20 August 2018

To whom it may concern,

iBeta Quality Assurance conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-3. iBeta is accredited by NIST/NVLAP to test and provide results to this PAD standard (certificate and scope may be downloaded from the NVLAP website).

This testing was conducted with the FaceTec ZoOm® v6.6.0 modified from the production version currently available for iOS and Android devices to remove 2 anti-reverse-engineering mechanisms that would have caused a 5+ minute wait time for every 6 spoof attempts, as well as user deletion after 6 failed attemps in a row. Testing was conducted from 13-25 July, 2018 on two smartphones considered mid-level (iPhone 6S iOS Version 11.4 and Galaxy Note 5 Android Version 7).

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create artefacts of the genuine biometric for use in the presentation attack. The subjects for the test effort were cooperative – meaning that they were willing and able to provide any and all biometric samples, including high quality photos and videos of their likeness. The test time for each PAD test per subject was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

On each test platform, five subjects enrolled and authenticated three times succesfully. Six species of presentation attacks (PAs) were then attempted five times each. As each attempt was conducted, the application would state to 'try again' a number of times before presenting the user with the message that the authentication was unsucessful. As a result, approximately 1500 presentation attacks were attempted. At the conclustion of the PAD testing, the subject returned and authenticated three times successfully to verify that the facial recognition application was still able to recognize the genuine subject.

iBeta was not able to gain unauthorized access with the PAs on either test platform yeilding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Match Rate (IAMPR) for both systems of 0%.

The bona fide non-response error rate (BPNRR), Failure to Enroll (FTE) and Failure to Acquire (FTA) rates were also calculated and may be found in the final report.

Best regards,

Gail Audette
iBeta Quality Assurance Biometric Program Manager
(303) 627-1110 ext. 182
gaudette@ibeta.com

ZoOm® 3D Face Login SDK v6.6.0
PAD Certification Test Report

Prepared for

FaceTec, Inc.

1707 Village Center Cir, Suite 200,
Summerlin, NV 89134 USA

Version 1.0
20 August 2018
Report #180820-iBetaCTR-v1.0

Trace to Standards
ISO 30107-3
Sections 1.3, 6.0, 7.1, 7.2, 8.1, 10.2, 11.3, 11.5, 13.1, 13.2, 13.3 and 13.4
NIST Handbook 150-25
Sections 4.1.5, 5.10.1 through 5.10.4

Test Results in this report apply to the biometrics system configuration tested. Testing of biometric systems that have been modified may or may not produce the same test results. This report shall not be reproduced, except in full. iBeta Quality Assurance is accredited for Biometric System Testing:

TESTING
NVLAP LAB CODE 200962-0

2675 S. Abilene Street, Suite 300, Aurora, Colorado, 80014

Version History				
Ver #	**Description of Change**	**Author**	**Approved by**	**Date**
v.1.0	Initial report incorporating draft versions	*Kevin Wilson*	*Gail Audette*	20-Aug-2018

TABLE OF CONTENTS

1 Executive Summary

iBeta conducted certification testing in compliance with the requirement of ISO/IEC 30107-1 and ISO/IEC 30107-3 with the FaceTec ZoOm Version 6.6.0 facial recognition biometric system from 13 July through 25 July 2018. The testing was conducted on two smartphones loaded with the application.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create an artefact of the genuine biometric for use in the presentation attack.

For each smartphone (a Samsung Galaxy Note 5 with Android Version 7 and an iPhone 6S iOS Version 11.4), five (5) subjects enrolled and verified. There were then 6 species of presentation attacks (PAs) attempted 5 times per subject. The PAs were presented as directed by the application until the application stated that the authentication was unsuccessful. In most cases, the application allowed for 5 to 6 attempts prior to declaring an unsuccessful attempt which, in turn, corresponds to over 1500 presentation attacks over the entire test effort.

On both test platforms, iBeta was not able to gain unauthorized access with a presentation attack 5 times with each of 6 species of attacks. With 25 transaction attempts for each species, the Presentation Attack (PA) success rate is 0%.

The overall combined Imposter Attack Presentation Match Rate (IAPMR) for both systems equates to an overall PA success rate of 0%. The summary of testing is provided below in Table 1.

