17 August 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 Knomi® S Live application – FaceLiveness version 2.7.1.1 (Android) and version 2.7.1 (iOS). The application uses passive liveness detection. Testing was conducted from 28 July through 13 August 2020 on two smartphones considered mid-level (iPhone 8 with iOS 13.6 and Galaxy S8 with Android 8.0.0).

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 and the artefacts consisted of latex masks, inexpensive silicone masks, a mannequin, 3D animation software, and handmade masks from 2D photos. This is considered a Level 2 PAD test effort (second of three levels).

The test method was to apply 1 bona fide subject presentation that 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 "Transaction complete - Facial Liveness: Live" for the bona fide as well as a “Transaction complete - Facial Liveness: Not Live” message for the non-live person and live person.

On both the iPhone 8 and Galaxy S8 used in the test, 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 per device, the total number of attacks for both devices were 1500 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 Knomi® S Live anti-spoofing capability provided by Aware, Inc., in their Knomi® S Live application was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and passed Level 2 on both the iPhone 8 and Galaxy S8.

Best regards,

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