ISO/IEC 30107-3 Presentation Attack Detection Testing - Test Report

Prepared for
BRYK Pty Ltd

by

BixeLab

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

BRYKGROUP
BRYK.ID

PAD Level 2 Evaluation for:

BRYK.ID with FaceTec server v9.6.30 – item under test (IUT)

NVLAP TESTING
NVLAP LAB CODE 600301-0

ilac-MRA

Document Code	*23-018-TR-20*
Submit Date	*27 June 2023*
Submitted by	*BixeLab Pty Ltd*
Contact	*Ms. Somya Singh*
	M: 0412802334
	E: s.singh@bixelab.com

Attention: David Brykman

davidb@bryk.systems

Version History			
Version Number	**Description of change**	**Author**	**Date**
V1.0	report release 1.0	S.Singh	27 June 2023

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.

Executive Summary

This report contains the findings from the Level 2 PAD evaluation of ***BRYK.ID with FaceTec server v9.6.30* – item under test (IUT)**. The evaluation took place between April and May 2023.

Following is noted based on the testing completed:

- The testing adhered to the methodologies specified in the ISO/IEC 30107-3 standard.
- BixeLab conducted a Level 1 and Level 2 PAD evaluation, comprising 900 Level A attack presentations, and comprising 1200 Level B attack presentations. Additionally, 150 bona fide tests were performed with a test crew of 15 unique and consenting individuals.
- 150 tests were completed using each attack type (presentation attack species) below and the following results were noted for the IUT:

PAI	Attack Presentations	Successful Attacks	APCER	APNRR
Level A				
Passport style photograph printed on matte paper	150	0	0%	0%
Passport style photograph printed on glossy paper	150	0	0%	0%
Selfie style photograph printed on a matte paper	150	0	0%	0%
Selfie style photograph printed on a glossy paper	150	0	0%	0%
Digital photograph presented on a mobile screen	150	0	0%	0%
Digital photo presented on a laptop screen	150	0	0%	0%
Level B				
Video presented on a mobile screen	150	0	0%	0%
Video presented on a laptop screen	150	0	0%	6.67%
2D Paper Mask	150	0	0%	0%
Balaclava Mask	150	0	0%	0%
Simple Digital Animation presented on a mobile screen	150	0	0%	0%
Simple Digital Animation presented on a laptop screen	150	0	0%	0%
Posed digital photos presented on a mobile screen	150	0	0%	0%
Posed digital photos presented on a laptop screen	150	0	0%	0%

- 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 the results presented in this report are based on the FIDO biometric component certification testing completed recently for the BRYK.ID with FaceTec server v9.6.30 – item under test (IUT).

Table of Contents

Executive Summary 3

Introduction 6

Background 6

Test Objectives 6

Test Constraints 6

Scope 7

Scenario Description 8

System Information 8

Concept of Operations 8

Configuration Audit 9

Expected Outputs 10

Expected Output Data 10

Expected Output Performance 10

Dataset Description 12

PAD Evaluation 12

Presentation Attack Instruments 12

Test Crew Profile 17

Test Execution 18

Test Subjects' Level of Habituation 18

Attack presentations 18

Bona fide presentations 19

Performance Results 20

Presentation Attack Detection Evaluation 20

Deviations and Exclusions 24

Findings and Recommendations 25

Appendix 1: Verification Metrics 26

PAD Evaluation 26

Appendix 2: Terms and Definitions 27

Glossary **27**

Appendix 3: Configuration Logs ***28***

Introduction

Background

BRYK Group as an Australian a provider of intelligent security service to manage identity proofing, user authentication and fraud detection has undertaken a Presentation Attack Detection evaluation of its technology to verify solution performance as per the applicable ISO/IEC 30107-3 requirements.

BixeLab has been tasked by BRYK Group to perform an evaluation in their biometric testing laboratory that has been accredited by the NIST (National Institute of Standards and Technology) 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.

Test Objectives

The objective of this evaluation report involves:

1. Determination of the robustness of the end-to-end ***BRYK.ID with FaceTec server v9.6.30*** for Presentation Attack Detection (PAD) – listed as the Item Under Test (IUT)

The evaluation of the IUT's PAD mechanisms was configured according to a Bixelab evaluation design that considered configurations and settings for - data capture (enrolment), dataset collection and profile, the presentation attack instruments, presentation attack detection metrics, and componentry in the biometric subsystem.

