16 September 2020

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 the Digital Onboarding Toolkit (DOT) passive liveness application – Android version 3.0.0 and iOS version 2.1.0(1). Testing was conducted from 21 August through 04 September 2020 on two smartphones considered mid-level (iPhone 8 with iOS 13.6 and Google Pixel 2 with Android 8.1.0).

The test method was designed to simulate user enrollment into a biometric authentication system. This test did not perform matching and was purely a test of liveness detection effectiveness. 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 a 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, 2D and 3D paper masks/photos and videos of their likeness to allow for the creation of the artefacts.

The test time for each PAD test per species 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 alternated with 3 presentations of each species resulting in 150 Presentation Attacks (PAs) and 50 bona fide presentations per artefact per device. The application displayed a successful message that stated "Status: Passed" for the bona fide as well as a “Status: Rejected” message for the artefact.

On both the iPhone 8 and Google Pixel 2 used in the test, iBeta was unable to gain a liveness classification (simulated enrollment) with a presentation attack of 150 times with each species of attack per device. With 150 transaction attempts for each species per device, the total number of attacks for both devices were 1800 and the Attack Presentation Classification Error Rate (APCER) was 0%. The Bona Fide Presentation Classification Error Rate (BPCER) was also calculated and may be found in the final report.

The passive liveness anti-spoofing capability provided by Innovatrics in their DOT application was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 1 on both the iPhone 8 and Google Pixel 2.

Best regards,

Gail Audette
iBeta Quality Assurance Biometric Program Manager
(303) 627-1110 ext. 182
GAudette@ibeta.com