21 December 2021

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® Secure Onboarding Process version 1.2.5.1 on two Samsung devices associated with the associated server version 1.29.0 (VU® Onboarding API). Testing of the active liveness detection onboarding solution was conducted from the 2nd of December to the 21st of December 2021 on two smartphones (Samsung Galaxy S10 and S10+ running Android 11 and 10, respectively).

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create artefacts 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 photos and videos of their likeness. The test time for each PAD test per PAI was limited to 24 hours. This is considered a Level 2 PAD test effort (second of three levels).

The test method involved enrolling subjects and having them authenticate five times successfully. Six species of presentation attacks (PAs) were then attempted ten times each. For one (1) subject, the latex mask was not tested and only one (1) subject had a resin mask. As each attempt was conducted, the application would generally provide instructional messages. The application would state 'Autenticacion fallida: Login Fail', defining an unsuccessful result which, in turn, corresponded to over 350 total presentation attacks over the entire test effort on the Samsung Galaxy S10 and S10+. At the conclusion of the PAD testing, the subject returned and authenticated five times successfully to verify that the Presentation Attack Detection application was still able to recognize the genuine subject. On each smartphone used in the test, iBeta was only able to gain unauthorized access with a single presentation attack resulting in a system IAPMR of 0.9%.

The Secure Onboarding Process version 1.2.5.1 was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 2.

Best regards,

Gail Audette
IBeta Quality Assurance Director of Biometrics
(303) 627-1110 ext. 182
GAudette@ibeta.com