07 January 2021

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 Identomat web based application Release 12. Testing was conducted from 09 December through 23 December 2020 on a smartphone considered mid-level (iPhone 8 with iOS 13.6).

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 a 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 to allow for the creation of the artefacts.

The test time for each PAD test per species was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method involved enrolling subjects and having them authenticate five times successfully. Five 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 'Face Changed', 'Not Smile', 'Early Start Smile', and 'Early Stop Smile', prior to declaring an unsuccessful result which, in turn, corresponds to over 250 total presentation attacks over the entire test effort on the iPhone 8 (iOS 13.6). 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.

On the iPhone 8 used for testing, 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 (IAPMR) of 0%. The bona fide False Non-Match Rate (FNMR) may be found in the final report.

The Raizomat Identomat anti-spoofing capability was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 1.

Best regards,

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