ISO/IEC 30107-3 Biometric Presentation Attack Detection (PAD) Evaluation

Amendment to report: Additional Testing

Prepared for

Xperix Inc.

By

BixeLab

3/16 Bentham Street, Yarralumla,

ACT 2600, Australia

xperix

Biometric Presentation Attack Detection Evaluation to Level 1 for:

RealScan-G10 and RealScan-G10i [HW Version: V02C & V02A, SDK Version: v2.0.0]

Attention: Changmin Kim

cmkim@xperix.com

NVLAP®

TESTING

NVLAP LAB CODE 600301-0

Document Code 24_BXL021_TR_32

***Submit Date*: 7th March 2024**

***Version*: 2.0**

***Submitted by*: Somya Singh**

***Contact*: s.singh@bixelab.com**

Version History			
Version Number	**Description of change**	**Author**	**Date**
V1.0	Test Report – Initial Release	BixeLab	31st January 2024
V2.0	Details of the follow up testing performed to validate performance of the IUT on test scenarios of interest and based on outcomes from the primary testing	BixeLab	6th March 2024

BIXELAB PTY LTD PROPRIETARY NOTICE

BixeLab Pty Ltd has taken every care in preparing this document. Information contained within is accurate to the best of BixeLab's knowledge at the date of release. BixeLab cannot accept any liability to any person or company for any financial loss or damage arising from the use of this document. It should not be reproduced or made available in any form to persons outside the group/s directly responsible for evaluating its contents, without the written consent of BixeLab Pty Ltd.

All brands and products referenced in this document are acknowledged to be trademarks or registered trademarks of their respective owners.

This report must not to be used by the client to claim certification, approval, or endorsement of a product, by NIST, NVLAP or any agency of the U.S government.

EXECUTIVE SUMMARY

This report presents the findings (see Performance Results) from Level 1 biometric presentation attack detection (PAD) evaluation of the RealScan G10/G10i [HW version: V02C (RS-G10) / V02A (RS-G10i), SDK version: 2.0.0 (IUT) tested on Windows OS (see Evaluation Details) under controlled laboratory environment that simulated attack scenarios expected in the intended use case. The IUT was accompanied with a backend application SDK (RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)) that allowed testers to initiate tests and store result information.

The evaluation conducted between December 2023 and January 2024 aimed to assess the liveness/PAD performance of the IUT against biometric impostor presentation attacks, following the guidelines of the ISO/IEC 30107 – 1 and ISO/IEC 30107 – 3 standards. The PAD test efforts were undertaken to Evaluation Assurance Level (EAL) 1 involved using 6 Level A presentation attack instruments (PAI) species. Testing was completed for 10 unique, conformant, and consenting test subjects. In total 360 Level A attack presentations were completed including 180 cooperative and 180 uncooperative scenarios in addition to 60 bona fide presentations. Testing was focused on the "Index" and "Thumb" fingers, with 5 test subjects assigned to their left “Index” and “Thumb” and the remaining 5 test subjects assigned to their right “Index” and “Thumb”. The IUT was configured and tested with the following parameters as described by the provider:

- LFD Level: 4
- Capture Mode: Flat Single (Ex)
- Other Settings: Default

The evaluation targeted the end-to-end verification process, specifically examining whether a presentation attack could bypass all stages of control. These stages of control include assessing sample quality, detecting liveness, and performing biometric matching. 4 presentation attacks involving latent inked fingerprints lifted from a wooden surface using blue tac were able to successfully pass the quality assessment, liveness detection, and achieve a match; this presentation attack instrument (PAI) species consequently lead to successful end-to-end attacks. 4 presentation attacks involving play-doh fingerprints lifted from wax moulds were also able to successfully pass the quality assessment, liveness detection, and achieve a match, thus leading to successful end-to-end attacks for this presentation attack instrument (PAI) species.

The tables below provide an overview of the performance measured for the IUT:

Table 1 Summary of performance metrics: Attack presentations

Presentation Attack Instrument (PAI) species	Total number of PAI presentations	Total number of PAI sources	APCER	IAPAR	RIAPAR[1]	APNRR
Latent fingerprint dusted with graphite powder and lifted using scotch tape from a ceramic surface	60	10	0 errors	0 errors	0 errors	0 errors
Latent fingerprint dusted with baby powder and lifted using scotch tape from a phone surface	60	10	0 errors	0 errors	0 errors	0 errors
Latent inked fingerprint lifted using blu-tac from a wooden laminate	60	10	5 errors	4 errors	0 errors	0 errors
Fingerprint printed on matte paper	60	10	0 errors	0 errors	0 errors	60 errors
Wax fingerprint created using a play-doh mould	60	10	0 errors	0 errors	0 errors	60 errors
Play-doh fingerprint created using a wax mould	60	10	5 errors	4 errors	0 errors	0 errors

60 bona fide presentations were subjected to evaluation using a series of tests. The tests were comprised of 20 instances with subjects presenting dry fingerprints; 20 instances with subjects simulating a sweaty fingerprint scenario by presenting moist fingerprints; and another 20 instances where subjects presented wet fingerprints to emulate an outdoor rainy scenario. Based on the analysis: 0 classification errors were found across 20 bona fide presentations; 2 classification errors were found across 20 presentations where subjects' fingers were moist or sweaty during the authentication attempt; 2 classification errors were found across 20 presentations where subjects' fingerprints were wet by spraying water to emulate outdoor rainy weather.

Table 2 Summary of performance metrics: bona fide presentations and live presentations under varying quality conditions

Presentation	Total number of presentations	Total number of sources	BPCER	BPNRR
Subjects presented their own face in the manner intended for the application	20	10	0 errors	0 errors
Subjects' fingers were moist or sweaty during the authentication attempt.	20	10	2 errors	0 errors
Subject attempted authentication in wet	20	10	2 errors	0 errors

[1] RIAPAR is described as sum of impostor attack presentation identification rate (IAPAR) and false reject rate (FRR) at a fixed decision threshold. Here FRR pertaining to 20 bona fide presentations (i.e., no adverse quality presentations) was considered.

Presentation	Total number of presentations	Total number of sources	BPCER	BPNRR
environments, such as outdoors during rainy weather				

This report tested compliance of the IUT against common attack types that meet the Level 1 criteria outlined in ISO/IEC 30107 and other relevant standards. Presentation attacks are constantly evolving, and performance measurement is undertaken at a point in time with results specific to the scenarios covered. After conducting thorough research and considering the context of the item under test (IUT), relevant attacks and attack combinations were selected. These selections were also based on an assessment of the likelihood of an attack mechanism being used, claims made in reference to the IUT and the ISO-defined level that the attack tool corresponds to for the testing. As this is a Level 1 PAD test report, the results and findings solely pertain to Level A attack types – as tested, respectively.

Additional Testing

At the request of the client, additional testing was done after the completion of the primary testing to validate performance of the IUT against previously successful spoof results found during the official testing of RealScan G10/G10i [HW version: V02C (RS-G10) / V02A (RS-G10i), SDK version: 2.0.0 (IUT). Provider was given up to 3 weeks to provide the SDK associated with the IUT after making only the allowed technical changes. Provider of the IUT confirmed that any technical changes to the device that would impact the device's ability to produce comparable results from previous tests were not made and that the performance of the system was substantially the same with improvements in relevant areas.

Based on the primary and additional testing completed, the IUT measured 0 errors against the IAPAR metric across 5 out of 6 presentation attack species tested. 5 IAPARs were recorded for 48 new tests on the IUT for PAI species "Play-doh fingerprint created using a wax mould".

Results pertaining to the performance measured during additional testing is provided in section Appendix F: Additional Testing.

Table of Contents

Executive Summary ..... *iii*

A. Introduction *7*

Background 7

Laboratory Details 7

Evaluation Details 7

B. Evaluation Plan *10*

Evaluation Data 14

Evaluation Methodology 17

C. Evaluation Report *23*

Performance Results 25

D. Findings and Recommendations *28*

Findings 28

Recommendations 28

Constraints 28

Deviations and Exclusions 28

Conclusions 28

Appendix A: Evaluation Management *29*

Data and Privacy Management 29

System Configuration Management 29

Test Readiness Criteria 29

Test Completion Criteria 30

Test Environment 30

Test Setup 30

Appendix B: Terms and Definitions *32*

Appendix C: References *36*

Appendix D: Configuration Audit *37*

Appendix E: Application For IUT Assessment *38*

Appendix F: Additional Testing *39*

A.INTRODUCTION

Background

Xperix Inc., the provider of RealScan-G10 and RealScan-G10i [HW Version: V02C & V02A, SDK Version: v2.0.0] referred to as item under test (IUT), has engaged BixeLab as an independent third-party biometric testing lab to conduct an ISO/IEC 30107-3 compliant biometric presentation attack detection evaluation of the IUT. This evaluation aims to assess the performance of the IUT in compliance with the applicable specifications of the 30107 standards.

