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:

BioMini Slim-2: Single fingerprint authentication scanner

HW Version: V03B

SDK Version: v3.10.1

Attention: Changmin Kim

cmkim@suprema.co.kr

NVLAP TESTING

NVLAP LAB CODE 600301-0

Document Code	*23-021-TR-00*
Submit Date	*15 June 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 A Test Report	BixeLab	15 June 2023

Table of Contents

Executive Summary 6

1.0 Introduction 7

1.1. Background 7

1.2. Test Objectives 7

1.3. Test Constraints 8

1.4. Scope 8

2.0 System Description 10

2.1. System Information 10

2.2. Concept of Operations 10

2.3. Configuration Audit 12

2.4. Expected Outputs 12

Expected Output Data 12

Expected Output Performance 12

3.0 Dataset Description 13

3.1. Test Crew Profile 13

3.2. Planned Presentation Attack Instrument Types 14

4.0 Test Execution 16

4.1. Pre-Test Review 16

Exploratory Testing to inform Presentation Attack Instrument Types 16

4.2. PAD Test Execution 18

Test Subjects' Level of Habituation 18

Attack Presentations 18

Bona fide Presentations 18

4.3. Levels of Effort and Decision Policies 20

Failure to Enrol 20

Failure To Acquire 20

4.4. Post Test Review 20

5.0 Performance Results 21

5.1. Presentation Attack Detection Evaluation 21

Attack Presentations 21

Bona fide Presentations 23

6.0 Findings 24

7.0 Appendix 1: Application for IUT Assessment – Overview 25

8.0 Appendix 2: Performance Per Finger Type **28**

9.0 Appendix: 3 – Configuration Audit Logs **29**

10.0 Appendix 4: PAD Level 1 Testing: System Information **30**

11.0 Appendix 5: 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 BioMini Slim 2 fingerprint authenticator (IUT) with Hardware version V03B and SDK version v3.10.1 (refer to Appendix 4: PAD Level 1 Testing: System Information). The evaluation, conducted in May 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 and Observations:

- The testing adhered to the methodologies specified in the ISO/IEC 30107-3 standard.
- BixeLab conducted a Level 1 PAD evaluation, comprising 180 Level A attack presentations, including 90 cooperative and 90 uncooperative scenarios. Additionally, 30 bona fide tests were performed with a test crew of 10 unique and consenting individuals.
- Testing was focused on the "Right Index" and "Right Thumb" fingers, with 5 test subjects assigned to each finger.
- The IUT was configured and tested with the following parameters as described by the provider:
    - Fake Level: 0
    - Brightness was set to 100
    - Sensitivity was set to 7
    - Do not select “Detect core” and “Ex” options
- 30 tests were completed using each attack type (presentation attack species) below and the following results were noted for the IUT:

Presentation Attack Species	Result	Count
Latent fingerprint dusted with graphite powder and lifted using scotch tape from a ceramic surface	Fake Finger Detected	18
	Verification Failed	1
	Capture Failed	11
Latent fingerprint dusted with baby powder and lifted using scotch tape from a phone surface	Fake Finger Detected	21
	Capture Failed	9
Latent inked fingerprint lifted using blu-tac from a wooden laminate	Fake Finger Detected	30
Fingerprint printed on matte paper	Capture Failed	30
Wax fingerprint created using a play-doh mould	Fake Finger Detected	27
	Capture Failed	3
Play-doh fingerprint created using a wax mould	Fake Finger Detected	4
	Capture Failed	26

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

- The evaluation yielded a Bona fide Presentation Classification Error Rate (BPCER) of 0% and a Bona fide Presentation Non-Response Rate (BPNRR) of 0%.

Please note that this report does not aim to identify vulnerabilities within the system. Instead, it focuses on 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), the most effective 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 BioMini Slim-2 single fingerprint authentication scanner SDK version 3.10.1 – Item Under Test (IUT). Testing was conducted to be 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 BioMini Slim 2 fingerprint scanning solution with Presentation Attack Detection (PAD) mechanisms, has engaged BixeLab as an independent third-party tester to conduct an ISO/IEC 30107-3 compliant PAD evaluation to Level 1. This evaluation aims to verify the performance of the PAD mechanisms against simple types of presentation attacks where access to the biometric characteristics is easy to obtain, low equipment/cost is required, and attack expertise and knowledge is minimal.

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 BioMini Slim-2: Single fingerprint authentication scanner (HW Version: V03B, SDK Version: v3.10.1) - IUT for Presentation Attack Detection (PAD) completed to Level 1 sophistication. This is to meet both the NIST standards as well as comply to the vendor set claims of *less than 1% APCER and less than 15% BPCER*.

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 includes a table for the hardware and/or software that implemented instruments to the PAD mechanisms and makes an explicit declaration regarding the applicability to the claimed performance as described above.

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 focussed 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 PAD subsystem's capacity to correctly classify presentation attacks. In this regard, the classification metrics presented in this document are confined to APCER, BPCER, APNRR, and BPNRR. Other classification metrics associated with full system evaluation, such as comparison and PAD subsystem outcomes, were not measured for this evaluation.
- It is critical to recognize that 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.