Table 1 Summary of Test Results

	Test Species	Android Versio 6.6.0			iOS Version 6.6.0		
		PAs	IAPM	IAPMR	PAs	IAPM	IAPMR
1.	2-D printed color photo with no liveness simulation	5 per subject	0 of 25	0%	5 per subject	0 of 25	0%
2.	2-D printed color photo with blink simulation	5 per subject	0 of 25	0%	5 per subject	0 of 25	0%
3.	2-D printed color photo mask	5 per subject	0 of 25	0%	5 per subject	0 of 25	0%
4.	“selfie” presented on a separate smartphone	5 per subject	0 of 25	0%	5 per subject	0 of 25	0%
5.	“selfie” 30 second video displayed on a separate smartphone	5 per subject	0 of 25	0%	5 per subject	0 of 25	0%
6.	30 second video displayed on a laptop monitor	5 per subject	0 of 25	0%	5 per subject	0 of 25	0%

1.1 *Background*

iBeta is nationally accredited as a test lab by the National Voluntary Lab Accreditation Program (NVLAP) to the requirements of ISO/IEC:17025 (General requirements for the competence of testing and calibration laboratories). In 2011, iBeta was accredited by NIST under the National Voluntary Laboratory Accreditation Program (NVLAP) for Biometric Testing under NIST handbook 150-25 and has become an expert in the field of biometrics. In addition, iBeta procedures against the ISO 30107-3 Presentation Attached Detection (PAD) standard were audited by our accrediting body and iBeta’s scope was increased to include certification to the ISO 30107-3 standard in April 2018.

The terms and definitions within this report are directly from the ISO 30107-3 standard.

1.2 *Internal Documentation*

The documents identified below are iBeta internal documents used in certification testing.

Table 2 Internal Documents

Version #	Title	Abbreviation	Date	Author (Org.)
iBeta	Contractual Documents			

Version #	Title	Abbreviation	Date	Author (Org.)
	Agreement for Presentation Attack Detection ISO 30107-3 Testing Services v02	SOW	18 May 2018	iBeta Quality Assurance
	Change Order 001 – Presentation Attack Detection Retest	CO 1	2 July 2018	iBeta Quality Assurance
	Mutual Confidential Disclosure Agreement	NDA		iBeta Quality Assurance
iBeta	PAD Procedures			
1.0	Biometric Deliverable Receipt Procedure		6/1/11	iBeta Quality Assurance
3.0	Biometric Security Procedure		5/20/13	iBeta Quality Assurance
1.0	Biometrics Configuration Management Procedure		6/9/11	iBeta Quality Assurance
1.0	PAD Certification Test Procedure		1/24/18	iBeta Quality Assurance
1.0	Biometric Training and Training Records Procedure		6/1/11	iBeta Quality Assurance
B	Biometric Certification Report Template		1/24/18	iBeta Quality Assurance
iBeta	Project Documents			
	PAD Test Case-Facetec ZoOm.xlsx		7/25/18	iBeta Quality Assurance

1.3 *External Documentation*

The documents identified below are external resources used to in certification testing.

Table 3 External Documents

Version #	Title	Abbreviation	Date	Author (Org.)
NIST Handbook 150 2006 Edition	NVLAP System Testing	NIST 150	February 2006	National Voluntary Lab Accreditation Program
NIST Handbook 150-25	NVLAP Biometric System Testing	NIST 150-25		National Voluntary Lab Accreditation Program
2010	International Standard: Conformity assessment – General requirements for proficiency testing	ISO/IEC 17043:2010	2010-02-01	ISO/IEC
2017-09	ISO/IEC 30107-3 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting	ISO 30107-3	September 2017	ISO/IEC
2016-01-15	ISO/IEC 30107-1 Information technology — Biometric presentation attack detection — Part 1: Framework	ISO 30107-1	January 2015	ISO/IEC
2012-12-15	ISO/IEC 2382-37, Information technology — Vocabulary — Part 37: Biometrics		December 2012	ISO/IEC
2016	Presentations and attacks, and spoofs, oh my." Image and Vision Computing 55 (2016): 26-30	Schuckers(2016)	2/3/2016	Schuckers, Stephanie, Clarkson University

1.4 *Technical Documents*

The Technical Documents submitted for this certification test effort are listed in Section 3 System Identification.

1.5 *Test Report Contents*

The contents of this Test Report include:

- Section 1: The Introduction identifies the scope of certification testing.
- Section 2 The Certification Test Background identifies the process for certification testing.
- Section 3 The Biometrics System Identification identifies the system configuration including hardware, software and the technical documentation.
- Section 4 The Biometrics System Overview identifies the overall design and functionality of biometrics system.
- Section 5 The Certification Review and Test Results are the methods and results of the testing effort.
- Section 6 The certification statement of the biometrics system.

Test Operations, Findings and Data Analysis are in the appendices.

- Appendix A: Certification Test Results for PAD Level 1 (bound separately).

