing§

Offline testing measures FAR and leverages all possible combinations between test subjects.

5.2.3.1. Offline: Software Validation§

As the evaluation procedure might utilize online testing for the evaluation of false reject rate and offline testing for the evaluation of false accept rates, it is important for the evaluation laboratory to assure that the offline biometric functionality is a functionally equivalent to the online biometric functionality. The evaluation laboratory SHALL perform a series of genuine verification transaction tests online and offline and make sure that the results are the same.

The on-line verification testing SHALL result in a sequence of stored verification transactions and decisions for every transaction that did not have a failure to acquire. The off-line verification testing SHALL run these stored verification transactions in the same order and SHALL result in the exact same sequence of decisions. The complete sequences SHALL be compared by the laboratory to ensure their identity.

5.2.3.2. Offline: Verification Impostor Transactions

5.2.3.2.1. Pre-Verification

To facilitate estimation of false accept rate, all enrollment transactions and verification transactions are stored to allow for offline computation of the FAR.

5.2.3.2.2. Verification Impostor Transaction

The verification offline module provided by the vendor is used to compute all impostor (between person) combinations for estimating FAR.

Verification impostor transactions SHALL be performed according to[ISOIEC-19795-1], 7.6.1.1b, 7.6.1.2b, 7.6.1.3, 7.6.1.4, and 7.6.3.1. Different fingers or irises from the same person SHALL NOT be compared according to [ISOIEC-19795-1] 7.6.1.3.

5.2.3.2.3. Verification Impostor Transaction Failures

The impostor verification process compares an enrollment template and a stored verification transaction from different persons.

For fingerprint, up to four different fingers from a single person can be considered as different test subjects. For eye-based biometrics, both the left and right eye can be considered as two different test subjects. However, impostor scores between two fingerprints or two irises from a single person SHALL be excluded from computation of the FAR.

A false accept error SHALL be declared if any attempts in the stored verification transaction results in a match decision.

> Note: It is not possible to obtain an FTA rate for FAR Offline Testing. FTAs are not considered in Offline Testing.

5.2.3.2.4. FAR

False accept rate SHALL be calculated according to requirements inFAR and statistical analysis in Statistics and Test Size.

5.3. Self-Attestation (Optional)

5.3.1. Procedures for Self-Attestation and FIDO Accredited Biometrics Laboratory Confirmation using Independent Data (Optional)

The previous sections are a description of certification by FIDO Accredited Biometrics Laboratory. The independent testing focuses on a maximum FAR level where the upper bound of the confidence interval for FAR MUST be less than 1:10,000 and FRR is [3:100]. Biometrics and platform vendors MAY choose to demonstrate a lower FAR: e.g. FAR @ 1:100,000 at a FRR of less than [3:100]. This section describes the processes for optional self-attestation for lower FAR of 1:X, e.g. 1:50,000 at the vendor's discretion utilizing biometric data to which they have access.

Self-attestation is optional. If the vendor chooses self-attestation, the following requirements apply. The vendor SHALL follow all procedures that were described in the Test Procedures with the following definitions

and exceptions:

- The Vendor SHALL attest to an FAR of [1:25,000, 1:50,000, 1:75,000, or 1:100,000, or others?] at an FRR of less than [3:100].
- The Vendor SHALL attest that the biometric system used for self-attestation is the same system functioning at the same operating point as the test harness submitted FIDO independent testing.
- The number of subjects* SHALL follow the following table:

Self-Attestation Number of Subjects

	1:25,000	**1:50,000**	**1:75,000**	**1:100,000**
Number of Subjects*	390	550	675	775

*Up to four different fingers or two irises from a person MAY be used as different subjects.

- To document that they followed the procedures the vendor SHALL provide a report which includes the information in Report to the Vendor.

In addition, the laboratory SHALL compare the FAR bootstrap distribution generated as a result of the independent testing and determine if it is consistent with the self-attestation value. The mean of the bootstrap distribution SHALL be less than or equal to the self-attestation value.

6. Test Procedures for Presentation Attack Detection (PAD)§

This section provides testing plan for Presentation Attack (Spoof) Detection. It focuses on presentation attacks which require minimal expertise. The testing SHALL be performed by the FIDO-accredited independent testing laboratory on the TOE provided by vendor. The evaluation measures the Impostor Attack Presentation Match Rate (IAPMR), as defined in ISO 30107 Part 3.

PAD Testing shall be completed by using the following approach.

