Certification makes ecosystem tick

Functional Certification (End-to-End):

- Conformance Testing
- Interoperability Testing
- Universal Server

Security Certification Levels

- How well do you protect the private key?
- 3rd-party laboratory verification
- Complemented by Biometric Component certification

Biometric Certification Program

- Empirically validate biometrics through third-party labs
- Assure that they correctly identify users regardless of biometric modality on all FIDO implementation types

Biometric Certification: Value Proposition

Authority

Requirements defined by international stakeholders

Standards

Evaluations based on ISO standards

Laboratories

International Network of Accredited Laboratories

Biometric Certification: Value Proposition

Standards-based certification program

- Developed by the FIDO Alliance, an international **authority** of stakeholders from industry, government, and subject matter experts
- Offered by FIDO-accredited **network of laboratories** worldwide

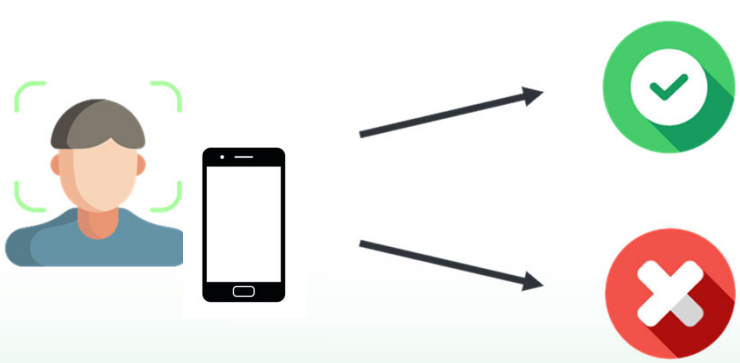
Two Biometric Certification Programs

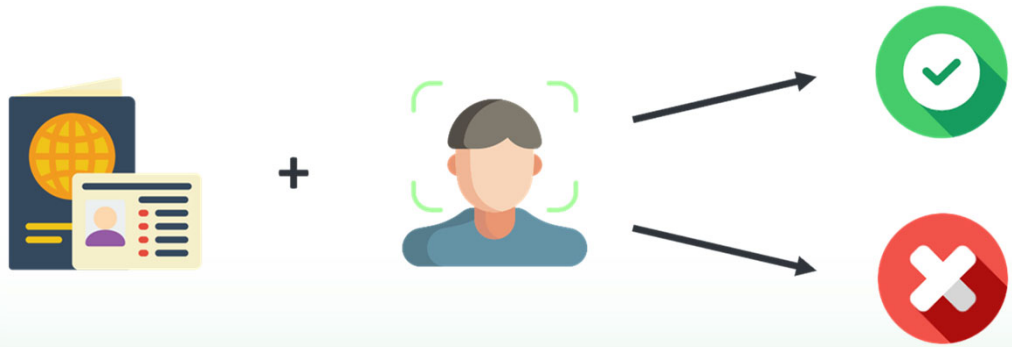
Biometric Component for Authentication

The process of ensuring same person as enrolled.

Face Verification for Remote Identity Verification (rIDV)

The process of providing sufficient information to establish an identity.





New for Biometric Component Certification (4.0)