BixeLab is a biometric testing laboratory that has obtained accreditation from the National Institute of Standards and Technology (NIST) under the National Voluntary Laboratory Accreditation Program (NVLAP Testing Lab Code 600301-0). This accreditation conforms to the outlined requirements of ISO/IEC 17025:2017 (General Requirements for Competence of Testing and Calibration laboratories) listed in the NIST Handbook 150-25.

BixeLab provides international test capabilities and evaluation services to the biometric market. This includes providing a formalised and standardised setting for biometric and identity software application testing, as well as certification services that are compliant with best practice in laboratory and biometric testing ISO/IEC standards and consistent with the NIST accreditation standards.

Laboratory Details

Table 3 Laboratory details

Field	Response
Laboratory Name	BixeLab Pty Ltd
Evaluator(s) Name	Somya Singh
Evaluation Start Date	December 2023
Evaluation End Date	January 2024
Evaluation location	3/16 Bentham Street, Yarralumla, ACT 2600, Australia

Evaluation Details

Table 4 Evaluation details

Evaluation Details	Response
PAD testing level	Level 1 Sophistication
Justification for chosen level	Presentation attack instruments selected at level 1 (or level A) sophistication: Simple complexity/expertise Easy access to biometric characteristics

Evaluation Details	Response
	Low to medium equipment/cost of creation
Subsystem under test	Full system
Subsystem functionality	Verification
Objective	The primary objective is to test the security features of the verification system and assess the resilience of its performance against Level A attack types.
In Scope	To assess the biometric PAD performance of the IUT using presentation attack instruments (PAIs) at Level 1 or Level A sophistication.
	To assess IUT on compatible platforms (e.g. windows OS)
	This evaluation centres on vulnerability assessment, employing a representative set of presentation attack instruments and bona fide data capture subjects. This entails deploying presentation attack instruments (PAIs) against the verification subsystem (against live enrolments), all conducted under certified laboratory conditions.
Out of Scope	Evaluation of biometric performance accuracy is not within the scope
	Evaluation of operational performance within a deployment context is not within the scope
	Assessment of all possible sensor level presentation attacks is not possible.
	Security assessment such as penetration testing is not within the scope
	Assessment for biometric quality performance assessment is not within the scope
Constraints	Assessment of IUT against all possible presentation attacks is not possible. During the IUT evaluation, only conventional and well-known presentation attacks were attempted, drawing from the recommendations outlined in the ISO/IEC 30107-3 standard. There may be presentation attack types, PAI species, and variables that were not investigated when analysing the performance of a PAD subsystem. As a result, the reported performance of the IUT may not give any information about its effectiveness in identifying presentation attacks that were not tested during this evaluation. The outcomes of this report are

Evaluation Details	Response
	specific to the testing undertaken. BixeLab is not responsible for any claims made outside the results reported in this document.
	The evaluation was limited to assessing IUT's ability to accept or reject a presentation attack. In this regard, the classification metrics presented in this document include APCER, BPCER, APNRR, BPNRR, and IAPAR
	Both attack presentations and bona fide presentations were conducted with a small group of test subjects, and a limited number of tests were completed. The associated metrics have validity within restricted confidence levels.
	BixeLab has tested what it believes to be a representative sample of the commercially available solution. Where changes affecting the PAD/liveness detection performance are made to the IUT, the results pertaining to this evaluation may not be applicable.
	The results presented in this report serve as validation that the IUT has undergone testing in accordance with the ISO/IEC 30107-3 standard to sophistication Level 1. Because the standard does not provide pass or fail levels for the metrics, this report does not indicate a pass or fail in association with this standard.
	The attack instruments that were chosen for this testing effort have been decided through research, the lab's attack classification criteria and the claims made by the provider on their website. The approach considered both uncooperative and cooperative attack presentation scenarios,noting that all sources obtained for mounting these attacks were from cooperative and consenting test subjects.
	The vendor self-attested that the RealScan G10 and G10i scanners were comparable in terms of factors that could influence presentation attack detection performance. The exploratory testing and pretesting completed on both RealScan G10 and G10i confirmed that the outputs were comparable between the two models. For ease of testing, only the RealScan G10i model was used. The results for this model, to the best of BixeLab's knowledge, also apply to the G10 model, with the caveat that any changes, such as form factor, are likely to have an impact on expected performance.
	For the SDK accompanying the IUT, the version mentioned on the application when used for testing is v1.9.5.615. However, the client reports the version to be v2.0.0. Version as reported by the vendor has been reflected within the report.

B. EVALUATION PLAN

Table 5 Information specific to item under test (IUT) and other associated information

System Information	Response
Vendor company name	Xperix Inc.
End customer name *(for example bank on behalf of whom the vendor product is being evaluated)*	N/A
Contact name	Changmin Kim
Contact email	cmkim@xperix.com
Applicable standard	ISO/IEC 30107-1 ISO/IEC 30107-3
Applicable clauses within the standard	Clause 6 to 11.1 and 13.1 Clause 13.4
Standard version	2017[2]
Vendor claims	“RealScan-G10 provides advanced artificial Intelligence-based Live Finger Detection technology that distinguishes fake fingerprints made from various materials including clay, rubber, silicon, glue, paper, film and more.” See https://www.xperix.com/en/contents/detail.php?code=020102.
External pass/fail requirements	N/A
Modality	Fingerprint (contact – optical scanner)
Evaluation label	Biometric Presentation Attack Detection (PAD) Evaluation
IUT Name	RealScan G10/G10i [HW version: V02C (RS-G10) / V02A (RS-G10i), SDK version: 2.0.0
IUT Hardware name & version	RealScan G10/G10i

[2] The report complies with the relevant standards outlined in ISO/IEC 30107-3:2023, taking into account BixeLab's existing accreditation scope, which is presently confined to ISO/IEC 30107-3:2017. The terminology and reporting criteria adhere to the most recent version, with a meticulous review to ensure fulfillment of all pertinent requirements from the 2017 edition.

System Information	Response
	[HW version: V02C (RS-G10) / V02A (RS-G10i)
IUT Software name & version	SDK Version: v2.0.0
IUT associated Operating system (if applicable)	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)
IUT build number	N/A
Were Lab devices used? If yes list all hardware and software details	Yes WIN-DSK-BL: BXL138 Edition: Windows 11 Pro Version: 23H2 OS Build: 22631.3007
Set up process description	1. Once hardware is received from vendor, confirm if the hardware is received in good condition. Label and log received hardware according to appropriate BixeLab protocols. 2. Follow user manual provided by vendor to install the required SDKs to the target device. 3. Follow user manual to connect fingerprint scanner to the target device (personal computer running Windows 11 Pro). Adjust the settings of the application according to set-up manual to ensure the application is properly running and set-up correctly. 4. Confirm whether the steps mentioned in the user manual work fine.
Set up date	20th December 2023
Exploratory test process description	1. Connect IUT with the target device. 2. Ensure necessary drives are installed, along with the appropriate SDK. 3. Make note of all relevant hardware and software specifications correctly in the lab IT audit log. 4. Complete exploratory tests to get an understanding of how the IUT operates. Validate the expected PAD subsystem outputs for testing.
Exploratory test date	20th December 2023
Pre-test process description	1. Connect IUT with the target device. 2. Ensure necessary drivers are installed, along with the appropriate SDK. 3. Make note of all relevant hardware and software specifications correctly in the lab IT audit log. 4. Complete pretests using randomly selected artefacts to get a better understanding of the PAD outputs and to validate the established test cases. 5. Record pretest results within the Pretesting Runsheet.

System Information	Response
Pre-test date	21st December 2023
Evaluator comments or notes	Certain observations noted during exploratory testing were communicated to the vendor to attain clarifications. For example, The G10i model was not saving the enrolment templates, and G10 model kept crashing. The issues were resolved by the vendor before proceeding to pretesting. The issue related to not being able to enrol fingerprints using the G10i due to our library not recognising the license. For the "Write USB Timeout" issue, it was found that it can be caused by a bad connection between the scanner and the PC. Furthermore, vendor communicated that the G10 / G10i, there is an additional process called "Dirty check" before taking a fingerprint, where the scanner will show a green light even though it is not ready for capture. Vendor recommended that tester waits for approx. 1 second after pressing the capture button before entering fingerprint. If the scanner keeps blinking at regular intervals, it may not have passed the dirty check and is retrying, so it was recommended to remove the fingerprint and wipe the dirty surface and it will stop blinking.