This report has been formatted for key project personnel within BRYK Group

Test Constraints

- The evaluation of the IUT's PAD mechanisms falls under the category of 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.
- 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 recognise that there may be presentation attack types, PAI species, and variables that have not been investigated when analysing the performance of a PAD subsystem. As a result, the reported performance of the PAD subsystem (IUT) does not give any information about its effectiveness in identifying presentation attacks that were not tested during this evaluation.
- In the evaluation preparation phase a number of exploratory tests were performed to inform the testing process and the development of the test plan. Through this discovery phase, the Android platform was found to provide comparable performance to an iOS platform for this type of evaluation. It is essential to note however that native applications built for iOS or Android may incur differences in terms of quality of the image captured for instance due to the influencing factors such as the sensor hardware that usually depend on the acquisition device. Based on this findings associated with pretesting of the IUT, PAD evaluation was undertaken on both iOS and Android mobile device environments (see Table 1 for details).

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 30107-3 compliant evaluation that provides PAD accuracy rates using Level A and Level B attack types. The PAD mechanism for the Item Under Test IUT – ***BRYK.ID with FaceTec server v9.6.30***. This testing falls into the area of vulnerability assessment by utilising 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 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 . In this regard, the focus is on verifying that the BRYK.ID Application meets the performance requirements for PAD mechanism set by the TDIF Role requirements.

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.
- Evaluation of the matching accuracy performance of the technology.

Scenario Description

System Information

This section provides information related to the IUT – listed as the ***BRYK.ID with FaceTec server v9.6.30*** and the testing procedures for PAD evaluation. The item under test was a mobile application accessible on both iOS and Android platforms. In laboratory conditions this was accessed through both mobile device types – the exact specifications of hardware and software used for the PAD evaluation are in the table below.

Table 1 System Under Test (PAD Evaluation)

IUT name (Mobile application)	Hardware (Mobile Phone)		Browser	SDK Build
BRYK.ID with FaceTec server v9.6.30 ***iOS app 9.6.20*** ***Android app 9.6.21***	iOS	BXL104 BXL106 iOS 11 Pro Max (version 16.0.2) iOS 11 (version 14.3.1)	N/A	30
	Android	BXL108 Galaxy S21+ 5G		

Concept of Operations

The test cases for evaluation of PAD mechanisms in the BRYK.ID IUT mechanisms were designed to mimic the functional and procedural aspects of the application under conditions expected for operational security for the 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.

The aim of this test was to determine the performance of the liveness detection functionality for an attack mode of presentation as well as for a bona fide mode of presentation.

Figure below provides a pictorial representation of the IUT application flow:

This identifies two subsystems within the end-to-end application flow:

- the liveness (presentation attack) detection subcomponent – the target of evaluation and
- the biometric matching

