



29 September 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 UZINFOCOM's MyID/Ikat v1.0 application and its backend component myid-api-demo. Testing was performed on a Samsung Galaxy S25 running Android 15 and an Apple iPhone 16 Pro running iOS 18.0. iBeta conducted active liveness facial recognition testing from 5 August to 29 September 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 seven subjects and having them authenticate five times successfully. Five species of presentation attacks (PAs) were then attempted ten times each per subject. Results appeared on the device as "Verification completed successfully" for a successful match, "Detected artefact" or "Verification failed" or an unsuccessful attempt; a failed to acquire the PA three times for 30 seconds per attempt was also considered unsuccessful. A total of 600 presentation attacks were attempted (300 per 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 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% on both the Samsung Galaxy S25 and Apple iPhone 16 Pro. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

UZINFOCOM's MyID/Ikat v1.0 application and its backend component myid-api-demo were tested by iBeta as a biometric facial recognition system to the ISO 30107-3 Biometric Presentation Attack Detection Standard and were found to be in compliance with Level 2.

Best regards,

A handwritten signature in black ink, appearing to read "Ryan Borgstrom".

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