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

FIDO Biometrics Requirements

Final Document, May 22, 2024

This version:
https://fidoalliance.org/specs/biometric/requirements/Biometrics-Requirements-v4.0-fd-20240522.html

Issue Tracking:
GitHub

Editors:
Stephanie Schuckers (Clarkson University)
Greg Cannon (Amazon)
Nils Tekampe (FIDO Alliance)
Anthony Lam (iProov)

Former Editors:
Elham Tabassi (NIST)
Meagan Karlsson (FIDO)
Elaine Newton (formerly of NIST)

Abstract

This document contains the requirements and test procedures for:

- Biometric Component for FIDO Authenticators (BCA)
- Face Verification for Remote Identity Verification (IdV - Face) solutions.

Table of Contents

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.
2017-04-14	#45	0.9	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 Biometric Reference 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 Impostor Presentation Attack Errors sections.
2017-10-12	#76, #75, #78	0.22	#76: Updates related to PAI species for IAPAR. 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.
2017-12-07	#84, #85	0.24	Added PAI for Voice Section, clean up of open issues.
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.
2019-3-10		0.3	Minor change to make bootstrapping FAR more clear.
2019-05-30		1.0	Editorial upgrade of version number for publication
2019-06-06	133, 134, 135,126	1.1	Adressing issues 133, 134, 135, 126

2019-08-15	141	1.2	Adressing issues 141
2020-08-26	148 to 194	2.0	Edits to definitions for transactions and attempts, Change FRR to 5%, Change in PAD requirements to 7%, edits to PA levels, Edits to test environment
2021-9-30	207, 212	2.1	Added levels that map to using 15% (Level 1) and 7% (Level 2) thresholds for IAPAR for PAD
2021-9-30	220	2.2	Changed PAD Enrollment Subjects from 25 to 15 and PAI Level B Species from 6 to 8
2022-1-6	228	2.2.1	Editorial Changes due to laboratory feedback
2022-3-3	226	2.3	Multimodal authenticators
2022-3-3	242	3.0	Replaced Level 1 with new framework of BioLevels, updated definitions to align with ISO
2023-8-3	252, 262	3.1	Added additional information to support biometric certification operating in remote and local mode, as well as supporting remote test subjects. Added deepfake video testing to presentation attack Levels A and B. Fixed typos for the levels in the self attestation sections.
2024-4-17	258, 273	4.0	The document now covers two certification programs: (1) Original--Biometric Component for FIDO Authenticators (BCC) and (2) New--Face Verification for Remote Identity Verification (IdV - Face) solutions This document has a common set of testing procedures for both programs as well subsections specific to each program, colored in blue and pink, respectively. This version also adds an optional evaluation for differential performance across demographics.

2. Introduction§

This document provides biometric requirements and test procedures for evaluating the following:

- Biometric Component for FIDO Authenticators (BCA)
- Face Verification for Remote Identity Verification (IdV - Face) solutions

Evaluations are performed by FIDO Accredited Biometric Laboratories and FIDO issues a certification if the solution meets the requirements.

The performance metrics that are assessed in the document for both programs include:

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

The requirements and test procedures in this document apply to both programs unless otherwise specified. Each section may include a subsection that is specific to each program.

Associated documents to this document include:

- FIDO Biometrics Laboratory Accreditation Policy
- FIDO Biometrics Certification Policy

Biometrics requirements SHALL be reviewed periodically to assess appropriateness.

2.1. BCA - Specific§

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 that includes the biometric subsystem.

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

In scope for BCA:

1. Matching - Comparison of a biometric sample with a previously acquired biometric reference
2. Presentation attack detection - automated discrimination between bona-fide subjects and presentation attacks

Performance Testing Requirements for FIDO certification are included in[ISOIEC-19795-9], Annex A. PAD Testing Requirements for FIDO certification are included in [ISOIEC-30107-4], Clause 7.

2.2. IdV - Specific§

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

In scope for IdV - Face:

1. Matching - Comparison of a photo/video of a subject with a reference face image from an identity document
2. Presentation attack detection - automated discrimination between bona-fide subjects and presentation attacks

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

3. Automatically verifying identity document authenticity

2.3. Reference Documents§

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

ISO/IEC 19795-1:2021 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework [ISOIEC-19795-1]

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

ISO/IEC 19795-5:2011 Information technology -- Biometric performance testing and reporting -- Part 5: Access control scenario and grading scheme [ISOIEC-19795-5]

ISO/IEC TS 19795-9:2019 Information technology — Biometric performance testing and reporting — Part 9: Testing on mobile devices [ISOIEC-19795-9]

ISO/IEC TS 19795-10:2024 Information technology — Biometric performance testing and reporting — Part 10: Quantifying biometric system performance variation across demographic groups [ISOIEC-19795-10]

ISO/IEC 30107-1:2016 Information technology -- Biometric presentation attack detection -- Part 1: Framework[ISOIEC30107-1]

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

ISO/IEC 30107-4:2020 Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices [ISOIEC-30107-4]

ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics[ISOBiometrics]

2.4. Audience§

The intended audience of this document is the Certification Working Group (CWG), Biometrics Working Group (BWG), Identity Verification & Binding Working Group (IDWG), FIDO Administration, the FIDO Board of Directors, Biometric Authenticator Vendors, Biometric Subsystem Vendors and Test Labs.

The owner of this document is the Biometrics Working Group.

2.5. 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 Working Group (BWG)
: FIDO working group 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.

Identity Verification & Binding Working Group (IDWG)
: FIDO working group responsible for defining the Biometric Requirements and Test Procedures as it relates to the IDWG 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.

2.6. FIDO Terms§

FIDO Certified Authenticator
: An Authenticator that has successfully completed FIDO Certification, and has a 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.

2.7. Biometric Data and Evaluation Terms§

Biometric Claim
: claim that a biometric capture subject is or is not the bodily source of a specified or unspecified biometric reference

Note 1 to entry: A biometric claim can be made by any user of the biometric system.

Note 2 to entry: The phrase "claim of identity" is often used to label this concept.

Note 3 to entry: Claims can be positive, i.e., that the biometric capture subject is enrolled; negative, i.e., that the biometric capture subject is not enrolled; specific, i.e., that the biometric capture subject is or is not enrolled as a specified biometric enrollee; or non-specific, i.e., that the biometric capture subject is or is not among the set or subset of biometric enrollees.

Note 4 to entry: Biometric claims are not necessarily made by the biometric capture subject.

Note 5 to entry: The biometric reference could be on a database, card or distributed throughout a network.

Note 6 to entry: The biometric claim has to fall within the biometric system boundary.

> NOTE: Notes 1 through 6 above are part of the ISO definition. In the FIDO context, a FIDO authenticator is a personal device. The biometric reference is stored locally on the device. A claim within FIDO occurs when a person presents themselves to their own device. [ISOBiometrics]

Biometric Mated Comparison Trial

comparison of a biometric probe and a biometric reference from the same biometric capture subject and the same biometric characteristic as part of a performance test

Note 1 to entry: Biometric mated comparison trials have historically been referred to as “genuine trials”. However, the term “genuine” historically implied an intent on the part of the biometric capture subject. Ultimately, the trial has nothing to do with the intention of the biometric capture subject. [ISOBiometrics]

Biometric Non-Mated Comparison Trial

comparison (37.05.07) of a biometric probe (37.03.14) and a biometric reference (37.03.16) from different biometric data subjects (37.07.05) as part of a performance test

Note 1 to entry: Biometric non-mated comparison trials have historically been referred to as “impostor trials”. However, they do not accurately model operational system behaviour in the presence of impostors.

Note 2 to entry: A set of biometric non-mated comparison trials need not contain all possible comparisons of biometric probes (37.03.14) and biometric references from different biometric data subjects. [ISOBiometrics]

Biometric Presentation

interaction of the biometric capture subject and the biometric capture subsystem to obtain a signal from a biometric characteristic

Note 1 to entry: The biometric capture subject is not necessarily aware that a signal from a biometric characteristic is being captured. [ISOBiometrics]

Biometric Reference

one or more stored biometric samples, biometric templates, or biometric models attributed to a biometric data subject and used as the object of biometric comparison

EXAMPLE:Face image stored digitally on a passport; fingerprint minutiae template on a National ID card or Gaussian Mixture Model for speaker recognition in a database.

Note 1 to entry: A biometric reference may be created with implicit or explicit use of auxiliary data such as Universal Background Models.

Note 2 to entry: The subject/object labelling in a comparison can be arbitrary. In some comparisons a biometric reference can potentially be used as the subject of the comparison with other biometric references or incoming biometric samples and input to a biometric algorithm for comparison. For example, in a duplicate enrollment check, a biometric reference will be used as the subject for comparison against all other biometric references in the database. [ISOBiometrics] Note: For the purposes of IdV - Face, the Biometric Reference is the stored face image from the document that the TOE obtains through a photo of the document or transfer of the digital image through near-field communication (NFC) or other means.

Biometric Sample

analogue or digital representation of biometric characteristics prior to biometric feature extraction

EXAMPLE:A record containing the image of a finger is a biometric sample.[ISOBiometrics]

> NOTE: For the purposes of IdV - Face, a Biometric Sample is a face image taken by the subject of themselves, i.e., a "selfie". This excludes non-selfie live face capture of the subject by another person. Data capture subsystems may include a mobile device, webcam, or laptop camera, for example.

Biometric Verification
process of confirming a biometric claim (37.06.04) through comparison (37.05.07)

Note 1 to entry: The term “verification”, in the above definition refers to verifying biometrics (37.01.01).

Note 2 to entry: Use of the term “authentication” as a substitute for biometric verification is deprecated[ISO Biometrics]

Capture Attempt
interaction of the biometric capture subject with the biometric capture subsystem (37.02.01) with the intent of producing a captured biometric sample

Note 1 to entry: The capture attempt is the interface between the presentation by the biometric capture subject and the action of the biometric capture subsystem.

Note 2 to entry: The “activity” taken can be on the part of the biometric capture subsystem or the biometric capture subject. [ISOBiometrics]

Captured Biometric Sample
biometric sample (37.03.21) resulting from a biometric capture process (37.05.02)[ISOBiometrics].

> NOTE: For the purposes of IdV - Face, the Captured Biometric Sample is a selfie of the individuals' face.