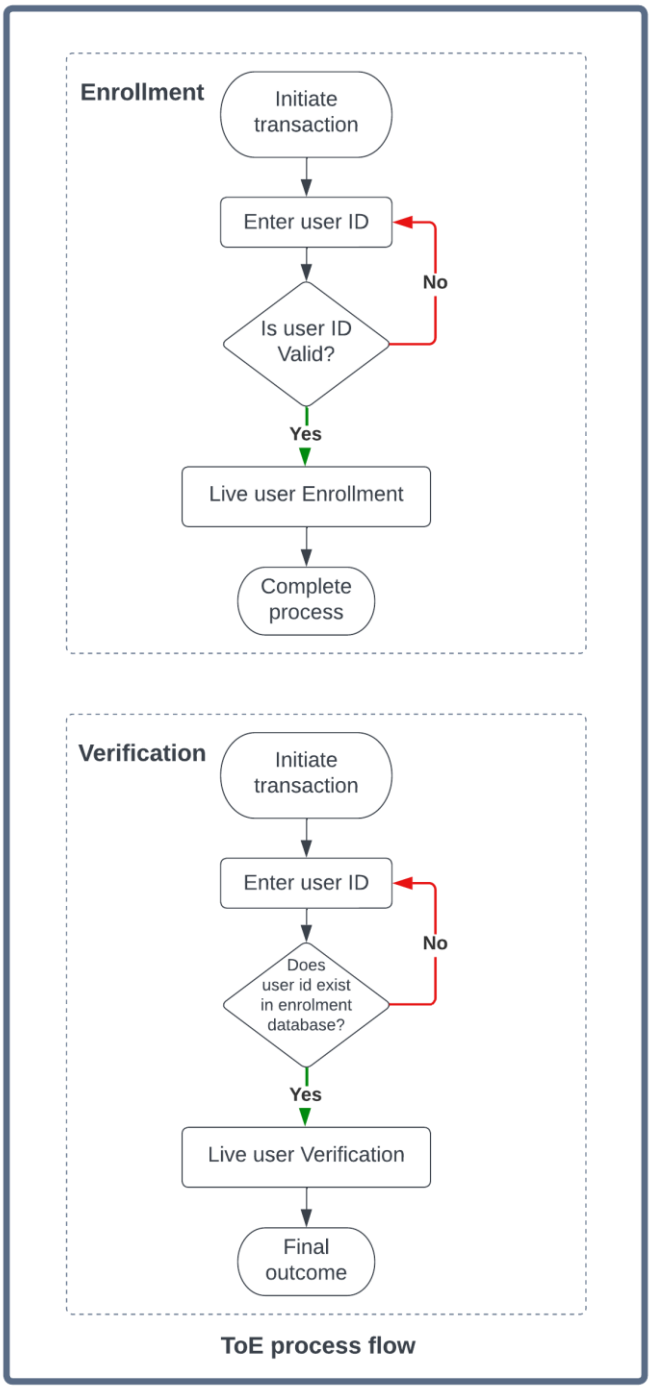

Figure 1 Overview of application process flow for item under test (PAD evaluation)

Configuration Audit

An audit of the system configuration in the IUT submitted for PAD evaluation was conducted on each day of the test executions. 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.

Table in the section Appendix 3: Configuration Logs provides a detailed configuration logs focussing on the above with no identified anomalies.

Expected Outputs

Expected Output Data

Summary of the expected output data on PAD mechanisms is provided in the table below.

Table 2 Summary of Expected output data

Target of Evaluation Component	Components	Score	Result Options as presented on the dashboard
Presentation Attack Detection	3D Liveness	N/A	Passed Retry Required (Failed)

Expected Output Performance

In traditional biometric performance evaluations, ground truth plays a pivotal role to ensure the validity of verification metrics. Ground truth, broadly, is the actual state pertaining to a match. In other words, it is the truth of whether or not a given match is genuine (enrolment and verification images compared belong to the same person) or represents an imposter (enrolment and verification images compared belong to different people) derived in the technology evaluation.

In PAD evaluation context, the truth relates to whether or not a given liveness detection response is genuine (bona fide) or represents an imposter (attack).

The metrics include an attack presentation classification error rate and a bona fide presentation classification error rate for evaluating the performance of presentation attack mechanisms in liveness detection - IUT.

For this evaluation the ground truth was established based on the results that BixeLab reviewed following pretesting cycles of the IUT.

The goal of this evaluation was to measure the accuracy of liveness detection mechanism. Here, a bona fide presentation translated to a real human submitting selfies as directed by the application UI. Hence where a presentation attack was mounted, the expected output was a ‘Retry Required (Failed)’ outcome and in the case of bona fide presentation, submitted as a selfie, then the expected output was a ‘Passed’ outcome.

The table below provides the expected output performance for the PAD evaluation in liveness detection.

Table 3 Summary of expected output performance for PAD

Target of Evaluation Component	Components	Ground Truth	Result Options presented on the dashboard
Presentation Attack Detection (Liveness challenges)	3D Liveness	bona fide	Passed
		Attack	Retry Required (Failed)

Dataset Description

PAD Evaluation

Presentation Attack Instruments

The presentation attack types utilised in this evaluation were based on operational thresholds for the highest score achieved in following criteria to establish the rationale for making substantial biometric security claim about the item under test:

- **Type**: A designation of the artefact defined by its properties and origin.
- **Access to biometric characteristics**: The relative ease of access to suitable sources from which the artefact can be produced.
- **Equipment/Cost**: The relative difficulty and expense to produce the artefact.

These factors are described in the table below.

