30 January 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 Testing 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 Technologies, Inc. Incode Omni v1.0 application and its backend server component, smile-demo-pad:2. Two different application builds were tested: Build 221210.75 on an iPhone 12 Pro running iOS 16.0.2, and Build 2649 on a Galaxy S21 running Android 12. iBeta conducted testing from 10 January to 30 January 2023. Liveness detection was passive.

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 during 24 hours of testing per species. The process was to present an artefact to the application. Successful presentations were indicated by a "Success" message from the application, and unsuccessful presentations were indicated by a message stating either "Something went wrong" or "Poor conditions for selfie, try in another place" followed by "Failed".

During testing on iPhone 12 Pro, iBeta was unable to gain unauthorized access with the 5 species of PAs over a total of 750 attempts, resulting in an Attack Presentation Classification Error Rate (APCER) of 0%. During testing on Galaxy S21, iBeta gained unauthorized access 1 time with 1 species out of 5 over 750 attempts, resulting in an APCER of 0.67% for that species, and an APCER of 0.13% for the Galaxy S21 across all 5 species of PAs. With 150 PAs for each of the 5 species per device, the total number of attacks was 1500. The Bona Fide Presentation Classification Error Rate (BPCER) was also calculated and may be found in the final report.

Incode's Incode Omni v1.0 application and the associated smile-demo-pad:2 backend server component was tested by iBeta 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
RBorgstrom@ibeta.com
303.627.1110 extension 182