ISO/IEC 30107-3 Presentation Attack Detection Level 1 Evaluation – Test Report

Prepared for

Xperix Inc.

By

BixeLab

3/16 Bentham Street, Yarralumla,
ACT 2600, Australia

Presentation Attack Detection Evaluation for:

RealScan S60/S60M: Fingerprint Scanner

HW Version: v1.9.5

SDK Version: v1.6.6

Attention: Changmin Kim

cmkim@suprema.co.kr

NVLAP TESTING
NVLAP LAB CODE 600301-0

Document Code 23-021-TR-10

Submit Date: 25th August 2023

Submitted by BixeLab Pty Ltd

Contact Ms. Somya Singh



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 the 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.

Version History			
Version Number	**Description of change**	**Author**	**Date**
V1.0	Level 1 Test Report	BixeLab	25th August 2023

Table of Contents

Executive Summary 5

1.0 Introduction 7

1.1. Background 7

1.2 Test Objectives 7

1.3 Test Constraints 8

1.4 Test Scope 8

2.0 System Description 10

2.1 System Information 10

2.2 Concept of Operations 10

2.3 Configuration Audit 12

3.0 Expected Outputs 13

Expected Output Data 13

Expected Output Performance 13

4.0 Dataset Description 14

Test Crew Profile 14

Planned Presentation Attack Instrument Types 15

5.0 Test Methodology 17

Pre-Test Assessment 17

Test Execution 17

Post Test Review 18

6.0 Performance Results 19

Bona fide Presentations 19

Attack Presentations 20

7.0 Findings 22

Appendix 1: Application for IUT Assessment – Overview 23

Appendix 2: Configurations Audit Logs 24

Appendix 3: System Information 30

Appendix 4: ISO/IEC 30107-3 Reporting Requirements 31

Executive Summary

This report presents the findings from the Level 1 Presentation Attack Detection (PAD) evaluation of the RealScan S60/S60M fingerprint authenticator (IUT) with Hardware version V1.9.5 and SDK version v1.6.6 tested using the accompanying application - RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615). The evaluation, conducted in July 2023, aimed to assess the robustness of the IUT against biometric imposter presentation attacks, following the guidelines of ISO/IEC 30107-1 and ISO/IEC 30107-3 standards. This report contains findings from the PAD Level 1 test efforts. A similar report for PAD Level 2 will follow.

Key Findings

60 presentation attack detection tests were completed using each attack type (presentation attack species) – 360 tests in total. 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. 1 presentation attack involving a latent inked fingerprint lifted from a wooden surface using blue tac was able to successfully pass the quality assessment, liveness detection, and achieve a match, thus leading to a successful attack. The testing could not replicate this presentation attack.

Table below provides an overview of the performance measured for the IUT:

Presentation Attack Species	Total Attacks	Failure to Acquire	Fake Finger Detected	Identification Failed	Identification Passed
Latent fingerprint dusted with graphite powder and lifted using scotch tape from a ceramic surface	**60**	**0**	**52**	**8**	**0**
Latent fingerprint dusted with baby powder and lifted using scotch tape from a phone surface	**60**	**0**	**52**	**8**	**0**
Latent inked fingerprint lifted using blu-tac from a wooden laminate	**60**	**6**	**40**	**13**	**1**
Fingerprint printed on matte paper	**60**	**0**	**53**	**7**	**0**
Wax fingerprint created using a play-doh mould	**60**	**60**	**0**	**0**	**0**
Play-doh fingerprint created using a wax mould	**60**	**60**	**0**	**0**	**0**
Overall	**360**	**126**	**197**	**36**	**1**

60 bona fide presentations were subjected to evaluation using a series of tests. These tests comprised 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. The analysis of these evaluations resulted in an overall Bona fide Presentation Classification Error Rate (BPCER) of 0%, along with a Bona fide Presentation Non-Response Rate (BPNRR) of 6.7%, indicating a minimal rate of non-responsiveness to adverse quality presentations.

The testing adhered to the methodologies specified in the ISO/IEC 30107-3 standard. BixeLab conducted a Level 1 PAD evaluation, comprising 360 Level A attack presentations, including 180 cooperative and 180 uncooperative scenarios. Additionally, 60 bona fide tests were performed with a test crew of 10 unique and consenting individuals. 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

See section **Performance Results** for a detailed overview of Presentation Attack Detection Performance Metrics measured.

This report tests compliance of the presentation attack/liveness detection mechanism against common attack types that meet the Level 1 criteria outlined in ISO/IEC 30107 and other relevant standards. It is important to acknowledge that attacks are constantly evolving. After conducting thorough research and considering the context of the system under test (IUT), relevant attacks were selected. These selections were also based on Xperix Inc.’s claims, the feasibility of creating an attack tool, and the ISO-defined level that the attack tool corresponds to. As this is a Level 1 PAD test report, the results and findings solely pertain to Level A attacks.

1.0 Introduction

This document defines the results for the evaluation of Xperix inc.'s RealScan S60/S60M with Hardware v1.9.5 and SDK version v1.6.6 – Item Under Test (IUT). Testing was conducted in compliance with the applicable principles and methods for performance assessment of Presentation Attack Detection (PAD) mechanisms as per the following standards:

1. ISO/IEC 30107-1: Information technology – Biometric presentation attack detection – Part 1: Framework
2. ISO/IEC 30107-3: Information technology – Biometric presentation attack detection – Part 3: Testing and Reporting

1.1. Background

Xperix Inc., the provider of the RealScan S60/S60M with Hardware version v1.9.5 and SDK version v1.6.6 with Presentation Attack Detection (PAD) mechanisms, has engaged BixeLab as an independent and accredited third-party biometric testing lab to conduct an ISO/IEC 30107-3 compliant PAD evaluation to Level 1. This evaluation aims to verify the performance of the PAD mechanisms.

