iBeta
QUALITY ASSURANCE

7 March 2024

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 Android SDK v3.0.1 application on a OnePlus Nord 200 running Android 12, as well as Facia's iOS SDK v3.0.4 application on an Apple iPhone 12 Pro Max running iOS 16. Testing of the passive liveness solution and its backend component facia_models v955e8824d22faf56273eeb5dfa7cbd59 was conducted from 19 February to 7 March 2024.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized mid-level methods to create an artefact 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 biometric facial samples. The test time for each PAD test per Presentation Attack Insturment (PAI) 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 that alternated with 3 artefact presentations such that the presentation of each species consisted of 150 Presentation Attacks (PAs) and 50 bona fide presentations on each device, or until 24 hours had passed per device. 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 the OnePlus Nord 200 or iPhone 12 Pro Max. With 150 PAs for each of 5 species, the total number of attacks was 1,500 (750 per device), 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 Android SDK v3.0.1 application on a OnePlus Nord 200 running Android 12, as well as Facia's iOS SDK v3.0.4 application on an Apple iPhone 12 Pro Max running iOS 16, were tested by iBeta with the backend component backend component facia_models v955e8824d22faf56273eeb5dfa7cbd59 to the ISO 30107-3 Biometric Presentation Attack Detection Standard and found to be in compliance with Level 2.

Best regards,

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