4 March 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 the 1Kosmos BlockID v1.10.00 Build:65C098B0 application, and its backend component, v1.10.00.08d60f3e66adbe2c2751b53ee5d2fe2cbb0161ee.1707212640. Testing was performed on a Google Pixel 4a running Android 11 and an Apple iPhone XR running iOS 16.3.1, as well as multiple Windows PCs used to access the system dashboard via Internet browser. iBeta conducted active liveness detection testing from 12 February to 4 March 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 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. Successful results were displayed on the Android and iOS devices as, “Thank you! You have successfully authenticated to log in,” and on the dashboard (accessed via Windows PCs) as a successful login. Failure results either appeared on the Android and iOS devices as “Error: Live ID authentication failed,” or were represented by the device failing to respond to the PA three times, for 30 seconds per attempt. In addition, failures resulted in the dashboard not proceeding to the successful login screen. A total of 720 presentation attacks were attempted, with 360 performed on each device. 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 overall combined Imposter Attack Presentation Accept Rate (IAPAR) of 0% on both the Google Pixel 4a and Apple iPhone XR. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The 1Kosmos BlockID v1.10.00 Build:65C098B0 application, and its backend component, v1.10.00.08d60f3e66adbe2c2751b53ee5d2fe2cbb0161ee.1707212640, were tested by iBeta as a biometric facial system to the ISO 30107-3 Biometric Presentation Attack Detection Standard and were 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