5 March 2025

To whom it may concern,

iBeta Quality Assurance conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-1 and 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 1Kosmos's BlockID v1.10.90 Build:678A6EC6 application and its backend cloud component 1.09.01.24c700778b58e26314cef0675f5c28e5358bcc8c.1717080512. Testing was performed on a Google Pixel 8 running Android 14 and an Apple iPhone 16 running iOS 18.0. iBeta conducted active liveness detection testing from 5 February to 5 March 2025.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized mid-level methods to create an artefact 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 biometric facial samples. The test time for each PAD test per Presentation Attack Instrument (PAI) was limited to 24 hours. This is considered a Level 2 PAD test effort (second of three levels).

The test method involved enrolling six bona fide subjects, who then authenticated five times each. After authentication, five species of Level 2 presentation attacks (PAs) were used for each subject. Successful results were indicated on the devices as, "LiveID verified successfully," and unsuccessful results appeared on the devices as "Error: LiveID liveness check failed." 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 unable to gain unauthorized access with either the Pixel 8 or iPhone 16 over a total of 600 transaction attempts, yielding an overall combined Imposter Attack Presentation Accept Rate (IAPAR) of 0%. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The 1Kosmos BlockID v1.10.90 Build:678A6EC6 application and its backend cloud component 1.09.01.24c700778b58e26314cef0675f5c28e5358bcc8c.1717080512, installed on a Google Pixel 8 and an Apple iPhone 16, were tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and were found to be in compliance with Level 2.

Best regards,

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