22 May 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 IDEMIA Web Capture® SDK - version 3.10. Capture SDK is part of Idemia Global Identity offer that allows omni-channel acquisition through web and native Android/iOS applications. The solution uses passive liveness detection. Testing was conducted from 4 May through 15 May, 2020 on one smartphone considered mid-level (iPhone 8 with iOS 12.1.4.).

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 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, including high resolution photographs and molds of their faces for masks. The test time for each PAD test per species of attack was limited to 24 hours. This is considered a Level 2 PAD test effort (second of three levels).

The test method was to apply one bona fide subject presentation that alternated with 3 presentations of each species resulting in 150 Presentation Attacks (PAs) and 50 bona fide presentations per species. The application displayed a 'You passed liveness' message for successful liveness confirmation or a 'Liveness failed' message for an unsuccessful liveness confirmation.

On the iPhone 8 used in the test, iBeta was not able to gain unauthorized access (simulated enrollment) with a presentation attack of 150 times with each species of attack. With 150 presentation attacks for each species, 750 total attacks were presented 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 anti-spoofing capability provided by IDEMIA in their Web Capture® SDK was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 2.

Best regards,

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