20 June 2024

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 Fujitsu Frontech Ltd's PalmSecure system, consisting of a PalmSecure F-Pro device and PalmSecure SDK v02, installed on a Windows 11 PC. Testing of the passive palm vein verification solution was conducted from 11 June to 20 June 2024.

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 palm print and palm vein 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 subjects and having them authenticate five times successfully. Six species of presentation attacks (PAs) were then attempted ten times each. A successful match would state "You are [SUBJECT]", or a failure message such as "You are not [SUBJECT]" or "Invalid credentials." A total of 360 presentation attacks were attempted on the PalmSecure F-Pro device and its PalmSecure SDK v02. At the conclusion of the PAD testing, the subject returned and authenticated five times successfully to verify that the capture device and 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 overall combined Imposter Attack Presentation Accept Rate (IAPAR) of 0% on the PalmSecure F-Pro device and its associated software. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The Fujitsu Frontech PalmSecure system, consisting of a PalmSecure F-Pro device and its PalmSecure SDK v02 installed on a Windows 11 PC, was tested by iBeta as a biometric palm vein 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