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.

1.2 Test Objectives

The objective of this test report is to determine the robustness of the RealScan S60/S60M with Hardware v1.9.5 and SDK v1.6.6 - IUT for Presentation Attack Detection (PAD) completed to Level 1 sophistication. This is to meet both the NIST standards.

The evaluation of IUT PAD mechanisms was configured according to a BixeLab evaluation design that considered configurations and settings for – data capture (enrolment), test crew profile, the presentation attack instruments, verification metrics and componentry in the biometric subsystem.

This report has been formatted for key project personnel within Xperix Inc. The objective of the submission is to verify BixeLab's assessment of Xperix's technology as compliant with the applicable ISO/IEC 30107-1 & ISO/IEC 30107-3 standards.

1.3 Test Constraints

- The evaluation of the IUT's PAD Mechanisms was focused on vulnerability assessment, as the usage of a PAI against the biometric system is an effort to evade the IUT's security functions. During the IUT evaluation, only conventional and well-known presentation attacks were attempted as per the recommendations outlined in the ISO/IEC 30107-3 standard. Certain PAIs were also considered and used due to claims made against them by Xperix Inc. regarding the robustness of the IUT against such PAD attacks.
- The PAD evaluation was limited to assessing the system's ability to accept or reject a presentation attack. In this regard, the classification metrics presented in this document include APCER, BPCER, APNRR, and BPNRR, as well as IAPAR.
- 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 PAD subsystem (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 specific to the testing undertaken. BixeLab is not responsible for any claims made outside the results reported in this document.
- The preliminary evaluation of the IUT highlighted enrollment failures for bona fide fingerprint presentations. This was immediately communicated to Xperix, with a request for clarification on the requisite testing settings. Subsequent inquiry uncovered that the accompanying IUT software lacked essential registration and authentication components. However, certain adjustments had been made to incorporate features for PAD testing. These alterations potentially disrupted the liveness assessment during enrollment, owing to a bug within the provided liveness detection test program. Following a swift resolution, it was ascertained that the issue did not extend to the SDK version. This confirmation was substantiated by verifying the File version in the details tab upon right-clicking the RS_SDK.dll file.
- Technology provider has two variations of the RealScan S60 device - RealScan S60 fingerprint authentication scanner & RealScan S60M with Hardware version V1.9.5 and SDK version v1.6.6. Pretesting of both devices was undertaken to validate that the only difference between the two is the integrability of S60M variation along with lighter weight and a more compact size. On the basis of the exploratory test results, the testing was completed on RealScan S60 with Hardware v1.9.5 and SDK v1.6.6 - IUT to derive performance insights on the common PAD/liveness mechanisms.

1.4 Test Scope

This evaluation report is based on the objectives identified in the section above, and the following activities are defined within the operational scope of this evaluation:

- Conduct an ISO/IEC 30107-3 compliant assessment that derives PAD error rates using Level A attack types. The assessment targets the PAD mechanism of the item under test (IUT), specifically the RealScan S60/S60M with Hardware v1.9.5 and SDK v1.6.6. This evaluation centers 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 biometric verification system, all conducted under certified laboratory conditions. The primary objective is to test the security features of the PAD subsystem and assess the resilience of its performance against Level A attack types.

- The target of evaluation for testing was defined by the provider and was as follows: “live fingerprint is enrolled followed by PAD attacks on the verification”.
- The Level 1 PAD evaluation entails subjecting the IUT to Level A PAIs. This encompasses assessments involving both cooperative and non-cooperative attack types. Notably, in accordance with the ISO/IEC 30107 standard, attackers might directly obtain a capture subject's biometric characteristic. Such acquisition can be either cooperative (where the subject willingly provides their fingerprint to a sensor) or non-cooperative (where the subject leaves a fingerprint on a surface or a biometric capture device, enabling the attacker to lift the fingerprint). Different attack scenarios are associated with each acquisition type, leading to potential differences in the quality of artifacts generated. Cooperative acquisitions may yield higher-quality artifacts compared to non-cooperative acquisitions, thereby influencing PAD rates and overall biometric performance rates.

The activities deemed outside of the scope of this evaluation report are.

- Evaluating performance variations of the IUT and biometric subsystem based on presentation data from individual variance in adjustments to makeup, hairstyles, smile, pose, etc.
- Evaluation of the end-to-end solution comprising a full end-to-end system check of operational performance by conducting a scenario evaluation with real human test subjects with biometric comparison tests into a PAD subsystem and data capture.

Evaluating the robustness of the PAD mechanism against all possible threat vectors in the operational scenario is outside of the scope of this lab evaluation. The reported performance of the IUT does not provide any information regarding its effectiveness in detecting presentation attacks which have not been tested.

2.0 System Description

2.1 System Information

This section provides information related to the Items Under Test (IUT) – **RealScan S60/*S60M* with Hardware version v1.9.5 and SDK version v1.6.6** for PAD evaluation. The item under test was accessed using a USB C to USB on a Windows XP Operating System within standard laboratory conditions. The exact specifications of the hardware and software utilised for this evaluation are in the Table below.

Table 1 System Information

IUT name (Fingerprint scanner)	Hardware (Scanner)	Software (utility)	SDK (Fingerprint Scanner)	BixeLab OS (Laptop)	BixeLab Hardware (Laptop) Code
RealScan S60	Hardware version v1.9.5	v1.9.5.615	SDK version v1.6.6	Windows XP (version 21H2)	BXL129 OS build: 19044.3086

2.2 Concept of Operations

The test cases for evaluation of the IUT PAD mechanisms were designed to mimic the functional and procedural aspects under conditions expected for operational security for PAD. The evaluation of PAD mechanisms and the reported test results are based on NIST-established definitions of common criteria, which state that presentation attack detection processes fall under the category of vulnerability assessment because using PAI against the biometric system is an attempt to circumvent the security mechanisms of the IUT.