1.4. 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:

- Undertake an ISO/IEC 30107-3 compliant evaluation that provides PAD error rates using Level A attack types. The PAD mechanism for the item under test IUT – ***BioMini Slim 2 with Hardware version V03B and SDK version v3.10.1.*** This testing falls into the area of vulnerability assessment by using a representative set of presentation attack instruments and a representative set of bona fide data capture subjects. This includes the use of presentation attack instruments (PAI) against the biometric verification system which is done under certified laboratory conditions. The aim is to attempt to circumvent the security functionality of the PAD subsystem and evaluate the robustness of its performance.
- 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 involves the testing of the IUT against Level A PAIs. This includes testing with both cooperative and non-cooperative attack types. Note that: According to ISO/IEC 30107 standard, in the case of biometric presentation attacks, attackers may obtain a capture subject's biometric characteristic directly from the capture subject. This acquisition can be cooperative (for example, the captured subject provides a fingerprint to a sensor) or non-cooperative (e.g., the capture subject leaves a fingerprint on a glass or a biometric capture device allowing the attacker to lift the fingerprint). Different attack scenarios are associated with cooperative and non- cooperative characteristic data capture. Artefacts created from cooperative acquisitions may be of higher quality than those from non-cooperative acquisition, which may in turn impact PAD rates and 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) – ***BioMini Slim 2 with Hardware version V03B and SDK version v3.10.1*** for PAD evaluation. The item under test was accessed using a 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 Table below.

Table 1 System information

IUT name (Fingerprint scanner)	Hardware (Scanner)	Browser	SDK Build	BixeLab Hardware (Laptop) Code
BioMini Slim 2	Hardware version V03B	Windows XP (version 21H2)	SDK version v3.10.1	BXL139 OS build: 19044.2846

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.

UniFinger Engine SDK 3.0 Demo (Biomini_Demo VC) 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:

- Fake level was set to 4
- Brightness was set to 100
- Sensitivity was set to 7
- Do not select “Detect core” and “Ex” options

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 –

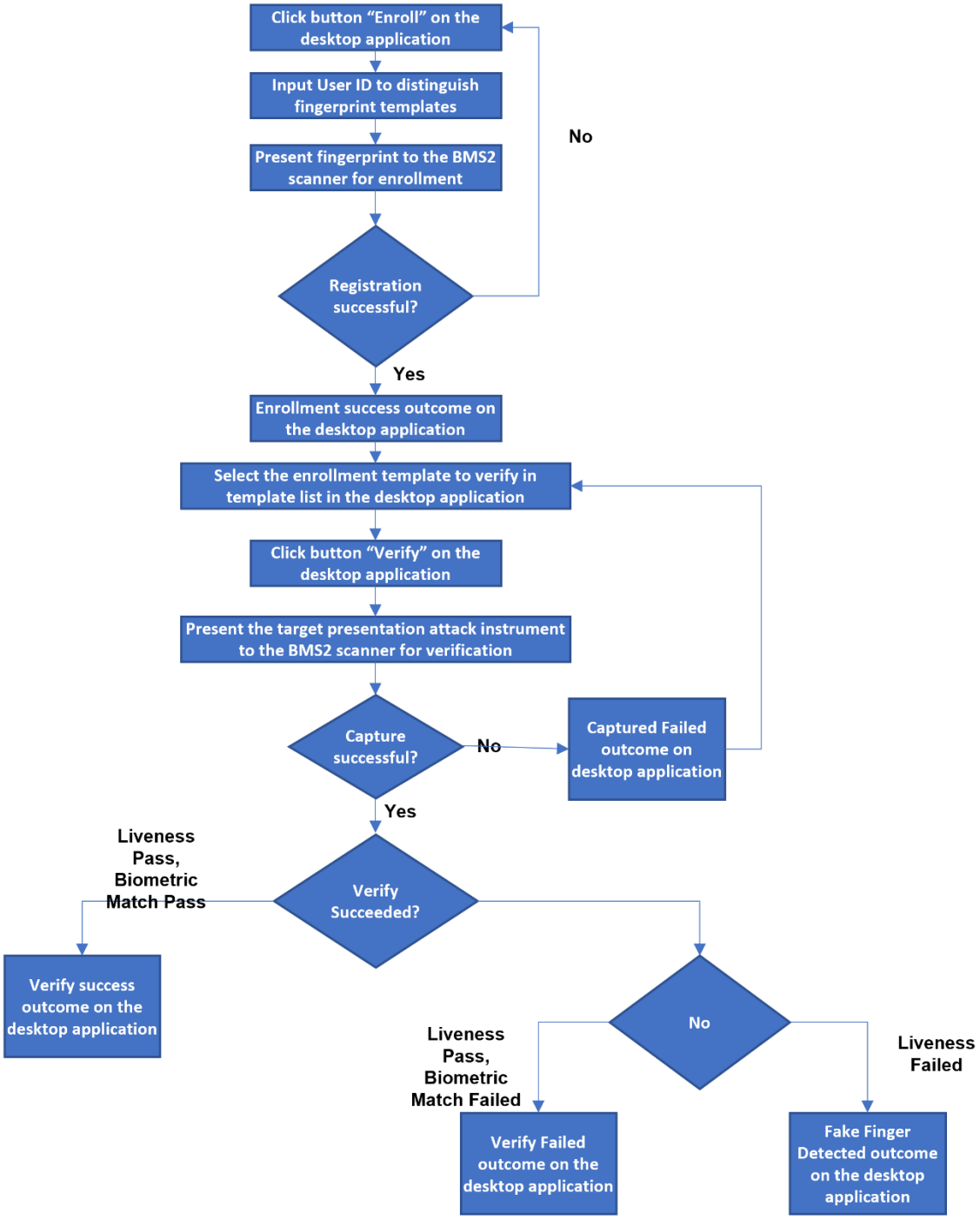


Figure 1 Test Process Flow (Overview)

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: 3 – Configuration Audit Logs provide detailed configuration audit logs focusing on the above with no identified anomalies.

2.4. 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	Registration successful	Enrollment success
	Registration unsuccessful	Capture Failed
Verification	**Capture successful**	-
	Capture unsuccessful	**Capture Failed**
	Liveness Pass, Match Pass	**Verification Success**
	Liveness Pass, Match Failed	**Verification Failed**
	Liveness Failed	**Fake Finger Detected**

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 a Fake Level Threshold of 4 to make decisions for whether the acquired sample was live (Verification Success/ Verification Failed) or artificial (Fake Finger Detected).

