28 July 2026

To whom it may concern,

iBeta Quality Assurance conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-3. iBeta is accredited by NIST/NVLAP (NVLAP Lab Code: 200962) to test and provide results to this PAD standard (certificate and scope may be downloaded from the NVLAP website).

This testing was conducted with Identy.io's Finger AI v1.0.967 application, derived from the same Vendor's Finger SDK v8.1.0 and supported by backend server component finger-identy-web-1. The application was installed on a Samsung Galaxy S20 running Android 12 and an Apple iPhone 15 running iOS 17.2.1. iBeta conducted liveness testing from 13 July to 28 July 2026.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create artefacts of the genuine biometric for use in the presentation attack. The subjects for the test effort were cooperative – meaning that they were willing and able to provide any and all biometric samples, including high-quality photos and videos of their likeness. The test time for each PAD test per Presentation Attack Instrument (PAI) was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method was to apply 1 bona fide subject presentation that alternated with 3 artefact presentations such that the presentation of each species consisted of 150 Presentation Attacks (PAs) and 50 bona fide presentations, or until 8 hours had passed. Successful results were shown to the tester via the messages "Successfully Verified", "Unsuccessfully recognized, try again", "Verification Failed", or "Authentication Unsuccessful"; unsuccessful attempts were shown to the tester via the messages "Something is weird, we need to retake the picture" or "Picture quality failed, we need to retake the picture."

iBeta was not able to gain a liveness classification with the presentation attacks (PAs) on Identy.io's Finger AI v1.0.967 application over a total of 1800 attacks (900 per device), resulting in an Attack Presentation Classification Error Rate (APCER) of 0%. The Bona Fide Presentation Classification Error Rate (BPCER) was also calculated and may be found in the final report.

Identy.io's Finger AI v1.0.967 application, derived from the same Vendor's Finger SDK v8.1.0 and supported by backend server component finger-identy-web-1, was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and found to be in compliance with Level 1.

Best regards,

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
(303) 627-1110 ext. 182
RBorgstrom@ibeta.com