Capture Transaction
one or more capture attempts with the intent of acquiring all of the biometric data from a biometric capture subject necessary to produce either a biometric reference or a biometric probe [ISOBiometrics].

False Accept Rate (FAR)
proportion of biometric (37.01.01)transactions with false biometric claims erroneously accepted[ISOBiometrics]

False Reject Rate (FRR)
proportion of verification transactions with true biometric claims erroneously rejected[ISOBiometrics]

Failure-to-Aquire (FTA)
failure to accept for subsequent comparison the biometric sample of the biometric characteristic of interest output from the biometric capture process

Note 1 to entry: Acceptance of the output of a biometric capture process for subsequent comparison will depend on policy.

Note 2 to entry: Possible causes of failure to acquire include failure to capture, failure to extract, poor biometric sample quality, algorithmic deficiencies and biometric characteristics outside the range of the system. [ISOBiometrics]

Failure-to-Aquire Rate (FTAR)
proportion of a specified set of biometric acquisition processes that were failures to acquire

Note 1 to entry: The results of the biometric acquisition processes may be biometric probes or biometric references.

Note 2 to entry: The experimenter specifies which biometric probe (or biometric reference), which acquisitions are in the set, as well as the criteria for deeming that a biometric acquisition process has failed.

Note 3 to entry: The proportion is the number of processes that failed, divided by the total number of biometric acquisition processes within the specified set. [ISOBiometrics]

Failure-to-Enroll (FTE)
failure to create and store a biometric enrollment data record (37.03.10) for an eligible biometric capture subject (37.07.03) in accordance with a biometric enrollment (37.05.03) policy

Note 1 to entry: Not enrolling someone ineligible to enroll (37.05.08) is not a failure to enroll[ISOBiometrics]

Failure-to-Enroll Rate (FTER)

proportion of a specified set of biometric enrollment transactions that resulted in a failure to enroll

Note 1 to entry: Basing the denominator on the number of biometric enrollment transactions can result in a higher value than basing it on the number of biometric capture subjects.

Note 2 to entry: If the FTER is to measure solely transactions that fail to complete due to quality of the submitted biometric data, the denominator should not include transactions that fail due to non-biometric reasons (i.e., lack of eligibility due to age or citizenship). [ISOBiometrics]

Impostor Attack Presentation Accept Rate (IAPAR)
proportion of impostor attack presentations using the same PAI species that result in accept. See [ISOIEC-30107-3].

Injection Attack Detection (IAD)
automated determination of a biometric data injection attack [[!CENUnpublished]]

Offline
Pertaining to execution of biometric enrollment or comparison of stored biometric data subsequent to and disconnected from the biometric acquisition process

Note 1 to entry: Collecting a corpus of images or signals for offline enrollment and calculation of comparison scores allows greater control over which probe and reference images are to be used in any transaction. [ISOIEC-19795-1]

Online
Pertaining to execution of biometric enrollment or comparison directly following the biometric acquisition process [ISOIEC-19795-1]

Presentation Attack
biometric presentation attack presentation to the biometric capture subsystem (37.02.01) with the goal of interfering with the operation of the biometric system (37.02.03)

Note 1 to entry: Biometric presentation attacks can be implemented through a number of methods, e.g., artefact, mutilations, replay, etc..

Note 2 to entry: Biometric presentation attacks can have a number of goals, e.g., impersonation or not being recognized.

Note 3 to entry: Biometric systems (37.02.03) can be unable to differentiate between presentations with the goal of interfering with the systems' operation and non-conformant presentations. [ISOBiometrics]

Presentation Attack Detection (PAD)
automated discrimination between bona-fide presentations (37.06.36) and biometric presentation attacks (37.06.25)

Note 1 to entry: PAD cannot infer the biometric capture subject's (37.07.03) intent.[ISOBiometrics]

Presentation attack instrument (PAI)
Biometric characteristic or object used in a presentation attack, in[ISOIEC30107-1]

PAI species
Class of presentation attack instruments created using a common production method and based on different biometric characteristics, in [ISOIEC-30107-3]

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

Target of Evaluation (TOE)
The product or system that is the subject of evaluation

> NOTE: See the TOE section in this document

Verification Attempt
biometric claim (37.06.04) and capture attempt(s) (37.06.08) that together provide the inputs for comparison(s) (37.05.07) [ISOBiometrics]

> NOTE: For the purposes of IdV - Face, a verification attempt is the capture of a face "selfie".

Verification Transaction
one or more verification attempts resulting in resolution of a biometric claim[ISOBiometrics]

categorical demographic variable
demographic characteristic of an individual that is nominally or ordinally described[ISOIEC-19795-10]

EXAMPLE: Gender categories can consist of “Male”, “Female”, “Non-binary”, “Neutral”, etc.

continuous demographic variable
demographic characteristic of an individual that is observable, measurable, and not necessarily constrained to discrete categories [ISOIEC-19795-10]

EXAMPLE: An individual’s age or the measurement of a phenotypic trait, such as an individual’s skin lightness.

differential performance
difference in biometric system metrics across different demographic groups[ISOIEC-19795-10]

false negative differential performance
difference in false negative error rates calculated across multiple demographic groups[ISOIEC-19795-10]

2.8. 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[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%)[ISOIEC-19795-1]

2.9. Personnel Terms§

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

Target Population
Set of users of the application for which performance is being evaluated

> NOTE: see Section 4.3.4 in[ISOIEC-19795-1]

Test Organization
functional entity under whose auspices the test is conducted[ISOIEC-19795-1]

2.10. 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.

2.11. Document Structure§

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

3. Requirements§

3.1. Requirements - BCC§

BCC Specific: This section lists the requirements for achieving FIDO Biometric Component Certification. Unless noted as "Optional", all requirements must be met in order to achieve certification. There are four levels of certification which have different requirements. Otherwise, the testing procedure is the same for both levels.

> NOTE: Performance Testing Requirements for FIDO certification are summarized in[ISOIEC-19795-9], Annex A

> NOTE: Presentation Attack Detection Testing Requirements for FIDO certification are summarized in[ISOIEC-30107-4], Annex A

3.1.1. FIDO Certification Criteria - BCC§

Biometric Requirements by Levels

	BioLevel 1	**BioLevel 1+**	**BioLevel 2**	**BioLevel 2+**
# Subjects for FAR/FRR	25	245	25	245
# Subjects for PAD	15	15	15	15
Lab Tested FAR	1%	.01%	1%	.01%
Lab Tested FRR	7%	5%	7%	5%
Lab Tested IAPAR (Modality Agnostic Requirements)	15%	15%	7%	7%
# Species A/B	6/8	6/8	6/8	6/8
# IAPAR Subjects	15	15	15	15
Documented Self Attestation FAR	Mandatory at <= 1/10000	Optional at <= 1/10000	Mandatory at <= 1/10000	Optional at <= 1/10000
Documented Self Attestation FRR	Mandatory at <= 5%	Optional at <= 5%	Mandatory at <= 5%	Optional at <= 5%

3.2. Requirements - IdV Face§

This section lists the requirements for achieving FIDO IdV - Face Certification. Unless noted as "Optional", all requirements must be met in order to achieve certification. There are two levels of certification for each Reference Type. Each level has different requirements. Otherwise, the testing procedure is the same for all levels.

Biometric Requirements by Levels

	Level 1 - Reference Type 1	**Level 1 - Reference Type 2**	**Level 2 - Reference Type 1**	**Level 2 - Reference Type 2**

# Subjects for FAR/FRR	25	25	100	100
# Subjects for PAD	15	15	15	15
Lab Tested FAR	1%	1%	.033%	.033%
Lab Tested FRR	7%	7%	7%	5%
Lab Tested IAPAR (Modality Agnostic Requirements)	7% (per species), 4% (all species)	7% (per species), 4% (all species)	7% (per species), 4% (all species)	7% (per species), 4% (all species)
# Species A/B	6/8	6/8	6/8	6/8
# IAPAR Subjects	15	15	15	15
Documented Self Attestation FAR	Mandatory at <= 1/10000	Mandatory at <= 1/10000	Mandatory at <= 1/10000	Mandatory at <= 1/10000

3.3. 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.

The Allowed Integration Document SHALL be provided for reference to the Laboratory. It SHALL be coherent with the configuration and operation of the Test Harness.

While the allowed integration document may follow a different structure, the Laboratory SHALL ensure that the information required by the template for the Allowed Integration Document ([[BiometricAIDTemplate]]) is present.

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

3.3.1. Target of Evaluation - BCC§

TOE(s) which represent a range of configurations (e.g., different thickness of glass) covered by the Allowed Integration Document SHALL be provided to the FIDO laboratory for testing. The range of configurations to be tested is agreed upon by the FIDO laboratory and the vendor, and SHALL be approved by the FIDO Biometric Secretariat. The configurations tested SHALL be documented in the FIDO report.

Also, the Laboratory SHALL ensure that the descriptions of the allowed steps for integration and the expected environment of the TOE in the allowed integration document does not contain aspects that may negatively interfere with the functionality of the biometric component. As an example: If a developer would allow protective covers over a camera system, the Laboratory SHALL ensure that those covers do not have a negative impact to the functionality of the biometric component. While this analysis can primarily be performed on a theoretical basis, the Laboratory SHALL perform testing if a conclusion cannot be reached by theoretical means.

The environment under which the TOE operates SHALL also be described as part of the Allowed Integration Document. More details are provided in Test Environment.

The TOE SHALL be provided to the Laboratory from the Vendor in the form of aCommon 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.

TOEs can utilize the fusion of multiple biometrics, often different modalities such as face and voice, but can be performed with different algorithms or sensors for the same modality. Fusion approaches may also include multiple captures of the same modality within a transaction. Other similar approaches could fall into this category of authenticators which use fusion.

For a TOE which utilizes such a combination of biometrics to authenticate, the vendor SHALL describe what

modalities, algorithms, sensors, etc., that are utilized for the TOE's fusion approach. In addition, the vendor SHALL indicate whether (1) the TOE collects all biometrics for each transaction, prior to a decision; OR (2) the TOE collects biometrics in a sequential fashion, i.e, where a decision resulting from initial biometric(s) determine whether subsequent biometric(s) need to be collected. The FIDO certified Laboratory will determine the testing needed based on how the TOE operates and this test protocol SHALL be approved by the FIDO Biometric Secretariat.

Details on changes to procedure are provided inMultiBiometric Performance Testing and MultiBiometric Testing for PAD.

