26 December 2019

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 face authentication system, containing Idemia SmartBioSdk® SDK V4.20.0 (2.3.7), production version currently commercially available for iOS, Android and Web. This application verifies the user liveness through active liveness. The application instructs the user to follow and hold a position displayed by three dots. Testing was conducted from 11 December through 20 December 2019 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 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 2 PAD test effort (second of three levels).

The test method was to apply one bona fide subject presentation that alternated with 3 presentation attacks (PAs) of each species resulting in 150 Presentation Attacks (PAs) and 50 bona fide presentations per artefact. (PA). The test method was designed to simulate user enrollment into a biometric authentication system. As each attempt was conducted, the application would display 'Success', capture timeout or '…, possible of attack' under 'Local liveness verification'.

On the smartphone used in the test, iBeta was not able to gain unauthorized access (simulated enrollment) with a presentation attack 150 times with each of 5 species of attacks. With 150 attempts for each species, the total number of attacks were 750 and the Attack Presentation Classification Error Rate (APCER) was 0%.

The Bona Fide Non-Response Rate (BPNRR) and the Bona Fide Presentation Classification Error Rate (BPCER) were also calculated and may be found in the final report.

Best regards,

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