23 August 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 Incode Omni face authentication system (containing the highfive® v1.0 applciation that was tested), production version currently available for iOS, Android, desktop and mobile web. The application leverages LiveBeam, Incode's proprietary liveness technology, which is passive liveness detection and requires no user interaction. Testing was conducted from 15 July through 24 July, 2019 on two smartphones considered mid-level (Samsung Galaxy S8 with Android 8.0.0 and 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 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 300 Presentation Attacks (PAs) and 100 bona fide presentations per artefact. The application displayed messages with a green lock for successful liveness confirmation or a red lock for an unsuccessful liveness conformation.

On the smartphones used in the test, iBeta was not able to gain unauthorized access (simulated enrollment) with a presentation attack 300 times with each of 5 species of attacks. With 300 attempts for each species, the total number of attacks were 1,500 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
iBeta Quality Assurance Biometric Program Manager
(303) 627-1110 ext. 182
GAudette@ibeta.com