18 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 iProov application Version 7.4.1 (219), SDK Version 7.5.0 (1). Testing was conducted from 05 August through 17 August 2020 on a smartphone (iPhone 11 with iOS 13.0).

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. This is considered a Level 2 PAD test effort (second of three levels).

On the test platform, enrolled subjects authenticated five times successfully. Six species of presentation attacks (PAs) were then attempted ten times each. As each attempt was conducted, the application would generally provide instructional messages. The application would state “Ambiguous Outcome”, “Please keep still”, “Please don’t talk”, or “Ambient light too strong” prior to declaring an unsuccessful result which, in turn, corresponds to well over 250 presentation attacks over the entire test effort on the iPhone 11 (iOS 13.0). At the conclusion of the PAD testing, the subject returned and authenticated five times successfully to verify that the facial recognition application was still able to recognize the genuine subject.

iBeta was not able to gain unauthorized access with the PAs yeilding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Match Rate (IAMPR) of 0%. The bona fide False Match Rate (FMR) and False Non-Match Rate (FNMR) may be found in the final report.

The iProov anti-spoofing capability was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and passed Level 2 on the iPhone 11.

Best regards,

Gail Audette
iBeta Quality Assurance Director of Biometrics
(303) 627-1110 ext. 182
GAudette@ibeta.com