2 Certification Test Background

The testing performed was completed per ISO-IEC 30107-3, which does not have specific pass/fail criteria or target IAPMR. Instead, the results of the testing presented in this report serve as a certification that the system as described was tested to provide the reported results.

The Systems under Test (SUT) is a facial recognition biometric system developed by FaceTec. iBeta was also informed by the Draft ISO 30107-4 for mobile device based application testing. iBeta follows the Levels of Testing as defined below in Table 4 that closely relates to the Levels A, B, and C as defined as the Level of Effort of PAD Artefact Generation from Schuckers, Stephanie. "Presentations and attacks, and spoofs, oh my." Image and Vision Computing 55 (2016): 26-30.

Table 4 iBeta Levels of PAD Testing

Level	Time	Expertise	Artefact source
Level 1	8 hours per subject	None	Cooperative subject and equipment is readily available in a normal home or office environment
Level 2	2-4 days per subject	Moderate – participated in at least 1 other PAD test with the target modality	Cooperative subject and equipment is more expensive (such as a 3D printer)
Level 3	3 weeks per subject	Significant – has dedicated at least 16 hours to research of presentation attacks of the target modality and has participated in at least 2 other PAD tests with the target modality	Cooperative Subject and latent sources for subject data. Equipment is extensive e.g., special order contact lenses, facial masks, and 3D printed spoofs

As part of their application for certification testing, FaceTec submitted their implementation statement (see section 3.0) for the ZoOm 3D Face Login SDK. The system under test consisted of Android and iPhone executables that exercised this SDK. Certification testing of the ZoOm® 3D Face Login SDK included Level 1 type testing, which includes fairly simplistic attacks that could be generated by non-skilled imposters with readily available materials. The PAD testing assumed that the biometric samples from the bona fide subject were available and in this study provided by a cooperative subject. Weekly status reports were sent to FaceTec certification management staff and iBeta project test staff. These reports included project activity status, issues, and other relevant information.

2.1 *Terms and Definitions*

The Terms and Definitions identified below are used in this test report.

Table 5 Terms and Definitions

Term	Abbreviation	Definition
attack potential		measure of the capability to attack an IUT (TOE) given the attacker's knowledge, proficiency, resources and motivation
attack type		element and characteristic of a presentation attack, including PAI species, concealer or impostor attack, degree of supervision, and method of interaction with the capture device
bona fide presentation		interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system
Bona fide presentation non-response rate	BPNRR	proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem.
Failure to acquire	FTA	The system fails to capture a sample from the subject. This is normally reported as a rate based on the number of subjects x attempts that the system attempted to acquire.
Failure to enroll	FTE	The system fails to enroll the subject. This is normally reported as a rate based on the number of subjects whom the system attempted to enroll.
Full-system evaluations		Full-system evaluations add a comparison subsystem to the IUT, generating a comparison score or candidate list. This situation is illustrated in ISO/IEC 30107-1:2016, Figure 3.
impostor attack presentation match rate	IAPMR	proportion of impostor attack presentations using the same PAI species in which the target reference is matched
presentation attack	PA	presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system
presentation attack detection	PAD	automated determination of a presentation attack
presentation attack instrument	PAI	object used in a presentation attack
PAI species		class of presentation attack instruments created using a common production method and based on different biometric characteristics
PAI series		presentation attack instruments based on a common medium and production method and a single biometric characteristic source
Implementation under test	IUT	that which implements the standard(s) being tested
Subject		The person from whom the biometric enrolment was taken. The target of the attack.
System under test	SUT	The computer system of hardware and software on which the implementation under test operates.
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
Tester		The person performing the simulated PAD attack.
Vendor		biometrics system manufacturer

2.2 *Presentation-Attack-Detection Certification*

As described above, the results in this report serve as a certification. No target values for these results exist.

2.2.1 Definition of Test Criteria

The test criteria determined the configuration and test cases were performed. The ZoOm® 3D Face Login SDK conformance checklist was provided by the vendor during contracting.

Evaluations of PAD mechanisms are classifiable as one of three general types – concealer, verification, or identification. This report is limited to:

- verification or authentication presentation attacks
- application-focused evaluations of PAD mechanisms in which the set/range of attack types is selected to be appropriate to the application, such as those discussed in Clause 11 of ISO 30107-3;
- in particular, this report covers only Level 1 or Level A types of attacks. Such attacks are performed with cooperation by the subject, using readily available materials, and produced and tested in less than an eight hour period per subject.

The evaluation did not cover:

- Concealer attacks – such as when an actor attempts to subvert the system by concealing that their biometric is enrolled in a given system.
- Identification attacks – such as when an actor is attempting to be identified in a one-to-many search of a database.
- Enrolment attacks – such as when an actor attempts to enroll a non-live face for purposes of subverting the system for some reason.

