



18 April 2019

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 Pte. Ltd ZOLOZ® v4.6 application currently available for iOS and Android devices. Testing was conducted from 06 March -12 April, 2019 on two smartphones considered mid-level (iPhone 8 iOS Version 11.2.2 and Google Pixel Android Version 8.1.0).

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 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 photos and videos of their likeness. The test time for each PAD test per subject was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

On each test platform, enrolled subjects authenticated five times successfully. Six species of presentation attacks (PAs) were then attempted five times each. As each attempt was conducted the application would generally provide instructional messages. The application would then state 'Failed to scan face, try again' a number of times before presenting the user with the unsuccessful authentication messages including 'Sorry, we couldn't identify you,' or 'Fail, face match failed.' As a result, approximately 900 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 either test platform yielding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Match Rate (IAMPR) for both systems of 0%.

The bona fide False Non-Match Rate (FNMR) and False Match Rate (FMR) were also calculated and may be found in the final report.

Best regards,

A handwritten signature in blue ink that reads "Gail Audette".

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