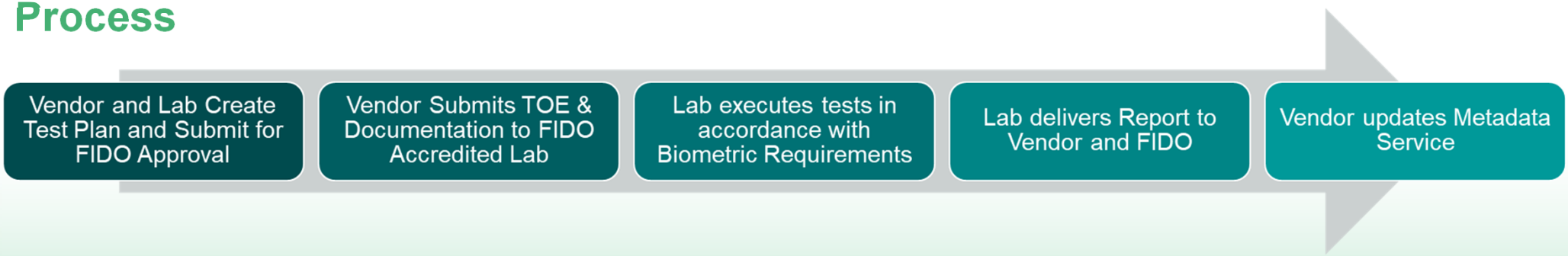
Two Options for Certification

- Biometric Component Certification
  - Evaluates FRR, FAR, and IAPAR
  - Same device from enrollment and verification
  - **Focused on FIDO authentication**
- Face Verification for Remote Identity Verification
  - Evaluates FRR, FAR, and IAPAR
  - Comparison of face on document (e.g. passport) with a selfie
  - **Focused on applications that utilize remote identity verification**

FIDO Biometric Testing and Certification Overview

- Accredited 3rd party lab testing
- Certification provides value for relying parties
- Certified products listed on FIDO website
- Vendor controls availability of comprehensive test reports
- Alignment with ISO standards

Process



Overview of Biometric Evaluation

- Live subjects used for testing
  - End-to-end system test
- Considers both genuine users (FRR) and imposter testing (FAR)
- Extensive spoof testing (IAPAR)
- Evaluations based on ISO-standards
  - FIDO Profile included in ISO 19795 Part 9
  - FIDO Profile to be included ISO 30107 Part 4 (in process)

Snapshot of Requirements- Biometric Component Certification

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%

Snapshot of Requirements
Face Verification for rIDV

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	Optional at <= 1/10000	Mandatory at <= 1/10000	Optional at <= 1/10000

Under development

Performance Differentials - Optional Certification

- Address significant concern around bias and fairness in biometric recognition
- Available for:
  - Biometric Component: Levels 1+ and 2+
  - Face verification for rIDV: Level 2 increased to 245 subjects
- Performance requirements for each demographic sub-group
  - Age - 3 groups (18-30; 31-50; >50)
  - Gender - 2 groups (Male, Female, Other)
    -Other is an option, but will not be analyzed due to low sample size
  - Monk Skin Tone – Combined to 3 groups

https://skintone.google/the-scale

Spoof Type Triaged by Attack Potential		**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, mobile phone display, deep fake display (easy)	paper printout of iris image, mobile phone display of iris photo	replay of audio recording
	Source of biometric characteristic: easy to obtain	lift of fingerprint off the phone	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), deepfake display (medium)	video display of an iris (with movement /blinking); paper printout w/ contact lens/doll eye	replay of audio recording of specific passphrase, voice mimicry, voice synthesis (easy)
	Source of biometric characteristic: moderate	Lift of latent print from elsewhere, stolen fingerprint image Cooperative molds - out of scope	video of subject, high quality photo	video of subject, high quality photo	recording of voice of specific phrase
Level C	**Time**: >7days **Expertise**: expert(s) **Equipment**: specialized. bespoke	3D printed spoofs	silicon masks, theatrical masks, deepfake display (hard)	contacts lens or prosthetic with a specific pattern	voice synthesizer (sophisticated)
	Source of biometric characteristic: difficult	3D fingerprint information from subject	3D face information from subject	high quality photo in Near IR	multiple recordings of voice to train synthesizer

PAD Testing – PAI Species

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

Requirement related to Injection Attacks

In order to address injection attacks as an attack vector for face verification 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 around the TOE to protect from injection and replay attacks.

Tester: The FIDO certified laboratory shall verify the documentation meets the requirement.

Alignment with ISO Standards

Terminology

ISO/IEC 2382-37:2022 Information technology — Vocabulary — Part 37: Biometrics

Presentation Attack Detection

ISO/IEC 30107-3:2023 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting

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

-Will include FIDO Annex, to be published 2024

Performance (e.g. FRR, FAR)

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

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

-Includes FIDO Annex

Bias (differentials due to demographics)

ISO/IEC 19795-10:2024 Information technology — Biometric performance testing and reporting — Part 10: Quantifying biometric system performance variation across demographic groups (expected)

Overview of the program

https://fidoalliance.org/certification/biometric-component-certification/

Biometric Certification Policy

https://fidoalliance.org/specs/biometric/certificationpolicy/

Certification Requirements

https://fidoalliance.org/specs/biometric/requirements/

List of accredited laboratories:

https://fidoalliance.org/certification/biometric-component-certification/fido-accredited-biometric-laboratories/