19 May 2026

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 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 ZOLOZ's ZOLOZ v1.0.0 (Native SDK) application installed on a Samsung Galaxy S23 running Android 14 and an Apple iPhone 15 Pro running iOS 18.3.2, with both installments supported by the same backend server components. iBeta conducted active liveness facial recognition testing from 15 April to 19 May 2026.

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 subjects and having them authenticate five times successfully. Five species of presentation attacks (PAs) were then attempted ten times each per subject. Successful attempts were indicated by a "Verification Result: Success" message, and unsuccessful attempts were indicated by a "Verification Result: Failure" message. 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 over a total of 600 attempts (300 per device), 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 ZOLOZ v1.0.0 (Native SDK) application. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The ZOLOZ v.1.0.0 (Native SDK) application provided by ZOLOZ, and supported by its backend server components, was installed on a Samsung Galaxy S23 and Apple iPhone 15 Pro, 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 2.

Best regards,

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