iBeta
QUALITY ASSURANCE

16 April 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 Luma Liveness application iOS 2.1.44 which includes onboarding and facial recognition biometric system on a single smartphone device in conjunction with the backend Luma Liveness cloud based component version 7.F.4.3e7ac85d. Testing was conducted from 26 March through 12 April 2021 on a single smartphone (an iOS iPhone 12 Pro Max).

Testing was conducted in accordance with the contract for a level of spoofing technique that utilized materials available for under $300 (USD) and where 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).

The test method involved enrolling 6 subjects and having them authenticate 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.

A successful match would ‘Login’ the user, or a failure message that stated ‘Authorization failed’. On each device, over 300 total presentation attacks were attempted. 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 12 Pro Max 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 NEC Luma Liveness 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 2.

Best regards,

Gail Audette

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