iBeta
QUALITY ASSURANCE

04 March 2022

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 the Integrated Biometrics KOJAK_v3.1.2 (13900277-E00K) device using the Integrated Biometrics Kojak hardware and the PadValidation_153_Config_A software on a PC. The PAD classifier system consisted of both software (AI image processing) and hardware (electrical characteristic sensing). Testing of the fingerprint verification solution was conducted from the 22nd of February through the 3rd of March, 2022.

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 fingerprint images and cooperative molds. 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 "Hi, (subject name)", or a failure message that stated "Detected Spoof-SW=Classifier". Over 360 total presentation attacks were attempted on the KOJAK_v3.1.2 (13900277-E00K) device. 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% on both devices, which then equates to the overall combined Imposter Attack Presentation Match Rate (IAPMR) of 0% on the KOJAK_v3.1.2 (13900277-E00K) device. The bona fide False Non-Match Rate (FNMR) may be found in the final report.

The Integrated Biometrics KOJAK_v3.1.2 (13900277-E00K) solution 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,

Ryan Borgstrom
iBeta Quality Assurance Deputy Director of Biometrics
(303) 627-1110 ext. 182
RBorgstrom@ibeta.com