29 August 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 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 Veriff's Veriff Biometric Liveness v7.1.0 application and its backend cloud component Standard-face-match-iBeta-liveness-test-v16, installed on an iPhone 15 running iOS 17.5.1. iBeta conducted passive liveness detection testing from 5 August to 29 August 2024.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized mid-level methods to create an artefact 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 biometric facial samples. The test time for each PAD test per Presentation Attack Insturment (PAI) was limited to 24 hours. This is considered a Level 2 PAD test effort (second of three levels).

The test method involved enrolling subjects and having them authenticate five times successfully. Five species of presentation attacks (PAs) per subject were then attempted ten times each, with six different species used over the course of the testing. The PAs were presented to the application, and testers then reviewed an online dashboard for results. The online dashboard showed "Approved" for a successful attempt, and "Declined" for an unsuccessful attempt. There were 300 presentation attacks conducted over the entire test effort. 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 presentation attacks (PAs) on the Apple iPhone 15. With 10 PAs for each of 5 species per subject, the total number of attacks was 300, and the Imposter Attack Presentation Accept Rate (IAPAR) was 0%. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

Veriff's Veriff Biometric Liveness v7.1.0 application and its backend cloud component Standard-face-match-iBeta-liveness-test-v16, evaluated on an Apple iPhone 15 running iOS 17.5.1, were tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and were found to be in compliance with Level 2.

Best regards,

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