The figure below provides the process flow for the IUT.

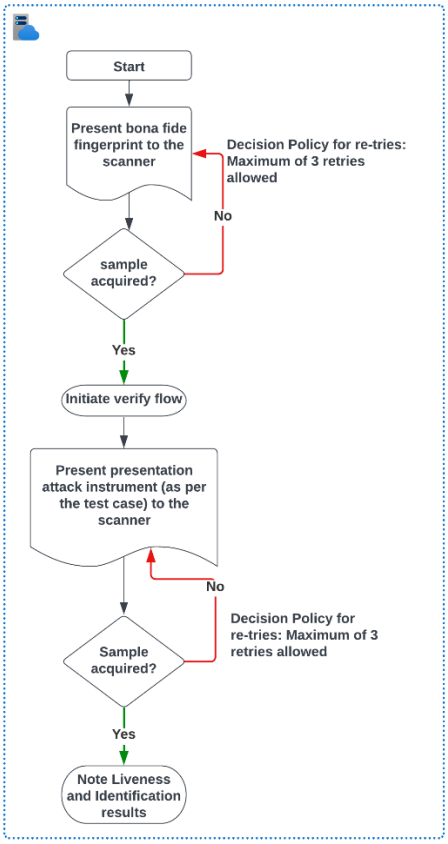


Figure 1 Application process flow

Note that it is the responsibility of the owner of the technology to ensure that the settings align with the objective of the evaluation and no configurations associated with the IUT are changed during the evaluation. Before the testing process is initiated, BixeLab will ensure that the software versions are installed and configured appropriately and verify that the system is operating correctly.

Table 6 Target of Evaluation (ToE)

Target of Evaluation	Expected outputs	
	Component name	**Available output fields**
Data capture subsystem	N/A	N/A
Biometric quality assessment subsystem	N/A	N/A
Automated document capture subsystem	N/A	N/A
Document optical character recognition subsystem	N/A	N/A
Automated document authenticity detection subsystem	N/A	N/A
Enrol subsystem	N/A	N/A
Authentication subsystem	See below	See below
Liveness detection or presentation attack detection subsystem	See below	See below
Complete system (include all subsystems within the target of evaluation)	Full System	Liveness – - Live Finger - Fake Finger Verification – - Identification Failed (Liveness Pass, Non-Match) - Identification Success (Liveness Pass, Match)

Evaluation Data

Test Crew

Table 7 Breakdown of test crew

Subject Metadata/Input factors	Metadata Breakdown	Recommended Distributions	Achieved Distributions	Adherence to recommended distributions
Age group	< 18 y/o	0%	0%	☒
	18 – 30 y/o	25-40%	90%	☐
	31 – 50 y/o	25-40%	0%	☐
	51 – 70 y/o	25-40%	10%	☐
	> 70 y/o	0%	0%	☒
Sex	Male	40-60%	80%	☐
	Female	40-60%	20%	☐
	Not disclosed	-	0%	☒
Ethnic Origins	European/Caucasian	-	40%	☒
	East Asian	-	20%	☒
	South and Central Asian	-	40%	☒

For this evaluation, the aforementioned data was recorded. The pseudonymised version of this information will remain within the secured BixeLab information management system for data analysis purposes post-test execution. Any other subject metadata that would not normally be available to the IUT will be excluded from the analysis set.

BixeLab adopted all measures to ensure that the data labels are free from data logging errors for the purpose of this evaluation and test corpus was not required to be retired at any stage of post testing. The test corpus was validated to ensure the following:

- Reliable ground truth
- Correct data format
- Correct data collection

Presentation Attack Instrument (PAI) species

Table 8 Breakdown of applicable presentation attack instrument (PAI) species

Level	PAI Species Label	PAI Species description	Number of sources used	Total number of attacks	Creation Method	Presentation technique
A	**Latent Fingerprint lifted from Ceramic surface using graphite powder and scotch tape**	Test Subjects' fingerprints were placed on a ceramic plate. This fingerprint was dusted with graphite powder and was lifted using Scotch Tape. This lifted fingerprint on the tape was presented directly to the sensor.	10	60	Uncooperative – Biometric characteristics were captured simulating uncooperative conditions (i.e., participant waving in a photo). This is to simulate an attacker sourcing biometrics from social media and other publicly available photo sources.	Lifted fingerprint mounted directly onto the scanner
	Latent Fingerprint lifted from phone surface using baby powder and scotch tape	Test Subjects' fingerprints were placed on an iPad screen. This fingerprint was dusted with baby powder and was lifted using Scotch Tape. This lifted fingerprint on the tape was presented directly to the sensor.	10	60		
	Latent inked fingerprint lifted from wood surface using blu-tac	Test Subjects' fingerprints were placed on a wooden table using ink. This inked fingerprint lifted using blu-tac. This lifted fingerprint on the blu-tac was presented directly to the sensor.	10	60		
	2D Print on Matte	Test subjects placed their fingerprints on a wooden laminate. This fingerprint was dusted with magnetic dust. A high-quality image of the dusted fingerprint was taken, processed, and later printed on matte paper to match the size of the scanner. This print was presented directly to the sensor.	10	60	Cooperative – Biometric characteristics were captured directly from test crew participants in addition to some additional participants who did not participate in person but provided their biometrics for the purpose of creating presentation attacks.	2D paper fingerprint mounted directly onto the scanner
	Wax fingerprint using Playdoh mould	Test Subjects' left their fingerprints on some playdoh which was used as a mould. Molten wax was poured into this mould, to produce a	10	60		Wax fingerprint mounted

Level	PAI Species Label	PAI Species description	Number of sources used	Total number of attacks	Creation Method	Presentation technique
		wax fingerprint. This wax fingerprint was presented directly to the sensor.				directly onto the scanner
	Playdoh fingerprint using Wax mould	Test Subjects' left their fingerprints on some melted wax which was used as a mould. A ball of playdoh was pressed against this mould to acquire a Playdoh fingerprint. This Playdoh fingerprint was presented directly to the sensor.	10	60		Play-doh fingerprint mounted directly onto the scanner

Evaluation Methodology

Presentation Attack Detection (PAD) evaluation

The presentation of an artefact or human characteristics to a biometric capture subsystem in a fashion intended to interfere with system policy is referred to as a presentation attack. Techniques for automated detection of presentation attacks are referred to as presentation attack detection (PAD) mechanisms. Testing of PAD mechanisms using a range of presentation attack instruments (PAIs) can be defined as presentation attack detection testing.

The presentation attack instruments shall be selected as per the test method and modality requirements. This section shall describe the presentation attack instrument species to be utilised and the volume of presentation attack instruments to be utilised (per test subject).

BixeLab uses a tiered system to describe three levels of increasing sophistication of attacks against the presentation attack detection system. This system is based upon the relative difficulty of accessing and turning the source of a biometric characteristic into an artefact of varying complexities. This is comparable in approach to the FIDO Biometric Requirements[3] and the BEAT Framework.

Table 9 System for defining presentation attack instrument (PAI) species evaluation assurance levels (EALs)

Factor	Rating	Assessment	Description
Complexity/expertise	A	Simple	Typically, two-dimensional and/or repurposed from another source
	B	Specialised	Typically, three-dimensional, and/or specially produced or altered from a source
	C	Sophisticated	Specifically produced, sophisticated artefacts that typically leverage multiple instances of the biometric characteristics
Access to biometric characteristics	A	Easy	Publicly or commonly available, usually without knowledge of the target
	B	Moderate	Usually requires cooperation of the target or access to the biometric or biometric template itself
	C	Difficult	Usually requires multiple sources which may be altered or augmented. Often involves access to the biometric or biometric template itself

[3] https://fidoalliance.org/specs/biometric/Biometrics-Requirements-v1.0-wd-20190606.html

Factor	Rating	Assessment	Description
Equipment/cost	A	Low	Can be produced with standard materials using office or home equipment
	B	Medium	May require the use of generic suppliers, software, or equipment

This system removes the BEAT Framework and FIDO Framework requirement that assesses factors by elapsed time and also makes modification to the interpretation of other factors. The summary of reasonings for this methodology includes:

- Removing the elapsed time factor as this has no bearing on the ability of a PAI to be falsely accepted. Preparation time is rarely of interest to a test, as PAIs may already exist or be sourced from a third party.
- The complexity or expertise has a more specific meaning within the context of PAI preparation. A crude artefact involves the reuse of an existing source of the characteristic (such as a photograph) whereas a complex artefact with the likeness of a real person requires specific production processes that leverage more than one source of the characteristic (such as a silicon mask produced using multiple photographs of the subject).
- Equipment is expanded to include cost as it is likely that an attacker could or would outsource production to a third party. For example, specific expertise in mask production is not required if this is performed by a third party at a cost.

