FIDO Biometrics Requirements

Working Draft, August 30, 2018

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 the Pull 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 the TOE 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:

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

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.

$$FAR_{MT} = 1 - ((1 - FAR_{MT})^{\wedge}B)$$

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%

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.
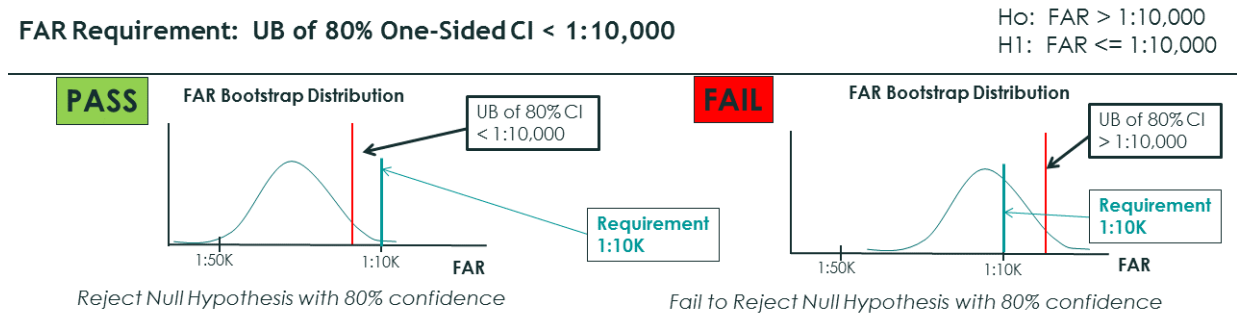
Figure 1 *Bootstrapping FAR Schematic*

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 ([FIDOMetadata Statement]) 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 to Enrollment 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 inCommon 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 [[Fingerprint Recognition], [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.

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.

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

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

↑

→