RealScan UI SDK v1.9.5 Application was installed onto the BixeLab laptop device - Windows XP (version 21H2), to get results associated with the testing. The settings for this application were dictated by the provider and were as mentioned below:

- LFD (Live Finger Detection) Level was set to 4
- Capture Mode was set to Flat Single (Ex)
- Rest of the settings were left as they were (Default)

Refer to Appendix 1: Application for IUT Assessment – Overview for information relating to the desktop Application utilised to assist with the PAD evaluation.

The Target of Evaluation (ToE) was the verification subsystem with PAD mechanisms. Figure below provides an overview of the process flow relating to PAD testing of the IUT –

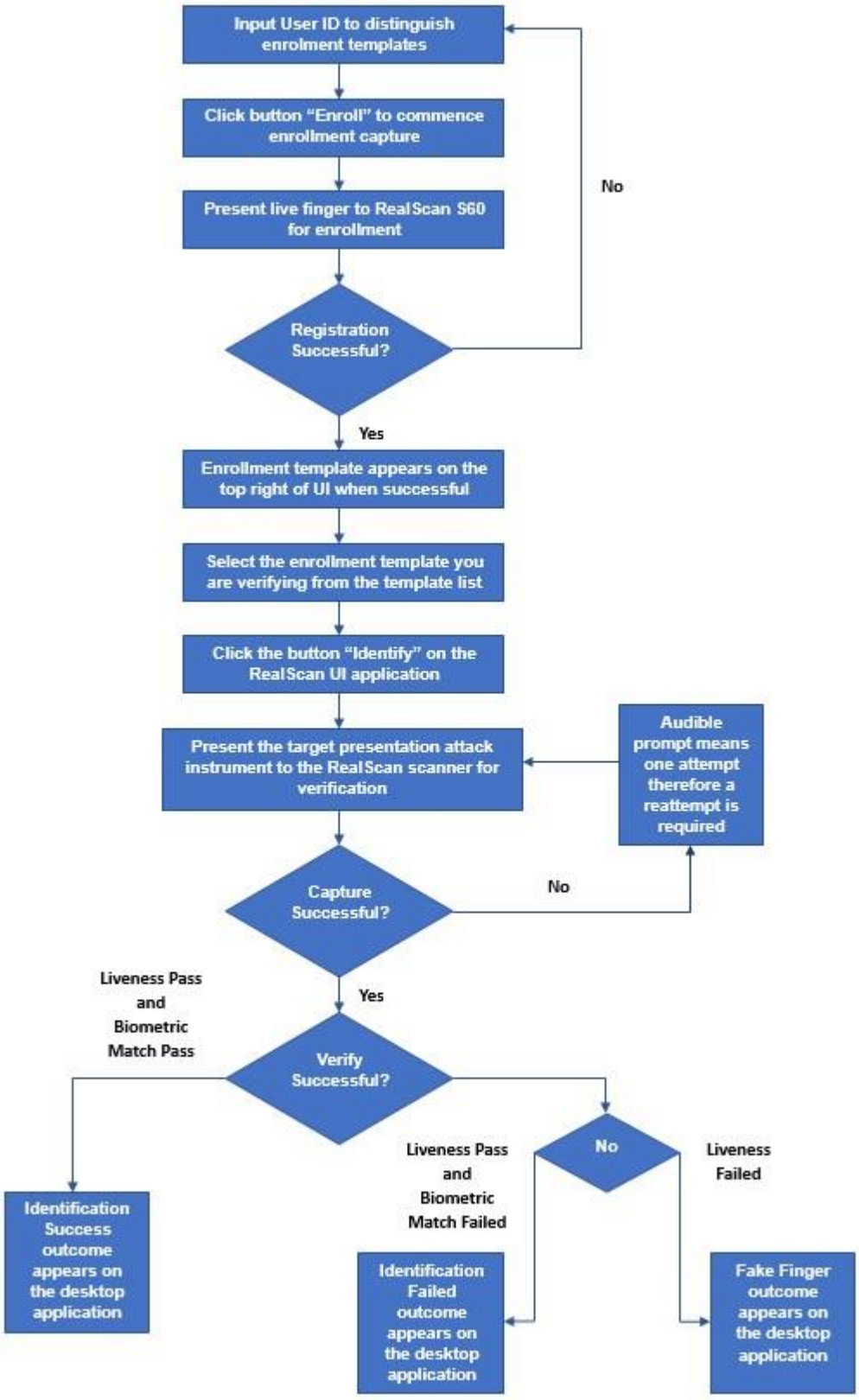


Figure 1 Test Process Flow (Overview)

2.3 Configuration Audit

An audit of the system configuration in the IUT submitted for PAD evaluation was conducted on each day of testing. The information recorded is outlined in an audit log that includes hardware and software specifications, OS versions, serial number, and build.

This audit log is to verify that all software and hardware configurations related to each testing remained unchanged through the execution. The aim is to mitigate system software and hardware related variations and to perform essential laboratory protocol for integrity.

Tables in the Appendix 2: Configurations Audit Logs provide detailed configuration audit logs focusing on the above with no identified anomalies.

3.0 Expected Outputs

Expected Output Data

A summary of the output data related to PAD mechanisms of the IUT is provided below. The data fields identified in bold format represent the target of evaluation.