3.0 Dataset Description

This section provides details of the test crew recruited for this evaluation as well as the Presentation Attack Instrument Species tested.

3.1. 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 subject 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	Yes
51 – 70 y/o	Yes
> 70 y/o	-

Table 4 Sex Distribution

Sex	BixeLab sourced percentage
Male	70%
Female	30%

Table 5 Ethnicity Distribution

Ethnic Origin	BixeLab sourced
European	Yes
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

3.2. 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.

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 using graphite powder and scotch tape	10	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.	**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.
	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 Mould	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.	

Presentation Attack Level	Artificial Presentation Attack Instruments	Source	Description	Description of Attack Scenario
	Playdoh fingerprint using Wax Mould	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.	

Each presentation attack species had a minimum of 3 presentation attack instruments as per the best practice guidance in ISO/IEC 310704.

4.0 Test Execution

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

4.1. Pre-Test Review

A pre-test 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 the test plan. This readiness review was conducted at the start of the evaluation process. For this PAD evaluation, this included the following:

1. A review of the proposed test plan in conjunction with the test runsheet to inform the test execution.
2. Formalising a plan for data collection to ensure high data quality and consistency for test analysis.
3. Ensuring the planned test cases were fit for purpose.
4. Ensuring the PAIs were fit for purpose.
5. Ensuring compatibility of IUT with the target laptop device with Windows OS using a 2.0 High Speed USB.
6. Completing set up and installing necessary drivers.
7. Log relevant hardware and software specifications in the IT Audit Log.
8. Conducting exploratory testing to understand how the IUT operates and validate the expected PAD subsystem outputs for testing.
9. Ensure that the Presentation Attack Instruments meet the artefact properties as described in section 8 of the ISO/IEC 30107-3 standard.

Exploratory Testing to inform Presentation Attack Instrument Types

According to the published claims of the IUT, it has the ability to differentiate between counterfeit fingerprints produced from various materials such as clay, rubber, silicon, glue, paper, film, and more. To align with these claims, a selection of presentation attack species (PAS) has been chosen for this evaluation. An extensive exploratory testing process was carried out to ensure that the planned attack scenarios and instruments are appropriate.

This section presents an overview of the exploratory testing that was conducted to establish the final list of attack types. The intention was to have an equal distribution between cooperative and uncooperative attacks for both levels of PAS.

For uncooperative attack scenarios, the objective was to generate a presentation attack where the test subject, who is providing the biometric characteristics for attack creation, is uncooperative and motivated to prevent a successful biometric acquisition process.

On the other hand, for cooperative attack scenarios, the aim was to create a presentation attack where the test subject is cooperative and motivated to complete the biometric acquisition process successfully.

A brief overview of some key exploratory testing results is provided below:

- Initial attempts to lift a latent print using thin tape on a wood laminate surface proved to be ineffective due to the coarse texture of the surface, which resulted in the loss of significant detail. Exploratory testing was conducted using graphite powder from a pencil to lift a latent print from a wood surface, but the resulting lifted print was of low quality and failed to acquire the necessary biometric characteristics. Therefore, a ceramic or mirror surface was chosen instead which proved to be more effective in lifting high-quality prints while still being easily accessible for biometric acquisition.
- Consideration of materials such as blue tac, scotch tape, matte paper, wax, and play-doh was based on the labs experience of similar testing senarios, as well as their availability and affordability for both Level A and Level B attack scenarios.
- An etched fingerprint mould was considered for mounting clay, silicon, and rubber fingerprint attacks. Such etched fingerprints are well documented forms of attacks and that attackers with sufficient determination could acquire a latent print by dusting it, taking a high-resolution photo, and using simple photoshop techniques to create an etching mould. To validate this theory, we selected a test operator with minimal knowledge in this area to mimic an attacker's behaviour. Although the operator was able to create prototypes using an etching kit, the resulting mould was of subpar quality, with significant information loss on the ridges, and attempts to create a clay presentation attack using this mould resulted in low-quality prints and FTAs. Therefore, polymer clay moulds were opted as an alternative which proved to be more effective in creating high-quality prints that could be read by the scanner. If coorparative attacks using the same materials are rejected then it seems certain that lower quality latent prints would also be successfully detected as presentation attacks.
- Some presentation attacks were kept on the planned PAS list despite resulting in FTAs. This decision was based either on public claims related to the materials used, or the attackers' best efforts in accordance with the level of attack they mounted.

4.2. PAD Test Execution

The ISO 30107-3 standard recommends that PAD mechanisms be evaluated throughout a defined range of attack types. This includes defining and utilising a representative collection of presentation attack instruments and a representative set of bona fide test subjects for data capture. Testing with bona fide participants is necessary to establish the frequency with which the PAD mechanism may incorrectly identify bona fide presentations. This is crucial for PAD testing to determine if high classification error rates for bona fide people might impair the operational system usability and the rate at which a PAD mechanism may confuse bona fide presentations for attack presentations.

Hence, the PAD evaluation of the Xperix Inc.'s BioMini Slim-2: Single fingerprint authentication scanner (HW Version: V03B,SDK Version: v3.10.1) - item under test (IUT) followed a workflow which involved both types of tests. The test execution process is described below.

Note that on each day of testing software and hardware specifications associated with the system under test and any hardware/software being used for testing were audited refer to Appendix: 3 – Configuration Audit Logs).

5.0 Refer to

Appendix 5: ISO/IEC 30107-3 Reporting Requirements section for detailed information relating to presentation attack detection test instruments, roles, artefacts, etc.

