29 October 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 VU Security's Secure Onboarding Process v2.28.0 application (SDK v2.5.11), installed on a Samsung Galaxy S24 Ultra running Android 16 and a Redmi Note 10 5G running Android 11, and supported by its backend server components. iBeta conducted testing from 25 August to 29 October 2026.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized high-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 56 hours. This is considered a Level 3 PAD test effort (third of three levels).

The verification testing utilized 6 bona fide presentation subjects and 3 species of presentation attacks (PAs). The results were displayed for the tester on the device as "Login Success: Confidence" with a numeric score in the range of 0.7 to 0.99 for a successful matching presentation, or "Login Failure: Confidence" with a numeric score 0.69 and below for an unsuccessful matching presentation. The message "Error2024: Login fail" was also treated as an unsuccessful match result.

iBeta was not able to gain a liveness classification with the presentation attacks (PAs) on either the Samsung Galaxy S24 Ultra or Redmi Note 10. With 450 PAs for each of 3 species per device, the total number of attacks was 2,700 (1,350 per device), and the overall Impostor Attack Presentation Accept Rate (IAPAR) was 0%. The False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

VU Security's Secure Onboarding Process v2.28.0 application (SDK v2.5.11) and supporting server components were tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and found to be in compliance with Level 3.

Best regards,



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