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 NEC Japan NEC_v1.0 facial recognition biometric system. The solution uses active liveness detection. Testing was conducted from 11 November through 19 November, 2020 on two smartphone devices (iPhone XR with iOS 12.3.1 and Galaxy S20 with Android 10).

The test method was designed to simulate user enrollment into a biometric authentication system. This test did not perform matching and was purely a test of liveness detection effectiveness. 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 a 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).

The test method was to apply one bona fide subject presentation that alternated with 3 presentations of each species resulting in 150 Presentation Attacks (PAs) and 50 bona fide presentations per species. The application displayed a 'Real' message for successful liveness confirmation or a 'Fake' message for an unsuccessful liveness confirmation.

On both smartphone devices used in the test, iBeta was not able to gain unauthorized access (simulated enrollment) with a presentation attack of 150 times with each species of attack. With 150 presentation attacks for each species, 1500 total attacks were presented and the Attack Presentation Classification Error Rate (APCER) was 0%. The Bona Fide Presentation Classification Error Rate (BPCER) was also calculated and may be found in the final report.

The anti-spoofing capability provided by NEC Japan NEC_v1.0 was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 1.

Best regards,

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