Test Subjects' Level of Habituation

The degree to which a test crew is familiar with IUT, according to the appropriate standards, can have a significant influence on error rates. Testing with a crew that is familiar with the IUT produces lower FTE values than testing with a non-acquainted crew.

All test crew personnel recruited for bona fide testing subcomponent were unfamiliar with the IUT, based on the notion that all real-world Xperix Inc. solution users are expected to have a low level of familiarity with the Hardware and SDK.

Attack Presentations

The following is a high-level summary of the testing sequence for attack presentations:

1. Ensure that the IUT and test set up are ready for PAD testing.
2. Click "Enroll" button on the desktop application
3. Input User ID to distinguish fingerprint templates
4. Request subject to complete Enrollment (Live, conformant fingerprint)
5. Acquire the target presentation attack instrument.
6. Select the Enrollment template to verify in template list on the desktop application
7. Click "Verify" button on the desktop application
8. Present the target presentation attack instrument in the manner that best represents the target attack scenario.
9. Each presentation attack instrument was be applied a maximum of five times or until the application provides a result corresponding to PAD/verification outcome.

Bona fide Presentations

Bona fide is analogous to normal or routine, when referring to a bona fide presentation. Each participating test subject was requested to perform 3 transactions where their interaction with the target of evaluation was in the fashion intended by the policy of the IUT. These presentations are intended to help determine the frequency with which the PAD mechanism incorrectly classifies bona fide presentations as attack presentations. A high classification error rate for bona fide capture subjects would correlate to lower system usability.

A high-level overview of the planned bona fide presentation testing methodology has been provided below:

1. Test operator ensures that the IUT and test set up are ready for bona fide testing
2. Test subject receives verbal instructions on completing the required testing from the operator and provide their written consent to participating in testing before commencement.
3. Operator clicks "Enroll" button on the desktop application and inputs the assigned User ID to distinguish fingerprint templates
4. Operator requests subject to complete Enrollment (Live, conformant fingerprint). Subject is request to present either their right thumb or right index finger.

5. Once Registration is successful, Operator selects the Enrollment template to verify in template list on the desktop application
6. Operator clicks “Verify” button on the desktop application
7. Subject completes the bona fide transaction using the same finger used to enrol noting that they are allowed a maximum of 5 re-attempts after which the transaction will be recorded as a failure to acquire.
8. Test operator notes the results from the test

Steps 6 and 8 are repeated two more times

5.1. Levels of Effort and Decision Policies

The purpose of this section is to define the acceptable levels of effort and decision policies associated with transactions and attempts made during the evaluation by defining the point at which a subject may reasonably be considered to have falsely accepted, failed to enrol, falsely rejected, and/or failed to acquire.

Summary of the requirements for levels of effort and the decision policies is provided in the section below.

Failure to Enrol

Failure to Enroll is defined as the subject's inability to provide biometric samples from which features can be extracted. This is categorised as failure to enrol and reflects inconsistent biometric data. The subjects were allowed up to five retries within 5 seconds in the case an Enrollment attempt does not result in a successful registration.

Failure To Acquire

Failure to Acquire is defined as the system’s inability to acquire biometric samples from which features can be extracted. A maximum of 5 re-attempts were allowed per presentation attack or bona fide presentation.

5.2. 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 BioMini Slim-2: Single fingerprint authentication scanner (HW Version: V03B,SDK Version: v3.10.1) - item under test (IUT). The reported results are in line with the applicable specifications of ISO/IEC 30107-3. The following sections will describe the testing conducted on bona fide and Level A Presentation Attack Instrument Species (PAIS).

6.1. Presentation Attack Detection Evaluation

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. Evaluation of the PAD mechanism was undertaken using 3 non-cooperative and 3 cooperative Level A presentation attack species. Equal proportion of presentation attacks were mounted between right hand index finger and right-hand thumb 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.
All bona fide presentations, represented in blue, produced "Verification Successful". This is in line with the Ground Truth.
In total 180 attack presentations were mounted across 6 presentation attack instrument species (90 right hand index finger, 90 right hand thumb). Generalised presentation attack detection performance rates for PAD mechanisms at the verification subsystem are as below:

- 79 "Capture Failed". This corresponds to Failure to Acquire.
- 100 "Fake Finger Detected". This corresponds to correct attack presentation classification.
- 1 "Verification Failed". This was interpreted to be an attack presentation that received an incorrect liveness/PAD pass but failed to match ultimately resulting in the verification attempt being rejected owing to match failure. On a PAD subsystem level, this still corresponds to a liveness/PAD pass outcome.

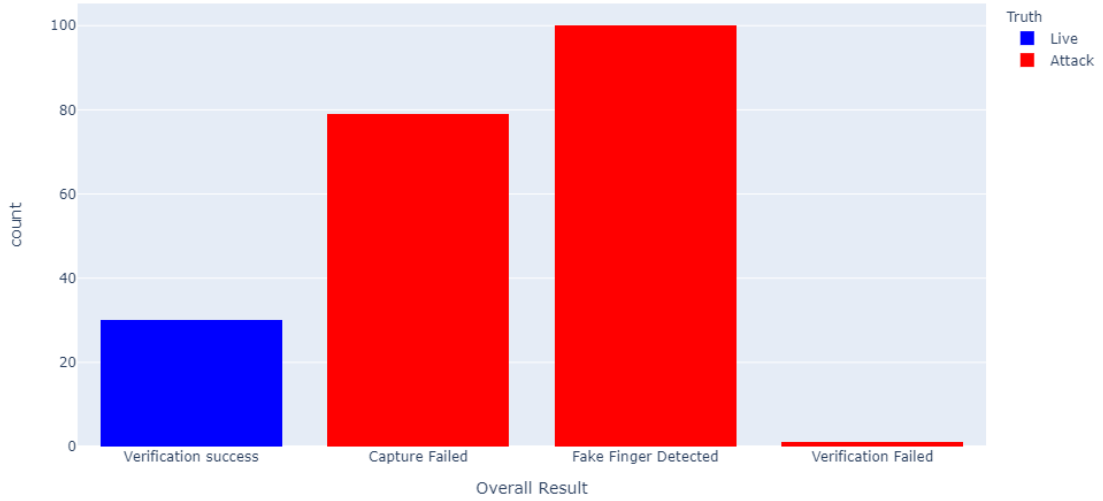


Figure 2 Performance overview: live presentations (blue) vs. presentation attacks (red)