Table 2 Summary of expected output data

Target of Evaluation (ToE) interpreted component	BixeLab Interpreted Outcomes	Configured Outcomes
Enrollment	Enrollment Successful	Enrollment Template Saved
	Enrollment Failed	Fake Finger
Verification	**Capture Successful**	**-**
	Capture Unsuccessful	**Audio Prompt**
	Liveness Failed	**Fake Finger**
	Liveness Pass, Match Failed	**Identification Failed**
	Liveness Pass, Match Pass	**Identification Success**

Expected Output Performance

In traditional biometric performance evaluations, ground truth plays a pivotal role to ensure the validity of the reported error metrics. In PAD evaluation context, the ground truth relates to whether a given liveness detection response is genuine and bona fide or represents an imposter (attack).

A bona fide presentation referred to a live human subject submitting fingerprints as directed by the application, and a presentation attack referred to the test operator mounting the target's biometric using a PAI.

The IUT used an LFD (Live Finger Detection) Level of 4 to make decisions for whether the acquired sample was live (Identification Success/ Identification Failed) or artificial (Fake Finger).

4.0 Dataset Description

This section provides details of the test crew recruited for this evaluation as well as the Presentation Attack Instrument (PAI) species tested.

Test Crew Profile

The recruitment of test subjects was aligned with the ISO/IEC 19795-5 recommendation for the purpose of enrolment and recognition in testing evaluations. As such, a test crew of 10 volunteers was recruited for PAD evaluation and composed according to requirements for uniqueness, voluntary consent to the amount and type of data to be collected, including the distribution of age, gender, and ethnicity. Summary of the test crew demographics is described in the tables below.

Table 3 Age group distribution

Age Range	BixeLab sourced
< 18 y/o	-
18 – 30 y/o	Yes
31 – 50 y/o	No
51 – 70 y/o	Yes
> 70 y/o	-

Table 4 Sex Distribution

Sex	BixeLab sourced percentage
Male	80%
Female	20%

Table 5 Ethnicity Distribution

Ethnic Origin	BixeLab sourced
European	Yes

Ethnic Origin	BixeLab sourced
Polynesian	-
North African and Middle Eastern	-
North-East Asian	Yes
Southern and Central Asian	Yes
Sub-Saharan African	-

For this evaluation, the aforementioned data was recorded. The pseudonymized 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 SUT 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. The test corpus was validated to ensure the following:

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

Planned Presentation Attack Instrument Types

This section provides an overview of the types of presentation attacks and attack scenarios used for purposes of testing.

This evaluation aimed to cover biometric imposter attack scenarios where the attacker intends to be recognized as an individual other than themselves. In this regard, the artefact properties will be in line with Clause 8 of ISO/IEC 30107-3 standard. Each presentation attack species had a minimum of 3 presentation attack instruments as per the best practice guidance in ISO/IEC 30107-4.

The table below provides an overview of the Level A presentation attack instrument species used for evaluation:

Presentation Attack Level	Artificial Presentation Attack Instruments	Source	Description	Description of Attack Scenario
Level A	Latent Fingerprint lifted from Ceramic surface	10	Test Subjects' fingerprints were placed on a ceramic plate. This fingerprint was dusted with graphite powder and was lifted	**Uncooperative –** Biometric characteristics were captured simulating

Presentation Attack Level	Artificial Presentation Attack Instruments	Source	Description	Description of Attack Scenario
	using graphite powder and scotch tape		using Scotch Tape. This lifted fingerprint on the tape was presented directly to the sensor.	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.
	Latent Fingerprint lifted from phone surface using baby powder and scotch tape	10	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.	
	Latent inked fingerprint lifted from wood surface using blu-tac	10	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.	
	2D Print on Matte	10	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.	**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. Photos of fingerprints were taken on a high-quality camera. Ink pressed fingerprints were acquired under supervision of test operators.
	Wax fingerprint using Playdoh Mold	10	Test Subjects' left their fingerprints on some playdoh which was used as a mold. Molten wax was poured into this mould, to produce a wax fingerprint. This wax fingerprint was presented directly to the sensor.	
	Playdoh fingerprint using Wax Mold	10	Test Subjects' left their fingerprints on some melted wax which was used as a mold. A ball of playdoh was pressed against this mould to acquire a Playdoh fingerprint. This Playdoh fingerprint was presented directly to the sensor.	

5.0 Test Methodology

This section provides an overview of the test execution sequence informed by the evaluation goals.

Pre-Test Assessment

This section provides an outline of the pre-testing activities undertaken, elucidating both the rationale behind test execution and the methodologies employed.

The setup process followed instructions from the IUT provider as per the test program manual provided on the 13th of July 2023. These instructions related to configuring the desktop application settings for viewing logs related to the IUT. Once the setup was done, the pre-test assessment began. The main goal of this assessment was to understand the process flow and validate planned test cases.

An overview of the pre-test assessment process is provided below:

- Pre-test assessment was completed for bona fide presentations and impostor attacks using both variations of IUT provided – RealScan S60 and RealScan S60M to validate that the performance was consistent across the two.
- For the tests where a subject was able to successfully enrol, the bona fide presentations on verification side were generally successful leading to the "Identification successful" outcome.
- Impostor attacks were tested on both device types resulting in consistent outcomes and similar results in terms of ability to detect and identify attacks.
- The only difference between the two devices was the absence of an audible prompt for S60M after the red light turned off during scans.
- Pre-test assessment also revealed that the IUT did not have a time out/lock out feature after the maximum allowed re-attempts were reached. Based on this finding, following decision policies were used for the test execution:
    - A maximum of 5 re-attempts before a transaction is considered a "Failure to Acquire".
    - Each time the audible sound was recorded by the operator upon making an attempt prompted a re-attempt. This is indicated when the scanner omits red light.

