19 October 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 IDmission 7.3.4.6 passive liveness application developed by ID Mission. The tested solution consisted of on-device passive liveness detection on the Android device (without the need for internet connection). Testing was conducted from 7 October through 14 October 2020 on one smartphone considered mid-level (Google Pixel with Android 10).

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. The test time for each PAD test per subject was limited to 24 hours. This is considered a Level 2 PAD test effort (second of three levels).

The test method was to apply 1 bona fide subject presentation alternated with 3 presentations of each species resulting in 150 Presentation Attacks (PAs) and 50 bona fide presentations per artefact per device. The application displayed a successful message that stated "Success: Face Detected" for the bona fide as well as a “Live face not detected. Please try again” message for the artefact.

On Google Pixel used in the testing, iBeta was unable to gain a liveness classification (simulated enrollment) with a presentation attack of 150 times with each species of attack per device. With 150 transaction attempts for each species, the total number of attacks were 750 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 passive liveness anti-spoofing capability provided by ID Mission in their IDmission application was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 2 on the Google Pixel.

Best regards,

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