6.1. Test Crew§

The Test Crew is the Test Subjects gathered for evaluation.

6.1.1. Number of Subjects§

Number of subjects for a test SHALL be 10.

For fingerprints, PAD testing SHALL be constrained to the index, thumb, or middle fingers of the test subject.

The same test subjects as used for FRR testing may be used for PAD testing.

In the event there is an enrollment failure according toEnrollment Transaction Failures, an additional Subject SHALL be enrolled for each enrollment failure.

6.1.2. Test Visits§

Collection from test subjects MAY occur in one visit.

6.1.3. Enrollment§

Enrollment procedures SHALL be provided in writing to the Laboratory by the Vendor. These procedures

SHALL be followed by the Test Crew. Instructions MAY be provided in any form, including interactive on screen guidance to the Test Subject. The Administrator SHALL record any FTE, if appropriate, with any divergence from enrollment instructions that MAY have caused the failure.

6.1.4. Reporting Requirements§

6.1.4.1. Test Reports§

The following SHALL be included in a report to the vendor, following (ISO/IEC 19795-1, 10.5):

- Summary of the FIDO Biometric Certification and Requirements
- Number of individuals tested
- Description of the Test Environment
- Description of the Test Platform
- Number of enrollment transactions
- Number of genuine verification transactions
- Number of impostor verification transactions
- Failure to Enroll Rate
- Failure to Acquire Rate

And the following from (ISO/IEC 30107-3, 13.1):

- Number and description of presentation attack instruments, PAI species, and PAI series used in the evaluation
- number of test subjects involved in the testing
- number of artefacts created per test subject for each material tested
- number of sources from which artefact characteristics were derived
- number of tested materials
- Impostor attack presentation match rate (IAPMR)
- Number of impostor attack presentation transactions

Please note that the log SHALL also include all information about the PAD tests.

6.1.4.2. FIDO Reports§

FIDO will verify Metadata according to the Biometric Assurance Metadata Requirements.

6.2. Test Methods§

Testing will be performed through Online Testing using the Common Test Harness defined in Common Test Harness (Optional).

6.2.1. Pre-Testing Activities§

Pre-test activities SHALL be performed according to [ISOIEC-19795-2]:

- Section 6.1.8 Pre-test procedures
- Section 6.1.8.1 Installation and validation of correct operation

6.2.2. Testing for PAD§

This section will focus on PAD Testing.

6.2.3. Enrollment§

Each subject SHALL be enrolled. Enrollment SHALL be performed according to ISO/IEC 19795-1, 7.3. Presentation attacks will be performed against this enrollment. Similar to FRR/FAR testing, enrollment transactions will be performed without operator guidance and is flexible with regard to the vendor in that in may allow multiple presentation for the enrollment.

The test lab SHALL also collect biometric characteristic data required for creating a Presentation Attack Instrument. For example, for fingerprint, a copy of the enrolled person's fingerprint is needed and can be acquired via collection of a fingerprint image on a second fingerprint scanner or by leaving a latent print. The method used to acquire the biometric characteristic SHALL be consistent with the recipe of each Presentation Attack Instrument Species to be tested.

6.2.4. Triage of Presentation Attacks by Attack Potential Levels§

For the modalities that can be evaluated by the FIDO test procedures, presentation attacks are described at a high level in Table 1. Table 1 triages presentation attacks into levels based an increasing level of difficulty to mount, based on frameworks from Common Criteria and applied to biometric presentation attacks in [[FingerprintRecognition], [SOFA-B], [PresentationsAttacksSpoofs], [PAD], [BEAT]]. In ISO 30107-Part 3, this is called the attack potential, defined as the "measure of the capability to attack a TOE given the attacker's knowledge, proficiency, resources and motivation."

In , the factors are as follows:

1. Elapsed time: <=one day, <=one week, <=one month, >one month
2. Expertise: layman, proficient, expert, multiple experts
3. Knowledge of TOE: public, restricted, sensitive, critical
4. Access to the TOE/Window of Opportunity: easy, moderate, difficult
5. Equipment: standard, specialized, bespoke
6. Access to biometric characteristics: immediate, easy, moderate, difficult

Elapsed time includes time required to create the attack. The definitions for each of the factors are the same as [BEAT].

In [BEAT], these factors are considered for both the Identification and the Exploitation phase. In other words, the factors are scored differently for the phase when the attacker in the process of identifying the attack compared to the phase where they are actually mounting or exploiting the attack once it has been identified.