Test Execution

Note: Initial phase of test execution revealed an issue pertaining to the IUT's ability to enrol live fingerprints. This was based on "Liveness Failed" outcomes for bona fide enrolment attempts by 3 live subjects for index and/or thumb. This was promptly communicated to the provider on the 25th of July 2023 and clarification sought to confirm the requisite settings for the accompanying utility provided for testing (v1.9.5.615). Based on the correspondence received, this was owing to a bug found which was promptly fixed. Following the resolution of this issue, confirmation was received that this has not impacted the version related to the IUT and testing resumed.

This section an overview of the test execution process.

Bona fide presentations and latent print collection for Impostor attack presentations.

1. Test subject is invited to the lab facility and provides consent.
2. Test subject provides a bona fide presentation for enrolment. Guidance on the target finger was provided by the test operator.
3. Test subject is then prompted to provide latent fingerprints on three surfaces – ceramic surface, phone screen, and inked fingerprint on wooden laminate. These latent prints were used for presentation attacks by the test operator later.
4. Test subject 3 bona fide presentations for verification under three test scenarios – moist, wet and dry.
5. Test operator records the results associated with the bona fide presentations.
6. Steps 1 to 5 are repeated for the next subject.

Impostor attack presentations

1. Test operator acquires the target attack instrument and selects the reference ID for the target enrollment on the utility.
2. When prompted to verify, operator mounts the target attack instrument.
3. Operator records the results associated with the attack presentation and wipes the surface of the scanner.
4. Steps 1 to 3 are repeated for the next attack instrument.

Post Test Review

A post-test review was performed to confirm that the evaluation was completed and to ensure the data collected during the evaluation enabled effective performance measurement of the item under test (IUT). For the PAD evaluation, this included the following:

1. Ensuring enough tests were completed and logged to ensure effective measurement of the IUT.
2. Completing formalised IT audit logs to ensure that the IUT remained consistent throughout the evaluation process.

6.0 Performance Results

This section provides the performance results associated with the PAD evaluation of Xperix Inc.'s RealScan S60: Fingerprint Scanner (HW Version: v1.9.5, SDK Version: v1.6.6) – item under test (IUT). The reported results are in line with the applicable specifications of ISO/IEC 30107-3. Following sections describe the testing completed on bona fide and Level A attack presentations.

Bona fide Presentations

ISO 30107 describes bona fide presentation classification error rate (BPCER) as the proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario.

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

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

Table below provides a summary of overall bona fide performance across the tested scenarios.

Table 6 bona fide performance rates

Bona fide Performance Rate	Bona fide Performance
Bona fide presentation count	60
Bona fide acquisitions	56
Bona fide non-responses	4
Bona fide Presentation Classification Error Rate (BPCER)	0%
Bona fide Presentation Non-Response Rate (BPNRR)	6.7%

Attack Presentations

Performance of PAD mechanism of the item under test (IUT) is expressed in terms of classification error rates and non-response rates as prescribed in the ISO/IEC 30107-3 standard. To assess the PAD mechanism, a total of 180 cooperative and 180 non-cooperative presentation attacks at Level A were employed. These tests involved the use of only the index finger and thumb, with an equal distribution of test subjects between left and right hands. This distribution ensured an equivalent number of presentation attacks per hand across the 10 test subjects.

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.

The figure below describes the overall presentation attack detection performance for the IUT.

93.3% of bona fide presentations (shown in blue) were successfully identified. The remaining 6.7% of bona fide presentations led to a failure to acquire (FTA), particularly in cases of adverse quality.

In total, there were 360 attack presentations across 6 different presentation attack instrument species: 90 each for the right index finger, right thumb, left index finger, and left thumb. The overall performance of the presentation attack detection (PAD) mechanisms at the verification subsystem can be summarized as follows:

- 126 cases exhausted all 5 attempts, constituting instances of Failure to Acquire (FTA).
- 197 cases were correctly identified as "Fake Finger," indicating accurate classification of attack presentations.
- 36 cases were labeled as "Identification Failed." These were attack presentations that initially passed the liveness/PAD check but failed to match during the subsequent verification attempt. On the PAD subsystem level, this still registered as a liveness/PAD pass.
- Only 1 case was classified as "Identification Success." This signifies a successful spoof, where the attack presentation passed the liveness/PAD check incorrectly and also succeeded in matching.

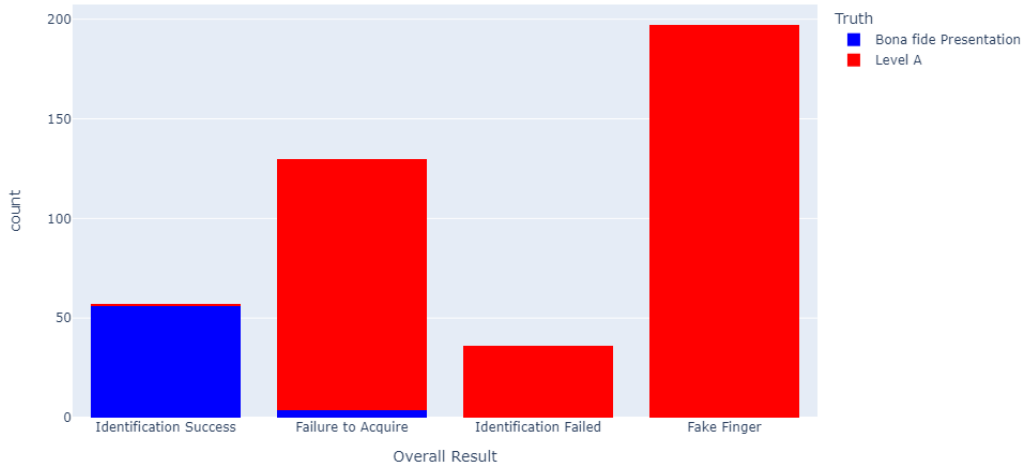


Figure 1 Performance overview: live presentations (blue) vs. presentation attacks (red)

The table below provides a summary of PAD performance metrics associated with assessment of the IUT at the Evaluation Assurance Level 1 using Level A attacks. Performance results measured against different finger types have been combined for the purposes of this evaluation. Results specific to individual fingerprint types can be provided upon request.

