



Biometrics Identity Experience & Evaluation Laboratory



## Demonstration of Compliance

Issued to *Makesure*

for the test reports *23-024-TR-10* and *24-024-TR-20* for  
ISO/IEC 30107-3 compliant presentation attack detection (PAD) evaluation of  
*RatifyID version 1.0.0 (app build 34)* -Item under test (IUT)

To whom it may concern,

BixeLab is a biometric testing laboratory accredited by National Institute of Standards and Technology (NIST) under the National Voluntary Laboratory Accreditation Program (NVLAP) with testing Lab code: 600301-0 ([certificate and scope](#) may be downloaded from the NVLAP website). BixeLab also conforms to the requirements of ISO/IEC 17025:2017 (General Requirements for Competence of Testing and Calibration laboratories). BixeLab shall not be held liable for any interpretations, decisions, or actions based on the information contained in this confirmation letter. BixeLab does not certify or make any claims regarding the performance of the IUT outside of the described context in this letter.

BixeLab undertook an ISO/IEC 30107-3 compliant presentation attack detection evaluation of the Item Under Test (IUT). Further details about the ISO/IEC compliance can be found in the test reports *23-024-TR-10* and *24-024-TR-20*. This evaluation was also conducted in order to comply with the standards set out in *Chapter 2 Part 1 Sections 2.1-2.3* in the [Digital ID \(Accreditation\) Data Standards 2024](#) (Data Standards) (version 12th November 2024) related to the testing of presentation attack detection and biometric performance technology.

A full demonstration of compliance with the Data Standards can be found in the table included within this document.

A detailed test and analysis report was generated to support the findings. For the associated metrics and testing outcomes, please refer to the test reports *23-024-TR-10* and *24-024-TR-20*.

This letter confirms that the IUT was tested according to the applicable ISO/IEC 30107-3 specifications for presentation attack detection testing and reporting, and was found to be in compliance with Levels 1 and 2. Consequently, the IUT meets the overall biometric performance expectations set by the *Digital ID (Accreditation) Data Standards 2024* for the assessed threat scenarios, with an APCER of 0% observed across all presentation attack instrument species under the evaluated conditions.

Handwritten signature of Ms. Somya Singh in black ink.

Ms. Somya Singh  
Operations Manager  
BixeLab Pty Ltd  
info@bixelab.com

Handwritten signature of Dr. Ted Dunstone in black ink.

Dr. Ted Dunstone  
Senior Responsible Officer  
BixeLab Pty Ltd  
info@bixelab.com

Table of reference demonstrating compliance with the Digital ID (Accreditation) Data Standards 2024

Data Standards requirements for ISPs, as per the Data Standards (Accreditation)	Demonstration of compliance, as per the ISO/IEC 30107-3 compliant presentation attack detection evaluations completed by BixeLab
<p>Section 2.2 (1): Biometric testing must be conducted by a person that:</p> <ul style="list-style-type: none"> <li>(a) uses personnel experienced in conducting biometric testing;</li> <li>(b) is, or uses, a laboratory accredited against ISO/IEC 17025:2017 that is certified for the assessment of biometric technology testing standards;</li> <li>(c) has, and applies, a policy for working with human test subjects that has been approved by a relevant national body;</li> <li>(d) has established test methods for:                             <ul style="list-style-type: none"> <li>(i) presentation attack detection testing informed by ISO/IEC 30107-3:2023, if conducting testing of presentation attack detection technology.</li> </ul> </li> <li>(e) is independent from the design, implementation, operation and management of the accredited entity's accredited services and DI data environment and is:                             <ul style="list-style-type: none"> <li>(i) external to the entity; or</li> <li>(ii) if the entity is part of a group, external to the group.</li> </ul> </li> </ul>	<p>All testing personnel were appropriately experienced in conducting biometric testing.</p> <p>As stated, BixeLab is conformant to ISO/IEC 17025:2017.</p> <p>BixeLab has NHMRC ethics approvals for dealing with human subjects and, as part of that approval, policies that detail treatment of human test subjects.</p> <p>BixeLab and its methodology for undertaking PAD testing are accredited under ISO/IEC 30107-3:2023.</p> <p>BixeLab is completely independent from the design, implementation, operation and management from the Item under Test. BixeLab is also external to Makesure.</p>
<p>Section 2.2 (2): A person that meets all the requirements in subsection (1) is a <b>biometric testing entity</b>.</p>	<p>BixeLab fulfills all requirements set out in Section 2.2 (1).</p>
<p>Section 2.3 (1):</p> <p><b>level A presentation attack instrument species</b> means a category of presentation attack instruments which:</p> <ul style="list-style-type: none"> <li>(a) have an elapsed creation time equal to or less than one day;</li> <li>(b) can be created or undertaken by a layperson;</li> <li>(c) can be undertaken with standard equipment; and</li> <li>(d) involve a source of biometric information which is easy to obtain such as a photo from social media or a voice recording.</li> </ul> <p><b>level B presentation attack instrument species</b> means a category of presentation attack instruments which:</p> <ul style="list-style-type: none"> <li>(a) have an elapsed creation time equal to or less than 7 days;</li> <li>(b) can be created or undertaken by a person who has the required expertise to do so;</li> <li>(c) can be undertaken with standard or specialised equipment; and</li> <li>(d) involve a source of biometric information which is moderately difficult to obtain such as a stolen fingerprint image or a voice recording of a specific phrase.</li> </ul>	<p>The provided definitions are appropriately aligned with BixeLab's own PAI species category definitions, as detailed in the provided test plan.</p>
<p>Section 2.3 (2): Where an ISP conducts online biometric binding, its presentation attack detection technology and liveness detection must be tested by a biometric testing entity in accordance with the requirements specified in ISO/IEC 30107-3:2023 and this Part.</p>	<p>As discussed previously, BixeLab fulfills all requirements to be considered a biometric testing entity, as per the standards, and in turn conducted testing in accordance with the requirements specified in ISO/IEC 30107-3:2023 and the Data Standards.</p>