Table 4 Presentation attack species assessment

Document Type	Score	Description
Type	Simple	Typically, two-dimensional and/or repurposed from another source
	Specialised	Typically, three-dimensional, and/or specially produced or altered from a source
	Sophisticated	Specifically produced, sophisticated artefacts that typically leverage multiple high-quality sources
Access to biometric characteristics	Easy	Publicly or commonly available, usually without knowledge of the target
	Moderate	Usually requires cooperation of the target or access to the biometric or biometric reference itself
	Difficult	Usually requires multiple sources which may be altered or augmented. Often involves access to the biometric or biometric reference itself
Equipment/cost	Low	Can be produced with standard materials using office or home equipment
	Medium	May require the use of generic suppliers, software, or equipment
	High	May require the use of specialised suppliers, software, or equipment

Presentation attack species (as artefact types) were created based on both source of the biometric characteristics and ISO/IEC 30107-3 criteria for artefact property creation, provenance, usage, and handling – pertaining from creation to test utilisation – as formalised criteria to evaluation of PAD mechanisms. As specified in section 8.1 of the ISO/IEC 30107-3 standard, the presentation attacks planned for this evaluation fell into the category of biometric imposter attacks and had the following three properties:

1. The samples appeared as natural biometric characteristics to the IUT
2. The samples appeared as natural biometric characteristics to the biometric data quality checks in place for the IUT
3. The samples acquired by the device camera from the presented artefact contained extractable features that matched against the targeted individual's references.

Based on ISO assessment criteria, the presentation attack species were then classified into Levels A and B. The test operator posing as an attacker had access to each level of attack representations based upon the original biometric characteristics obtained through cooperative subjects.

The table below provides a specification of presentation attacks, level classifications and number of sources per attack species.

Table 5 Summary of Presentation Attack species

Presentation Attack Level	Presentation Attack Instruments	Description	Presentation Technique	Source
Level A	**Passport style photograph printed on matte paper**	This 2-D printout attack consists of coloured photo printed on A4 matte ink jet photo paper of thickness 332 micrometers Biometric characteristics from conformant sources printed using standard printing settings	A flat presentation technique for mounting. This could include a slight variation in the pitch angle to avoid light reflections from the surface of the photo	15
	Passport style photograph printed on glossy paper	This 2-D printout attack consists of coloured photo printed on A4 glossy ink jet photo paper of thickness 332 micrometers. Biometric characteristics from conformant sources printed using standard printing settings.		15

Presentation Attack Level	Presentation Attack Instruments	Description	Presentation Technique	Source
	Selfie style photograph printed on a matte paper	This 2-D printout attack consists of coloured selfie style photo of the target printed on A4 matte ink jet photo paper of thickness 332 micrometers. Biometric characteristics from conformant sources printed using standard printing settings.		15
	Selfie style photograph printed on a glossy paper	This 2-D printout attack consists of coloured selfie style photo of the target printed on A4 glossy ink jet photo paper of thickness 332 micrometers. Biometric characteristics from conformant sources printed using standard printing settings.		15
	Digital photograph presented on a mobile screen	This static digital attack consists of presenting digitally acquired photographs of the target subject on a mobile screen.	Standard presentation technique requiring the test operator to move the ToE closer to the screen, which sometimes can result in reflections.	15
	Digital photo presented on a laptop screen	This static digital attack consists of presenting digitally acquired photographs of the target subject on a laptop screen.		15
Level B	**Video presented on a mobile screen**	This type of digital replay attack consists of: Recording videos of cooperative consenting individuals for the purposes of this testing. Providing guidance to the recording subjects requesting them to simulate blinking, slight movement of the head and smiling. The videos do not match the specific behavior that the ToE expects from the user. Playing and presenting recorded videos on a HD mobile screen to the liveness solution.		15