Table 7 PAD Subsystem Testing Results

Presentation Attack Level	Artificial Presentation Attack Instruments	Total Number of Attacks	Attack Presentation Classification Error Rate (APCER)	Impostor Attack Presentation Accept Rate (IAPAR)	Attack Presentation Non-Response Rate (APNRR)
Uncooperative	**Latent Fingerprint lifted from ceramic surface using graphite powder and scotch tape**	60	8	0	0
	Latent Fingerprint lifted from phone surface using baby powder and scotch tape	60	8	0	0
	Latent Inked Fingerprint lifted from a wooden laminate using blu-tac	60	13	1	6
Cooperative	**2D fingerprint on Matter Paper**	60	7	0	0
	Wax fingerprint using play-doh mould	60	0	0	60
	Play-doh fingerprint using wax mould	60	0	0	60

7.0 Findings

BixeLab has completed Level 1 PAD evaluation of RealScan S60/S60 M fingerprint authenticator (IUT) with Hardware version V1.9.5 and SDK version v1.6.6. The purpose of this document is to report on the testing that was undertaken as well as the metrics that were gathered as an outcome of the testing.

Among the total of 360 attack presentations, one attack of the uncooperative type, specifically the "inked thumb print latent lifted from a wooden laminate surface using blue tac," managed to successfully navigate through all layers of security. This encompassed being captured, eluding liveness detection mechanisms, and achieving a match. Testing could not repeat this attack (See Table 7 PAD Subsystem Testing Results).

For the 60 bona fide presentations, a 0% bona fide presentation classification error rate (BPCER) was measured.

Constraints

BixeLab has evaluated what it believes to be a representative sample of the commercially available solution with the utilization of appropriate testing methodology stemming from the specifications of ISO/IEC 30107-3 standard.

The results associated with the PAD evaluation of the IUT have been reported in section **Error! Reference source not found.** and are specific to the scenarios tested at this point in time.

Note that the results presented in this report serve as validation that Xperix inc.'s ***RealScan S60/S60M fingerprint authenticator (IUT) with Hardware version V1.9.5 and SDK version v1.6.6*** has undergone testing in accordance with the ISO/IEC 30107-3 standard. Because the standards do not provide pass or fail levels for the metrics, this report does not indicate a pass or fail in association with this standard.

Deviations

BixeLab has taken every measure to ensure that no deviations were made from the specifications of the standard.

Conclusion

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

Appendix 1: Application for IUT Assessment – Overview

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).