The following metrics were measured and reported here.

IAPMR – Imposter Attack Presentation Match Rate

Overall IAPMR – is the largest IAPMR reported for all species

$$IAPMR = \frac{Number\ of\ Imposter\ Matches}{Number\ of\ Imposter\ Attempts}$$

BPNRR – Bona Fide Presentation Non-Response Rate

Overall BPNRR – is the largest BNPRR reported for all species

$$BPNRR = \frac{Number\ of\ Bona\ Fide\ Failures\ to\ Match\ or\ Acquire}{Number\ of\ Bona\ Fide\ Attempts}$$

FTA – Failure to Acquire

$$FTA = \frac{Number\ of\ Failed\ Acquisitions}{Number\ of\ Acquisition\ Attempts}$$

FTE – Failure to Enroll

$$FTE = \frac{Number\ of\ Failed\ Enrollments}{Number\ of\ Enrollment\ Attempts}$$

2.2.1.1 *Levels of Evaluation*

Evaluation of PAD could occur at various levels within the biometric system. For example:

- The PAD subsystem may return a classification of attack, non-attack or live or non-live,
- The data capture subsystem may return a classification of attack, non-attack, live, non-live, and/or
- The full system may report the above, or it may only report match/no-match result for a given verification attempt.

Evaluation of PAD for this report consisted of the following:

- The PAD subsystem was tested as it returned the authentication or failure to authenticate the subject using the PAD species. In this particular implementation under test, scores were also available to the test personnel, but normally such scores would not be available to the end user (imposter in this case) of such a system if it was properly implemented according to vendor documentation.
- Thus, the full system only reported match/no-match result for a given verification attempt. However, on a separate screen available to the test personnel for this system, a match score was also provided.

The attack potential of PAD evaluation for this study was performed somewhat similar to Level A of Schuckers (2016), which corresponds to iBeta defined levels as provided in Table 5.

Table 6 Industry Accepted Levels of Attack

Level	Attack Potential	Examples
Level A = iBeta Level 1	Time: short (iBeta 8 hours) Expertise: anyone Equipment: readily available	paper printout of face image, mobile phone display of face photo iBeta also included: video (from mobile phone) display of face (with movement and blinking)
Level B = iBeta Level 2	Time: >3 days Expertise: moderate skill and practice needed Equipment: available but requires planning	paper masks, video display of face (with movement and blinking)
Level C = iBeta Level 3	Time: >10 days Expertise: extensive skill and practice needed Equipment: specialized and not readily available	silicon masks, theatrical mask

2.2.2 Test Environment Setup

The test environment was the Lab 4 within iBeta Aurora, Colorado offices. The lab contains a dark room, normal office lighting and bright photography lights as well as an 18% grey backdrop. For this PAD test effort, the lighting was documented each test day using a calibrated lux meter and recorded on the test data sheets.

The test platforms were two smartphones provided from the iBeta inventory and consisted of an iPhone 6s with iOS 11.4 and a Samsung Galaxy Note 5 with Android 7.0.

2.2.2.1 *Bona-fide population*

iBeta acquired 5 subjects to provide bona-fide / authentic samples as well as imposter samples of the facial recognition biometric. For diversity in the testing, subjects were recruited across age, gender, and ethnic backgrounds such that 40% of the subjects were female, representation was provided from each age group (2 subjects were between the ages of 18-35, 1 subject was between the ages of 36-53, and 2 subjects were between the ages of 54-70), and 1 non-Caucasian subject presented. Subjects were cooperative. For the two subjects that presented with glasses, the test was then conducted with glasses.

Each subject enrolled in each test device and then completed 3 authentications to verify that the application allowed the bona-fide subject access. At the end of the PAD testing, the subject then completed an additional 3 authentications to verify that the application would again allow the bona-fide subject access.

2.2.2.2 *Artefact Generation*

For biometric impostor attacks where the subject intends to be recognized as a specific, targeted individual known to the system, it was necessary to create artefacts with three properties:

- Property 1. The sample appears as a natural biometric characteristic to any PAD mechanisms in place.
- Property 2. The sample appears as a natural biometric characteristic to any biometric data quality checks in place.
- Property 3. A sample acquired by a capture device from the artefact contains extractable features that match against the targeted individual's reference.

Artefacts for the testing consisted of six species:

1. 2-D printed color photo with no liveness simulation
2. 2-D printed color photo with blink simulation
3. 2-D printed color photo mask
4. “selfie” presented on a separate smartphone
5. “selfie” 30 second video displayed on a separate smartphone
6. 30 second video displayed on a laptop monitor

As the subjects were cooperative, each species appeared as a natural facial duplication (meeting the requirements of Property 1 and 2). All of the facial features captured in the artefacts contained extractable features as they were acquired from the genuine subject (meeting the requirement of Property 3).

