30 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 ID R&D IDLive™ Face Version 1.16.0 facial recogntion biometric system for iOS and Android. The application leverages single frame passive liveness detection and requires no user interaction. Testing was conducted from the 17th of September through to the 28th of September 2020 on two smartphones considered mid-level (Samsung Galaxy S8 Plus with Android 8.0.0 and iPhone 6S Plus 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 more expensive and robust 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 species was limited to two to four days. This is considered a Level 2 PAD test effort (second of three levels).

The test method for each device 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 messages with a green 'Live' message for successful liveness confirmation or a red 'Spoof' for an unsuccessful liveness conformation.

On each 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 1500 (750 per device) and the Presentation Attack (PA) success rate 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

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