20 August 2018

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 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 FaceTec ZoOm® v6.6.0 modified from the production version currently available for iOS and Android devices to remove 2 anti-reverse-engineering mechanisms that would have caused a 5+ minute wait time for every 6 spoof attempts, as well as user deletion after 6 failed attemps in a row. Testing was conducted from 13-25 July, 2018 on two smartphones considered mid-level (iPhone 6S iOS Version 11.4 and Galaxy Note 5 Android Version 7).

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, five subjects enrolled and authenticated three times succesfully. Six species of presentation attacks (PAs) were then attempted five times each. As each attempt was conducted, the application would state to 'try again' a number of times before presenting the user with the message that the authentication was unsucessful. As a result, approximately 1500 presentation attacks were attempted. At the conclustion of the PAD testing, the subject returned and authenticated three 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 yeilding 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 non-response error rate (BPNRR), 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