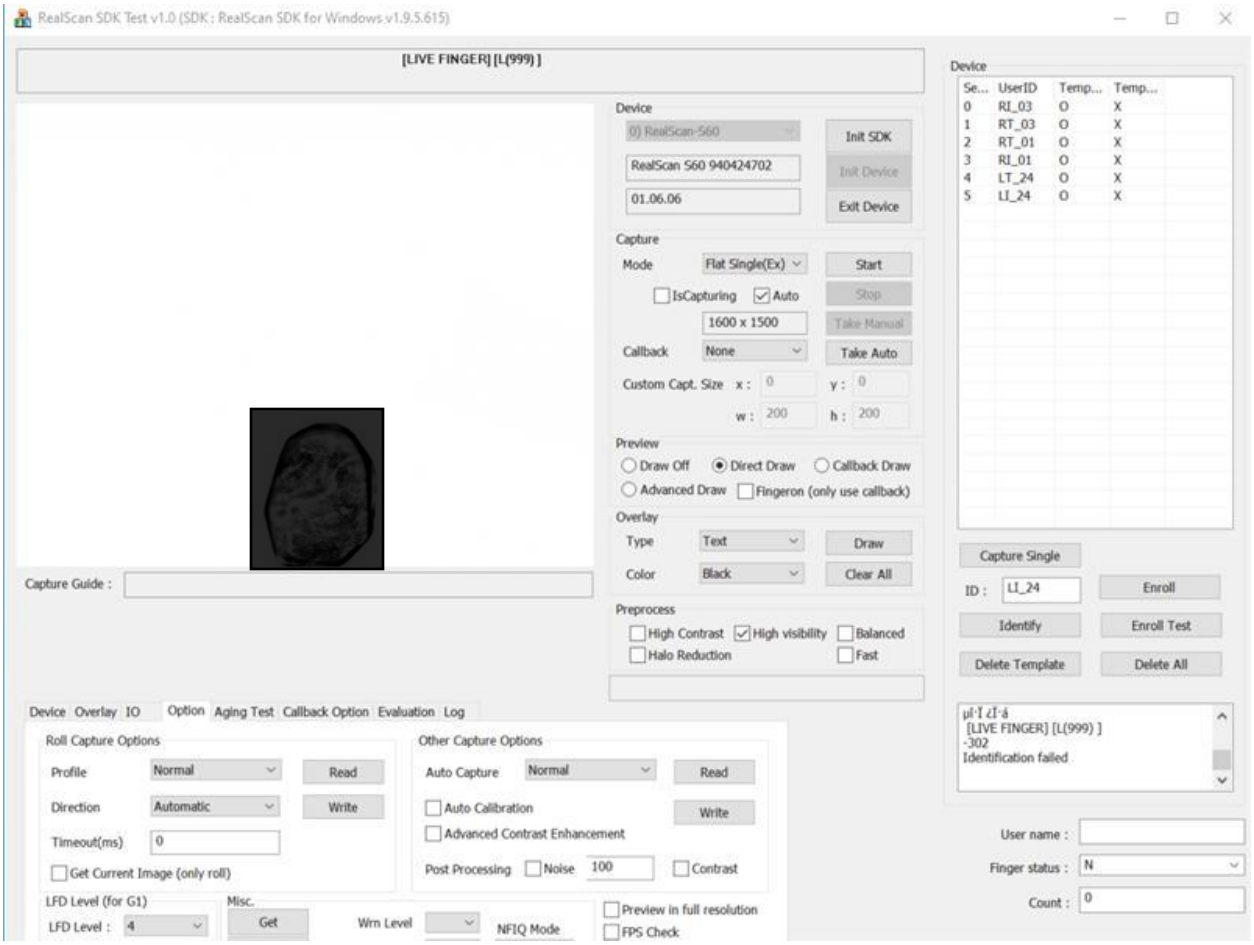


Figure 2 Accompanying application to IUT

Appendix 2: Configurations Audit Logs

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		Yes	22nd August 2023	N/A

Comprehensive Audit (at the Start and End of testing)

	Before testing:		After testing:	
Software	**Version**	**Build**	**Version**	**Build**
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086
Windows 10 Pro	21H2	19044.3086	21H2	19044.3086

CLIENT NAME: Suprema

Specifications regarding the test being conducted are noted below

Test Case	Test Objective	Date	Validator(s)
Exploratory testing	Validate Audit Log Sheet, Validate Set Up Manual set by Xperix, Validate Outputs/Performance of devices	17-Jul-23	Divij, Melechedek, Tristan
Exploratory testing	Tested RealScan S60 with all PAIs to see the results of each PAI	19-Jul-23	Melechedek, Tristan
Exploratory testing	Tested RealScan S60M with all PAIs to see the results of each PAI then compared performance	20-Jul-23	Melechedek, Tristan

	between the two scanners		
Level 1 Testing	Commencement of Level 1 Testing	24-Jul-23	Melec hedek
Level 1 Testing	Continuation of Level 1 Testing	25-Jul-23	Melec hedek
Level 1 Testing	Validate Hotfix made by Xperix on liveness issue found during testing on the 25th of July and resuming Level 1 Testing	1-Aug-23	Melec hedek
Level 1 Testing	The completion of Level 1 Testing for 8 out of 10	2-Aug-23	Melec hedek
Level 1 Testing	Testing 9th test subject out of 10	7-Aug-23	Melec hedek
Level 1 Testing	Testing final test subject	14-Aug-23	Melec hedek
Level 2 Testing	Start testing level 2	16-Aug-23	Tristan
Level 2 Testing	Finish testing level 2	21-Aug-23	Tristan
Exploratory testing	Exploratory Testing to validate all "Failure to Acquire" PAIs	22-Aug-23	Melec hedek

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 S60		BXL018 - 1	N/A	940424702	N/A		17/07/2023 10:05 AM
Xperix RealScan S60M		BXL018 - 2	N/A	940924166	N/A		17/07/2023 10:10 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		19/07/2023 1:45 PM
Xperix RealScan S60M		BXL018 - 2	N/A	940924166	N/A		20/07/2023 10: 10 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		24/07/2023 1:20 PM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		25/07/2023 9:30 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		01/08/2023

							8:20 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		02/08/2023 10:00 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		07/08/2023 11:10 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		11/08/2023 1:02 PM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		14/08/2023 10:11 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		16/08/2023 9:30 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		21/08/2023 10:00 AM
Xperix RealScan S60		BXL018 - 1	N/A	940424702	N/A		22/08/2023 2:42 PM

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**
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	17/07/2023 10:30 AM
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	18/07/20231:45 PM
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	24/07/2023 1:20 PM
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	25/07/2023 9:30 AM
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	01/08/2023 8:20 AM
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	02/08/2023 10:00 AM
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	07/08/2023 11:10 AM
Lenovo WIN-DSK-08	BXL 139	Wndows 10 Pro	N/A	21H2	11/08/2023 1:02 AM

Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	14/08/2023 10:11 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	16/08/2023 9:30 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	21/08/2023 10:00 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	22/08/2023 2:42 PM

The Client application software specifications are noted below

Provider	**Title**	**Client CODE (If Applicable)**	**Version**	**Build**	**Identified Anomalies**	**Biometric Modality**	**Date and Time Check Performed**
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL 139	v1.9.5.615	N/A	None	Fingerprint	17/07/2023 10:30 AM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL 139	v1.9.5.615	N/A	None	Fingerprint	18/07/2023 1:45 PM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL 139	v1.9.5.615	N/A	None	Fingerprint	24/07/2023 1:20 PM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for	BXL 139	v1.9.5.615	N/A	None	Fingerprint	25/07/2023 9:30 AM

	Windows v1.9.5.615)						
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL139	v1.9.5.615	N/A	None	Fingerprint	01/08/2023 8:20 AM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL139	v1.9.5.615	N/A	None	Fingerprint	02/08/2023 10:00 AM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL139	v1.9.5.615	N/A	None	Fingerprint	07/08/2023 11:10 AM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL139	v1.9.5.615	N/A	None	Fingerprint	11/08/2023 1:02 AM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL139	v1.9.5.615	N/A	None	Fingerprint	14/08/2023 10:11 AM

Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL 139	v1.9.5.615	N/A	None	Fingerprint	16/08/2023 9:30 AM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL 139	v1.9.5.615	N/A	None	Fingerprint	21/08/2023 10:00 AM
Xperix RealScan S60	RealScan SDK Test v1.0 (SDK: RealScan SDK for Windows v1.9.5.615)	BXL 139	v1.9.5.615	N/A	None	Fingerprint	22/08/2023 2:42 PM

Appendix 3: System Information

Item	Response
Provider Name	**Xperix Inc.**
Solution Name	RealScan S60 / S60M
Solution Version	**HW version: V1.9.5** **SDK version: v1.6.6**
Solution description	Fingerprint Type Four Finger Flat / Two Finger Flat / Single Flat & Rolls Resolution/Gray scale 500 dpi / 256 gray levels Dimension (W x L x H) 118 x 120 x 19.3 mm (4.64'' x 4.74'' x 0.76'') 102.4 x 112 x 15.9 mm (4.03'' x 4.40'' x 0.63'') - RealScan S60M Platen Size (W x L) 83.3 x 78.2 mm (3.28'' x 3.07'') Capture Size (W x L) 81.28 x 76.2 mm (3.2'' x 3.0'') Image Size (W x L) Four Finger Flat: 1600 x 1500 Two Finger Flat: 900 x 900 Single Flat & Rolls: 800 x 750 Image Quality Standards FBI IQS Appendix F Ingress Protection IP65 (IP65-rated top surface) Operating Temperature -10℃ ~ + 55℃ Operating Humidity From 10 to 90%, non-condensing Power Supply USB Host Weight 220g / 189g (RealScan S60M) Interface USB 2.0 High Speed Operating Systems Windows: 7, 8, 8.1, 10 32 / 64bit Linux: Ubuntu, Debian, Fedora, Cent OS 32 / 64bit Android 5.0+ (Custom 4.0) Certificate FBI, KC, CE, FCC, UL, IEC62471, WEEE, RoHS, REACH, WHQL, USB-IF Sound Interface Buzzer Usage Environment Indoor
Any Performance Claims?	N/A
PAD Testing Level	Level 1
Modality	**Fingerprint (Contact - optical scanner)**
PAD/Data Capture/Full System Evaluation?	PAD subsystem

Appendix 4: ISO/IEC 30107-3 Reporting Requirements

#	ISO/IEC 30107-3 Reporting Requirements	BixeLab Responses
1	**number of presentation attack instruments used**	**120**
2	number of presentation attack instruments species (attack types) used	6
3	**number of presentation attack instruments series (class of PAIs created using common production method and based on the same biometric charectaristics) used**	**0**
4	number of individuals involved in the testing, including PAI presenters unable to utilize artefacts and test subjects unable to present non-conformant characteristics	13
5	**number of PAI sources from whom artefact characteristics were derived**	**10**
6	number of presentation attack instruments created per PAI source for each PAIS	1
7	**number of tested materials (for example, blutac/resin/etc.)**	**6**
8	description of output information available from PAD mechanism	**Enrollment:** Successful Enrollment: *Enrollment Successful* Unsuccessful Enrollment: *Liveness Failed/Try again* **Verification:** Successful Verification: Identification Success Unsuccessful Verification: Identification Failed Liveness Fail: *Fake Finger Detected* Liveness Pass: -
9	**ordering of subject presentations with PAI**	**Live subject enrols using thumb and index as advised by the operator. PAI is mounted against the bona fide enrollment of this subject**
10	ordering of subject presentations without PAI	Live subject enrols using thumb and index as advised by the operator. Live subject then verifies using the same finger that was used to enrol.
11	**number of total PAI presenters or test subjects and PAI presenters or test subjects that were reused**	**Total PAI Presenters: 3 Test Subject AND PAI Presenter: 3 Test Subjects Reused: 0**

#	ISO/IEC 30107-3 Reporting Requirements	BixeLab Responses
12	ordering of presentations to PAD-enabled and disabled system	For PAD Enabled System: 1. Enrollment Presentation 2. Bonafide Verification Presentation. 3. PAI Presentations.
13	**whether test subjects were reused**	**yes**
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	Yes, test subjects were required to enrol and conduct bonafide verification presentations which helped in the analysis of BPCER, BPNRR and FTEs.
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 is an individual or mechanism presenting the presentation attack instrument (PAI) to the biometric system. The role was material as the PAI presenter conducted tests and ensured accurate logging of results which was later used for analysis.**
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 is an individual or mechanism from which biometric samples are obtained for use in a presentation attack instrument (PAI). The role was material to test results as the various PAI sources allowed us to test various demographics.
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 Creator is individual or mechanism responsible for the conception, formulation, design and realization of a presentation attack instrument (PAI) species. The role was material for test results as the PAI creator helped ensure proper labelling and consistency of the various PAIs created and helped minimize deviations in the creation process.**
18	indicate the number of individuals who occupied each role (e.g. five individuals were PAD sources in the test)	PAD Sources: 10 PAI Creators: 3 PAI Presenters: 3
19	**for each role, describe individuals' level of experience with presentation attacks**	**PAD Sources: 2 Intermediate; 2 Expert; 6 Proficient PAI Creators: 3 Proficient PAI Presenters: 3 Proficient**
20	document occurrences in which individuals occupied multiple roles, e.g. PAI sources were also PAI presenters	There was 1 instance where an individual was all 3; Source, Presenter and Creator There were 2 Instances where an individual was both the Presenter and Creator