The table below provide a summary of Level A PAD performance metrics associated with the IUT. The performance results measured against right index and right thumb have been combined for the purposes of this evaluation. Separate results are available in Appendix 2: Performance Per Finger Type.

Table 6 PAD Subsystem Testing Results

Presentation Attack Level	Artificial Presentation Attack Instruments	Total Number of Attacks	Number of Correct Attack Classifications	Attack Presentation Classification Error Rate (APCER)	Attack Presentation Non-Response Rate (APNRR)
Uncooperative	**Latent Fingerprint from Graphite Powder**	30	18/30	1/30	11/30
	Latent Fingerprint using Baby Powder	30	21/30	0/30	9/30
	Latent Fingerprint using Ink and Blu-Tac	30	30/30	0/30	0/30
Cooperative	**2D print (Matte paper)**	30	0/30	0/30	30/30
	wax fingerprint using play-doh mould	30	27/30	0/30	3/30
	Play-doh fingerprint using wax mould	30	4/30	0/30	26/30

IUT measured 0% attack presentation classification error rate (APCER) and 0% impostor attack presentation accept rate (IAPAR) against all cooperative presentation attacks.

For Uncooperative presentation attacks, all except one attack type resulted in 0% APCER and 0% IAPAR.

Latent fingerprint dusted from a ceramic surface using graphite power and lifted using scotch tape for one out of thirty tests resulted in a 'Verification Failed' outcome on the accompanying application used to initiate, view, and log tests. Based on the interpreted flow described in Figure 1 Test Process Flow (Overview), this corresponded to Liveness/PAD

pass and match failed outcome. Where the IAPAR was 0% owing to non-match of the verification template against the enrolment template, this test was measured as attack presentation classification error.

Figure below provides a screenshot of the dashboard relating to the Latent Fingerprint from Graphite Powder test with attack presentation classification error –

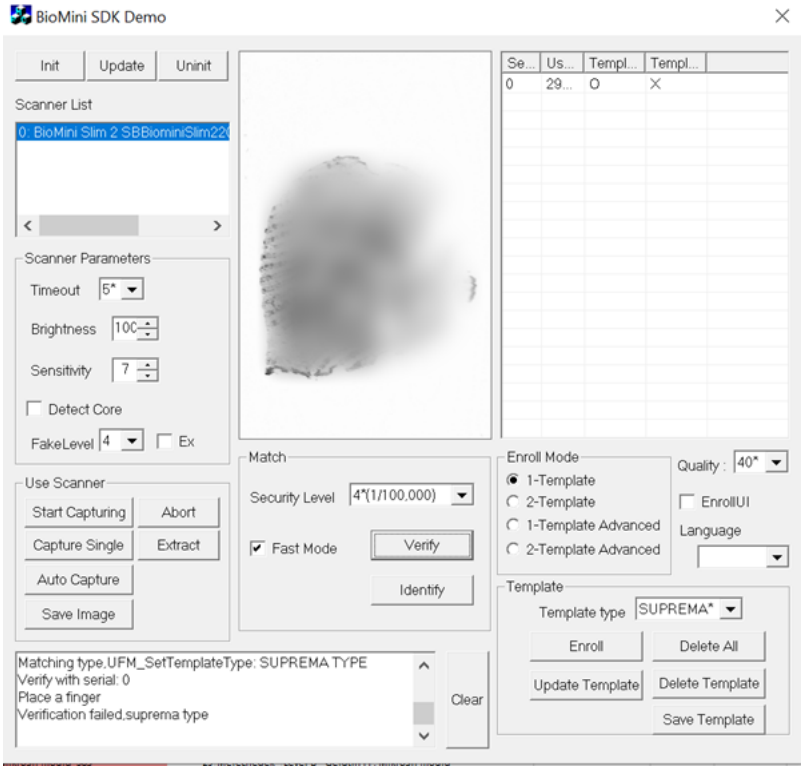


Figure 3 Screenshot for the latent fingerprint (graphite powder) test case resulting in verification failed outcome.

Note that personally identifiable information has been redacted from the screenshot above.

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

Table 7 bona fide performance rates

Bona fide Performance Rate	Bona fide Performance
Bona fide presentation count	30
Bona fide acquisitions	30
Bona fide non-responses	0
Bona fide Presentation Classification Error Rate (BPCER)	0%
Bona fide Presentation Non-Response Rate (BPNRR)	0%

7.0 Findings

BixeLab has completed Level 1 PAD evaluation of ***BioMini Slim 2 with Hardware version V03B and SDK version v3.10.1*** – item under test (IUT). 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. This evaluation also assessed performance claims as per the vendor: "*less than 1% APCER and less than 15% BPCER*."

IUT measured a 0% APCER and 0% IAPAR across the 5 out of 6 presentation attacks tested in this evaluation (see Table 6 PAD Subsystem Testing Results). IUT measured 1/30 (3.33% APCER for 1 presentation attack – Latent Fingerprint dusted using graphite power and lifted using scotch tape from a ceramic surface. However, the corresponding IAPAR for this presentation attack was 0% owing to verification failed outcome for this test.

