22 April 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 v2.25.1 application (SDK v2.5.9) installed on a Samsung Galaxy S24 Ultra running Android 16 and a Redmi Note 10 running Android 11, supported by the application's backend server components. Testing of the active liveness detection solution was conducted from 19 March to 22 April 2026.

VU Security's solution had previously passed both Level 1 and Level 2 PAD testing; this retest of the solution was requested by VU Security to confirm continued conformance. Testing was conducted in accordance with iBeta's retest procedures, which contractually utilizes both simple and 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. This was a retest effort, involving a smaller number of artefacts and requiring less time than a full Level 1 or Level 2 PAD test process.

The test method involved enrolling six bona fide subjects, who then authenticated five times each, at the beginning of both Level 1 and Level 2 testing. After authentication, testing for each Level 1 subject consisted of 30 Presentation Attacks (PAs) and 10 bona fide presentations, and the testing of each Level 2 subject consisted of 50 Presentation Attacks and 10 bona fide presentations. The results were displayed for the tester on the device as a numeric score in the range of 0.7 to 0.99 for a successful matching presentation, or a numeric score 0.69 and below for an unsuccessful matching presentation. At the conclusion of the PAD testing for each level, 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 presentation attacks (PAs) on either the Galaxy S24 Ultra or Redmi Note 10 devices. There was a total of 13 artefact species used, 6 Level 1 species and 7 Level 2 species, though only 5 Level 2 species were used per subject. With 180 PAs per device during Level 1 testing and 300 PAs per device during Level 2 testing, the total number of attacks was 960, and the Imposter Attack Presentation Accept Rate (IAPAR) was 0%. The False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

The VU Security Secure Onboarding Process v2.25.1 application (SDK v2.5.9) and its supporting backend components were tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and were found to remain in compliance.

Best regards,

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