30 June 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 OCR LABS Digital Identification Process V1.0 face authentication system. The application scans the photo from an ID and then records a "selfie" video for comparison to the ID image using active liveness detection on a cloud based server. Testing was conducted from 18 May through 3 June 2020 on two smartphones considered mid-level (Google Pixel 2 with Android 8.1.0 and iPhone XR with iOS 12.3.1).

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 subject 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 photographs 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 each test platform, five subjects matched successfully to the image extracted from a Western Australia Driver's License. Six species of presentation attacks (PAs) were then attempted five times each. As each attempt was conducted, the application would capture the video of the artefact and submit to the cloud-based matching engine and display 'High Risk' in the Spoof Risk determinate on the portal. As a result, over 250 presentation attacks were attempted. At the conclusion of the PAD testing, the subjects returned and matched successfully to the image from the ID to verify that the application was still able to recognize the genuine subject.

On the devices used in the test, iBeta was not able to gain unauthorized access with the PAs yielding an overall 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), 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