Additionally, the test procedure may change if the solution changes as a result of the environment, e.g., a visible camera during the day and an NIR camera at night. This is discussed in Section Test Environment.

The same requirements apply for fusion with non-biometric information, e.g., pin, geolocation, etc..

3.3.2. Target of Evaluation - IdV Face

A TOE SHALL be provided for each Allowed Integration, e.g., different methods of inputting the biometric reference and/or different operating points.

The vendor SHALL specify, in the Allowed Integration document, the types of inputs that the TOE supports for the Biometric Reference: either

Biometric Reference Type 1: photo of a document with face image; AND/OR Biometric Reference Type 2: electronic transfer of a digital face image from the document through NFC or other means

Testing SHALL be performed separately for each Biometric Reference Type.

> NOTE: Biometric comparisons with different Biometric Reference Types may yield different results due to quality differences between Types 1 and 2.

For TOEs which fall into category Biometric Reference Type 1, the FIDO certified laboratory SHALL recruit subjects with a variety of different document types, e.g., drivers license, passport, etc., depending on the types of documents that the TOE supports. The split of document types for the test SHALL be discussed in the testing plan and SHALL be approved by the FIDO Biometric Secretariat.

Also, the Laboratory shall ensure that the descriptions of the allowed steps for integration and the expected environment of the TOE in the allowed integration document does not contain aspects that may negatively interfere with the functionality of the biometric component.

The environment within which the TOE operates SHALL also be described as part of the Allowed Integration Document. More details are provided in Test Environment.

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

3.3.3. TOE that enables evaluation of software-only biometric solutions in remote mode

Biometric recognition technology can operate in two modes: local mode and remote mode [ISO 27553].

Local mode: This is applicable to the cases that the biometric data and derived biometric data do not leave the device, i.e., local modes [ISO 27553].

Remote mode: This is applicable to the cases that:

- the biometric sample is captured through mobile devices;<\li>

- the biometric data or derived biometric data are transmitted between the mobile devices and the remote services in either or both directions.<\li>
- The cases that the biometric data or derived biometric data never leave the mobile devices (i.e., local modes) are out of scope for remote mode.<\li> [ISO 27553]

A biometric component integrated into a FIDO authenticator is required to operate in local mode. Remote identity verification typically operates in remote mode. The FIDO biometric evaluation can be performed for either local mode or remote mode for either testing program.

If TOE is based on software-only with biometric capture devices that are generally available to individuals, e.g., mobile devices that produce accessible biometric data, the TOE SHALL be provided to the laboratory as a software container. The term container in this context can refer to a docker container, a complete VM or any other suitable virtualization technology. This container can be used for testing in-person subjects or remote subjects. This container can be hosted by the Laboratory or a cloud provider at the discretion of the Laboratory.

The vendor and FIDO certified Laboratory SHALL enter into an agreement specifying the terms and conditions:

- Vendor SHALL create a specific environment for testing, separate from the commercial or development environment.<\li>
- The TOE SHALL be in complete control of the FIDO Accredited Laboratory<\li> Note: Laboratory may choose to use a cloud vendor who provides computing storage and processing, the cloud vendor must not have access to the TOE itself, i.e., specific software and data under test. <\li>
- Laboratory SHALL have exclusive access to the TOE during the test. <\li>
- Testing images and any other personal data SHALL NOT be stored for later use by vendor or shared with the vendor in any other way.<\li>

> NOTE: For example, this can be accomplished by creating a virtual machine.

3.3.4. Testing Remote Subjects ###§

For solutions that can meet the requirements in the previous section, use of remote subjects for biometric testing is possible with the following caveats:

- Vendor SHALL specify acceptable biometric capture devices, e.g., cameras on smartphone. Biometric capture devices SHALL be readily available to a majority of potential remote subjects, e.g., cameras for a range of smartphone makes and models. The FIDO Biometric Secretariat SHALL approve the devices selected for testing as part of the FIDO accredited laboratory test plan. <\li>
- The Laboratory SHALL uniquely register Test subjects and this SHALL include details of the device they will use to ensure capability.<\li>
- FIDO accredited laboratory SHALL observe the collection throughout the session which SHALL be recorded for auditing purposes only, e.g., typically with web meeting on a separate device.<\li>
- The Laboratory SHALL have a mechanism to link each specific test subject and their results.<\li>

3.4. FIDO Biometric Performance Levels§

The FIDO Biometric Certification Program uses False Reject Rate (FRR) and False Accept Rate (FAR) to measure Biometric Performance and is further described in the next sections. The FAR and FRR are defined in terms of verification transactions.

NOTE: Requirements for performance levels for FAR and FRR take into account that vendors who seek to achieve certification through independent testing likely develop their system stricter than the target requirements. This is to ensure that they pass certification due to the inherent variability that occurs in any test. In other words, if a requirement is set at X%, vendors will target much stricter than X% to ensure that they do not risk not passing due to variability from one test to the next.

3.4.1. Verification Transactions§

The Allowed Integration Document provided by the vendor establishes the details of what constitutes a verification transaction (maximum number of verification attempts and timeout period) for a TOE while following the definitions for verification attempt and verification transaction provided in Biometric Data and Evaluation Terms. The end of a verification transaction SHALL be the point at which an Accept or Reject decision is made by the biometric subsystem. A transaction SHOULD NOT exceed 30 seconds.

NOTE: Following the definitions from ISO/IEC 2382-37:2017(en) and provided inBiometric Data and Evaluation Terms, a verification attempt results in a biometric comparison while a verification transaction results in a resolution of biometric claim (Accept or Reject). The ISO definition of a verification transaction is often commonly thought of as a successful attempt that leads to a decision and not a failure-to-acquire. Vendors SHALL define a verification transaction at the point when the TOE provides a response to the user of Accept or Reject. This MAY involve one or more attempts.

NOTE: For example, for fingerprint biometrics, verification attempts may include a user being asked to place the fingerprint again if the finger is wet, prior to making a decision.

NOTE: For example, for facial biometrics, verification attempts may include a user being asked to change environments and verify again if the lighting is too dark, prior to making a decision. Note: In another example, verification attempts may include a biometric system capturing multiple images in series, prior to making a decision.

NOTE: In the biometric certification testing, we test the biometric subsystem at the verification transaction level. Once a biometric component is integrated into a FIDO authenticator, a user verification decision for the purposes of FIDO authentication may involve multiple biometric verification transactions. For example, a FIDO authenticator may allow five biometric verification transactions and then switch to a fall-back authentication method, e.g., another biometric, a PIN or password.

3.4.2. False Reject Rate (FRR)§

Requirement

FRR is measured at the verification transaction level. The requirement at the various levels in given in Section FIDO Certification Criteria .

The actual achieved FRR SHALL be documented by the Laboratory. Requirements regarding reporting can be found in section § 7.2 FAR/FRR Reporting Requirements 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.

The calculation of FRR SHALL be based on:

FRR (%) = (Number of mated transactions for which decision is reject or FTA happens for all attempts) / (Number of mated transactions conducted) * 100

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

3.4.2.1. False Reject Rate (FRR) - BCC

For BioLevel 1 and BioLevel 2, the False Reject Rate SHALL meet the requirement of less than 7:100 for the upper bound of a 80% confidence interval. For BioLevel 1 and BioLevel 2, self-attestation of at least 5% false reject rate is also required and described in Section Documented Self-Attestation FRR.

For BioLevel 1+ and BioLevel 2+, the False Reject Rate SHALL meet the requirement of less than 5:100 for the upper bound of an 80% confidence interval.

3.4.2.2. False Reject Rate (FRR) - IdV Face

Two requirements depending the type of Biometric Reference Type: -Biometric Reference Type 1: photo of a document with face image; and/or -Biometric Reference Type 2: electronic transfer of a digital face image from the document through NFC or other means as described in Section Target of Evaluation - IdV Face.

For Biometric Reference Type 1: For IdVLevel 1 and IdVLevel2, False Reject Rate SHALL meet the requirement of less than 7:100 for the upper bound of an 80% confidence interval. FRR is measured at the verification transaction level.

For Biometric Reference Type 2: For IdVLevel 1, False Reject Rate SHALL meet the requirement of less than 7:100 for the upper bound of an 80% confidence interval. FRR is measured at the verification transaction level. For IdVLevel 2, False Reject Rate SHALL meet the requirement of less than 5:100 for the upper bound of an 80% confidence interval. FRR is measured at the verification transaction level.

3.4.3. False Accept Rate (FAR)

Requirement

FAR is measured at the transaction level. The requirement at the various levels is given in Section FIDO Certification Criteria .

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

> The false accept rate is the expected proportion of non-mated transactions that will be incorrectly accepted. A transaction may consist of one or more non-mated 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 both biometric references and stored verification transactions collected during online testing.

The vendor provides an SDK that inputs a biometric reference and a stored verification transaction then returns the decision to “accept” or “reject”. Each decision used in computing the FAR is based on inter-person (between person) combinations of a biometric reference and the related stored verification transaction 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, is set by the Vendor and SHALL be fixed during testing. The threshold SHALL be the same as the threshold used for FRR.

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

Limitation

For the purposes of this test, the definition of verification attempts and transactions defined in false reject rate on-line testing SHALL be used for each off-line verification transaction.

The calculation of FAR SHALL be based on the following equation:

FAR (%) = (Number of zero-effort non-mated transactions for which decision is Accept) / (Number of zero-effort non-mated transactions conducted) * 100

A false accept error SHALL be declared if the stored verification transaction results in a match decision. Since FAR is calculated off-line based on previously stored verification transaction, 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 Documented Self-Attestation FAR (Optional).

> NOTE: The FAR is an error that is related to a non-mated comparison where the attacker will spend no effort in order to be recognized as a different individual, but simply uses their own biometric characteristic. This metric does not provide any information on how the TOE would behave in cases where an attacker mounts a dedicated attack.

3.4.3.1. False Accept Rate (FAR) - BCC

For BioLevel 1 and BioLevel 1+, the False Accept Rate SHALL meet the requirement of less than 1:100 for the upper bound of an 80% confidence interval. For BioLevel 1 and BioLevel 1+, documented self-attestation of at least 1/10000 false accept rate is also required and described in Section Documented Self-Attestation FAR.

For BioLevel 2 and BioLevel 2+, the False Accept Rate SHALL meet the requirement of less than 1:10,000 for the upper bound of an 80% confidence interval.