For FIDO use case, for Identification phase, we assume that Knowledge of the TOE is "public" and Access to TOE/Window of Opportunity is "easy", since it would be quite trivial to purchase a sample of the TOE.

1. Knowledge of TOE: public
2. Access to the TOE/Window of Opportunity: easy

Since these factors are generally the same for the majority of FIDO use cases, they are not considered further.

> Note: The Window of Opportunity for Biometric Authenticators is impacted by rate-limits on user verification attempts, as required in FIDO Authenticator Security Requirements, Requirement 3.9.

In order to simplify for FIDO use case, we have collapsed the remaining characteristics into three levels and are described in the next sections. The level rating may change over time as information regarding mountimg an attack will be more broadly disseminated. As such, it is expected that the FIDO Biometric Requirements would be updated in the future to reflect this shift.

The difference of scoring for identification versus exploitation is not considered.

Spoof presentation attack examples separated by levels based on time, expertise, and equipment

		Fingerprint	Face	Iris/Eye	Voice
Level A	**Time:** < 1 day **Expertise:** Layman **Equipment:** Standard	paper printout, direct use of latent print on the scanner	paper printout of face image, mobile device display of face photo	paper printout of face image, mobile device display of face photo	replay of audio recording
	Source of Biometric Characteristic: Immediate, easy	lift of fingerprint off the device	photo from social media	photo from social media	recording of voice
Level B	**Time:** < 7 days **Expertise:** Proficient **Equipment:** Standard, Specialized	fingerprints made from artificial materials such as gelatin, silicon.	paper masks, video display of face (with movement and blinking)	video display of an iris (with movement and blinking); printed iris w/ contact lens/doll eye	replay of audio recording of specific pass phrase, voice mimicry
	Source of Biometric Characteristic: Moderate	latent print, stolen fingerprint image	video of subject, high quality photo	video of subject, high quality photo	recording of voice of specific phrase, high quality recording
Level C	**Time:** > 7 days **Expertise:** Expert(s) **Equipment:** Specialized, bespoke	3D printed spoofs	silicon masks, theatrical masks	contact lens/prosthetic eye with a specific pattern	voice synthesizer
	Source of Biometric Characteristic: Difficult	3D fingerprint information from subject	high quality photo, 3D face information from subject	high quality photo in Near IR	multiple recordings of voice to train synthesizer

Level A

Level A attacks are quite simple to carry out and require relatively little time, expertise, or equipment. Biometric characteristics under attack are quite easy to obtain (e.g. face image from social media, fingerprint from the device and reused directly).

1. **Elapsed time:** <=one day
2. **Expertise:** Layman
3. **Equipment:** Standard
4. **Access to biometric characteristics:** Immediate, easy

Level B

Level B attacks require more time, expertise and equipment. Additionally, the difficulty to acquire the

biometric characteristic is higher (e.g., stolen fingerprint image, high quality video of a person's face).

1. **Elapsed time:** <=one week
2. **Expertise:** Proficient
3. **Equipment:** Standard, Specialized
4. **Access to biometric characteristics:** Moderate

If at least one of these characteristics reaches the levels listed above, the attack is categorized as Level B.

Level C

Level C includes the most difficult attacks.

1. **Elapsed time:** <=one month, >one month
2. **Expertise:** Expert, multiple experts
3. **Equipment:** Specialized, bespoke
4. **Access to biometric characteristics:** Difficult

If at least one of these characteristics reaches the levels listed above, the attack is categorized as Level C.

6.2.5. PAI Species§

A Presentation Attack Instrument (PAI) is the device used when mounting a presentation attack. A PAI species is a set of PAIs which use the same production method, but only differ in the underlying biometric characteristic. Table 1 is a high level description of presentation attacks by level. The next section provides additional detail of PAI species for each modality.

The laboratory SHALL select PAI species appropriate for biometric modality of the TOE.

PAI Species are described at a high level for fingerprint, face, iris/eye, and voice. If the TOE is a different biometric modality than these, the vendor SHALL propose to a set of PAI species for Levels A and B for FIDO's approval. Upon FIDO approval, the test laboratory can proceed with PAD evaluation.

6.2.5.1. PAI Species for Fingerprint§

Level A attacks for spoofing a fingerprint biometric are to retrieve and print an image of a fingerprint which can be obtained through taking a image of a dusted latent fingerprint. This requires equipment that is readily available to most individuals and requires very little skill. Examples of different Presentation Attack Instrument Species (PAI Species) for Level A are a set of fingerprint images printed on inkjet printers or laser printers. Each make/model of the printer would be considered a species. In addition, preprocessing could be used to enhance the image. Any alterations such as this would be categorized as a different PAI species.

