iBeta
BIOMETRICS TESTING

IBETA BIOMETRICS

ISO PAD AND FIDO TESTING COMPARISON 2022

PAD Testing: ISO vs FIDO

Two of the most popular testing services that iBeta offers are **ISO 30107** compliance, and **FIDO Biometrics Component Certification**. To prevent confusion, we here define the two and provide some details on the differences between them.

In a broad overview, these two testing protocols entail:

- The **ISO 30107** standard establishes two main levels of Presentation Attack Detection (PAD) testing, the results of which are internationally accepted as conforming with security standards.

- **FIDO Biometric Component Certification** also has two main levels of PAD testing, and includes performance testing at each level, which ISO 30107 testing does not. FIDO certification is accepted by a large and growing number of security-focused corporations.

ISO 30107 — PAD Testing

ISO (the **International Organization for Standardization**) is an independent, non-governmental organization through which 165 member countries voluntarily coordinate a wide range of technical and safety standards. Biometrics PAD (Presentation Attack Detection) testing, which evaluates an application's ability to detect imposters attempting to access a biometric security system, is just one of the many ISO standards. Most business entities, and some governmental bodies, require **ISO 30107** testing conformance in the biometrics products they consider for integration with their own systems. The compliance testing to this standard is a proven method to establish a well-accepted and industry-wide level of biometrics technology capability.

ISO conformance testing has two main modes: **liveness-only**, and **full-system**. Both modes involve the creation of PAIs (presentation attack instruments) such as masks, which are presented to the system in an attempt to penetrate its security safeguards. However, the two modes use different metrics:

ISO PAD Modalities

FACE

FINGERPRINT

IRIS

PALM

VOICE

Liveness-only testing evaluates a biometrics system's ability to differentiate between a bona fide presentation (a living human being) and an attack (an artefact such as a mask) but does not test its ability to identify an individual. It depends on the following four metrics:

- **APCER — Attack Presentation Classification Error Rate**. System penetrations for liveness-only tests are measured by APCER, the proportion of attack presentations using the same PAI species that are incorrectly classified as bona fide presentations in a specific scenario (the system erroneously identifies a non-living artefact as alive).

- **APNRR — Attack Presentation Non-Response Rate**. APNRR represents the proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem (system does not recognize the artefact).

- **BPCER — Bona Fide Presentation Classification Error Rate**. BPCER represents the proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario (the system erroneously identifies a living person as non-living).

- **BPNRR — Bona Fide Presentation Non-Response Rate**. BPNRR represents the proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem (system does not recognize the living person).

Full-system, or **matching testing**, evaluates a biometrics system's ability to correctly validate an individual enrolled in the system. It depends on the following three metrics:

- **IAPAR — Imposter Attack Presentation Attack Rate**. System penetration for full-system testing is measured by IAPAR, the proportion of attack penetrations using the same PAI species that result in acceptance by the system (the system erroneously identifies an attack as a specific enrolled individual).

- **FNMR — False Non-Match Rate**. FNMR represents the proportion of bona fide presentations incorrectly rejected by the system (the system erroneously fails to validate an enrolled individual).

- **FMR — False Match Rate**. FMR represents the proportion of bona fide presentations that are falsely declared to match a different bona fide presentation (the system erroneously identifies a living person as a different living person).

iBeta is accredited to test to the ISO 30107 (-1, -3, and -4) standards which have been accepted by the National Institute of Standards and Technology (NIST). ISO 30107-1 is the framework that lays out the terms and definitions. ISO 30107-3 describes the principles and methods for testing PAD mechanisms. This standard includes both local and cloud-based biometric solutions. ISO 30107-4 is a standard that is strictly for testing a full-system on mobile devices with local biometric recognition.

iBeta's accredited biometrics testing lab provides testing that meets ISO conformance requirements at **Level 1** and **Level 2**. **PAD Level 1** is designed to test against basic/layman level attacks, and **PAD Level 2** is designed to test against more sophisticated attackers with more knowledge and access to specialized materials and equipment.

<table>
<tr><th colspan="7">PAD LEVEL 1 – ISO Conformance</th></tr>
<tr><th>Type</th><th>Length of project</th><th># of subjects</th><th># of attack species</th><th>Allowable cost of material per species</th><th>Total # of presentations</th><th>Limit of penetrations allowed</th></tr>
<tr><td>Liveness only</td><td>4–6 weeks</td><td>10</td><td>6</td><td>$30</td><td>900</td><td>0% penetration rate allowed</td></tr>
<tr><td>Full-System 1:1</td><td>4–6 weeks</td><td>6</td><td>6</td><td>$30</td><td>360</td><td>0% penetration rate allowed</td></tr>
<tr><td colspan="7">Additional: PAD Level 1 must be completed before PAD Level 2 can be attempted. Typical PAD Level 1 attack species include photographs, paper masks, and short videos displayed on a smartphone or laptop screen.</td></tr>
<tr><th colspan="7">PAD LEVEL 2 – ISO Conformance</th></tr>
</table>

Type	Length of project	# of subjects	# of attack species	Allowable cost of material per species	Total # of presentations	Limit of penetrations allowed
Liveness only	6–8 weeks	10	5	$300	750	1% penetration rate allowed
Full-System 1:1	6–8 weeks	6	5	$300	300	1% penetration rate allowed
Additional: PAD Level 1 must be completed before PAD Level 2 can be attempted. Typical PAD Level 2 attack species include silicon, latex, or resin masks, and 3D animation software.						

FIDO Alliance Biometric Component Certification

The **FIDO** ***(Fast IDentity Online)*** **Alliance** is an organization composed of and supported by multiple large security-focused business and technology companies; it is focused on creating standards for authentication that reduces reliance on passwords, driven by the current business needs. FIDO authentication processes include multiple technologies for gathering biometric information.