Artefact generation for this system did not rely on white-box or gray-box analysis of the SUT. Iterative techniques were not used during this certification.

Based in the modality and type of PAD testing being performed, artefact generation was chosen to be captured on a smartphone ("selfie" photos and video") and from a mid-level digital camera as these are devices that a novice or Level 1 attacker would have available. Similarly, the images were printed either at FedEx or on office printers that iBeta determined would be accessible to a novice or Level 1 attacker. The "selfie" photos and video were displayed on a Samsung Galaxy S8 and a Dell Laptop.

Per the statement of work for this Level 1 test effort, iBeta performed the testing using cooperative subjects. For example, videos of the test subjects were obtained in office lighting conditions and those videos were later used as the PAIs for the testing.

The artefacts were created with minimum effort by the tester in that the creation of the artefacts and presentation of the artefacts were completed in an 8 hour day for each of the 5 subjects. The testers had no specific knowledge of the application functionality and had not habituated to the SDK prior to testing. The source of the biometric artefacts was access to the cooperative subject. The majority of the testers (3 of the 5) had conducted a previous facial recognition spoofing project (but not a 30107-3 certification effort).

2.2.2.3 *Artefact Usage*

Each tester was provided with the same types of species and artefacts but the decision to use the normal household items within the lab as well as the lighting levels was not dictated. Each tester was allowed to use the items within the lab and items that they had at their workstation with no limits applied. As such, artefacts were presented at 3 different light levels (dark at 46 lux, bright between 930 and 1030 lux, and office between 200 and 405 lux). Artefacts were also attached to different backgrounds and treated with lotion, Saran wrap, and Vaseline.

Sufficient artefacts were printed so that the photographs could be cut-out as the tester determined. The Lead Tester provided guidance and monitored test progression. At no time was the subject allowed in the lab while the artefacts were being presented.

2.2.2.4 *Iterative Approaches to Artefact Design*

No iterative approaches were used to generate and use artefacts.

2.2.2.5 *Test Design*

The test design and test case development was conducted for the verification process only. Prior to testing, iBeta met with the vendor at the vendor facility in San Diego, California and was allowed to view the artefacts that the vendor had been using to test their facial recognition application. iBeta did make notes as to what artefacts had been tested; however, the standard set of species for facial recognition was not altered based on the knowledge gained from the visit.

FaceTec provided an application that was modified to remove two anti-reverse-engineering mechanisms that would have caused a 5 minute wait time for every 6 spoof attempts as well as user deletion after 6 failed attempts in a row. This modification was required for testing to proceed. It was noted during the test case development that the application would provide a statement to the user to either raise the phone to eye level or adjust the lighting conditions. After 5 or 6 of those types of messages, ZoOm would then provide the matching results 'Authentication Unsuccessful'. iBeta would then select the Results button and record the liveness score. That score was the only indication provided by the application that gave operator insight into how the artefacts were being evaluated by ZoOm.

2.2.3 Test Execution

Test execution was conducted 7/13/18 through 7/25/18 and the results are listed in Appendix A. Two software deliveries were provided by FaceTec of the ZoOm product. The results within this certification test report contain only the summary of the test execution with the second and final software application.

The subject demographics is provided below in Table 7.

Table 7 Subject Demographics

Subject	Age	Gender	Self-declared ethnicity	Glasses
1	64	Male	Caucasian	Yes
2	58	Female	Caucasian	Yes
3	30	Male	Caucasian	No
4	45	Male	Caucasian	No
5	49	Female	African American	No

In summary, the testing was conducted on each smartphone as follows:

1. 5 subjects enrolled and logged in three times (to verify that the application was working). iBeta attempted to capture the verification a samples in varying lighting (1 each in dark, office, and bright light). Failures to Enroll (FTEs) and Failure to Acquire (FTAs) were recorded.
2. The tester(s) then applied Presentation Attack Instrument Species (PAIS) five times each until the application provided the message 'Authentication unsuccessful'. All photos and videos were in color and captured with a digital camera/video camera in Quad HiDef (2560 x 1440). The species were:
    a. 2-D printed color photo with no liveness simulation – simply a picture without manipulation or cut-outs
    b. 2-D printed color photo with blink simulation – either a hand wave or the flipping of a closed eye photo with an open eye photo
    c. 2-D printed color photo mask - curved the photo to simulate the face shape and placed the testers eyes in the cutout of the photo eyes
    d. "selfie" presented to the ZoOm app on a separate smartphone (Samsung Galaxy S8)
    e. "selfie" 30 second video presented to the ZoOm app on a separate smartphone (Samsung Galaxy S8)
    f. 30 second video displayed on a laptop monitor –
        - the laptop was placed on its side so the video was neck up with phone on desk at close proximity,
        - glare did interfere with taking the picture so the light was reduced in the lab, and
        - none of the edges of the laptop showed in the ZoOm face frame.
3. After the testing was complete, the live subject logged in three times in normal office light to verify that the application was still working.
4. All results were recorded.

