26 April 2021

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 2.2 and iOS version 4.0. The DOT is a digital platform for omnichannel onboarding through web and native Android and iOS applications. The tested solution consisted of on-device passive liveness detection on the Android and iOS devices (without the need for internet connection). Testing was conducted from the 9th of April to the 20th of April 2021 on two smartphones (Google Pixel 2 with Android 8.1.0 and iPhone 10 with iOS 14.2).

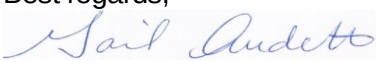
Testing was conducted in accordance with the contract for a level of spoofing technique that utilized materials available for under $300 (USD), and which artefacts of the genuine biometric could be created in less than 24 hours, for use in the presentation attack. The subjects for the test effort were cooperative – meaning that they were willing and able to provide any and all biometric samples. The test time for each PAD test per subject was limited to 24 hours. This is considered a Level 2 PAD test effort (second 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 10 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 1500 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 application was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 2 on the iPhone 10 and Google Pixel 2.

Best regards,



Gail Audette
iBeta Quality Assurance Director of Biometrics
(303) 627-1110 ext. 182
GAudette@ibeta.com