Presentation Attack Level	Presentation Attack Instruments	Description	Presentation Technique	Source
	Video presented on a laptop screen	This type of digital replay attack consists of: Recording videos of cooperative consenting individuals for the purpose of testing. Providing guidance to the recording subjects requesting them to simulate blinking, slight movement of the head and smiling. The videos do not match the specific behavior that the ToE expects from the user. Playing and presenting recorded videos on a HD laptop screen to the liveness solution.		15
	2D Paper Mask	This 2-D printout attack consists of: High-quality coloured photographs printed on A4 Matte Ink-jet Photo Paper of thickness 332 micrometer (dimensions 210W x 297 H mm). Biometric characteristic from conformant sources printed in 300 ppi. Eye holes and mouth holes, and photo background cut-out. Presentation of the attack species to the ToE	Standard presentation front on with camera. It was ensured that the face mask was placed against the testers face to simulate eye blinking and mouth movements.	15
	Balaclava Mask	This 3-D attack consists of: Faces printed onto a cylindrical piece of stretchy polyester material with the eyecut out.	Ensures that eyeholes lined up with tester eyes. Standard presentation technique adopted	15

Presentation Attack Level	Presentation Attack Instruments	Description	Presentation Technique	Source
	Simple Digital Animation presented on a mobile screen	This tailored digital attack consists of: High-quality coloured digital photographs that are animated using a simple animation software. The software simulates smiling, blinking, head movement, eyebrow movement by manipulating the still image. Presented on a HD mobile screen.	The presentation technique used is standard and requires the test operator to move the ToE closer to the screen, which sometimes resulted in reflections.	15
	Simple Digital Animation presented on a laptop screen	This tailored digital attack consists of: - High-quality coloured digital photographs that are animated using a simple animation software. The software simulates smiling, blinking, head movement, eyebrow movement by manipulating the still image. Presented on a HD monitor or TV screen.		15
	Posed digital photos presented on a mobile screen	This tailored photo attack requires the attacker to acquire static photos of the target subject and use simple techniques to mimic the expected liveness challenges. The series of photos are presented on a mobile screen to the ToE in accordance with the liveness challenge presented by the application.		15
	Posed digital photos presented on a laptop screen	This tailored photo attack requires the attacker to acquire static photos of the target subject and use simple techniques to mimic the expected liveness challenges. The series of photos are presented on a laptop screen to the ToE in accordance with the liveness challenge presented by the application.		15

Test Crew Profile

The recruitment of test subjects for the purposes of creating the attack instruments 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 15 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 6 Age group distribution (PAD evaluation)

Age Range	BixeLab sourced percentage
< 18 y/o	0%
18 – 30 y/o	47%
31 – 50 y/o	33%
51 – 70 y/o	20%
> 70 y/o	0

Table 7 Sex distribution (PAD evaluation)

Sex	BixeLab sourced percentage
Male	73%
Female	27%

Table 8 Ethnic group distribution (PAD evaluation)

Ethnicity	BixeLab sourced
Caucasian	Yes
Polynesian	-
North African and Middle Eastern	-
North-East Asian	Yes
South-East Asian	Yes
Southern and Central Asian	Yes
Sub-Saharan African	-

Test Execution

This section provides a high-level overview of the test execution sequence informed by the evaluation goals.

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 item under test (IUT) followed a workflow which involved both types of tests. Test execution process for each test types is described below.

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 error rates 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 BRYK.ID solution users are expected to have a low level of familiarity with the application (at least for some time following the roll-out).

Attack presentations

High level summary of the PAD test execution process is provided 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 section 9.0).

Before test commencement, a runsheet was prepared to indicate the type of attack instruments to be corresponding to the planned test case.

PAD testing process is as follows-

1. Enter the user ID for the target whose biometric characteristics are present on the attack instrument.
2. Place the attack instrument in position when prompted on screen with the following message: "Get Ready For Your Video Selfie: Frame Your Face in the Oval, Press I'm Ready & Move Closer".
3. Press "I'm Ready".
4. Follow the liveness prompts when mounting the attack.
5. Attempt 5 times in case of an on-screen error when using a Level A attack instrument and 3 times in case of an error when using a Level B attack instrument.

6. If successful within the maximum number of specified attempts in step 5, move on to test logging.
7. If not successful after the maximum number of specified attempts in step 5, record a FTA.
8. To log the test outputs, refer to the web portal (dashboard) and log liveness outcome.
9. The operator also notes down any additional information which may be useful for analysis.
10. For each presentation attack instrument complete 10 transactions.

Bona fide presentations

1. Seeking consent for participation from the volunteering test subject.
2. Verbal training involved explaining how to proceed once application is installed, overview of steps to expect, maximum from of attempts for enrolment, verification, and liveness completion
3. Test subject completing steps 1 to 5, as described above but presenting their live face instead of attack instruments
4. Operator completing steps 6 and 9, as described above.