Level B attacks for spoofing a fingerprint biometric are to retrieve and print an image of a fingerprint which can be obtained through taking a image of a dusted latent fingerprint or retrieving a stolen fingerprint image from a database or other source of stolen fingerprint images. Level B attacks are similar to Level A attacks, except rather than simply printing a fingerprint image, the image could be converted into a mold. A mold could be created through etching a printed circuit board or simply printing a fingerprint image on a transparency. Once a mold is created, a PAI (or cast) can be created by placing other materials such as gelatin, silicon, play-doh, etc into the mold. The difficulty of making the translation from a 2D fingerprint image to a mold moves this attack from Level A to Level B. Additives could be added to the PAI to increase conductivity such as graphite or lotion. Any alterations such as this would be categorized as a different PAI species.

> Note: Fingerprint molds obtained from a cooperative individual through pressing a finger into silicon or other molding material are out of scope for FIDO since it is assumed that a user would not cooperate with attacker to provide his or her fingerprint.

Level C attacks are more elaborate and capture additional information such as pores, veins, sweating, and 3D details. PAI could also be a 3D printed finger. These PAIs take more time to create, are more expensive, require experts to prepare, and need a high resolution and/or 3D finger information.

Table of Example PAI Species for Fingerprint

Species	Level
Fingerprint image printed on inkjet or laser printer	A
Fingerprint image converted to a mold which is used to make a cast with materials such as gelatin or silicon	B
Same as previous with graphite or other material placed on surface of mold	B
3D printed fingerprints	C
Fingerprint models which capture sweating, veins, blood flow or more sophisticated finger information	C

6.2.5.2. PAI Species for Face

Level A attacks for spoofing a face biometric are to retrieve and utilize a photograph of the individual under attack. For example, an attacker can copy a photograph from a social media site and print the photograph or display the photo on a mobile device to the biometric recognition system. This requires equipment that is readily available to most individuals and requires very little skill. Examples of different Presentation Attack Instrument Species (PAI Species) for Level A are a set of face images printed on inkjet printers, laser printers, or photographs printed at a photograph laboratory. Each make/model of the printer would be considered a species. In addition, preprocessing could be used to enhance a photograph, as well as holes could be cut out for the eyes, nose, mouth, or outline of face. Any alterations such as this would be categorized as a different PAI species. Examples of different PAI species for displayed photos on mobile devices would be changing a phone, tablet, and computer monitor make/models.

Level B attacks are similar to Level A attacks, except rather than a face photograph, a video of the subject is needed. The difficulty in acquiring a video rather than a photograph is what moves it from Level A to Level B; even though it is possible, it is less likely to obtain a video of a person compared to a photograph. Additionally, with a high resolution face image, it is possible to create a paper mask of the person. This requires proficient expertise and therefore is also included as a Level B attack. Examples of different PAI species for displayed videos on electronic devices would be changing a phone, tablet, and computer monitor make/models.

Level C attacks involve more elaborate masks that are not made a paper, but rather other specialized materials (e.g. ceramic, silicone). These masks take more time to create, are more expensive, and need a high resolution photograph and/or 3D information. 3D information can also be derived from a 2D photo using sophisticated computer vision techniques. Masks include rigid 3D with and without eye holes, flexible silicone masks, and 3D printed, color face replicas.

> Note: Twins or genetically identical siblings may be more likely to have a similar face signature. We have not included twins or genetically identical siblings in the attacks that are being tested.

Table of Example PAI Species for Face

Species	Level
Face image printed on inkjet or laser printer	A
Face image printed at photograph laboratory	A

Displayed photos on electronic/mobile devices	A
Displayed videos on electronic/mobile devices	B
Paper masks	B
Masks made of specialized materials (ceramic, silicone, and/or theatrical)	C
3D printed faces	C

6.2.5.3. PAI Species for Iris/Eye

Level A attacks for spoofing an iris or eye biometric are to retrieve and utilize a photograph of the individual under attack. For example, an attacker can copy a photograph from a social media site and print the photograph or display the photo on a mobile device to the biometric recognition system. This requires equipment that is readily available to most individuals and requires very little skill. Examples of different Presentation Attack Instrument Species (PAI Species) for Level A are a set of images of an iris or eye printed on inkjet printers, laser printers, or photographs printed at a photograph laboratory. Each make/model of the printer would be considered a species. In addition, preprocessing could be used to enhance a photograph, as well as holes could be cut out for the pupils. Any alterations such as this would be categorized as a different PAI species. Examples of different PAI species for displayed photos on mobile devices would be changing a phone, tablet, and computer monitor make/models.

