13 February 2025

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 Testing 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 RealNetworks's SAFR Scan SFR-SC100 device and SAFR SCAN Console v2.1.217. iBeta installed the software on a Windows 11 PC and conducted passive facial verification testing from 27 January to 13 February 2025.

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 facial images. The test time for each PAD test per PAI was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method involved enrolling six subjects and having them authenticate five times successfully. Six species of presentation attacks (PAs) were then attempted ten times each per subject. Successful attempts were represented by an on-screen display of "Welcome" in green and an audio response of "Access granted"; unsuccessful attempts were represented by an on-screen display of "No Access" in red and an audio response of "Access denied." A total of 360 presentation attacks were attempted. At the conclusion of the PAD testing, the subject returned and authenticated five times successfully to verify that the application was still able to recognize the genuine subject.

iBeta was not able to gain unauthorized access with the PAs, yielding an overall Presentation Attack (PA) success rate of 0%, which then equates to the Imposter Attack Presentation Accept Rate (IAPAR) of 0% with the SAFR Scan SFR-SC100 device and application SAFR SCAN Console v2.1.217. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The SAFR Scan SFR-SC100 device and SAFR SCAN Console v2.1.217 provided by RealNetworks was installed on and accessed via a Windows 11 PC, tested as a facial recognition biometric recognition system to the ISO 30107-3 Biometric Presentation Attack Detection Standard, and was found to be in compliance with Level 1.

Best regards,

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
rborgstrom@ibeta.com
303.627.1110 extension 182