The assessed level of a given presentation attack instruments species is determined by its highest score following the assessment. For example:

Example Presentation Attack Instrument Assessment

PAI Species: Social media photograph displayed on mobile phone

- **Complexity/expertise: Simple**
  - **Repurposed photograph**
- **Access to biometric characteristic: Easy**
  - **Publicly available via social media channels**
- **Equipment/cost: Low**
  - **Use of a personal mobile phone**
- **Assessed Level: Level A**

Unless required otherwise, each test subject shall perform 3 genuine transactions, across 2 different fingers. For a test crew size of 10 test subjects, this corresponds to 60 total genuine transactions.

Unless required otherwise, there shall be three presentation attack instruments for each PAI species, and for each test subject. For a Level 1 evaluation using a test crew size of 10 subjects, this corresponds to 120 individual presentation attack instruments of a Level A species.

Unless required otherwise, each presentation attack instrument shall be presented for 5 transactions following the levels of effort as per applicable decision policy. For a test crew size of 10

test subjects, this corresponds to 240 total presentation attack instruments and 720 total presentation attacks.

Roles within the PAD testing will be assigned accordingly to the requirement following the ISO 30107-3. These roles will be defined within the report, and everyone involved in the testing will be assigned a test crew register code as to follow the privacy and consent policy regarding the use of an individual's identity as a PAI presenter, source, or creator.

The report will specify the number of individuals who occupy each of the roles and document whenever an individual occupies multiple roles.

Definitions of the roles according to ISO 30107-3:

1. **PAI presenter:** Individual or mechanism presenting the presentation attack instrument (PAI) to the biometric system.
2. **PAI source:** individual or mechanism from which biometric samples are obtained for use in a presentation attack instrument (PAI), realized in a PAI series.
3. **PAI creator:** individual or mechanism responsible for the conception, formulation, design, and realisation of a presentation attack instrument (PAI) species. These individuals will remain anonymous however their roles within the PAD testing will be clearly stated to ensure the clarity of how the PAD test PAIs were created and that their roles during the PAD testing comply to the ISO 30107-3 standard.

Note, it is stated in the ISO 30107-3 that a PAI source cannot be the PAI presenter of their own source, but a different PAI presenter may use another PAI presenters' source to test.

Table 10 Test case related information

Evaluation Label	Item under test	Applicable test cases	Description of specific test processes	Description of pre-test process	Description of test execution Process	Variables and uncertainty factors
Biometric PAD Evaluation	RealScan G10/G10i [HW version: V02C (RS-G10) / V02A (RS-G10i), SDK version: 2.0.0	**Bona fide** – Test subject instructed to ensure dry fingers to simulate dry environmental conditions **Moist** – Test subjects instructed to apply moisturiser to finger to simulate moist environmental conditions **Wet** – Test subjects instructed to wet their finger to simulate wet environmental conditions.	Provide verbal instruction to test subject regarding expectations from the test and regarding the various test cases. The test subject provides written consent before commencing.	Ensure the IUT and set up are ready for PAD testing. Ensure IUT is connected to testing device and the necessary drivers are installed. Ensure all material such as PAIs are readily available for each test case to be tested.	1. Connect IUT to testing device and initiate appropriate SDK. 2. Click on “Init Device” to initiate device. 3. Change LFD level to 4 and “Capture Mode” to Flat-Single (EX). 4. Enter test subject ID and click “Enrol” to initiate enrolment. Test subject presents bona fide finger to IUT. Record enrolment results in test runsheet. 5. Click on test subject ID and click on “Identify” to initiate verification flow. Test subject presents bona fide finger to IUT. Record verification results in test runsheet. 6. Repeat step 5 two more times (once with Moist finger and once with Wet finger). Record verification results in test runsheet. 7. Repeat steps 4 to 6 for all test subjects.	Lighting level: 650-700 lux

Evaluation Label	Item under test	Applicable test cases	Description of specific test processes	Description of pre-test process	Description of test execution Process	Variables and uncertainty factors
		Latent Fingerprint lifted from Ceramic surface using graphite powder and scotch tape Latent Fingerprint lifted from phone surface using baby powder and scotch tape Latent inked fingerprint lifted from wood surface using blu-tac 2D Print on Matte Wax fingerprint using Playdoh mould Playdoh fingerprint using Wax mould	Provide verbal instruction to test subject regarding expectations for data collection for the purposes of creating the PAIs. The test subject provides written consent before the data is collected. Create target attack instrument as per the lab procedures.		1. Connect IUT to testing device and initiate appropriate SDK. 2. Click on “Init Device” to initiate device. 3. Change LFD level to 4 and “Capture Mode” to Flat-Single (EX). 4. Enter test subject ID and click “Enrol” to initiate enrolment. Test subject presents bona fide finger to IUT. 5. Click on test subject ID and click on “Identify” to initiate verification flow. Acquire test subject’s PAI and present to IUT. 6. Wait for IUT to provide liveness result for mounted PAI. 7. Test Operator logs results for the completed transaction. 8. Repeat steps 4 to 6 3 times for each PAI for each target or until the maximum number of allowed re-attempts have been exhausted	

Levels of effort and decision policy

Table 11 Applicable levels of effort

Levels of effort criteria	Recommended	Tested criteria
The number of allowed enrolments attempts per transaction, if applicable	3	3
The number of allowed enrolment transactions, if applicable	3	3
The amount of time allowed per enrolment attempt	<45 seconds	<45 seconds
The number of allowed verification attempts per transaction	3	3
The amount of time allowed per verification attempt	<45 seconds	<45 seconds

C. EVALUATION REPORT

This section defines the test report based on the evaluation undertaken as per the test plan provided previously.

Table 12 Responses to applicable ISO/IEC 30107 reporting requirements

#	ISO/IEC 30107-3 [2023] Reporting Requirements	Responses
1	**number of presentation attack instruments used**	120 PAIs were used for testing (each PAI was mounted three times)
2	**number of presentation attack instruments species (attack types) used**	6 Level A PAI Species were used for testing
3	**number of presentation attack instruments series (class of PAIs created using common production method and based on the same biometric characteristics) used**	6 PAI Series were used for this testing effort
4	**number of individuals involved in the testing, including PAI presenters unable to utilize artefacts and test subjects unable to present non-conformant characteristics**	PAI presenters: 3 PAI Sources (including subjects for bona fide presentations): 10
5	**number of PAI sources from whom artefact characteristics were derived**	A total of 10 PAI sources were used
6	**number of presentation attack instruments created per PAI source for each PAIS**	A total of 2 PAIs were created from each PAI source (one for each finger)
7	**number of tested materials**	6 (Graphite, Baby Powder, Ink, Wax, Paper and Play-doh)
8	**description of output information available from PAD mechanism**	Fake Finger (Liveness Fail) Identification Success (Liveness Pass)
9	**ordering of subject presentations with PAI**	Bona fide presentations were completed for 9 test subjects initially followed by PAI presentations for 9 subjects. Subsequently, Bona fide presentation was conducted for 1 subject, followed by PAI presentation for that subject.
10	**ordering of subject presentations without PAI**	
11	**number of total PAI presenters or test subjects and PAI presenters or test subjects that were reused**	3 PAI presenters re-used as subjects
12	**ordering of presentations to PAD-enabled and disabled system**	PAD enabled system, see responses against criteria 9 and 10 in this table.

#	ISO/IEC 30107-3 [2023] Reporting Requirements	Responses
13	**whether test subjects were reused**	3 subjects were reused as PAI presenters
14	**define the purpose and responsibilities of the following roles in a PAD test: test subject (conducts bona fide presentations and non-conformant capture attempts). State whether the role was material to test results and provide a basis for this assertion**	Test subject conducted bona fide presentations. The role was material to test results as outcomes provided IUT's ability to correctly accept bona fide presentations.
15	**define the purpose and responsibilities of the following roles in a PAD test: PAI presenter. State whether the role was material to test results and provide a basis for this assertion**	PAI presenter conducted PAI presentations. The role was material to the test results as it provided the basis for the classification level of the PAI species
16	**define the purpose and responsibilities of the following roles in a PAD test: PAI source. State whether the role was material to test results and provide a basis for this assertion**	PAI source was provided by test subjects (and PAI presenters participating as test subjects). The role was material to the test results as it ensured that the PAIs were representative of the types of demographics expected by the IUT in production setting.
17	**define the purpose and responsibilities of the following roles in a PAD test: PAI creator. State whether the role was material to test results and provide a basis for this assertion**	PAI creators were responsible for developing each presentation attack instrument. The role was material to the test results as it ensured that the PAIs were created with adequate quality standards and were fit for purpose to assess the IUT.
18	**indicate the number of individuals who occupied each role (e.g. five individuals were PAD sources in the test)**	Test Subject: 10 PAI presenter: 3 PAI source: 10 PAI creator: 2
19	**for each role, describe individuals' level of experience with presentation attacks**	Test Subject: Moderate experience on part of at least 4 subjects, nil to minimum experience for remaining 6 subjects. PAI presenter: moderate experience PAI source: moderate experience PAI creator: moderate to advanced experience
20	**document occurrences in which individuals occupied multiple roles, e.g. PAI sources were also PAI presenters**	3 PAI sources were also PAI presenters and test subjects.