The two-step process for FIDO Biometric Component Certification requires online and offline lab testing with an organization such as iBeta. FIDO testing includes both **PAD testing**, in which a biometrics system is tested for its resilience against attacks in a laboratory setting, and **performance testing**, in which a biometrics system undergoes mass testing in a population mirroring real-world conditions.

FIDO testing is **full-system/matching testing**, which evaluates a biometrics system's ability to correctly validate an individual enrolled in the system. It depends on the following four metrics:

- **IAPAR — Imposter Attack Presentation Attack Rate**. System penetration for full-system testing is measured by IAPAR, the proportion of attack penetrations using the same PAI species that result in acceptance by the system (the system erroneously identifies an attack as a specific enrolled individual).

- **FAR — False Accept Rate**. FAR represents the proportion of bona fide presentations that are falsely declared to match a different bona fide presentation (the system erroneously identifies a living person as a different living person).

- **FNMR — False Non-Match Rate**. FNMR represents the proportion of bona fide presentations incorrectly rejected by the system, including instances in which the bona fide cannot be detected at all (the system erroneously fails to validate an enrolled individual, by either failing to detect them or failing to match to their enrollment in a database). It includes FRR, defined below.

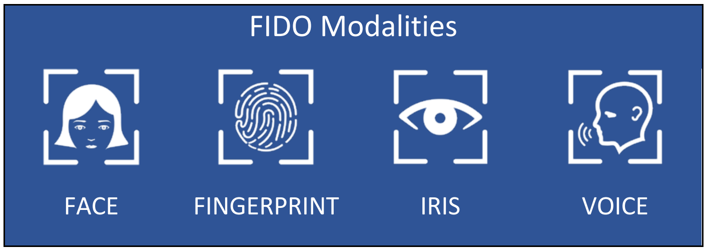
- **FRR — False Reject Rate**. FRR is the proportion of bona fide presentations that are incorrectly rejected by the system (the system correctly detects a living person, but erroneously fails to match them against to their enrollment in a database).

FIDO-permitted attack species on Level A are similar to those in ISO PAD Level 1 (e.g., photographs), and FIDO-permitted attack species on Level B are similar to those in ISO PAD Level 2 (e.g., latex masks).

FIDO Certification

Length of project	**# of subjects**	**# of attack species**	**Species requirements**	**Total # of presentations (PAD)**	**Limit of penetrations allowed**
2–3 months for PAD Level A, Level B, and performance testing	15	14 (6 level A and 8 level B), 4 of which must be tailored to system	Standard equipment, layman level of expertise (Level 1) Specialized equipment, proficient level of expertise (Level 2)	2100	15% penetration rate allowed (Level 1) 7% penetration rate allowed (Level 2)

An evaluation with an IAPAR of less than or equal to 15% will meet Level 1 requirements. An evaluation with an IAPAR of less than or equal to 7% will meet Level 2 requirements. This is determined after the completion of the test.



Frequently Asked Questions

Choosing ISO PAD or FIDO

The decision of which method to use is often driven by the practical application of the biometrics technology and the business model of the company creating it. For companies trying to sell their technology to banking or other financial institutions, those institutions will indicate which type of testing they require. For those companies developing a product to take to market themselves, they must assess the needs of the market and their competition to determine which path to take. Obviously, the FIDO route is more rigorous and can inspire more confidence in the product, given the addition of performance testing and the combining of the two levels of PAD testing. Companies developing biometrics technology need to carefully analyze their market and who they intend on selling to. If your organization is still in doubt about what is most appropriate for your product, the iBeta biometrics team's expertise is available for further assistance.

Can our product become ISO/IEC certified through your PAD testing?

No. ISO standards do not include an established set of metrics or limit that indicate "certification." NIST (the National Institute of Standards and Technology), the governmental body that oversees all US-based ISO biometrics lab accreditation, requires that neither iBeta nor our vendors claim that a biometrics system has been certified, approved, or endorsed by ISO standards.

What iBeta can provide is PAD testing in conformance and/or in compliance with ISO standards, and our clients must indicate this in their own documentation. ISO conformance or ISO compliance is the level of quality that most commercial and governmental bodies will accept for biometrics products they want to integrate into their existing systems.

iBeta does offer certification testing in other areas that use certification as their standard, such as FIDO, MasterCard, DEA EPCS, and Google Android.

Our company would like to choose which kinds of imposter attacks are used in testing. Can you test using the attacks we specify?

No. iBeta does need to independently establish which imposter attacks are used in testing, and they cannot be chosen by clients. Because so many different methodologies are used in configuring biometric systems, iBeta determines through the readiness review process which species of attack are relevant and applicable for each product it tests.

Why does iBeta use the specific numbers, repetitions, and sequences of imposter attacks and bona fide presentations during its testing process?

Conformance and certification standards for testing are established by the relevant accreditation bodies, and iBeta's testing methods have been approved by these same bodies. For each series of tests, we use the approved methods most appropriate for the biometrics system being reviewed, based on our industry experience.

Will the testing be any harder for our biometrics system compared to that performed for other vendors?

No. iBeta treats all vendors equally. The species of attack used in testing are tailored to each vendor's specific system, but all vendors are tested to the same current standard at the time of testing.

Summary

Two well-known forms of testing biometric technology for accuracy are ISO/IEC 30107 compliance and FIDO Biometric Component Certification. They entail similar testing protocols, in terms of conducting presentation attack detection. The FIDO Biometric Component Certification process includes the added component of testing the performance of the biometric technology, as well as always requiring sophisticated attack methods.