> Note: A majority of iris systems utilize NIR illumination and a NIR camera. For example, in typical visible spectrum images, the iris pattern does not show for dark eyes. Thus, photographs of an individual taken in the visible spectrum may not be an effective source of the iris biometric characteristics and needs to be considered when constructing an attack.

> Note: A majority of iris systems utilize NIR illumination and a NIR camera for which mobile display of iris may not be feasible for most device make and models.

Level B attacks are similar to Level A attacks, except rather than a photograph, a video of the subject is needed. The difficulty in acquiring a video rather than a photograph is what moves it from Level A to Level B; even though it is possible, it is assumed to be more difficult to obtain a video of a person compared to a photograph. This requires proficient expertise and therefore is also included as a Level B attack. Examples of different PAI species for displayed videos on electronic devices would be changing a phone, tablet, and computer monitor make/models. Another example of a Level B attack is inserting a printed iris into a fake eye that is readily available, e.g. doll eye. A printed eye with a contact lens on top is another example of a Level B attack.

> Note: As with Level A, a majority of iris systems utilize NIR illumination and a NIR camera for which mobile display of iris may not be feasible for most device make and models.

Level C attacks involve more elaborate eye prosthetics that are not made of paper, but rather silicon or materials that have similar spectral characteristics as human eye and/or iris. These prosthetics take more time to create, are more expensive, and need a high resolution photograph, 3D information, and/or spectral characteristics of the eye and/or iris.

Table of Example PAI Species for Iris/Eye

Species	**Level**
Iris/eye image printed on inkjet or laser printer	A
Iris/eye image printed at photograph laboratory	A
Displayed Iris/eye photos on electronic/mobile devices	A
Displayed Iris/eye videos on electronic/mobile devices	B

Printed iris/eye inserted in fake eye	B
Printed eye with contact lens on top	B
Prosthetics eye	C
Prosthetics eye with similar spectral characteristics to human eye	C

6.2.5.4. PAI Species for Voice§

Level A attacks for spoofing a voice biometric are to retrieve and utilize a voice recording of the individual under attack. For example, an attacker can record the voice of the individual and replay their voice to the biometric recognition system. This requires equipment that is readily available to most individuals and requires very little skill. Examples of different Presentation Attack Instrument Species (PAI Species) for Level A are a set of voice recordings replayed on different speakers. Each make/model of the recording device and speakers to replay the voice would be considered a species. In addition, preprocessing could be used to enhance the audio. Any alterations such as this would be categorized as a different PAI species. Equipment used for preprocessing, recording, and replay should be standard, readily available, easy to use equipment.

Level B attacks are similar to Level A attacks, except rather than any voice recording, a recording of a specific passphrase is needed. The difficulty in acquiring a recording of specific set of words rather than any words is what moves it from Level A to Level B; even though it is possible, it is less likely to obtain a recording of a specific passphrase. Also, multiple speech recordings from a person could be used to attack the system by cutting portions of words needed in a phrase using commodity off the shelf audio editors. Additionally, high quality recording and replay equipment also would be considered a Level B attack, where each equipment set-up would be considered a different PAI.

> Note: Text-independent systems may be vulnerable to any recording, where text-dependent systems are vulnerable to a recording of the specific pass-phrase.

Level C attacks involve more sophisticated voice synthesizers which can take a recording of a voice, build a model of that voice, and replay a person speaking any words. The model could also be built using speech samples from a large population, then tuned for a specific individual. These models take more time to create, require more skill, and need high resolution, long recordings to build accurate models. A person may also be skilled in the art of impersonation where they attempt to mimic someone else.

> Note: Twins or genetically identical siblings may be more likely to have a similar voice signature. We have not included twins or genetically identical siblings in the attacks that are being tested.

Table of Example PAI Species for Voice

Species	**Level**
Recording a voice saying any words from readily available equipment for recording and playback	A
Recording a voice saying specific passphrase from readily available equipment for recording and playback	B
Recordings of a specific passphrase created by cutting and pasting together words using readily available software	B
High quality recording a voice saying any words from high end equipment for recording and playback	B
Voice synthesizer which can playback any words, trained from long, high quality recordings or a database of recordings	C
Impersonation, where an attacker is able to mimic a person’s voice	C

6.2.6. PAD Evaluation with Presentation Attack Instruments (PAI)

Based upon the prior section, the test laboratory SHALL select six Level A and four Level B Presentation Attack Instrument Species to be used in the evaluation. One Presentation Attack Instrument (PAI) shall be created for each PAI species and each enrolled test subject.