Performance Results

Figure below provides an overview of the performance measured across the tested presentation attack presentations and bona fide presentations:

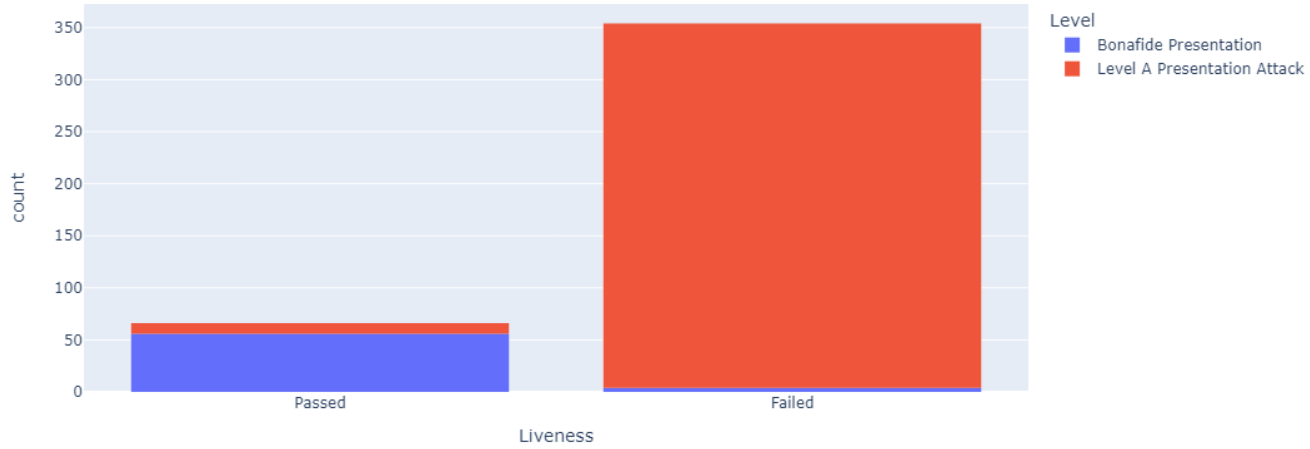


Figure 2 Overview of IUT performance

Table below provides the reporting criteria specific to verification (comparison) subsystem evaluations as per the ISO/IEC 30107-1 standard.

Subsystem	Metric	Type of Presentation	Reporting	Response
Comparison subsystem (verification)	FAR/FRR	Bona fide	Mandatory	Reported
	IAPAR	Attack	Mandatory for biometric impostors	Reported
	RIAPAR	Attack and bona fide	Mandatory for biometric impostors	Reported
	CAPRR	Attack	Mandatory for biometric concealers	N/A
	IAPAR (AP)	Attack	Optional	N/A
	FS-PD	Attack or bona fide	Optional	N/A

According to ISO/IEC 30107-3, the attack presentation classification error rate (APCER) is defined as the proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario. The standard defines attack presentation nonresponse rate (APNRR) as the proportion of presentation attacks using the same PAI species that result in no response at the PAD subsystem. Impostor attack presentation acceptance rate (IAPAR) is defined as the proportion of impostor attack presentations using the same presentation attack instrument (PAI) species that result in accept. Relative impostor attack presentation accept rate (RIAPAR) is

defined as the sum of impostor attack presentations identification rate (IAPAR) and false reject rate (FRR) at a fixed decision threshold.

Based on the reporting criteria as stated above, table below provides a summary of mandatory performance metrics associate with the IUT:

Table 13 Summary of applicable performance metrics as measured for the IUT: attack presentations

Presentation Attack Instrument (PAI) species	Total number of PAI presentations	Total number of PAI sources	APCER	IAPAR	RIAPAR[4]	APNRR
Latent fingerprint dusted with graphite powder and lifted using scotch tape from a ceramic surface	60	10	0 errors	0 errors	0 errors	0 errors
Latent fingerprint dusted with baby powder and lifted using scotch tape from a phone surface	60	10	0 errors	0 errors	0 errors	0 errors
Latent inked fingerprint lifted using blu-tac from a wooden laminate	60	10	0 errors	4 errors	0 errors	0 errors
Fingerprint printed on matte paper	60	10	0 errors	0 errors	0 errors	60 errors
Wax fingerprint created using a play-doh mould	60	10	0 errors	0 errors	0 errors	60 errors
Play-doh fingerprint created using a wax mould	60	10	5 errors	4 errors	0 errors	0 errors

ISO/IEC 30107-3 describes the bona fide presentation classification error rate (BPCER) as the proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario. The standard defines bona fide presentation non-response rate (BPNRR) proportion of bona fide presentations that cause no response at the presentation attack detection (PAD) subsystem or data capture subsystem. ISO/IEC 2832 – 37 defines false reject rate (FRR) as the proportion of verification transactions with true biometric claims erroneously rejected.

Evaluation of the IUT against bona fide presentations was undertaken under three presentation scenarios:

1. **Dry fingerprint (bona fide presentation)**

[4] RIAPAR is described as sum of impostor attack presentation identification rate (IAPAR) and false reject rate (FRR) at a fixed decision threshold. Here FRR pertaining to 20 bona fide presentations (i.e., no adverse quality presentations) was considered.

This scenario reflects a bona fide presentation, where a subject presents their fingerprint as intended for identification. Each member of the test crew completed two tests under this scenario. This resulted in 20 tests.

2. **Moist fingerprint**
   In this scenario, the focus is on adverse quality situations where the subject's fingers are moist or sweaty during the authentication attempt. Each member of the test crew completed two tests under this scenario. This resulted in 20 tests. 2 Failure to acquire (FTA) were measured for this test case.
3. **Wet fingerprint**
   This scenario simulates adverse conditions where the subject attempts authentication in wet environments, such as outdoors during rainy weather. Each member of the test crew completed two tests under this scenario. This resulted in 20 tests. 2 Failure to acquire (FTA) were measured for this test case.

The table below provides a summary of IUT performance for bona fide presentations.

Table 14 Summary of performance metrics: bona fide presentations and live presentations under varying quality conditions

Presentation	Total number of presentations	Total number of sources	BPCER	BPNRR
Subjects presented their own face in the manner intended for the application	20	10	0 errors	0 errors
Subjects' fingers were moist or sweaty during the authentication attempt.	20	10	2 errors	0 errors
Subject attempted authentication in wet environments, such as outdoors during rainy weather	20	10	2 errors	0 errors

D. FINDINGS AND RECOMMENDATIONS

ISO/IEC 30107-3 covers the presentation attack types, system operational types, and evaluation techniques. This report confirms only the following item tested: RealScan G10/G10i [HW version: V02C (RS-G10) / V02A (RS-G10i), SDK version: 2.0.0: item under test (IUT) for PAD evaluation to Level 1 sophistication.

The purpose of this report is to report on the testing that was undertaken as well as the metrics that were gathered as an outcome of the testing. Attacks involved 6 Level A (or Level 1) classification attacks. Testing of PAD mechanism of the IUT corresponded to evaluation of the full system and the target of evaluation was the verification subsystem.

Findings

Refer to Evaluation Report section in this document.

Recommendations

There are no recommendations from BixeLab.

Constraints

Refer to section Evaluation Details for constraints associated with this evaluation.

Deviations and Exclusions

BixeLab has undertaken every step to ensure no deviations or omissions from the ISO/IEC 30107-1 and ISO/IEC 30107-3 standards were made.

Conclusions

There are no other comments or thoughts from BixeLab that are not addressed in this report.

