22 May 2023

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 Facia's iOS SDK v2.2.0 application on an iPhone 12 Pro Max running iOS 16, as well as Facia's Android SDK v2.4.1 application on a OnePlus Nord 200 running Android 12, and the backend cloud component Facia-ML-models-0145 that supports both versions. Testing of the active liveness detection solutions was conducted from 10 May to 22 May 2023.

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 the 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 Presentation Attack Insturment (PAI) was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method was to apply 1 bona fide subject presentation that alternated with 3 artefact presentations such that each species consisted of 150 Presentation Attacks (PAs) and 50 bona fide presentations. The results were displayed for the tester on the device as "Liveness Verified" for a successful attempt or "Liveness could not be Verified" for an unsuccessful attempt.

iBeta was not able to gain a liveness classification with the presentation attacks (PAs) on either the iPhone 12 Pro Max or the OnePlus Nord 200. With 150 PAs for each of 6 species on two devices, the total number of attacks was 1800, 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.

Facia's iOS SDK v2.2.0 application on an iPhone 12 Pro Max running iOS 16, and Facia's Android SDK v2.4.1 application on a OnePlus Nord 200 running Android 12, were tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and found to be in compliance with Level 1.

Best regards,

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
(303) 627-1110 ext. 182
RBorgstrom@ibeta.com