14 April 2025

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 Microsoft's Azure Cognitive Services Face Liveness and its backend component Liveness Model Version 2024-11-15 on an Apple iPhone 14 Pro Max running iOS 18.2. Testing of the liveness verification solution was conducted from 5 March to 15 April 2025.

Microsoft's liveness verification solution had previously passed both Level 1 and Level 2 PAD testing; this retest of the solution was requested by Microsoft 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. After authentication, six species of Level 1 presentation attacks (PAs) and five species of Level 2 PAs were used for each subject. Successful results were indicated on the devices as, "Pass," and unsuccessful results appeared on the devices as "Fail." 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.

On the iPhone 14 Pro Max, iBeta was not able to gain a liveness classification with the presentation attacks (PAs). There was a total of 13 artefact species used, six Level 1 species and seven Level 2 species, though only five Level 2 species were used per subject. With 5 PAs for each of the 11 species used per subject, the total number of attacks was 330, yielding an overall combined Imposter Attack Presentation Accept Rate (IAPAR) of 0%. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

Microsoft's Azure Cognitive Services Face Liveness and backend Liveness Model Version 2024-11-15 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