Dr. Ted Dunstone

Chief Executive Officer

ted@bixelab.com

6th March 2024

APPENDIX A: EVALUATION MANAGEMENT

Effective test management is critical to ensuring usable data is produced for analysis. Test management will involve factors such as:

- Ensuring that all data is collected accurately and in a relevant manner.
- Associating test subject IDs with the correct individuals to maintain ground truth in presentation attack test cases.
- Effective data logging at the completion of each test during execution
- To measure performance, conduct evaluation in such a way that the IUT is tested as per the applicable standards. For example, for PAD evaluation, the IUT must be first evaluated against simple attacks, with attack potential progressively increased.

Data and Privacy Management

Testing process requires the exposure of a limited amount of Personally Identifiable Information (PII). To the maximum extent possible BixeLab seeks to protect privacy of test subjects by:

- Ensuring explicit consent and understanding of the required personal data to perform testing
- Ensuring the minimum required personal data is collected
- Performing all test transactions within the BixeLab laboratory or office where possible. If off-site testing is required, BixeLab will monitor test conditions and report accordingly.
- Recording only transaction results relevant to the evaluation
- Deleting/destroying all transaction data as soon as possible after completion of the transaction
- Referring to test subjects only by deidentified tester ID's and demographic groupings in the Testing and Evaluation Report
- Ensuring a statement of compliance by the vendor that data is not retained or used other than in accordance with the test processes, including complete removal of all test data upon completion of the tests.

System Configuration Management

The client is expected to provide the technology to be evaluated. The hardware and software configurations associated with these are monitored throughout the evaluation period.

IT Audit logs produced for each day of testing record data such as equipment ID, manufacturer and model name, operating system names and versions, identified anomalies if any, system version, date, time, and any other relevant specifications for all software/hardware utilised to conduct the review.

Test Readiness Criteria

A test readiness review is performed to assess whether the IUT is ready for formal testing by determining whether the test procedures are complete and confirming compatibility with test plan. This readiness review is conducted at the start of the evaluation process and includes the following:

1. Review of the proposed test plan

2. Formalising a plan for data collection to ensure high data quality and consistency for test analysis.
3. Ensuring the planned test cases are fit for purpose.
4. Ensuring the selected artefacts for evaluation are fit for purpose.

Test Completion Criteria

The evaluation will be considered complete if the data collected during the evaluation enables effective measure of IUT in terms of the following criteria as applicable to the evaluation scope:

1. Measuring likelihood of a presentation attack spoofing the liveness detection mechanism
2. Measuring likelihood of a live (bona fide) customer failing the liveness detection mechanism
3. Measuring biometric matching performance of the matching subsystem
4. Measuring the performance of the end-to-end system

Test Environment

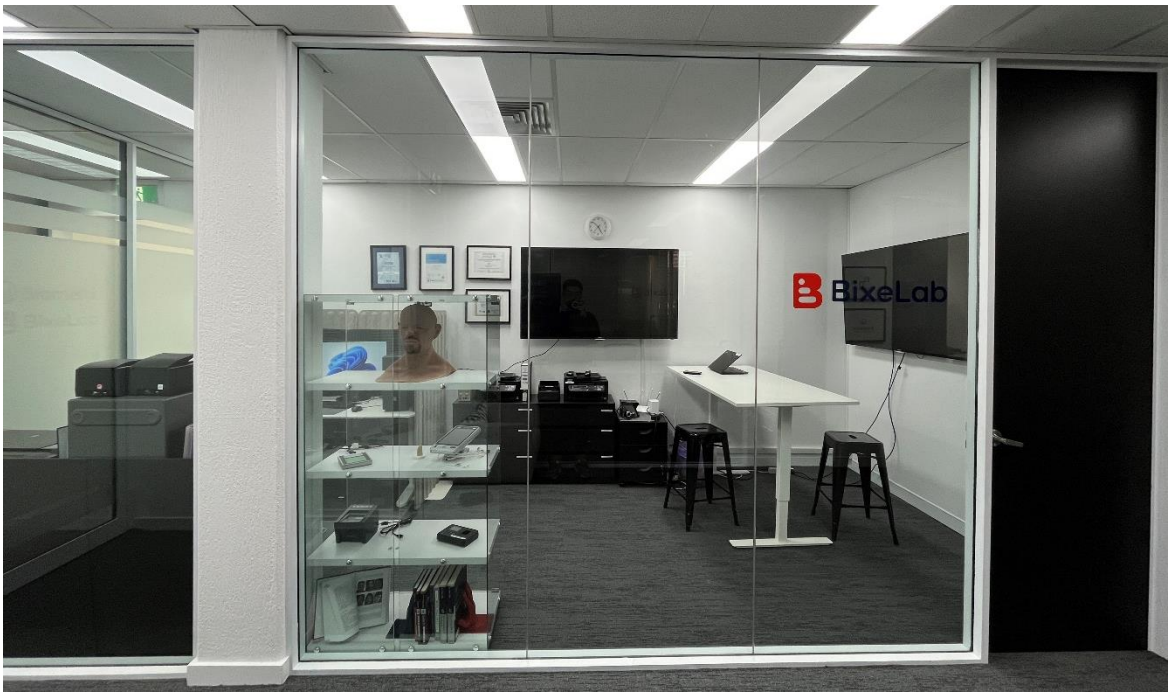


Figure 3 Layout of the BixeLab physical testing environment

The evaluation will be held at BixeLab headquarters, 3/16 Bentham Street, Yarralumla, ACT 2600. Figure 2 shows the layout of the test laboratory, which includes dedicated workstations for the system under test, test crew and test operator.

The testing environment will be carefully controlled to ensure that external factors such as temperature and lighting conditions do not have an impact on system performance. This information will be recorded at the beginning of each test session. If severe deviations are found, corrections will be made to ensure consistent testing conditions. An IT audit will also be completed for all evaluations, monitoring, and recording the IT components used for testing.

Test Setup

A detailed overview of the actual test set up will be provided in the final test report. Figure below provides the expected test set up for the IUT.



Figure 4 Example of the IUT set up

APPENDIX B: TERMS AND DEFINITIONS

Table 15 Terms and definitions

Term	Abbreviation	Definitions
Presentation Attack Detection Evaluation		
Attack potential		Measure of the capability to attack an IUT (TOE) given the attacker's knowledge, proficiency, resources, and motivation
Attack presentation acquisition rate	APAR	Proportion of attack presentations using the same PAI species from which the data capture subsystem acquires a biometric sample of sufficient quality
Attack presentation classification error rate	APCER	Proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario
Attack presentation non-response rate	APNRR	Proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem
Attack type		Element and characteristic of a presentation attack, including PAI species, concealer or impostor attack, degree of supervision, and method of interaction with the capture device
Bona fide presentation		Interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system
Bona fide presentation classification error rate	BPCER	Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario
Bona fide presentation non-response rate	BPNRR	Proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem
Concealer attacks		When an actor attempts to subvert the system by concealing that their biometric is enrolled in the system

Term	Abbreviation	Definitions
Ground Truth		Ground truth is the actual state of nature, as pertaining to a match. In other words, it is the truth of whether or not a given match is genuine or imposter.
Impostor attack presentation accept rate	IAPAR	Proportion of impostor attack presentations using the same presentation attack instrument (PAI) species that result in accept
Liveness detection		Measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture
Mobile device		Small, compact, handheld, lightweight, standalone computing device, typically having a display screen with digitizer input and/or a miniature keyboard
Normal presentation		Interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system
Presentation attack	PA	Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system
Presentation attack detection	PAD	Automated discrimination between bona fide presentations and biometric presentation attacks
Presentation attack instrument	PAI	Biometric characteristics or object used in a biometric presentation attack
Presentation attack species	PAS	Class of presentation attack instruments created using a common production method and based on different biometric characteristics
PAI creator		Set of one or more individuals or mechanisms responsible for the conception, formulation, design, and realization of a PAI species
PAI presenter		Set of one or more individuals or mechanisms presenting the PAI to the biometric system

Term	Abbreviation	Definitions
PAI series		Presentation attack instruments based on a common medium and production method and a single biometric characteristic source
PAI source		Set of one or more individuals or mechanisms from which biometric samples are obtained for use in a PAI, realized in a PAI series
PAI species		Class of presentation attack instruments created using a common production method and based on different biometric characteristics
System under test	SUT	The system that implements the standard(s) being tested
Quality Instruments		A test instrument for quality testing e.g. a spotlight
Target of evaluation	TOE	Within Common Criteria, the IT product that is the subject of the evaluation. Note: The TOE in Common Criteria evaluations is the equivalent of IUT in biometric evaluations.
Test approach		Totality of considerations and factors involved in PAD evaluation
Test Subject		A person who has been recruited to participate in a biometric evaluation.
Biometric Performance Evaluation		
Biometric candidate		Biometric reference identifier of a biometric reference in the biometric reference database determined to be sufficiently similar to the biometric probe to warrant further analysis
Biometric probe		Biometric sample or biometric feature set input to an algorithm for biometric comparison to a biometric reference(s)
Comparison score		Numerical value (or set of values) resulting from a comparison
Mated		Of or having to do with a paired biometric probe and biometric reference that are from the same biometric characteristic of the same biometric data subject