For each subject 4 photos were taken with the digital camera, 4 "selfie" photos were taken with the test smartphone, and 1 "selfie" video was taken with the test smartphone. Each tester determined how many printouts to use and anywhere between 4 and 10 were utilized for a subject test.

The number of subjects selected and the number of times each species was presented were documented within the contract scope of work. This number and presentation was limited by this being a Level 1 PAD test effort which, by definition, only allowed a tester 8 hours per subject.

Performance metrics discussed in ISO 30107-3 Clause 13 can fail to achieve statistical significance due to limitations in sample size. iBeta determined the metrics that would be recorded and reported during test case development as:

$$IAPMR_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right)\sum_{i=1}^{N_{PAIS}} Res_i \qquad (1)$$

Where

N_{PAIS} is the number of attack presentations for the given PAI species;

Res_i takes the value of 1 if the i^{th} presentation is classified as a match and value 0 if classified as a non-match.

$$BPNRR = \left(\frac{1}{N_{BF}}\right)\sum_{i=1}^{N_{BF}} Res_i \qquad (2)$$

Where

N_{BF} is the number of bona fide presentations;

Res_i takes value 1 if the i^{th} presentation produces a non-response or failure to match and value 0 if the bona fide subject matches.

2.2.3.1 *Deviations and Exclusions*

This report certifies only the following Presentation Attack Detection Testing performed. ISO 30107-3 covers a number of attack types, system operational types, and evaluation techniques. This report certifies only the following items tested:

- A mobile device authentication system using facial biometrics
- Attacks involving photos, videos, and 2D paper masks
- Evaluation of the overall system as opposed to the PAD classification subsystem. That is, the overall system did/did not report the difference between a failure to acquire and a failure to authenticate.

There were no deviations or omissions from the standard.

3 Biometrics System Identification

The System Identification stipulates the FaceTec ZoOm facial recognition biometric application submitted for certification and the hardware, software and the documentation used in testing.

3.1 *Submitted Biometrics System Identification*

Table 8 Biometrics System Name and Version

Biometric System Name	Version
ZoOm	6.6.0

This Biometrics System includes the following:

Table 9 Biometrics System Software

Software Applications	Version	Function Description
iOS SDK	Version 6.6.0-iBeta-2018071301	System Under Test on iPhone 6S
Android	Version 6.6.0-iBeta-2018071301	System Under Test on Samsung Galaxy Note 5

3.2 *Biometrics System Test Environment*

The Biometrics System Test Environment identifies the specific hardware that was used in the test environment. For this test effort, iBeta located all equipment in the biometrics lab.

Table 10 Biometrics System Test Hardware

Hardware	OS or Version	Manufacturer	Description (include functional purpose and condition of the equipment)
iPhone 6S	iOS 11.4	Apple	Test platform Serial Number DNPQQ4ZPGRXV
Galaxy Note 5	Android 7 (Nougat)	Samsung	Model SM-N920V Serial No. 0815f8d069592c01

Table 11 Biometrics System Technical Documents

Version #	Title	Abbreviation	Date	Author (Org.)
Jun-4-2018	FaceTec PAD Testing Methodology – A Detailed Look into Liveness & 3D Depth Detection		Jun-4-2018	FaceTec
6.4	ZoOm API documentation Android		Jun-12-2018	FaceTec
6.4	ZoOm API documentation IOS		Jun-12-2018	FaceTec

Table 12 Other Software, Hardware and Materials

Material	Material Description	Use in the Biometrics System
Other		
Dr. Meter LX1330B	Light (Lux) Meter	Measure light levels
Canon EOS Rebel T1	SLR Digital Camera color DS126231	Used to acquire color 2D facial images as attack species.
Samsung Galaxy S8	Model number SM-G950U Serial number RF8JA1T8H4y	Used to acquire video and also to present video on the cell-phone species
Dell Inspiron 15	Model 3542 Intel Pentium 3542 Windows 7 Home Premium SP1 64-bit	Presentation of attack videos.
Multiple desktop and laptop PCs	A variety of PCs running Microsoft operating systems	Supplied by iBeta: Preparation, management and recording of test plans, test cases, reviews, results and reports
Microsoft Office 2013	Excel and Word software and document templates	Supplied by iBeta: The software used to create and record test plans, test cases, reviews and results
SharePoint 2010	TDP and test documentation repository	Supplied by iBeta: Vendor document and test documentation repository and configuration management tool
Other standard business application software	Internet browsers, PDF viewers email	Supplied by iBeta: Industry standard tools to support testing, business and project implementation