3.4.3.2. False Accept Rate (FAR) - IdVFace

There are two levels of assessment of FAR.

For IdVLevel 1, the False Accept Rate SHALL meet the requirement of less than 1:100 for the upper bound of an 80% confidence interval. For IdVLevel 1 and IdVLevel 2, documented self-attestation of at least 1/10000 false

accept rate is also required and described in Section Documented Self-Attestation FAR.

For IdVLevel 2, the False Accept Rate SHALL meet the requirement of less than 1:3000 for the upper bound of an 80% confidence interval. (note: This is for 100 subjects and calculation of rule of 1.51.)

3.4.4. MultiBiometric Performance Testing - BCC Only

For TOEs that collect all biometric data for fusion prior to a decision, Testing SHALL be performed as written where subjects SHALL provide all modalities as part of authentication. FAR and FRR for the combined decision remain the same.

For TOEs that operate based on sequential fusion (i.e., where a decision resulting from initial biometric(s) determine whether subsequent biometric(s) need to be collected), the laboratory SHALL create a test protocol. If it is up to the user which modality goes first, a test plan SHALL be designed based on the information the vendor provides regarding the TOE and approved by the FIDO Biometric Secretariat. For example, the Laboratory MAY randomly assign the order of the modalities for each transaction. If it is up to the TOE which modality goes first, a test plan SHALL be designed based on the information the vendor provides regarding the TOE and approved by the FIDO Biometric Secretariat.

Methods for computing FAR and FRR remain the same and are based on the combined final decision.

For TOE that utilize different fusion approaches depending upon the environment, the Laboratory SHALL test each of these algorithms similar to Section Test Environment.

> NOTE: For example, if face modality is always captured first, followed by fingerprint, only if needed, the test plan will consider face first. In another example, if the TOE chooses which modality goes first, the Laboratory shall consider this in the test plan.

3.4.5. Documented Self-Attestation FAR

If the vendor establishes self-attestation for FAR, the following requirement applies.

The vendor SHALL attest to a FAR of [1:10,000, or 1:25,000 or 1:50,000 or 1:75,000 or 1:100,000] at a FRR of 5% or less. This claim SHALL be supported by test data as described in Documented Self Attestation (Optional) and documented through a report submitted from the Vendor to the Laboratory. The Laboratory SHALL validate that the report follows FIDO requirements described in Documented 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.

3.4.5.1. Documented Self-Attestation FAR - BCC

Dcoumented self-attestation for FAR is optional for BioLevel 1+ and BioLevel 2+, but required for BioLevel 1 and BioLevel 2.

3.4.5.2. Documented Self-Attestation FAR - IdVFace

Self-attestation for FAR is optional for IdVLevel 2, but required for IdVLevel 1.

3.4.6. Documented Self-Attestation FRR

Self-attestation for FRR is optional for BioLevel 1+ and BioLevel 2+, but required for BioLevel 1 and BioLevel 2.

If the vendor chooses self-attestation for FRR, the following requirement applies. The vendor SHALL attest to a FRR at no greater than 5% 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 Documented Self-Attestation (Optional) and documented through a report submitted from the Vendor to the Laboratory. The Laboratory SHALL validate that the report follows FIDO requirements described in Documented 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.

3.4.6.1. Documented Self-Attestation FRR - BCC

Self-attestation for FRR is optional for BioLevel 2 and BioLevel 2+, but required for BioLevel 1 and BioLevel 1+.

3.4.6.2. Documented Self-Attestation FRR - IdVFace

Not applicable. There is only one level for FRR.

3.4.7. Maximum Number of Biometric References from Multiple Fingers - BCC Only

Requirement

If a subject enrolls multiple fingers (e.g., index and thumb) and uses them interchangeably (i.e., one OR the other), 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.

If the analysis below is not performed, the maximum number of biometrics references SHALL default to one.

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

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

B=Max # Biometric References 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 biometric references which meet the FAR requirement MAY be stored in the meta-data and SHALL NOT be greater than the maximum number verified during biometric certification, according to the above. Self-attested FAR in the meta-data SHALL be based on the single biometric reference 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 laboratory SHALL use the same process to assess the maximum number of biometric references.

3.5. FIDO Presentation Attack Detection Criteria

The requirement for IAPAR takes into account that vendors who seek to achieve certification through independent testing may likely develop their system stricter than the target requirements. This is to ensure that they pass certification, due to the inherent variability that occurs in any test. In other words, if a requirement is set at X%, vendors will target much stricter than X% to ensure that they do not risk not passing due to variability from one test to the next.

3.5.1. Impostor Attack Presentation Accept Rate (IAPAR)

Requirement Each of the selected six Level A PAI species SHALL achieve an IAPAR of less than the threshold. Each of the selected eight Level B PAI species SHALL achieve an IAPAR of less than the threshold. Levels A and B are defined in Test Procedures for Presentation Attack Detection (PAD)

The actual achieved IAPAR 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, is set by the Vendor, and SHALL correspond to the claimed False Accept Rate (FAR) value to be tested.

Limitation

The PAI SHALL be presented until the end of the verification transaction (when a decision is made). An accept or match results in an error.

IAPAR (%) = ((Number of Impostor Presentation Attack Transactions for which Decision is Accept) / (Total Number of Impostor Presentation Attack Transactions Conducted)) *100

IAPAR 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 verification transaction ends when a decision is made. One or more failures to acquire may occur prior to a decision. The verification transaction (maximum number of verification attempts and timeout period) for a TOE is defined in the Allowed Integration Document as described in Verification Transactions. 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 presentation attack.

> NOTE: ISO/IEC 30107-3:2017 defines the metric as Impostor Attack Presentation Match Rate (IAPMR). A correction is currently pending publication for ISO 30107-3 which changes the name to Impostor Attack Presentation Accept Rate (IAPAR) so that it is consistent with biometric performance metrics.

3.5.1.1. Impostor Attack Presentation Accept Rate (IAPAR) - BCC

A TOE with an IAPAR of less than or equal to 15% will meet BioLevel 1 and BioLevel 1+ requirements. A TOE with an IAPAR of less than or equal to 7% will meet BioLevel 2 and BioLevel 2+ requirements.

The threshold for the level and the level achieved is stored in the FIDO Metadata as well as the FIDO Biometric Component Certificate.

3.5.1.2. Impostor Attack Presentation Accept Rate (IAPAR) - IdV Face

In addition to the IAPAR per-species requirement, FIDO has a second requirement that considers all transactions for presentation attacks across all species.

There are 2 requirements:

1. A TOE with an IAPAR of less than or equal to 7% for each PAI species.
2. The Number of Impostor Presentation Attack Transactions across all species for which Decision is Accept SHALL be less than 4% of the Total Number of Impostor Presentation Attack Transactions Conducted.

3.5.2. Rate Limits

3.5.2.1. Rate Limits - BCC

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 per FIDO Authenticator Security Requirements, Requirement 3.9.

For the purposes of biometric certification testing, rate limiting SHOULD be turned off.

3.5.2.2. Rate Limits - IdV Face

IdV Face Verification solutions SHALL rate-limit user verification to a maximum of 5 transactions.

For the purposes of biometric certification testing, rate limiting SHOULD be turned off.

3.5.3. Injection Attacks - IdV Face Only

In addition to attacks at the biometric capture device, which is measured by the imposter attack presentation accept rate (IAPAR) discussed in the prior section, another type of attack to the face verification system is to bypass the biometric capture device and inject a face image or video data in order to appear as if it was captured live. This is different from a presentation attack as the image or video is not presented to the capture device. The attacker is attempting to use prior captured data or deepfake data in order to appear as if the real person is present at the time of capture.

An injection attack shown in the above figure relates to attack point #2 where the attacker would modify or replace the biometric verification sample with a face image or a video with the intent to match the biometric reference retrieved from the document.

From ISO 19989-1, Section 6.1, referring to points 2 through 7, "Figure 2 illustrates generic attacks against a biometric system. Among these attacks, the attack indicated with arrow 1 is a presentation attack and those indicated with arrows 2 and 4 mark places where attacks can be made against captured biometric sample data and relate to biometric recognition performance. Points of attack 2 and 4 are considered in ISO/IEC 19989-2 only when the attack scenario is related to exploiting specific behaviour of biometric recognition performance (for example, algorithm weaknesses). The other aspects are covered by generic IT security evaluation approaches and are not specific to the security evaluation of a biometric system.

For ATE, ISO/IEC 19989-2 deals with the testing of biometric recognition performance in order to evaluate presentations from impostor attempts under the policy of the intended use following the TOE guidance documentation.

ISO/IEC 19989-3 deals with the testing of a presentation attack detection mechanism."

In other words, 19989-1, 19989-2, 19989-3 are primarily focused on presentation attack detection and performance, and not on injection attacks, like replacement of the biometric sample. While generic IT security protections are expected to be employed in biometric recognition systems, there are biometric-oriented

approaches that provide an additional layer of security for injection attacks that typically involve challenge response of the biometric sample. These would be difficult for the attacker to generate on-the-fly, therefore an attempted injection attack could be detected. For example, this may include projecting various colors of light on the face in a random order or asking the user to say a phrase that they were not told ahead of time or a visual nonce. As such, this makes injection attacks more difficult for the attacker and may help prevent attacks, particularly those less sophisticated.

In the following document, ENISA gives some examples of ways to mitigate injection attacks.
[[https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021]
(https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021)]

In order to address injection attacks as an attack vector during face verification and as part of remote identity verification solutions, the following is the security requirement. Future drafts may include more extensive evaluation which could include penetration testing by the FIDO certified laboratory.

Security Requirement: The vendor SHALL document the security projections implemented around the TOE to protect from injection and replay attacks.

Tester: The FIDO certified Laboratory SHALL verify that the documentation meets the requirement.

3.6. Evaluation of Differential Performance across Demographic Groups - Optional§

This optional evaluation considers biometric performance across age, skin tone, and gender.

For BCC program, this optional certification SHALL only be available for TOE that are undergoing certification at Levels 1+ and 2+ with at least 245 subjects.
For IdV-Face program, this optional certification SHALL only be available for TOE that are undergoing certification and will require increasing the number of subjects to 245.

All requirements SHALL be followed that are described in the FIDO Biometric Certification Program with additional requirements below.