Performance Results

This section provides the performance results associated with the IUT for PAD evaluation. The reported results are in line with the applicable specifications of ISO/IEC 30107-3 standard.

Presentation Attack Detection Evaluation

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 6 Level A and 8 Level B presentation attack species as described in section Presentation Attack Instruments.

This section provides a breakdown of successful and unsuccessful test cases based on the attack potential associated with each type of attack vector covered in testing.

Figure 2 below shows an overview of presentation attacks mounted on the IUT.

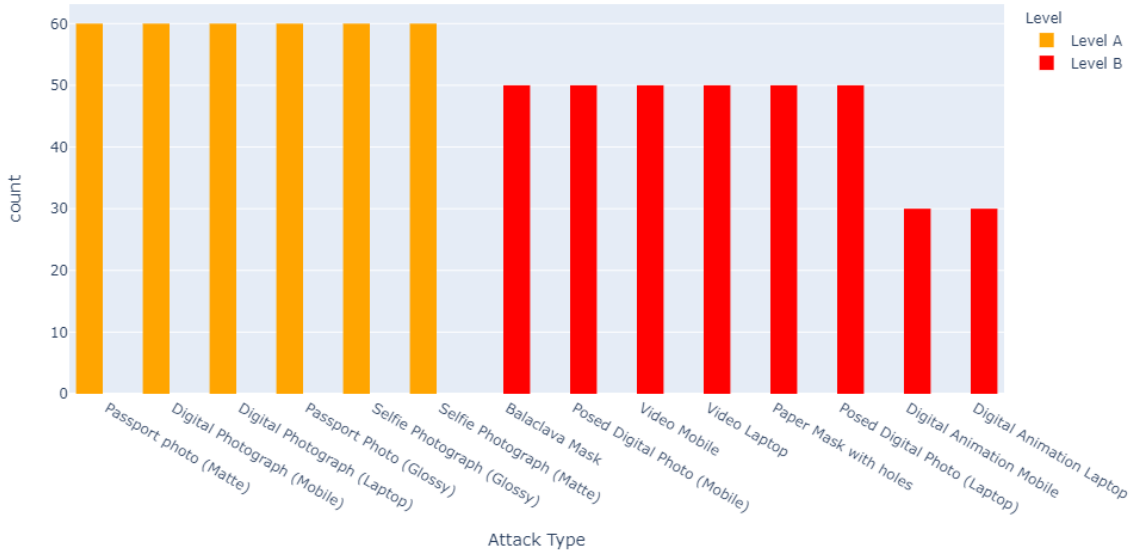

Figure 2 Overview of types of presentation attacks mounted

For each test, the test operator conducted ten imposter presentation attack transactions for each PAI. For Level A presentation attack instrument (PAI) species, maximum number of allowed attempts in a single transaction were 5. For Level B attack instruments, maximum number of allowed attempts in a single transaction were 3.