4 Biometrics System Overview

The FaceTec ZoOm 6.6.0 consists of a biometric facial recognition system. ZoOm's patented process scans a 3D face with a 2D camera to create a face map of the real user. This is conducted by the user bringing the smartphone or zooming closer to the face during the enrolment and verification process. ZoOm uses the changing perspective of the user's head, neck, ears, hair, facial features and the environment as the camera is moved closer to the face. The algorithm processes video frames while concurrently measuring the motion of the device.

ZoOm was tested on two smartphone test platforms using the front-facing or "selfie" camera. Enrollment was conducted in accordance to the instructions within the application. Enrollment and matching was performed on FaceTec servers.

5 Certification Review and Test Results

The results and evaluations of the tests are identified below. Detailed data regarding the Acceptance/Rejection criteria, reviews and tests are found in the appendices.

- Appendix A identifies all certification test results for Certification Testing

5.1 *Limitations*

The results and conclusions of this report are limited to the specific IUT/SUT applications and versions described below.

It is the responsibility of the vendor to provide the laboratory with systems and devices which are representative of those systems and devices produced for the consumer.

These results represent usage of falsification testing methodology. Testing can only demonstrate non-conformity, i.e., if errors are found, non-conformance of the SUT shall be proven, but the absence of errors does not necessarily imply the converse. These results are intended to provide a reasonable level of confidence and practical assurance that the SUT conforms to the standard. Use of these results will not guarantee conformity of an implementation to the standard; that normally would require exhaustive testing, which is impractical for both technical and economic reasons.

As described elsewhere, this report covers only level 1 or relatively low level PAD species for the biometric system under test.

iBeta did not attempt to differentiate classification errors from failure to match errors. All results are reported as overall-system types of errors in the sense that either the subject or attack species either matched or did not match. FaceTec has indicated that the system responses do not normally provide classification responses to mitigate hill-climbing attacks against the system.

5.2 *PAD Testing Results*

The iOS and Android ZoOm applications from FaceTec did operate identically. The Android test platform camera placement differed from the iOS test platform in that the iOS camera was located in the top, middle of the device and the Android camera was on the far top left-hand side of the device.

5.2.1 ZoOm Version 6.6.0 iOS Application Results

The iOS based SDK was able to function with less light than the Android version. The verification samples were taken in office, dark and bright light prior to the start of PAD Level 1 testing.

All users were able to enroll successfully although Subject 5 had a failed attempt before successful enrolment. The Failure to Enrol (FTE) rate was 16.7% in that 1 of the 5 subjects had a failed first attempt to enroll so enrollment was successful 5 out of 6 attempts.

Bona fide presentation non-response error rate (BPNRR, which is the percentage of time a bona fide user is rejected on an attempt to authenticate) on the iOS application was 23%. None of the subjects had any issues completing their verification samples after enrolling but 3 subjects had to try 4 times on the first try after the PAD

Level 1 testing was complete. In total, there were 39 verification attempts with 30 successes. Of note is that all of the non-responses occurred at the conclusion of the presentation attacks on the first authentication with the bona fide subject.

iBeta considered a bona fide presentation to fail if the system did not validate or authenticate the bona-fide presentation.

There were no unauthorized accesses with the artefacts as shown in Table 13 below. As defined above in the Test Design Section 2.2.2.5, iBeta considered a single results from the PAs when the application stated that the authentication was unsuccessful. As it took between 5 and 6 presentations of the artefacts (with statements to the user to "try again"), the artefacts were presented approximately 125 times each to yield the IAPMR of 0 of 25.

Table 13 iOS Results

	Test Species	iOS Version 6.6.0		
		PAs	IAPM	IAPMR
1.	2-D printed color photo with no liveness simulation	5 per subject	0 of 25	0%
2.	2-D printed color photo with blink simulation	5 per subject	0 of 25	0%
3.	2-D printed color photo mask	5 per subject	0 of 25	0%
4.	"selfie" presented on a separate smartphone	5 per subject	0 of 25	0%
5.	"selfie" 30 second video displayed on a separate smartphone	5 per subject	0 of 25	0%
6.	30 second video displayed on a laptop monitor	5 per subject	0 of 25	0%

5.2.2 ZoOm Version 6.6.0 Android Application Results

For obtaining the verification sample is dark lighting, the Android application required more light with levels as high as 116 lux. Even at this level, two of the subjects could not acquire verifications samples in the dark lighting and instead captured 2 verification samples in normal office light and one in bright light.