For the 30 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 Performance Results.

Note that the results presented in this report serve as certification that Xperix inc.'s ***BioMini Slim 2 with Hardware version V03B and SDK version v3.10.1*** – item under test (IUT) 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.

8.0 Appendix 1: Application for IUT Assessment – Overview

Figures below provide a pictorial representation of the outputs received on the application relating to Enrollment and verification using the IUT. Note that all personally identifiable information has been redacted from the screenshots below.

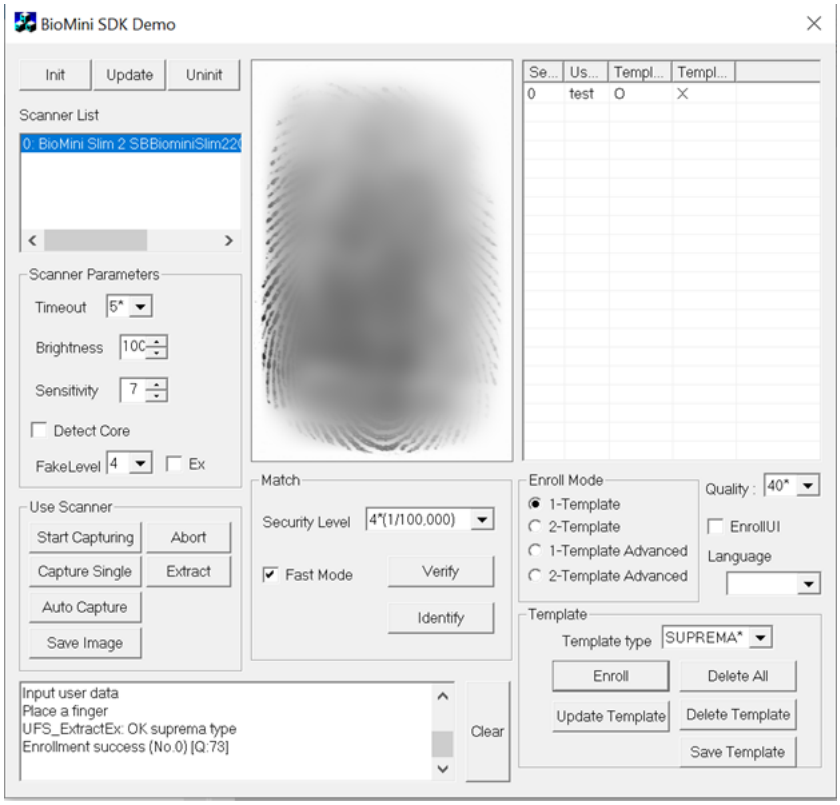


Figure 4 Accompanying application to IUT - Enrollment flow

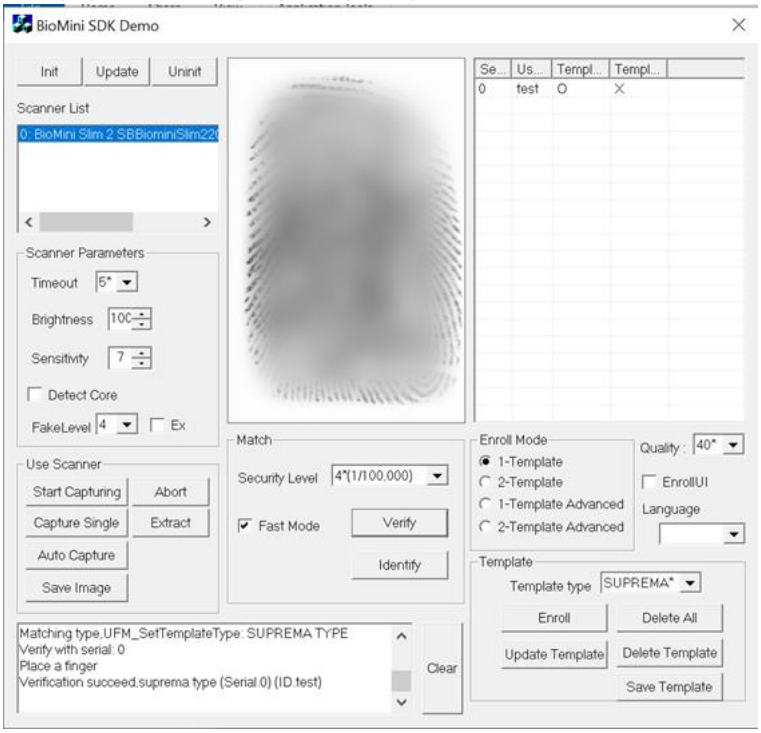


Figure 5 Accompanying application to IUT - Verification Success

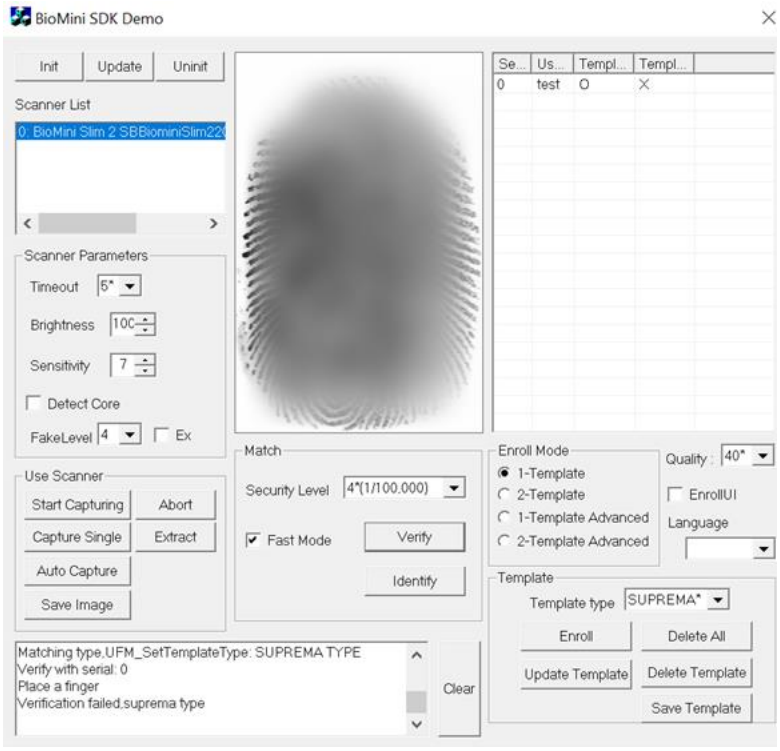


Figure 6 Accompanying application to IUT - Verification Failed

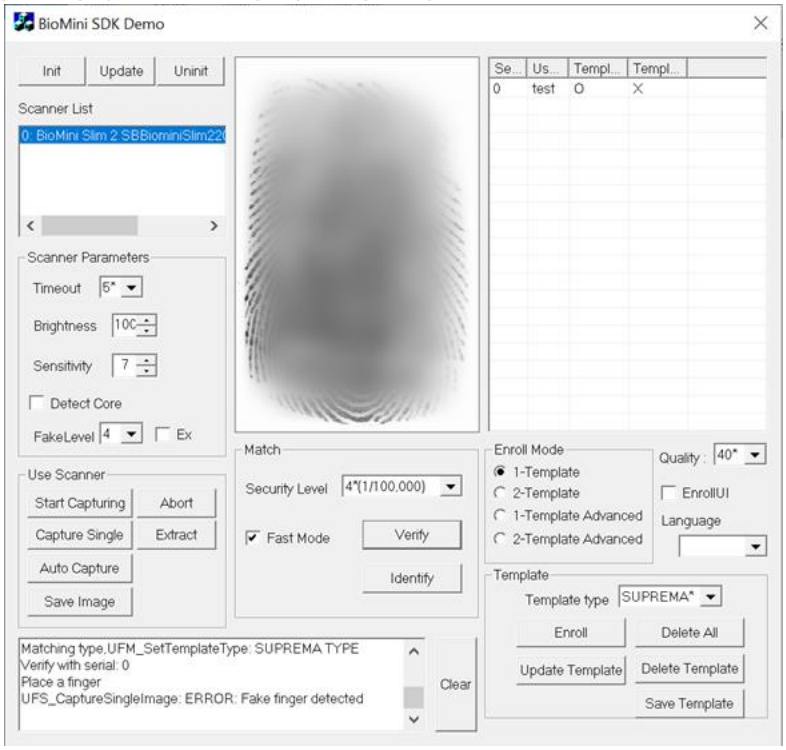