> Note: If the test laboratory creates PAIs for ten selected PAI species and ten enrolled subjects, the test lab would have to create 100 instruments. Examples of different PAI species include PlayDoh, gelatin using recipe 1, gelatin using recipe 2, and ABC Brand wood glue.

The recipes, procedures, and materials to be used for the selected PAI species shall be provided by the Accredited Biometric Laboratory to the vendor well in advance of testing. Recipes SHALL be provided to the FIDO Secretariat. The FIDO Secretariat SHALL ensure that PAI Species selected and created are relatively equivalent between laboratories.

A check SHALL be performed on each PAI or batch of PAIs to ensure that it is “valid”, i.e. validating that the batch of PAI species captures the biometric characteristic, is prepared properly, and performs as expected. For example, this check could be performed on a test laboratory reference biometric system that the laboratory determines is sufficiently similar to the TOE without PAD by observing the biometric image. The laboratory SHALL document their method for determining that a PAI is valid and submit as part of the report to FIDO and the vendor.

If a PAI degrades, additional PAIs SHOULD be created for each enrolled subject.

6.2.6.1. Impostor Presentation Attack Transactions

For each enrollment, the test lab operator SHALL conduct 5 impostor presentation attack transactions for each PAI. Any kind of guidance SHALL be provided by the biometric authentication system/capture sensor in similar manner to the final application. For testing purposes, this process SHALL not have more than five attempts per transaction. The transaction SHOULD not exceed 30 seconds. The PAI SHALL be presented the maximum number of attempts allowed for a transaction OR until it matches (which results in an error).

6.2.6.1.1. Impostor Presentation Attack Errors

A failure to acquire SHALL be declared when the biometric authentication system is not able to capture and / or generate biometric features during a verification transaction. The on-line verification test harness SHALL indicate to the laboratory when a failure to acquire has occurred.

A impostor presentation attack match error SHALL be declared if the biometric authentication system produces a match decision.

The manner in which the laboratory records failure to acquire and impostor presentation attack errors are left to the laboratory, but SHALL be done automatically to avoid introducing human error.

> Note: A failure to acquire for an impostor presentation attack transaction does not count as an error, as some systems may produce a failure to acquire in response to a detected presentation attack.

6.2.6.1.2. IAPMR

Imposter Attack Presentation Match Rate (IAPMR) SHALL be calculated according to requirements in Imposter Attack Presentation Match Rate (IAPMR).

Index§

Terms defined by this specification§

Test Subject

TOE

Transaction

Variance

Vendor

Verification

Zero-Effort Impostor Attempt

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

[FIDOMetadataService]
R. Lindemann; B. Hill; D. Baghdasaryan. FIDO Metadata Service v1.0. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-metadata-service-v1.2-rd-20171128.html

[FIDOMetadataStatement]
B. Hill; D. Baghdasaryan; J. Kemp. FIDO Metadata Statements v1.0. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-metadata-statement-v1.2-rd-20171128.html

[FingerprintRecognition]
On security evaluation of fingerprint recognition systems 2010. URL: http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/Henniger2_Olaf_IBPC_Paper.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

[ISOIEC-19795-2]
ISO/IEC 19795-5:2011 Information technology -- Biometric performance testing and reporting -- Part 5: Access control scenario and grading scheme. 2007. URL: https://www.iso.org/standard/41448.html

[ISOIEC-19795-5]
ISO/IEC 19795-5:2011 Information technology -- Biometric performance testing and reporting -- Part 5: Access control scenario and grading scheme. 2011. URL: https://www.iso.org/standard/51768.html

[PAD]
E. Newton; S. Shuckers. Recommendations for Presentation Attack Detection: Mitigation of threats due to spoof attacks. 2016.

[PresentationsAttacksSpoofs]
Stephanie Shuckers. Presentations and attacks, and spoofs, oh my.. 2016.

[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

[SOFA-B]

Strength of Function for Authenticators - Biometrics (SOFA-B). 2017. NIST Discussion Draft. URL: https://pages.nist.gov/SOFA/SOFA.html

↑

→

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.↵

↑

→

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 *e 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.

Rene al 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

↑

→