



24 June 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 PIPO Resource (SG)'s Veritas v2.0 (Android) application installed on a Samsung Galaxy S25 running Android 16 and PIPO Resource (SG)'s Veritas v2.1 (iOS) application installed on an Apple iPhone 16 Pro running iOS 18, with both installments supported by the same backend server components. iBeta conducted active liveness facial recognition testing from 1 June to 24 June 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 per device and having them authenticate five times successfully. Five species of presentation attacks (PAs) were then attempted ten times each per subject. Results were displayed for the tester on the device as "Authentication Successful You are [NAME]" for a successful attempt and "Liveness Check Failed" (for an unsuccessful liveness attempt) or "Authentication Failed Sorry we couldn't identify you" (for an unsuccessful identification attempt). 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 300 attempts on the Galaxy S25 and 320 attempts on the Apple iPhone 16 Pro, 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 applications. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The Veritas v2.0 (Android) and Veritas v2.1 (iOS) applications provided by PIPO Resource (SG) were respectively installed on a Samsung Galaxy S25 and Apple iPhone 16 Pro, tested as a facial recognition biometric recognition system to the ISO 30107-3 Biometric Presentation Attack Detection Standard while supported by their backend server components, 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