Figure 7 Accompanying application to IUT - Fake Finger Detected

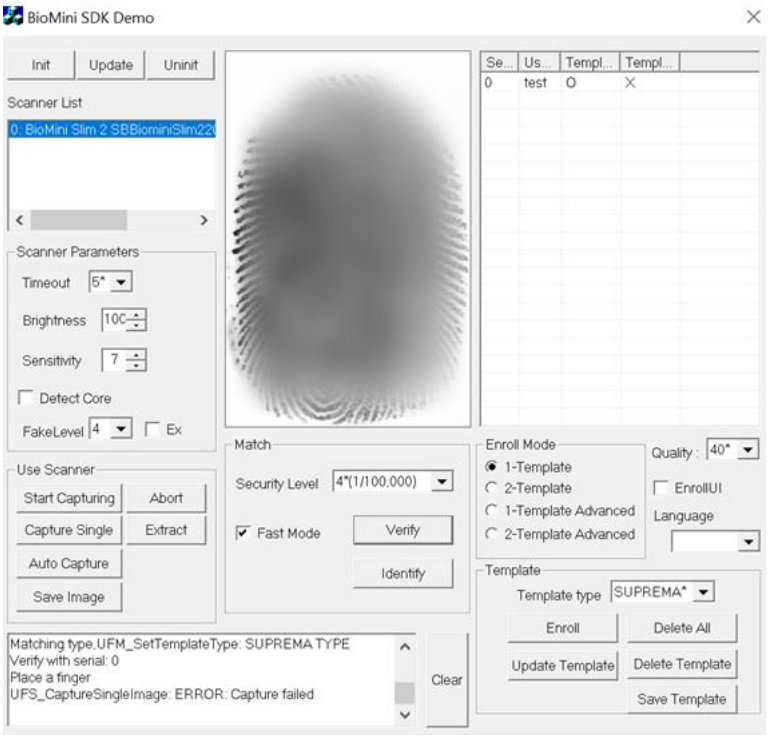


Figure 8 Accompanying application to IUT - capture failed

9.0 Appendix 2: Performance Per Finger Type

Right hand index finger: Presentation Attack Detection Performance (Level A)

Presentation Attack Level	Artificial Presentation Attack Instruments	Total Number of Attacks	Number of Correct Attack Classifications	Attack Presentation Classification Error Rate (APCER)	Attack Presentation Non-Response Rate (APNRR)	Impostor Attack Presentation Accept Rate (IAPAR)
Uncooperative	Latent Fingerprint from Graphite Powder	15	10/15	0/15	5/15	0/15
	Latent Fingerprint using Baby Powder	15	12/15	0/15	3/15	0/15
	Latent Fingerprint using Ink and Blu-Tac	15	15/15	0/15	0/15	0/15
Cooperative	2D print (Matte paper)	15	0/15	0/15	15/15	0/15
	wax fingerprint using play-doh mould	15	4/15	0/15	11/15	0/15
	Play-doh fingerprint using wax mould	15	12/15	0/15	3/15	0/15