This program only consider false reject rate, using the same methodology as SectionFalse Reject Rate. FRR SHALL be measured at the Transaction Level.

Test subject SHALL provide self-reported demographic information for age, gender, and skin tone.

3.6.1. Differential Performance Requirements§

For age, the FRR SHALL be less than 6% for each of the three age groups.

Age groups are further defined in SectionAge.

For gender, the FRR SHALL be less than 6% for each of the two gender groups.

Gender groups are further defined in SectionGender. Other SHALL be a self-reported choice, but will not be analyzed due to low subject numbers.

For skin tone, the FRR SHALL be less than 6% for each of the three groups of skin tones.

Groups based on skin tone are further defined in SectionSkin Tone.

Other dimensions MAY be evaluated, per agreement between the vendor, FIDO accredited laboratory, and FIDO biometrics Secretariat. For example, a vendor may want to evaluate the differential impact associated with color of the eye for iris and spoken language for voice.

The operating point SHALL be the same as used for FIDO Biometric Component Certification.

Multibiometrics will be performed as described in SectionMultiBiometric Performance Testing - BCC Only and Section MultiBiometric Testing for PAD - BCC Only.

NOTE: ISO 19795-10 has multiple options for measuring differential performance. One option is described in the Section: Reporting differential performance against a benchmark (Section 7.4.2). In this approach, testers seek to compare the performance of one or more demographic groups to a specific benchmark. FIDO has chosen this approach given the small sample size of the individual groups (50+ per group). The benchmarks was set at 6% (95% confidence interval), based on bootstrapping simulations. These simulations covered a spectrum of scenarios, population sizes, correlation between attempts. The benchmark chosen reduces the probability that a group will be considered different when it actually is not, i.e., finding a difference by chance (<5%). [Schuckers_DiffPerf]

4. Common Test Harness§

The following sections describe the Test Harness that SHALL be included for TOE.

4.1. Common Test Harness - BCC§

For each operating point to be evaluated, the Vendor SHALL provide a biometric system component of the FIDO authenticator which has, at a minimum, the items described in the next sections.

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 an on-line verification evaluation.
   6. Can provide enrollment biometric references 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 Biometric Verification on-line system which:
   1. Selects the operating point(s) to be evaluated.
   2. Has verification hardware/software to 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 a biometric reference.
   5. Makes an 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 the decisive sample(s) of an online verification transaction, i.e., all data used to make the verification transaction decision (called a stored verification transaction). This will be used for off-line verification.

C. Configurable Biometric Verification off-line software, which:
   1. Selects the operating point(s) to be evaluated.
   2. Has verification software to be executed by the FIDO authenticator.

3. Accepts a biometric reference and the stored verification transaction then performs matching in off-line batch mode.
4. Provides a decision (accept or reject).

D. Logging capabilities, which:
1. Records every interaction with the TOE.
2. Allows the tester to manually add 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 biometric reference 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. These stored attempts will be used for off-line verification testing.

4.2. Common Test Harness - IdV Face§

For each operating point to be evaluated, the Vendor SHALL provide a face verification component of the Remote Identity Verification solutions which has at a minimum:

A Configurable Enrollment system which:

1. Selects the operating point(s) to be evaluated.<\li>
2. Has enrollment hardware/software. Enrollment is the capture of the face image from the document, based on one or more of the following:<\li>
    1. Biometric Reference Type 1: photo of a document with face image; <\li>
    2. Biometric Reference Type 2: electronic transfer of a digital face image from the document through NFC or other means<\li> <\ol>
    3. The following are options for capturing the biometric reference:<\li>
        1. Simultaneous certification through two programs (1) Identity Document Authenticity Verification and (2) FIDO Biometric Face Verification<\li>
        2. The Face Verification Vendor provides their own solution for extraction of biometric reference.<\li>
        3. The Face Verification Vendor partners with another Vendor who provides software to extract biometric reference.<\li>

        > NOTE: The Vendor SHALL indicate in the Allowed Integration Document, the various configurations for enrollment that are supported. If a vendor supports multiple configurations, the vendor SHALL provide at least one TOE for each configuration. Each TOE SHALL be evaluated separately.

        <\ol>
    4. Can delete a biometric reference.<\li>
    5. Can store a biometric reference acquired from the document for use in on-line verification evaluation.<\li>
    6. Can provide biometric references acquired from the document for use in off-line verification evaluation.<\li>
    7. Indicates a failure to enroll ([ISOIEC-19795-1], 4.6.1)<\li> <\ol>

    Configurable Verification on-line system. Verification is a face image taken by the test subject of themselves, i.e., a "selfie". This excludes non-selfie live face capture of the test subject by another

person. Data capture subsystems may include a mobile device, webcam, or labtop camera, for example. The configurable verification on-line system shall have the following:

1. Selects the operating point(s) to be evaluated.<\li>
2. Has verification hardware/software to be executed by the Face Verification system.<\li>
3. Includes a biometric data capture sensor, a biometric matcher and a decision module.<\li>
4. Captures features from an acquired biometric sample to be compared against the biometric reference.<\li>
5. Makes an accept/reject decision at a specific operating point.<\li>
6. Indicates an on-line failure to acquire ([ISOIEC-19795-1], 4.6.2).<\li>
7. Indicates an on-line decision (accept or reject).<\li>
8. Provides the decisive sample(s) of an online verification transaction, i.e., all data used to make the verification transaction decision. This is called a stored verification transaction and will be used for off-line verification.<\li>

Configurable Verification off-line software, which:

1. Selects the operating point(s) to be evaluated.<\li>
2. Has verification software that will be executed by the Face Verification system.<\li>
3. Accepts a biometric reference and the stored verification transaction and performs matching in off-line batch mode.<\li>
4. Provides a decision (accept or reject).<\li>

Logging capabilities, which:

1. Record every interaction with the TOE. <\li>
2. Allow the tester to manually add interactions (e.g., the fact that a tester just cleaned the sensor device)<\li>

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

4.3. Security Guidelines§

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

> NOTE: For example, only the vendor and FIDO Accredited Laboratory SHALL 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 particular 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 performed using the Common Test Harness defined in Common Test Harness.

5.1. Test Crew

The Test Crew is the Test Subjects gathered for evaluation.

5.1.1. Number of Subjects

5.1.1.1. Number of Subjects - BCC

For BioLevel 1 and BioLevel 2 certification, the minimum number of subjects for a test SHALL be 25, based on [ISOIEC-19795-1] and associated analysis in the Statistics and Test Size section of this document.

For BioLevel 1+ and BioLevel 2+ certification, 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 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.

> NOTE: Having 123 test subjects will only require the use of 2 fingerprints per test subject at minimum. Allowing 4 fingers per test subject should allow the laboratory to acquire additional data if needed. It also allows to better align the test results of the Laboratory with the test results of a potential self attestation.

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.

5.1.1.2. Number of Subjects - IdV Face

For IdVLevel 1 certification, The minimum number of subjects for a test SHALL be 25, based on [ISOIEC-19795-1] and associated analysis in the Statistics and Test Size section of this document.

For IdVLevel 2 certification, The minimum number of subjects for a test SHALL be 100, based on [ISOIEC-19795-1] and associated analysis in the Statistics and Test Size section of this document.

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 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 SHALL 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 SHALL be used for age and gender. Minor deviations from these numbers may be acceptable if agreed by the FIDO biometric secretariat.

5.1.2.1. Age

Age Distribution Requirements

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

NOTE: for all Levels, the population shall still adhere to these age distribution requirements

5.1.2.2. Gender

Gender Distribution Requirements

Gender	Distribution
Male	40-60%
Female	40-60%
Other	0-20%

"Other" SHALL be provided as a choice to the test subject, but there is no requirement for the number of those selecting "Other".

NOTE: for all Levels, the population shall still adhere to these gender distribution requirements.

5.1.2.3. Skin Tone

Groups based on skin tone SHALL be defined based on the Monk Scale [MonkSkinTone], as follows.

Skin Tone Distribution Requirements

Skin Tone	Distribution
Monk Scale 1-3	25-40%
Monk Scale 4-6	25-40%
Monk Scale 7-10	25-40%

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.

NOTE: Twins or genetically identical siblings may be more likely to have a similar face signature. The test crew SHOULD not include genetically identical siblings, i.e., twins.

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 the 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 biometric references.
3. For each v(i), sample with replacement m transactions 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.

Please note that the bootstrapping algorithm works on the level of transactions and is agnostic to the individual attempts made in each transaction. As the FAR is the error rate that is tested, it is not relevant whether a certain transaction comprised 1, 2 or the maximum number of allowed attempts.

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 298,900 comparisons, 1000 bootstraps created using the ISO method. (Unlike this simulation, in the results from a laboratory test, it is possible to have fewer than 298,900 comparisons, as some transactions may result in an FTA.)

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. The 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 example schematic of the bootstrap distribution and FAR requirement. For example, 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.

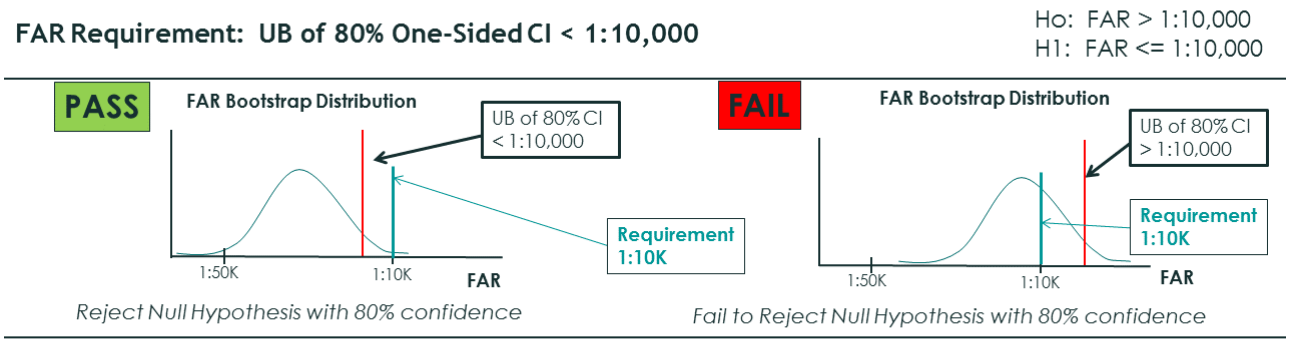

Figure 1 *Bootstrapping FAR Schematic*

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 transactions 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 non-mated comparisons, the TOE meets the FAR requirement on the basis of the "Rule of 3".