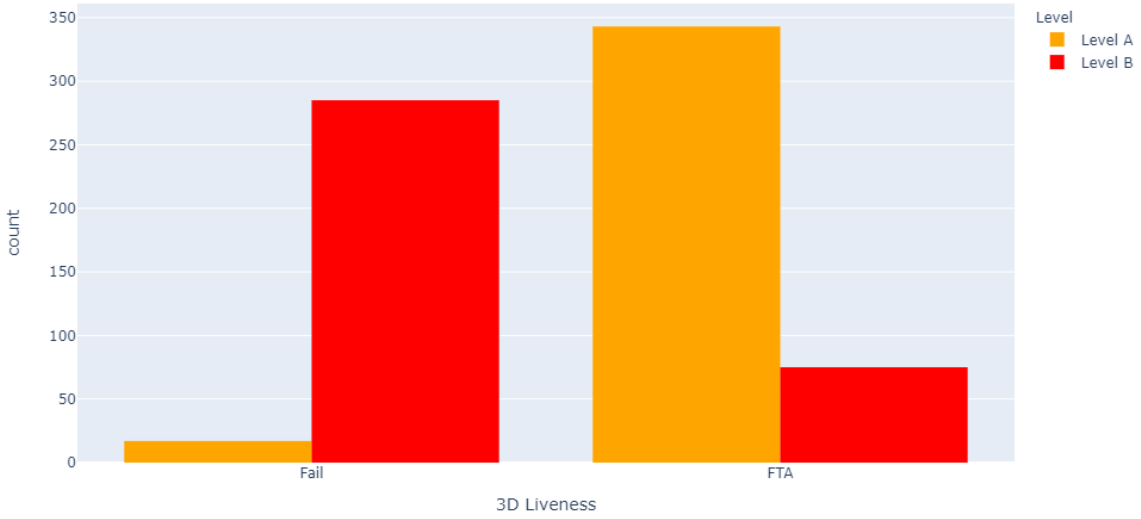

Figure 3 Breakdown of PAD performance for Level A and Level B attack types and live (bona fide) presentations

Figure 3 provides the distribution of liveness outcomes for Level A vs. Level B attack types. It can be seen that the PAD mechanism rejects both Level A and Level B attack types with no successful spoofs recorded.

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.

Table below provides a summary of PAD subsystem performance metrics associated with the IUT. This table along with Table 5 (Summary of Presentation Attack Species) provide all necessary information as recommended in clause 13.1 of the ISO/IEC 30107-3 standard.

Table 9 Summary of Test Results (PAD Evaluation)

Presentation Attack Level	Artificial Presentation Attack Instruments	Total Number of Attacks	Number of Successful Attacks	Attack Presentation Classification Error Rate (APCER)	Attack Presentation Non-Response Rate (APNRR)
Level A	**Passport style photograph printed on matte paper**	150	0	0%	0%
	Passport style photograph printed on glossy paper	150	0	0%	0%
	Selfie style photograph printed on a matte paper	150	0	0%	0%
	Selfie style photograph printed on a glossy paper	150	0	0%	0%

Presentation Attack Level	Artificial Presentation Attack Instruments	Total Number of Attacks	Number of Successful Attacks	Attack Presentation Classification Error Rate (APCER)	Attack Presentation Non-Response Rate (APNRR)
	Digital photograph presented on a mobile screen	150	0	**0%**	**0%**
	Digital photo presented on a laptop screen	150	0	**0%**	**0%**
Level B	**Video presented on a mobile screen**	150	0	**0%**	**0%**
	Video presented on a laptop screen	150	0	**0%**	**6.67%**
	2D Paper Mask	150	0	**0%**	**0%**
	Balaclava Mask	150	0	**0%**	**0%**
	Simple Digital Animation presented on a mobile screen	150	0	**0%**	**0%**
	Simple Digital Animation presented on a laptop screen	150	0	**0%**	**0%**
	Posed digital photos presented on a mobile screen	150	0	**0%**	**0%**
	Posed digital photos presented on a laptop screen	150	0	**0%**	**0%**

Based on the APCER metrics presented in table above, the APCER for attacks with an associated attack potential corresponding to Level A attacks is 0%. The APCER for attacks with an associated attack potential corresponding to Level B is also 0%.

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

As described in section Test Crew Profile, PAD evaluation leveraged presentations submitted by a demographically diverse test crew of 218 unique and consenting test subjects during the ISO/IEC 19795-2 Technology evaluation effort for 3D to 2D face matching accuracy analysis. The table below provides a summary of IUT performance for bona fide presentations.

Table 10 bona fide performance rates

bona fide Performance Rate	bona fide Performance
bona fide presentation Count	90
bona fide acquisitions	90

bona fide Performance Rate	bona fide Performance
bona fide non-responses	0
bona fide presentation classification error rate (BPCER)	0%
bona fide presentation non-response rate (BPNRR)	0%

Deviations and Exclusions

ISO/IEC 30107-3 covers the presentation attack types, system operational types, and evaluation techniques.

This report certifies only the following item tested:

- ***BRYK.ID with FaceTec server v9.6.30* – item under test (IUT) for PAD evaluation**
    - Attacks involved 6 Level A and 8 Level B classification attacks for 15 unique and consenting test subjects.
    - Testing of PAD mechanism of the IUT corresponded to evaluation of the PAD classification subsystem

BixeLab has undertaken every step to ensure no deviations or omissions from the ISO/IEC 30107-1 and ISO/IEC 30107-2 standards were made.

