08 April 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 ImageWare® Systems, Inc. GoVerifyID® application - iOS version 7.5.81 and Android version 7.5.20.3. The application uses passive liveness detection and the Biointellic^{TM} anti-spoofing technology. Liveness is assessed on a cloud component GoMobile Interactive® Version 2.2.9.0000.

Testing was conducted from 23 March through 02 April, 2020 on two smartphones: a Google Pixel 3 XL with Android 13.3.1 and an iPhone 7 with iOS 10.0.

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; however, the GoVerifyID® anti-spoofing uses the same algorithms of Biointellic^{TM} during the enrollment, verification, and authentication processes. 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 and videos of their likeness. The test time for each PAD test per subject was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method was to apply one bona fide subject presentation that alternated with 3 presentations of each species resulting in 90 Presentation Attacks (PAs) and 30 bona fide presentations per species per device. The application displayed a green 'Success' messages for successful liveness confirmation or a 'Face not found' message for an unsuccessful liveness confirmation.

On both smartphones used in the test, iBeta was not able to gain unauthorized access (simulated enrollment) with a presentation attack of 180 times with each of species of attack. With 180 transaction attempts for each species, the total number of attacks were 1080 and the Attack Presentation Classification Error Rate (APCER) was 0%.

The Biointellic^{TM} anti-spoofing capability provided by ImageWare® Systems, Inc. in their GoVerifyID® app and GoVerifyID® SDK (both on Android and iOS) along with their GoMobile Interactive® cloud SaaS was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 1.

Best regards,

Gail Audette

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