27 February 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 ZOLOZ® Face Login SDK v18.0 for iOS. The application uses active liveness detection and a cloud based server for both liveness detection and verification. Testing was conducted from 10 February through 18 February, 2020 on two smartphones considered mid-level (iPhone 7 Plus with iOS 13.3.1 and iPhone 8 with iOS 13.3.1).

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, including high resolution photograps and molds of their faces for latex masks. The 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, six subjects enrolled and authenticated five times succesfully. Four species of presentation attacks (PAs) were then attempted five times each. As each attempt was conducted, the application would provide the following results: "Failed - capture has been terminated" and "Failed - you have failed verification". As a result, approximately 210 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.

iBeta was not able to gain unauthorized access with the PAs on the test platform 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 false match rate (FMR), false non-match rate (FNMR), Failure to Enroll (FTE) and Failure to Acquire (FTA) rates were also calculated and may be found in the final report.

Best regards,

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