Term	Abbreviation	Definitions
Non-mated		Of or having to do with a paired biometric probe and biometric reference that are not from the same biometric characteristic of the same biometric data subject
Authentication		The act of proving or showing to be of undisputed origin or veracity
Biometric mated comparison trial		Comparison of a biometric probe and a biometric reference from the same biometric capture subject and the same biometric characteristic as part of a performance test
Biometric non-mated comparison trial		Comparison of a biometric probe and a biometric reference from different biometric data subjects as part of a performance test
Failure to acquire	FTA	Failure to accept for subsequent comparison the output of a biometric capture process, a biometric sample of the biometric characteristic of interest
Failure to enrol	FTE	Failure to create and store a biometric enrolment data record for an eligible biometric capture subject, in accordance with a biometric enrolment policy
False match rate	FMR	Proportion of the completed biometric non-mated comparison trials that result in a false match
False non-match rate	FNMR	Proportion of the completed biometric mated comparison trials that result in a false non-match
Subject		The person from whom the biometric enrolment was taken. The target of the attack
Target of evaluation	TOE	Within Common Criteria, the IT product that is the subject of the evaluation. Note: The TOE in Common Criteria evaluations is the equivalent of IUT in biometric evaluations.
Test approach		Totality of considerations and factors involved in technology evaluation

APPENDIX C: REFERENCES

Table 16 References

Version Number	Title	Abbreviation/ BixeLab code	Date	Owner
	Contractual Documents			
	230215_Service Assurance Agreement BixeLab and Suprema 27.3.2023		March 2023	Xperix-BixeLab
	Suprema Multi Service Proposal FINAL		August 2022	Xperix-BixeLab
	Project Documents			
V1.0	23-021-TP-03 Xperix PAD RealScan G10 - Test Plan v1.0	23-021-TP-03	December 2023	Xperix
	RS-G10_test_program_manual	External	December 2023	Xperix
	Standards and Frameworks			
2016	ISO/IEC 30107 Biometric performance testing and reporting part 1		2016	BixeLab
2017	ISO/IEC 30107 Biometric performance testing and reporting part 3		2017	BixeLab
2023	ISO/IEC 30107 Biometric performance testing and reporting part 3		2023	BixeLab
2022	ISO/IEC 2382 Vocabulary Part 37 Biometrics		2022	BixeLab
2020	NIST Handbook 150:2020, NVLAP procedures and general requirements		2020	BixeLab
2009	NIST Handbook 150-25:2009, NVLAP Biometrics Testing		2009	BixeLab

APPENDIX D: CONFIGURATION AUDIT

Figure 5 Images of configuration audit

- To record the findings associated with each testing day, please add rows against each fillable item
- Each log MUST be dated with all applicable information associated with the respective item as per requirements
- The IT Audit Log corresponding to each Project MUST be stored on LIMS under IT Audit Logs --> Client IT Audit Logs
- Please save the spreadsheet with client name at the end

AUDIT RESULT	YES/NO	Date	COMMENT (IF NOT THE SAME)
The information below was gathered BEFORE and AFTER testing was conducted and was found to be the same			

Comprehensive Audit (at the Start and End of testing)

	Before testing:		After testing:		Comments
Software	**Version**	**Build**	**Version**	**Build**	
Windows 11 Pro	23H2	22631.2861	23H2	22631.2861	
Windows 11 Pro	23H2	22631.2861	23H2	22631.2861	
Windows 11 Pro	23H2	22631.2861	23H2	22631.2861	
Windows 11 Pro	23H2	22631.2861	23H2	22631.2861	
Windows 11 Pro	23H2	22631.3007	23H2	22631.3007	Computer auto updated therefore there is a change of OS build
Windows 11 Pro	23H2	22631.3007	23H2	22631.3007	
Windows 11 Pro	23H2	22631.3007	23H2	22631.3007	
Windows 11 Pro	23H2	22631.3007	23H2	22631.3007	
Windows 11 Pro	23H2	22631.3007	23H2	22631.3007	
Windows 11 Pro	23H2	22631.3007	23H2	22631.3007	

CLIENT NAME: Suprema

Specifications regarding the test being conducted are noted below

Test Case	Test Objective	Date	Validator(s)
Pre-testing and set up Xperix devices	Pretest Xperix G10 & G10i to get expected outputs and to set up the devices. Xperix sending 2 will mean that gap analysis testing will be needed for the 2 devices.	20-Dec-23	MH,EM
Pre-testing and set up Xperix devices	Continuation pretest Xperix G10 & G10i to get expected outputs and to set up the devices. Xperix sending 2 will mean that gap analysis testing will be needed for the 2 devices.	21-Dec-23	MH,EM
Commencement of Test Execution	First testing session for Xperix G10i (Due to the similarity of the two devices it was decided that only one will be tested and G10i was the device selected)	8-Jan-24	MH
Continuation of Test Execution	Second testing session for Xperix G10i	9-Jan-24	MH
Continuation of Test Execution	Third testing session for Xperix G10i	10-Jan-24	TB
Continuation of Test Execution	Completion of Level A and Commencement of Level B testing	15-Jan-24	MH, TB
Continuation of Test Execution	Continuation of Level B Testing	15-Jan-24	MH
Continuation of Test Execution	Continuation of Level B Testing	17-Jan-24	EM
Additional Testing	Required retesting to be completed	4-Mar-24	MH
Additional Testing	Required retesting to be completed	5-Mar-24	MH

The Client hardware system specifications are noted below

Manufacturer & Model Name	Specifications	BXL CODE (If Applicable)	Operating System	Serial Number	Identified Anomalies	Firmware Version	Date and Time Check Performed
Xperix RealScan G10		BXL019 - 1	N/A	5709593	N/A		20/12/2023 1:59 PM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		20/12/2023 1:59 PM
Xperix RealScan G10		BXL019 - 1	N/A	5709593	N/A		21/12/2023 8:30 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		21/12/2023 8:30 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		08/01/2024 10:50 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		09/01/2024 9:42 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		10/01/2024 10:00 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		15/01/2024 8:29 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		16/01/2024 9:46 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		17/01/2024 9:32:00 AM
Xperix RealScan G10		BXL019 - 1	N/A	5709593	N/A		04/03/2023 9:00 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		04/03/2023 9:00 AM
Xperix RealScan G10i		BXL019 - 2	N/A	5714217	N/A		05/03/2023 9:29 AM

