iBeta
QUALITY ASSURANCE

5 July 2024

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 Testing 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 Advance Intelligence's Liveness Detection v3.1.6.1 and v3.1.6.5 on a Samsung Galaxy S22 running Android 12, and Liveness Detection v3.1.5 on an Apple iPhone 12 running iOS 15. iBeta conducted active liveness detection testing on these applications and their backend cloud components from 12 June to 5 July 2024.

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 facial images. The test time for each PAD test per PAI was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method involved enrolling subjects and having them authenticate five times successfully. Six species of presentation attacks (PAs) were then attempted ten times each per subject. A successful match would state "Pass," and a failure message stated, "Attack Behavior." A total of 720 presentation attacks were attempted, with 360 attacks occurring on each device. At the conclusion of the PAD testing, the subject returned and authenticated five times successfully to verify that the application was still able to recognize the genuine subject.

iBeta was not able to gain unauthorized access with the PAs, yielding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Accept Rate (IAPAR) of 0% on both Samsung Galaxy S22 and Apple iPhone 12. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The applications provided by Advance Intelligence, Liveness Detection v3.1.6.1 and v3.1.6.5 (Android), and Liveness Detection 3.1.5 (iOS), were tested with their backend components by iBeta as biometric facial recognition systems to the ISO 30107-3 Biometric Presentation Attack Detection Standard and were found to be in compliance with Level 1.

Best regards,

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
rborgstrom@ibeta.com
303.627.1110 extension 182