Findings and Recommendations

BixeLab has completed Level 2 PAD evaluation and technology evaluation of BRYK.ID-Demo version 1 (build number 12) – 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.

Refer to the findings and observations in the Executive Summary of this report.

Constraints

BixeLab has evaluated what it believes to be a representative sample of the commercially available solution with the utilisation of appropriate testing methodology stemming from the specifications of ISO/IEC 30107-3 and ISO/IEC 19795-2 standards.

The results associated with the PAD evaluation of the IUT have been reported in section Performance Results

Refer to section Test Constraints for limitations associated with this evaluation.

Note that, the results presented in this report serve as validation that BRYK.ID-Demo version 1 (build number 12) – item under test (IUT) has undergone testing in accordance with the ISO/IEC 30107-3 standard. Because the standard does not provide pass or fail levels for the metrics, this report does not indicate a pass or fail in association with this standard.

Deviations

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

Conclusions

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

Appendix 1: Verification Metrics

PAD Evaluation

The verification subsystem includes the PAD mechanism for the item under test. The verification procedure is anticipated to be monitored on both enrolment and verification ends in a real-world scenario, which has ramifications for artefact usage and non-conformant capture attempts. Real-world artefacts may not need a high level of visual plausibility however capture participants may not be able to experiment with various levels of non-conformant capture efforts to produce false accepts. Hence, PAD evaluation was undertaken with pre-defined presentation and decision policies as described in section Presentation Attack Instruments.

Metrics for PAD system evaluation –

Attack Presentation Classification Error Rate (APCER): proportion of attack presentations using same presentation attack instrument species that are incorrectly classified as bona fide presentations at the PAD subsystem in a certain scenario

APCER for a given presentation attack instrument species (PAIS) is calculated as follows:

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right) \sum_{i=1}^{N_{PAIS}} (RES_i)$$

Where N_{PAIS} is the number of attack presentations for the given presentation attack instrument PAI species and RES_i takes the value 1 if the ith presentation is classified as an attack presentation and value 0 if classified as bona fide presentation.

Bona fide Presentation Classification Error Rate (BPCER): proportion of bona fide presentations incorrectly classified as presentation attacks at the PAD subsystem in a certain scenario.

BPCER can be calculated as follows:

$$BPCER = 1 - \frac{\sum_{i=1}^{N_{BF}} (RES_i)}{N_{BF}}$$

Where N_{BF} is the number of bona fide presentations. RES_i takes the value 1 if the ith presentation is classified as an attack presentation and value 0 if classified as bona fide presentation.

Appendix 2: Terms and Definitions

Glossary

Term	Abbreviation	Definitions
Presentation Attack Detection (PAD) Evaluation		
Bona fide presentation		Interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system
Bona fide presentation classification error rate	BPCER	Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario
Bona fide presentation non-response rate	BPNRR	Proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem
Ground Truth		Ground truth is the actual state of nature, as pertaining to a match. In other words, it is the truth of whether or not a given match is genuine or imposter.
Liveness detection		Measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture
Bona fide presentation		Interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system
Target of evaluation	TOE	Within Common Criteria, the IT product that is the subject of the evaluation. Note: The TOE in Common Criteria evaluations is the equivalent of IUT in biometric evaluations.
Test approach		Totality of considerations and factors involved in PAD evaluation
Test Subject		A person who has been recruited to participate in a biometric evaluation.
Tester		The person performing the simulated PAD attack.
Item under test	IUT	implementation that is the object of a test assertion or test case

Appendix 3: Configuration Logs

The Client application software specifications are noted below						
Provider	**Title**	**Client CODE (If Applicable)**	**Version**	**Build**	**Identified Anomalies**	**Biometric Modality**
BRYK Pty Ltd	BRYK.ID with FaceTec	BXL018	-	30	None	Face (3D Facemap Liveness)
The BixeLab software and hardware system specifications are noted below						
Manufacturer & Model Name	**Software**	**BXL CODE (If Applicable)**	**Operating System**	**Identified Anomalies**	**Firmware**	
Apple and Samsung	N/A	BXL104, BXL106, iOS 11 Pro Max (version 16.0.2), iOS 11 (version 14.3.1), BXL108, Galaxy S21+ 5G	iOS and Android	None	N/A	