Right hand thumb: Presentation Attack Detection Performance (Level A)

Presentation Attack Level	Artificial Presentation Attack Instruments	Total Number of Attacks	Number of Correct Attack Classifications	Attack Presentation Classification Error Rate (APCER)	Attack Presentation Non-Response Rate (APNRR)	Impostor Attack Presentation Accept Rate (IAPAR)
Uncooperative	Latent Fingerprint from Graphite Powder	15	8/15	1/15	6/15	0/15
	Latent Fingerprint using Baby Powder	15	9/15	0/15	6/15	0/15
	Latent Fingerprint using Ink and Blu-Tac	15	15/15	0/15	0/15	0/15
Cooperative	2D print (Matte paper)	15	0/15	0/15	15/15	0/15
	wax fingerprint using play-doh mould	15	0/15	0/15	15/15	0/15
	Play-doh fingerprint using wax mould	15	15/15	0/15	0/15	0/15

10.0 Appendix: 3 – Configuration 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			

Comprehensive Audit (at the Start and End of testing)

	Before testing:		After testing:	
Software	Version	Build	Version	Build
Windows 10 Pro	21H2	19044.2846	21H2	19044.2846
Windows 11 Pro	22H2	22621.1555	22H2	22621.1555

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 devices to see if extra support is required from suprema regarding setting up fingerprint devices	1-May-23	Divij
Exploratory testing	Pre-testing	2-May-23	Dhruv
Exploratory testing	Pre-testing	4-May-23	Divij, Chedek
PAD Session 1	Conduct Level A PAD	17-May-23	Divij, Chedek, Tristan
PAD Session 2	Continue Level A PAD	18-May-23	Divij, Chedek, Tristan
PAD Session 3	Continue Level A PAD	19-May-23	Divij, Chedek, Tristan
PAD Session 4	Completed Level A PAD	22-May-23	Divij, Chedek, Tristan
PAD Session 5	Commenced Level B PAD	2-Jun-23	Divij, Chedek, Tristan
PAD Session 6	Continued Level B PAD	7-Jun-23	Divij, Chedek, Tristan
PAD Session 7	Continued Level B PAD	8-Jun-23	Divij, Chedek, Tristan

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
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		1/05/2023 10:32AM
Suprema BioMini Slim 2		BXL017 - 2	N/A	873035950	N/A		1/05/2023 10:32AM
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		02/05/2023 4:32PM
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		04/05/2023 10:22AM
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		17/05/2023 11:24 AM
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		18/05/2023 9:30 AM
Suprema BioMini Slim 2		BXL017 - 2	N/A	873035950	N/A		19/05/2023 9:45 AM
Suprema BioMini Slim 2		BXL017 - 2	N/A	873035950	N/A		22/05/2023 10:00 AM
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		2/06/2023 10:10 AM
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		7/06/2023 11:35 AM
Suprema BioMini Slim 2		BXL017 - 1	N/A	873036045	N/A		7/06/2023 11:35 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
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	17/05/2023 11:24 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	18/05/2023 9:30 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	19/05/2023 9:45 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	22/05/2023 10:00 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	2/06/2023 10:00 AM
Lenovo WIN-DSK-08	BXL 139	Windows 10 Pro	N/A	21H2	7/06/2023 11:35 AM

11.0 Appendix 4: PAD Level 1 Testing: System Information

Item	Response
Provider Name	**Xperix Inc.**
Solution Name	BioMini Slim-2: Single fingerprint authentication scanner
Solution Version	**HW version: V03B** **SDK version: v3.10.1**
Solution description	Optical fingerprint scanner. Resolution 500 ppi Image Grayscale: 8 bit, 256 levels Platen Size: 16.5 x 21.0 mm Sensing Area: 15.24 x 20.32 mm Image Size: 300 x 400 pixels Template Format: Suprema, ISO19794-2, ANSI 378 Image Format: RAW, BMP, WSQ, ISO 19794-4 Live Fingerprint Detection: Supported IP Rating: IP65(Sensor Surface) USB: 2.0 High Speed Sensor Surface: Optic Glass, Scratch free Operating Temprature: -10 to 50 degree celcius Operating Humidity: 0 to 90% RH Operating System: Windows XP, Vista, 7,8,8.1,10 32/64 bit Android 4.1 (Jelly Bean) and Above
Any Performance Claims?	**less than 1% APCER and less than 15% BPCER**
PAD Testing Level	Level 1
Modality	**Fingerprint (Contact)**
PAD/DataCapture/Full System Evaluation?	PAD subsystem

12.0 Appendix 5: ISO/IEC 30107-3 Reporting Requirements

#	ISO/IEC 30107-3 Reporting Requirements	BixeLab Responses
1	**number of presentation attack instruments used**	**60**
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**	**3**
4	number of individuals involved in the testing, including PAI presenters unable to utilize artefacts and test subjects unable to present non-conformant characteristics	12
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:** Successfull Enrollment: *Enrollment Successful* Unsuccessfull Enrollment: *Template Quality is too Low* **Verification:** Successfull Verification: *Verification Succeed* Unsuccessful Verification: *Verification Failed* Liveness Fail: *Fake Finger Detected* Liveness Pass: -
9	**ordering of subject presentations with PAI**	**Live subject enrolls using right thumb or right 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 enrolls using right thumb or right index as advised by the operator. Live subject then verifies using the same finger that was used to enroll.
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: 1** **Test Subjects Reused: 0**
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**	**No**
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