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.

> NOTE: Rule of 3 states the upper bound of the 95% confidence interval is 3/N, or 0.0100%.

> NOTE: For example, if the test includes n=245 subjects, this results in n(n-1)/2 or 29890 combinations (N). For an 80% upper bound, the upper bound is 1.61/N or 0.00535%, which meets the FIDO FAR requirement of 0.01%. For Rule of 1.61 for 80%, only 180 subjects are required to achieve a 0.01% FAR; However, we are exceeding the number of subjects needed, since bootstrapping utilizes 80% confidence due to reasons discussed in the bootstrapping section.

The following table provides the number of subjects needed to meet Rule of 3 for lower FAR and when two (a=2) instances (fingers or eyes) are used. Detail for each program BCC and IdV are provided in the subsections below.

Table: Rule of 3 for FAR

Rule of 3 ([ISOIEC-19795-1])	**FAR**						
	<1%	<0.033%	0.0100%	0.0040%	0.0020%	0.0013%	0.0010%
	1:100	1:3000	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)	25	100	245	390	550	675	775
# Combinations-C = n(n-1)/2	300	4950	29890	75855	150975	227475	299925
Claimed error = 3/C (when zero errors in C combinations)	<1% (0.536%)	<0.033% (0.325%)	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)	N/A	N/A	123	195	275	335	388
# unique samples (a)	N/A	N/A	2	2	2	2	2
# Combinations-C = $(a^2)*n*(n-1)/2$	N/A	N/A	30012	75660	150700	223780	300312
Claimed error = 3/C (when zero errors in C combinations)	N/A	N/A	0.0100%	0.0040%	0.0020%	0.0013%	0.0010%

5.1.3.3.1. Rule of 3: FAR - BCC

For BioLevel 1 and BioLevel 2, we have 25 subjects, 300 combinations, and 1.61/300 leads to .536% FAR (<1%). For BioLevel 1+ and BioLevel 2+, we have 245 subjects, 29890 combinations, and 1.61/29890 leads to 0.00535% FAR (<0.01%).

5.1.3.3.2. Rule of 3: FAR - IdV Face

For Level 1, we have 25 subjects, 300 combinations, and 1.61/300 leads to .536% FAR (<1%). For Level 2, we have 100 subjects, 4950 combinations, and 1.61/4950 leads to 0.0325% FAR (<0.033%).

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.

5.1.3.4.1. Rule of 3: FRR - BCC

For BioLevel 1 and BioLevel 2, we have 25 subjects, 25 genuine comparisons, and 1.61/25 leads to 6.4% FRR (<7%). For BioLevel 1+ and BioLevel 2+, we have 245 subjects, 245 genuine comparisons, and 1.61/245 leads to 0.65% FRR (<5%).

5.1.3.4.2. Rule of 3: FRR - IdV Face

For Level 1, we have 25 subjects, 25 genuine comparisons, and 1.61/25 leads to 6.4% FRR (<7%). For Level 2, we have 100 subjects, 100 genuine comparisons, and 1.61/100 leads to 1.61% FRR (<5%).

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. Test Environment

In this context, it should be noted that the definition of the testing environment of the TOE, (which is based on the environment of the TOE described in the Allowed Integration Document), plays an important role in the context of the certification. For this reason, potential environment(s) shall also be described in the Allowed Integration Document ([BiometricAIDTempate]). Every certificate will identify the testing environment under which the biometric component has been tested.

The definition of the environment may also have an impact on the testing activities. Testing shall always be carried out under consideration of the intended environment. The test requirements in this document allow for a certain variation in environmental conditions. However, such variations have their limits. This could lead into a situation where the Laboratory SHALL perform a test multiple times or with a larger amount of test subjects if a TOE has a very diverse definition of environments.

The question of whether a specific intended environment will lead to additional requirements for testing has to be seen in the context of a specific Target of Evaluation and shall be discussed with the FIDO biometric secretariat during the review of the test plan. Environments that may lead to increased FRR (i.e., more inconvenience for the user) will not necessarily be evaluated as part of the testing plan. However, a testing plan may include multiple environments for cases where the TOE may have multiple configurations to address multiple environments.

For example, this could include (1) a different operating point (e.g., threshold for the matcher) for a noisy environment or (2) an NIR-only face recognition in low/no light (and visible light is used in normal light). If a TOE has multiple configurations that address different environments, then the TOE SHALL be tested for each configuration and the test plan SHALL incorporate the variations for the different environments that result in a different configuration.

5.1.6. Biometric Reference Adaptation - BCC Only

Some systems perform biometric reference updates, that is, the biometric reference is adapted after successful verification transactions.

Vendor SHALL inform the Laboratory whether biometric reference 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 Biometric Reference Adaptation SHALL be turned off after the TOE has been fully trained on correct biometric references.

> NOTE: Biometric reference adaptation which requires an extensive amount of time may incur increased cost of the laboratory test.

The offline software SHALL utilize biometric references in the same way as the online software.

5.1.7. 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, along with any divergence from enrollment instructions that MAY have caused the failure.

5.1.7.1. Enrollment & Document Capture - IdV Face

Each subject in the test crew SHALL provide a document which includes a face image defined by the Allowed Integration Document. The reference image used in further face testing is an image captured from the document.

The laboratory SHALL capture a photograph of the document using a capture API which meets the following:

- Captures an image of the document according to the quality specified below
- Crops an image of the face according to the quality specified below

The capture API provided by the laboratory SHALL be vendor neutral, i.e., SHALL not be from a vendor who may go through Laboratory testing.

For a TOE that is undergoing both the Document Verification and Face Verification Certification programs, the image SHALL be captured using the TOE which was provided for the Physical Document Test [Section 6.2.2 in FIDO EnrollmentReqth Requirements] as part of the FIDO Document Verification Certification program. The face image captured from the document SHALL ensure there is at least 90 pixels between the eyes in the photograph of the individual.

Images shall be good enough quality to be processed. Vendors SHALL specify realistic image quality requirements that shall be used for the test and shall be specified in the TOE Description and FIDO Lab Report. The vendor and laboratory SHOULD come to an agreement on image quality of the test set. Typical parameters to be considered by the vendor and laboratory include:

- Resolution SHALL ensure there is at least 90 pixels between the eyes in the photograph of the individual.
- Compression (lossless compression, or lossy compression with minimal artifacts)
- Absence of image noise such as glare, lighting and blur
- Cropping (presence or absence of cropping in the test set)
- Absence of visual obstruction
- Absence of damage to the document

The quality characteristics of the test set SHALL be documented by the FIDO test Laboratory and reviewed by the FIDO Secretariat prior to testing.

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 a false accept rate, all biometric references and all stored 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 with the exception that the test operator may instruct the user to perform 5 mated transactions. Additionally, the operator is allowed to provide guidance as far as it concerns the test situation. Any kind of guidance SHALL be provided by the biometric authentication system/capture sensor in a way similar 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 biometric reference for the test subjects after executing three enrollment transactions.

5.2.2.2. Online: Mated Verification Transaction

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

Mated 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 enrollment should be in place for the collection of the test data. Systematic variation of presentation and channel effects between enrollment 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 enrollment and test sessions across all users.

In the ideal case between enrollment 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 biometric reference after successful verification, some interim use between enrolment and collection of mated 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 mated 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 enrollment, 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 a biometric reference. Some vendor software does not record a measure from an enrolled user unless it matches the biometric reference. 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.

NOTE: Details for FIDO as they relate to the ISO requirements are discussed in the following sections.

5.2.2.2.1. Pre-Verification

Before mated verification transactions, test subjects MAY perform practice transactions.

5.2.2.2.2. Mated Verification Transaction

Test Subjects SHALL conduct 10 mated verification transactions. Mated verification transactions SHALL be conducted such that there is variability between transactions by introducing environmental or behavioral factors. Examples for each modality are provided below:

- Face: lighting, pose, expression<\li>
- Fingerprint: pressure, moisture, angle<\li>
- Iris: gaze, lighting, closed eyes<\li>

The chosen variabilities SHALL be documented as part of the FIDO Test plan and approved by the FIDO Biometric Secretariat. The FIDO Biometrics Secretariat shall ensure equivalency across laboratories in the chosen variabilities.

Mated 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. The verification transaction (maximum number of verification attempts and timeout period) for a TOE is defined in the Allowed Integration Document as described in Verification Transactions. A transaction SHOULD NOT exceed 30 seconds.

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

The test harness SHALL provide the decisive sample(s) of a transaction for off-line testing, i.e., all data used to make the verification transaction decision.

5.2.2.2.3. Mated 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.

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 inFRR 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 a 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 functionally equivalent to the online biometric functionality. The evaluation Laboratory SHALL perform a series of mated 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: Non-mated Verification 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. Non-mated Verification Transaction

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

Non-mated Verification 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. Non-mated Verification Transaction Failures

The impostor verification process compares a biometric reference 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 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. Documented Self-Attestation (Optional) - BCC Only

5.3.1. Procedures for Documented 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 for FIDO independent testing.
- The number of subjects* SHALL follow the following table:

Documented 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 § 7 Test Reporting 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 the 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 the vendor. The evaluation measures the Impostor Attack Presentation Accept Rate (IAPAR), as defined in ISO 30107 Part 3.

PAD Testing shall be completed by using the following approach.

6.1. Test Crew

The Test Crew are the Test Subjects gathered for evaluation.

6.1.1. Number of Subjects

Number of subjects for a test SHALL be 15.

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. Population

The population SHALL 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 SHALL be used for age and gender. Minor deviations from these numbers may be acceptable if agreed by the FIDO biometric secretariat.

6.1.2.1. Age

Age Distribution Requirements

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

6.1.2.2. Gender

Gender Distribution Requirements

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

6.1.2.3. Skin Tone

Groups based on skin tone SHALL be defined based on the Monk Scale [MonkSkinTone] and reported.

> 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.

6.1.3. Test Visits

Collection from test subjects MAY occur in one visit.

6.1.4. 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.

6.2. 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 it may allow multiple presentations for the enrollment.

The test laboratory 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.

6.2.3.1. PAD Enrollment & Document Capture - IdV Face

Enrollment SHALL be performed according to the requirements in Enrollment & Document Capture - IdV Face.