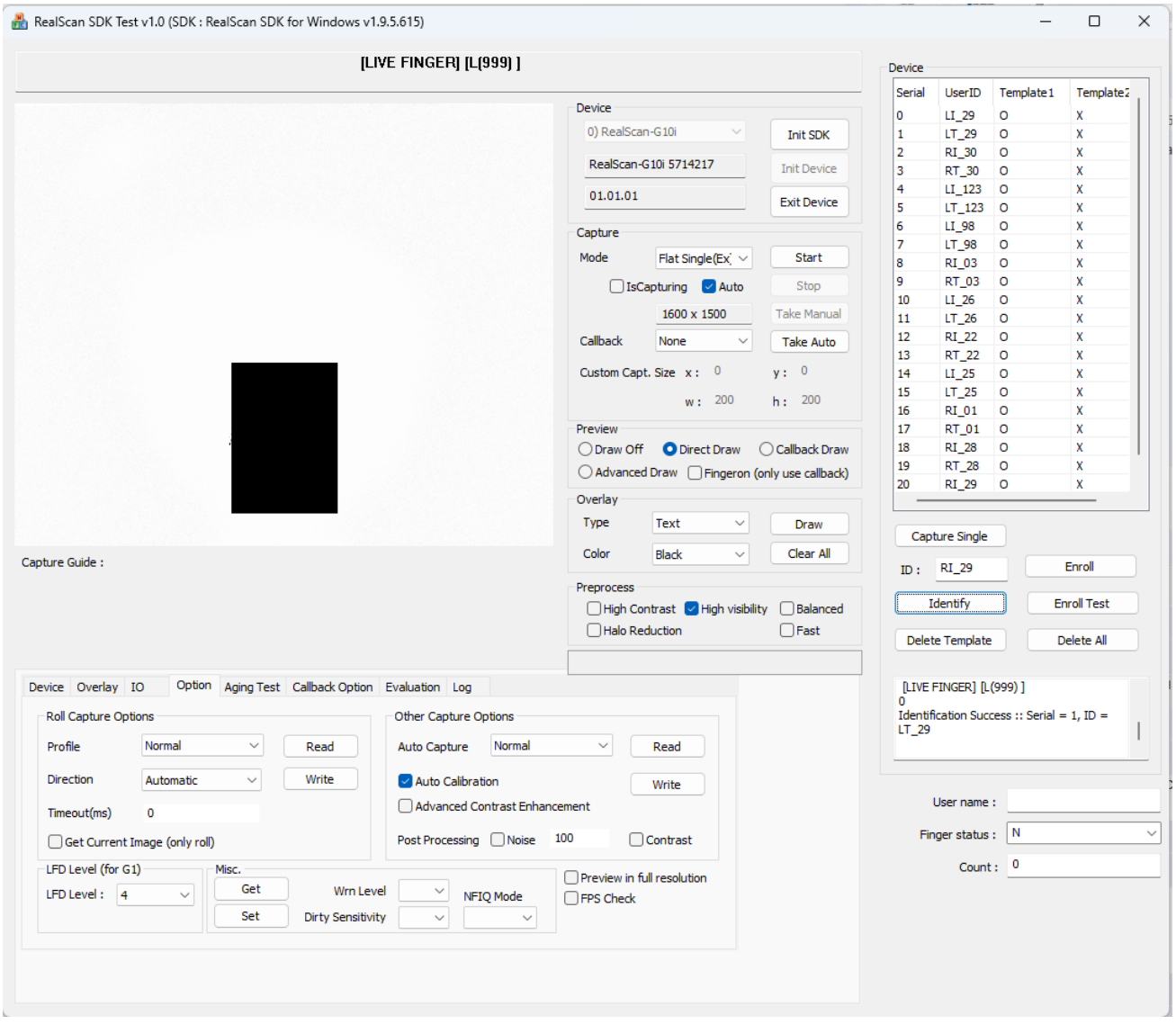
BixeLab hardware system specifications are noted below

Manufacturer & Model Name	BXL CODE (If Applicable)	Operating System	Identified Anomalies	Firmware Version	Date and Time Check Performed
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	20/12/2023 1:59 PM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	21/12/2023 8:30 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	08/01/2024 10:50 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	09/01/2024 9:42 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	Windows automatically updated despite auto-update being turned off causing the loss of enrolment templates	23H2	10/01/2024 10:00 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	15/01/2024 8:29 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	16/01/2024 9:46 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	17/01/2024 9:32:00 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	04/03/2023 9:00 AM
WIN-DSK-BL	BXL138	Windows 11 Pro	N/A	23H2	05/03/2023 9:29 AM

APPENDIX E: APPLICATION FOR IUT ASSESSMENT

Figure below provides a pictorial representation of the application SDK received for testing of the IUT using Windows - RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615).

Figure 6 Image of SDK for IUT



APPENDIX F: ADDITIONAL TESTING

Purpose

Under the contract with BixeLab, Xperix exercised their option for retesting to validate the performance of the RealScan-G10 and RealScan-G10i scanners [HW Version: V02C & V02A, SDK Version: v2.0.0] against specific presentation attack instruments (PAIs) and test subjects that had previously succeeded in spoofing the system during primary testing. Xperix submitted a revised SDK to BixeLab for this additional testing, with assurances that no changes impacting the biometric components of the Integrated Under Test (IUT) were made, ensuring the liveness detection and biometric matching subsystems, among other system components, remained unchanged.

Additional testing was undertaken across all 6-presentation attack instrument (PAI) species, with higher number of tests completed for PAI species against which errors were measured during primary testing.

Test Crew

The crew selected for the additional testing consisted of test subjects whose PAIs had previously succeeded in spoofing the system, along with an additional subject whose PAIs had not achieved any successful spoofs, aiming to verify the SDK's consistent performance across different subjects.

Presentation Attack Instruments

For the additional testing, a focus was placed on retesting all Level A PAIs, with particular attention on two PAIs that had led to successful spoofs in the past. The transaction volume for these PAIs was increased to ensure thorough testing. The two primary PAIs focused on were:

1. Latent inked fingerprint lifted using blu-tac from a wooden laminate
2. Play-doh fingerprint created using a wax mould.

Table below provides a breakdown of the number of sources and number of attacks mounted against each category of attack.

Table 17 Breakdown of applicable presentation attack instrument (PAI) species (Additional Testing)

Level	PAI Species Label	PAI Species description	Number of sources used	Total number of attacks	Creation Method	Presentation technique
A	**Latent Fingerprint lifted from Ceramic surface using graphite powder and scotch tape**	Test Subjects' fingerprints were placed on a ceramic plate. This fingerprint was dusted with graphite powder and was lifted using Scotch Tape. This lifted fingerprint on the tape was presented directly to the sensor.	4	24	Uncooperative – Biometric characteristics were captured simulating uncooperative conditions (i.e., participant waving in	Lifted fingerprint mounted directly onto the scanner

Level	PAI Species Label	PAI Species description	Number of sources used	Total number of attacks	Creation Method	Presentation technique
	Latent Fingerprint lifted from phone surface using baby powder and scotch tape	Test Subjects' fingerprints were placed on an iPad screen. This fingerprint was dusted with baby powder and was lifted using Scotch Tape. This lifted fingerprint on the tape was presented directly to the sensor.	4	24	a photo). This is to simulate an attacker sourcing biometrics from social media and other publicly available photo sources.	
	Latent inked fingerprint lifted from wood surface using blu-tac	Test Subjects' fingerprints were placed on a wooden table using ink. This inked fingerprint lifted using blu-tac. This lifted fingerprint on the blu-tac was presented directly to the sensor.	4	48		
	2D Print on Matte	Test subjects placed their fingerprints on a wooden laminate. This fingerprint was dusted with magnetic dust. A high-quality image of the dusted fingerprint was taken, processed, and later printed on matte paper to match the size of the scanner. This print was presented directly to the sensor.	4	24	Cooperative – Biometric characteristics were captured directly from test crew participants in addition to some additional participants who did not participate in person but provided their biometrics for the purpose of creating presentation attacks.	2D paper fingerprint mounted directly onto the scanner
	Wax fingerprint using Playdoh mould	Test Subjects' left their fingerprints on some playdoh which was used as a mould. Molten wax was poured into this mould, to produce a wax fingerprint. This wax fingerprint was presented directly to the sensor.	4	24		Wax fingerprint mounted directly onto the scanner
	Playdoh fingerprint using Wax mould	Test Subjects' left their fingerprints on some melted wax which was used as a mould. A ball of playdoh was pressed against this mould to acquire a Playdoh fingerprint. This Playdoh fingerprint was presented directly to the sensor.	4	48		Play-doh fingerprint mounted directly onto the scanner

Pre-testing

The IUT underwent pre-testing with both scanners to confirm performance consistency. This step determined no significant performance differences between the scanners, allowing for the continuation of additional testing with only the RealScan G10i, adhering to the constraints from the primary testing.

Results and Findings

The additional testing results revealed improvements in the detection capabilities of the IUT. Notably, the IUT successfully identified all lifted inked fingerprints as spoofs, a marked improvement over the results from the primary testing. The Play-doh fingerprint created using a wax mould demonstrated similar performance to the primary testing, indicating persistent vulnerabilities.

An unexpected outcome was the passage of one lifted graphite fingerprint and one lifted baby powder fingerprint in the liveness detection tests, however these attacks were prevented by the matching system subcomponent.

Table 18 Summary of applicable performance metrics as measured for the IUT: attack presentations (Additional Testing)

Presentation Attack Instrument (PAI) species	Total number of PAI presentations	Total number of PAI sources	APCER	IAPAR	RIAPAR[5]	APNRR
Latent fingerprint dusted with graphite powder and lifted using scotch tape from a ceramic surface	24	4	1 error	0 errors	0 errors	0 errors
Latent fingerprint dusted with baby powder and lifted using scotch tape from a phone surface	24	4	1 error	0 errors	0 errors	0 errors
Latent inked fingerprint lifted using blu-tac from a wooden laminate	48	4	0 errors	0 errors	0 errors	0 errors
Fingerprint printed on matte paper	24	4	0 errors	0 errors	0 errors	24 errors
Wax fingerprint created using a play-doh mould	24	4	0 errors	0 errors	0 errors	24 errors
Play-doh fingerprint created using a wax mould	48	4	9 errors	5 errors	0 errors	0 errors