Section 2.3 (3): Testing of presentation attack detection technology must be conducted in accordance with the standards in the following table.

Standards for testing of presentation attack detection technology		
Item	For:	the standard is:
1	the testing:	must comply with the following: <ul style="list-style-type: none"> <li>(a) be conducted on a system that incorporates all hardware and software involved in the ISP's biometric binding process;</li> <li>(b) be conducted using configurations and settings that align to the ISP's DI data environment;</li> <li>(c) calculate and record the completed presentation attack detection evaluation and corresponding results for each presentation attack instrument species as those artefacts and process for testing are defined by ISO/IEC 30107-3:2023, and this section;</li> <li>(d) include presentation attack instrument species to address potential presentation attack threats to the presentation attack detection technology and mechanism for liveness detection, as informed by the ISP's cyber security risk assessment and fraud risk assessment;</li> <li>(e) include at least 6 level A presentation attack instrument species and at least 6 level B presentation attack instrument species; and</li> <li>(f) include a minimum of 10 individuals.</li> </ul>

Makesure has confirmed that the IUT provided to Bixelab was appropriately aligned with production settings.

All results and transactions produced by the testing were appropriately logged by each individual PAI artefact.

The attack scenarios included by Bixelab in the evaluation were informed by Makesure.

Bixelab used at least six level A and six level B PAI species.

Bixelab used at least 10 unique, diverse, and consenting participants (test subjects).

2	each presentation attack instrument species:	must create at least one presentation attack instrument covering a minimum of 3 individuals and must be included in the testing.
---	--	--

For every level A and level B PAI species included in the testing, 10 PAI artefacts (equivalent to one per test subject) were made for every species. Therefore, at least 120 unique PAI artefacts were included in testing.

3	presentation attack instrument species used in testing:	<ul style="list-style-type: none"> <li>(a) must meet the requirement for an APCER of 0%;</li> <li>(b) however, if the reported APCER for any presentation attack instrument species does not meet the requirement in paragraph (a), the biometric testing entity must:                             <ul style="list-style-type: none"> <li>(i) conduct supplementary testing of any presentation attack instrument species that failed to meet the requirement in paragraph (a); and</li> <li>(ii) subject to paragraph (c), confirm that the supplementary testing concluded that the presentation attack instrument species successfully met the requirement in paragraph (a);</li> </ul> </li> <li>(c) if up to one level B presentation attack instrument species used in the testing has an APCER equal to or less to 5%, with all other level B and level A presentation attack instrument species having an APCER of 0%, the biometric testing entity must include in its report to the ISP a risk rating and recommended mitigation strategies.</li> </ul>
---	---	---

All Level A PAI species resulted in an APCER of 0%.

Some Level B species did not result in an APCER of 0% in the original testing. Consequently, supplementary testing (as detailed in 24-024-TR-20) was conducted on the species in question. In the supplementary testing, all PAI species resulted in an APCER of 0%. Note: supplementary testing was conducted on RatifyID v1.2.7 (app build 16).