6.2.4. 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 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. PAD Evaluation with Presentation Attack Instruments (PAI)

Based upon the prior section, the test Laboratory SHALL select six Level A and eight Level B Presentation Attack Instrument Species to be used in the evaluation.

Four of eight Level B PAI Species SHALL be tailored to the underlying technology. The PAI Species SHALL be selected by the laboratory and SHALL be approved by the FIDO Biometric Secretariat. Access to the TOE would be necessary. 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 8+6=14 selected PAI species and 15 enrolled subjects, the test Laboratory would have to create 210 instruments. Examples of different PAI species include PlayDoh, gelatin using recipe 1, gelatin using recipe 2, and ABC Brand wood glue.

The 15 subjects SHALL have variation in age and gender as well as be representative of the underlying population. Additional target guidance is provided in Population.

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 it as part of the report to FIDO and the Vendor.

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

For each built artifact, the Laboratory shall verify the quality of the artifact before using it in tests. The scope of this quality check is to ensure that the artifact is suitable for verification against the original biometric reference of the test subject.

The quality check can be performed in multiple ways. The particular implementation depends on the biometric modality being tested and on the sensor technology. Existing examples of such quality checks include

- the calculation of an NFIQ2 value for fingerprint images obtained from the artifact
- performing a successful verification with the artifact on a different biometric system without a PAD or with a disabled PAD

6.2.5.1. Impostor Presentation Attack Transactions

For each enrollment, the test Laboratory operator SHALL conduct 10 impostor presentation attack transactions for each PAI. Any kind of guidance SHALL be provided by the biometric authentication system/capture sensor in a similar manner to the final application. The verification transaction (maximum number of verification attempts and timeout period) for a TOE is defined in the Allowed Integration Document as described in Verification Transactions. 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).

> NOTE: Some presentations may be more successful than others at matching or bypassing PAD. The test crew SHOULD allow for natural variability in presentation of the PAI across the ten transactions.

NOTE: 15 PAIs will be created for each PAI Species, one for each of 15 enrolled subjects, and 10 imposter presentation attacks transactions will be conducted for each PAI. Therefore, each PAI species will have 150 transactions. To achieve a IAPAR of 7%, there is a maximum of 10 out of 150 errors for each PAI species in order to pass certification. To achieve a IAPAR of 15%, there is a maximum of 22 out of 150 errors for each PAI species in order to pass certification. For IdV Certification only, there is a requirement of less than or equal to 4% for all species, which translates to a maximum of 84 out of 2100 errors.

NOTE: If it should become clear that a certain kind of material selected for testing is not recognized by the TOE at all (i.e., the TOE does not respond by a rejection, acceptance, or request to try again), the Tester may skip the rest of the impostor transactions for the artifacts of this material. The Lab SHALL test at least three PAIs for that material before determining that it is not recognized by the TOE. This shall be documented in the report. In this case, an IAPAR of 0% shall be recorded as well as the number of PAIS and transactions for the material, and that the testing skipped the remaining PAIs. A failure to acquire for an impostor presentation attack transaction counts as a transaction and does not count as an error, as some systems may produce a failure to acquire in response to a detected presentation attack. In ISO 30107-3, this is considered an attack presentation non-response and computed as the attack presentation non-response rate (APNRR).

6.2.5.1.1. 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 failure to acquire for an impostor presentation attack transaction counts as a transaction and does not count as an error, as some systems may produce a failure to acquire in response to a detected presentation attack. In ISO 30107-3, this is considered a attack presentation non-response and computed as the attack presentation non-response rate (APNRR).

An 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 verification transaction ends when a decision is made. One or more failures to acquire may occur prior to a decision. The verification transaction (maximum number of verification attempts and timeout period) for a TOE is defined in the Allowed Integration Document as described in Verification Transactions.

6.2.5.1.2. IAPAR

Impostor Attack Presentation Accept Rate (IAPAR) SHALL be calculated according to requirements in Impostor Attack Presentation Accept Rate (IAPAR) .

6.2.6. MultiBiometric Testing for PAD - BCC Only

PAD testing SHALL include creation of a PAIs for all modalities.

For TOEs that collect all biometric data for fusion prior to a decision, Testing SHALL be performed as written where PAIs SHALL be presented for all modalities as part of authentication.

For TOEs that operate based on sequential fusion (i.e, where a decision resulting from initial biometric(s)

determine whether subsequent biometric(s) need to be collected), the Laboratory SHALL create a test protocol. If it is up to the user which modality goes first, a test plan SHALL be designed based on the information the vendor provides regarding the TOE and approved by the FIDO Biometric Secretariat. For example, the Laboratory may randomly assign the order of the modalities for each transaction. If it is up to the TOE which PAI modality goes first, a test plan SHALL be designed based on the information the vendor provides regarding the TOE and approved by the FIDO Biometric Secretariat.

For TOE that utilize different fusion approaches depending upon the environment, the Laboratory SHALL test each of these algorithms similar to Section Test Environment.

Methods for computing IAPAR remain the same and are based on the combined final decision.

> NOTE: For example, if face modality is always captured first, followed by fingerprint (only if needed), the test plan will present the face PAI first. In another example, if the TOE chooses which modality goes first, the test Laboratory shall consider this in the test plan.

> NOTE: Future testing could include presenting combinations of a PAI for one modality and an attackers own biometric.

7. Test Reporting

7.1. General Reporting Requirements

7.1.1. Report Development

The Laboratory SHALL prepare a report as described in the following sections A copy of the report SHALL be provided to the Vendor prior to being provided to FIDO. The report SHALL then be provided to FIDO

The Laboratory SHALL NOT disclose the report to any other recipients; only the Vendor CAN disclose the report to other recipients.

7.1.2. Protection of privacy for test participants

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

7.1.3. Description of ToE

Test reports shall provide a description of the ToE. The description shall contain

- complete description of ToE
- ToE configuration files
- ToE settings
- PAD mechanisms

When the ToE is part of a mobile device, the report shall contain the following

- Mobile device model, OS, and OS version
- Position of sensor (e.g. front, back, side), to include position relative to device's screen(s)
- If applicable, manner of test subject interaction with the biometric sensor (e.g., touch left index finger, swipe right or left thumb, look at front-facing camera, speak a passphrase)

7.1.4. 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 preparative 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 may need 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.

7.1.5. FIDO Metadata - BCC Only§

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

7.2. FAR/FRR Reporting Requirements§

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

Reporting test details

Test details	**Details to report**
The system(s) tested	Including details of algorithms, biometric sensors, user interface, supporting hardware, etc.
Test organization details	Test organization, location, date of test.
Type of evaluation	In the case of technology evaluation: details of the test corpus used. In the case of scenario evaluation: details of the test scenario. In the case of operational evaluation: details of the operational application.
Size of evaluation	Number of test subjects. Number of instances (fingers, hands or eyes, etc.) enrolled by each test subject. Number of visits made by test subject. Number of transactions per test subject (or test subject instance) at each visit.
Test crew	Demographics of the test crew (age, gender, etc.) The manner in which the test crew was assembled, to include exclusions, volunteers etc., as well as the degree to which the test crew mirrored the target population. The level of training, instruction, familiarization, and habituation of test crew in the use of the system.
Test environment	See 8.3.2.1, 8.4.2, and C.2.6.
Time separation between enrollment and	See 7.3.7.

recognition transactions	
Quality and decision thresholds used during data collection	The thresholds used, and those recommended for the target application (if different).
Control of factors potentially affecting performance	See 7.3 and Annex C.
Test procedures	E.g., policies for determining enrollment failures. Details of any abnormal cases occurring during testing that are excluded from performance analysis.
Estimated uncertainties	Estimated uncertainty in performance results, and method of estimation. See 9.11 and Annex B.
Deviation from guidelines	Deviations from the guidelines of this document should be explained. Sometimes it is necessary to compromise one aspect to achieve another; for example, randomizing the order of using fingers on a fingerprint device might lead to user confusion and a higher number of labelling errors.

Enrollment performance metrics

Metric	**Details to report**
Failure to enroll rate (FTER)	See 9.2.1.

Acquisition performance metrics

Metric	**Details to report**
Failure-to-acquire rate (FTAR)	See 9.3.1.

Biometric Verification system performance metrics

Metric	**Details to report**
False accept rate (FAR)/ False reject rate (FRR)	See 9.5.2 and 9.5.3. FAR and corresponding FRR shall be reported over the range of decision thresholds tested. A DET plot is recommended in the case of multiple operating points.
FTER	See 12.3. Otherwise a statement that FTER is unknown.
FTAR	See 12.4. Otherwise a statement that FTAR is unknown.

Other items of value MAY include:

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

7.3. PAD Reporting Requirements§

The following SHALL be included in a report to the vendor, following (ISO/IEC 30107-4, 7.2 and 13.4.2.1):

- Summary of the FIDO Biometric Certification and Requirements
- Number of individuals tested
- Distribution of Age
- Distribution of Gender
- Statement relating to selection of the test subjects and the representativeness of the people who will use the

system in the real application environment. (This statement does not apply to age and gender which are reported separately.)

- Description of the Test Environment
- Description of the Test Platform
- Number of enrollment transactions
- Number of verification transactions
- Failure to Enroll Rate
- Failure to Acquire Rate
- IAPAR, sample size
- IAPAR of most successful PAI species
- bonafide FRR/FAR calculations and basis of reports; See SectionFAR/FRR Reporting Requirements.

