

Identity.io Achieves ISO/IEC 30107-3 Level 2 PAD Compliance with Perfect Score Through NIST-Accredited Testing

Identity.io is the only ISO/IEC 30107-3 Level 2 PAD compliance certified mobile biometric vendor with full on-device processing.

DOVER, Del. — November 4, 2025 — Identity.io, a leader in biometric identification, today announced it achieved ISO/IEC 30107-3 Level 2 PAD (Presentation Attack Detection) compliance with a perfect score for its Face SDK v6.3.0 application. With this achievement, Identity.io is the only mobile biometric vendor certified at this level offering both server based and full on-device liveness processing, equally with very robust performance.

Independent testing by iBeta Quality Assurance, accredited by NIST/NVLAP, conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-3. The testing consisted of 1,500 attempted attacks using silicone masks, 3D-printed faces, latex masks and AI deepfakes against the Identity.io platform. On a Samsung Galaxy S20 running Android 12 and an Apple iPhone 15 running iOS 17.5.1, Identity.io's technology achieved zero fake acceptances and near-zero real user rejections (1 out of 550). This test is a refresh of a previous third party liveness certification done by the company several years ago with FIDO-certified lab IDIAP Research Institute.

"Fraud is a 20-billion-dollar problem. Deepfakes and sophisticated spoofing attacks are rising at an alarming pace and make it extremely difficult to decipher what's real from what's fake," said Jesus Aragon, CEO and Founder of Identity.io. "Technology like our Face SDK that's proven to keep pace with next-level spoofing attacks through testing under these types of federal standards—with zero successful attacks and near-zero user friction—will shape government's ability to protect against attacks of the future."

Whether identifying and tracking missing persons or providing public safety at large events like the upcoming World Cup and Olympics, there are numerous applications for facial biometrics technology in government and law enforcement communities.

"However, PAD protection alone is not enough," said Aragon. "At Identity.io, we've excelled in providing protection against all forms of digital attacks, whether image injection through emulators, virtual cameras, app cloning, memory hooks and more. We'll continue to stay ahead of all types of advanced threats."

In addition to face liveness and authentication, Identity.io's touchless fingerprint technology uses a standard smartphone rear camera and LED flash to capture clear, high-quality fingerprints without physical contact. Liveness for this technology has also been validated by a third party lab with perfect scoring. This allows users to instantly identify an individual using the front or rear device camera—indoors, outdoors and even in low-light environments. With on-device processing, Identity.io's mobile facial and finger recognition software guarantees

smooth performance and high-quality image capture, ensuring interoperability with third-party systems, like government or corporate matchers.

To learn more about Identity.io and its industry-leading biometrics technology, visit <http://identity.io>.

About Identity.io

Headquartered in the US with offices in Brazil, Mexico, Spain and India, Identity.io is the global reference in digital identity verification using touchless mobile biometrics. At Identity.io we believe in multi-factor authentication, while advocating the need to replace traditional methods of identity verification using passwords, tokens or OTPs (One Time Passwords), which do not guarantee the user's identity. At Identity.io we work with institutions to secure identity in their business processes by using touchless biometrics from users' mobile devices. Our liveness authentication protection makes biometrics secure and deployable on a large scale. For more information, visit <https://identity.io>