And the following from (ISO/IEC 30107-3 and 30107-4):

- Information available to the evaluator about PAD mechanisms in place
- Information about details of any implemented output information of the PAD mechanism other than accept or reject
- 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 PAI presenters unable to utilize the artifacts
- the purpose and responsibilities of each role in a PAD test, and how the role was material to test results
- number of individuals that assumed each role
- For each role, describe each individuals' level of experience with presentation attacks
- documentation about the # of individuals that assumed multiple roles (as an incidence matrix)
- information in which machines or automated mechanisms were used as PAI presenters or PAI sources
- number of test subjects unable to present non-conformant characteristics
- number of artifacts created per test subject for each material tested
- number of sources from which the artifact characteristics were derived
- number of tested materials
- Impostor attack presentation accept rate (IAPAR)
- Number of impostor attack presentation transactions
- documentation about ordering of presentations with and without PAIs, and whether PAI presenters or test subjects were reused
- how artifacts were created and prepared (30107-4 10.2)
    - creation and preparation processes
    - effort required to create and prepare artifacts
    - ability to consistently create and prepare artifacts with intended properties
    - customization of artifacts for specific PAI presenters
    - customization of artifacts for specific systems
    - sourcing of biometric characteristics
    - availability of public information on creation and preparation process
    - changes in artifact creation or preparation processes over the course of the evaluation

- how artifacts were used (30107-4 10.3)
  - level of PAI presenter training and habituation
  - artifact durability, including the number of presentations associated with each artifact
  - level of scrutiny or oversight applied during artifact usage
- PAD mechanisms applicable to verification processes (30107-4 11.3)
  - use of quality thresholds and presentation policy
  - parameters of the verification transaction, including the number and duration of presentations
  - level of operator oversight present in the process
  - manner in which operator functions were applied or emulated in the evaluation
  - whether the IUT checks sample quality and provides feedback to the test subject (e.g. “finger too wet”)
  - policy after failing all attempts, e.g., asking for a PIN, a password, or waiting for 30 seconds before attempting again
  - If the IUT provides feedback, a list of the feedback messages

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

Appendix A: 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 on increasing levels of difficulty to mount and based on frameworks from Common Criteria then 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 [BEAT], 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 in Section 4.5 in [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 is 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 transactions, as required in FIDO Authenticator Security Requirements, Requirement 3.9.

In order to simplify for the FIDO use case, we have collapsed the remaining characteristics into three levels which 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 will 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	latent fingerprint on 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.

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 an 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. Some TOEs may be based on a photograph of a person's finger(s). Level A spoof attacks for this type of fingerprint TOE could include a low resolution photograph of a person's hand. In attacks of this type, photographs may happen to include a hand, but are likely to be of low resolution.

Level B attacks for spoofing a fingerprint biometric are to retrieve and print an image of a fingerprint which can be obtained through taking an 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, laser etching, or simply printing a fingerprint image on a transparency. A 2D mold can also be made using an inexpensive 3D printer (e.g. less than $500) with sufficient resolution to print the fingerprint ridges (e.g. at a minimum, XY resolution of less than 0.05mm). 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. Some TOEs may be based on a photograph of a person's finger(s). In additional to attacks based on materials like gelatin or PlayDoh, Level B spoof attacks for this type of fingerprint TOE could include a high resolution photograph or a video of a person's hand.

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. Some molds may also be more elaborate, such as 3D printing. Level C PAIs take more time to create, are more expensive, require experts to prepare, and need a high resolution and/or 3D finger information.

NOTE: For creation of Presentation Attack Instruments (PAI) during testing, test subjects will provide biometric characteristics on which the PAI will be based through pressing their finger on a surface creating a latent print (Level A and above), taking a low-resolution photograph (Level A), capturing their fingerprint on a fingerprint scanner (Level B and above), or taking a high-resolution photograph (Level B and above). Fingerprint molds obtained from an individual through pressing a finger into silicon or other molding material are out of scope. Future PAD testing may include molds of fingerprint when attacks of this type impact FIDO-based use cases.

Table of Example PAI Species for Fingerprint

Species	Level
latent fingerprint captured and printed on inkjet or laser printer	A
Low resolution photograph of a person's fingers	A
Fingerprint molds created using PCB or laser etching	B
Fingerprint molds created by printing on a transparency	B
Fingerprint molds created by printing with an inexpensive (e.g. less $500) 3D printer with XY resolution of less than 0.05mm	B
Casts made from molds listed above with materials such as gelatin or silicone	B
Same as previous with graphite or other material placed on surface of mold or PAIs	B
High resolution photograph of a person's fingers	B
Laser etching a fingerprint directly on materials such as rubber or silicone	B
Video (low or high resolution) of a person's fingers	B
3D printed molds and/or PAIs with expensive, high resolution 3D printers	C
Fingerprint models which capture sweating, veins, blood flow or more sophisticated finger information	C

NOTE: Some TOEs may involve multiple fingerprints. PAIs should be created for each finger that is used in making a decision.

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 A also includes videos created by readily available, inexpensive deepfake tools which can animate a face based on a single photograph of an individual. Animation of a 2D image of a person's face may include blinking, smiling, or speaking. The videos are then displayed on electronic/mobile devices and used to attack a face recognition system. Injection attacks are out of scope for PAD testing.

NOTE: Some face recognition systems utilize NIR illumination and a NIR camera. However, photographs of an individual taken in the visible spectrum could be used as a source of the face biometric characteristics for creation of a PAI. Preprocessing the RGB image may be needed, such as only selecting the red channel. NIR reflectance of the printed photograph may also be impacted by the make and model of the printer used.

NOTE: Some face recognition systems utilize NIR illumination and a NIR camera for which mobile display of face may not be feasible for most device makes and 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 B also includes videos created by readily available, inexpensive deepfake tools which can animate a face based on multiple and/or video frames of an individual. Animation of a person's face may include blinking, smiling, or speaking. The videos are then displayed on electronic/mobile devices and used to attack a face recognition system.

NOTE: As with Level A, some face recognition systems utilize NIR illumination and a NIR camera for which mobile display of face or face video may not be feasible for most device make and models.

Level C attacks involve more elaborate masks that are not made of 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. A video can also be created by using sophisticated computer vision which animates a 2D image of a person's face to blink, smile, or speak (e.g. DeepFake). Level C also includes videos created by more sophisticated deepfake tools which can animate a face based on multiple and/or video frames of an individual. Animation of a person's face may include blinking, smiling, or speaking. The videos are then displayed on electronic/mobile devices and used to attack a face recognition system.

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
Videos created by readily available, inexpensive deepfake tools which can animate a face based on a single photograph of an individual (displayed on electronic/mobile devices)	A
Displayed videos on electronic/mobile devices	B
Paper masks	B
Videos created by readily available, inexpensive deepfake tools which can animate a face based on multiple and/or video frames of an individual (displayed on electronic/mobile devices)	B
Masks made of specialized materials (ceramic, silicone, and/or theatrical)	C
3D printed faces	C
Videos created by more sophisticated deepfake tools which can animate a face based on multiple and/or video frames of an individual (displayed on electronic/mobile devices)	C

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, but may be visible for light colored eyes (e.g. blue). 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. Preprocessing the RGB such as only selecting the red channel may be needed.

> 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 a 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
Prosthetic eye	C
Prosthetic eye with similar spectral characteristics to human eye	C

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. Leval B attacks also include readily available voice synthesizers which can take a recording of a voice, build a model of that voice, and replay a person speaking any words.

> 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 are 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
Readily available, inexpensive voice synthesizers which can be trained based on short recordings of an individual and playback any words	B
More sophisticated 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

Index§

Terms defined by this specification§

Biometric Sample

Biometrics Working Group

Biometric Verification

BWG

Capture Attempt

Captured Biometric Sample

Capture Transaction

categorical demographic variable

Certification Working Group

Confidence Interval

continuous demographic variable

CWG

differential performance

Failure-to-Aquire

Failure-to-Aquire Rate

Failure-to-Enroll

Failure-to-Enroll Rate

False Accept Rate

false negative differential performance

False Reject Rate

FAR

FIDO Accredited Biometrics Laboratory

FIDO Certified Authenticator

FIDO Member

FRR

FTA

FTAR

FTE

FTER

IAD

IAPAR

Identity Verification & Binding Working Group

IDWG

Impostor Attack Presentation Accept Rate

Injection Attack Detection

Laboratory

Level A

Level B

Level C

OEM

Offline

Online

Original Equipment Manufacturer

PAD

PAI

PAI species

Presentation Attack

Presentation Attack Detection

Presentation attack instrument

Stored Verification Transaction

Target of Evaluation

Target Population

Test Crew

Test Organization

Test Subject

TOE

Variance

Vendor

Verification Attempt

Verification Transaction

References§

Normative References§

[DocAuth]
Stephanie Schuckers (Clarkson University); et al. *Document Authenticity Verification Requirements*. 15 Aug 2022. Final Document. URL: https://fidoalliance.org/specs/idv/docauth/document-authenticity-verification-requirements-v1.0-fd-20220815.html

[ISOBiometrics]
ISO/IEC 2382-37 Harmonized Biometric Vocabulary. 2017. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en

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

[ISOIEC-19795-10]
Information technology — Biometric performance testing and reporting — Part 10: Quantifying biometric system performance variation across demographic groups. URL: https://www.iso.org/standard/81223.html

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

[ISOIEC-19795-9]
ISO/IEC TS 19795-9:2019 Information technology — Biometric performance testing and reporting — Part 9: Testing on mobile devices. 2019. URL: https://www.iso.org/standard/78101.html

[ISOIEC-30107-3]
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-30107-4]
ISO/IEC 30107-4:2020 Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile device. 2020. URL: https://www.iso.org/standard/75301.html

[ISOIEC30107-1]
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

[MonkSkinTone]
E. Monk. *The Monk Skin Tone Scale*. 2023. published. URL: https://doi.org/10.31235/osf.io/pdf4c

[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

[Schuckers_DiffPerf]
M. Schuckers, K. Fatima, S. Purnapatra, J. Drahos, D. Hou, S. Schuckers.*Statistical Methods for Testing Equity of False Non Match Rates Across Multiple Demographic Groups*. 2023. published. URL: https://ieeexplore.ieee.org/abstract/document/10346007

Informative 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

[BiometricAIDTempate]
N. Tekampe. *FIDO Allowed Integration Document template*. June 2019. Published. URL: https://media.fidoalliance.org/wp-content/uploads/2020/02/FIDOAllowedIntegrationDocumentTemplate_v1.2.pdf

[FIDOMetadataService]
B. Jack; R. Lindemann; Y. Ackermann. *FIDO Metadata Service*. 18 May 2021. Proposed Standard. URL: https://fidoalliance.org/specs/mds/fido-metadata-service-v3.0-ps-20210518.html

[FIDOMetadataStatement]
B. Jack; R. Lindemann; Y. Ackermann. *FIDO Metadata Statements*. 18 May 2021. Proposed Standard. URL: https://fidoalliance.org/specs/mds/fido-metadata-statement-v3.0-ps-20210518.html

[FingerprintRecognition]
On security evaluation of fingerprint recognition systems 2010. URL: https://www.nist.gov/sites/default/files/documents/2016/11/30/henniger2_olaf_ibpc_paper.pdf

[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.

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