All subjects were able to enroll successfully. The FTE was 0%.

BPNRR on the Android application was 35%. One subject had to attempt to verify twice after enrolling and all 5 subjects had to try multiple times on the first try after the PAD Level 1 testing was complete. In total, there were 46 verification attempts with 30 successes.

There were no unauthorized accesses with the artefacts as shown in Table 14 below. As defined above in the Test Design Section 2.2.2.5, iBeta considered a single result from the PAs when the application stated that the authentication was unsuccessful. As it took between 5 and 6 presentations of the artefacts (with statements to the user to "try again"), the artefacts were presented approximately 125 times each to yield the IAPMR of 0 of 25.

Table 14 Android Results

	Test Species	Android Version 6.6.0		
		PAs	IAPM	IAPMR
1.	2-D printed color photo with no liveness simulation	5 per subject	0 of 25	0%
2.	2-D printed color photo with blink simulation	5 per subject	0 of 25	0%
3.	2-D printed color photo mask	5 per subject	0 of 25	0%
4.	"selfie" presented on a separate smartphone	5 per subject	0 of 25	0%

5.	“selfie” 30 second video displayed on a separate smartphone	5 per subject	0 of 25	0%
6.	30 second video displayed on a laptop monitor	5 per subject	0 of 25	0%

5.2.3 Exclusions

When interpreting the performance of a PAD subsystem, it is important to recognize that there may be presentation attack types, PAI species and factors which have not been tested. Therefore, the reported performance of a PAD subsystem does not provide any information regarding its effectiveness in detecting presentation attacks which have not been tested.

6 Opinions & Recommendations

6.1 *Recommendations*

iBeta Quality Assurance has completed the Level 1 PAD testing of FaceTec ZoOm Version 6.6.0. The purpose of this report is to describe the testing performed and the metrics obtained for that testing. Conformance to any criteria was not tested.

Based on the test results of Section 5, the overall system design and construction of the application meets all of the normative requirements with the ISO/IEC 30107-3 for Level 1 testing.

iBeta Quality Assurance certifies that FaceTec’s ZoOm Version 6.6.0 meets the Level 1 criteria for Presentation Attack Detection.

6.1.1 Limitations

As described in section 5.1 Limitations, iBeta has tested what it believes to be a representative sample of the commercially available system and used the appropriate test methods to test conformance to the standards.

As stated also in Section 2.0, this report does not contain a certification per se, but only results of testing per a certified procedure. There are no ISO 30107-3 requirements stating specific levels of passing or failing values for example of IAPMR or BPNRR reported.

The results of this report rely on testing of a cloud-based system. As the authentic and artefacts were provided to the cloud environment and not entirely under iBeta control, the results of this test should be understood with this caveat in effect.

Furthermore, at the conclusion of the testing, iBeta became aware that FaceTec had, in fact, examined the log files and the videos present in the cloud environment from the test effort. All testing materials are considered proprietary to iBeta and covered by our New England Institutional Review Board approval for collecting PII. iBeta had not granted FaceTec explicit permission to monitor or examine test materials either during or after testing. After testing was concluded, iBeta did determine that FaceTec had specifically reviewed the test data. iBeta has not determined that this review of data impacted the integrity of the test results; however, iBeta cannot guarantee that FaceTec did not alter the test results.

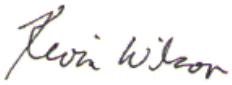
The results reported here were obtained after iBeta received a revision of the matching algorithm. During PAD testing of the previous version iBeta had observed a non-zero IAPMR but were assured by FaceTec that it had already fixed this problem in a new version. The version reported here was delivered five days after notification.

6.1.2 Exceptions

There were no exceptions to the test method. The data supporting this review are found in Appendix A.

6.2 *Opinions*

iBeta has no other remarks or opinions not reflected in the above report.



Dr. Kevin Wilson
Director of Biometrics
KWilson@ibeta.com
303-627-1110 extension 177

7 APPENDICES: TEST OPERATION, FINDINGS & DATA ANALYSIS

This appendix contains proprietary iBeta test methodology and test results and is bound separately.

7.1 *Appendix A: PAD Certification Test Results – Test Case 1*

7.2 *Appendix A: PAD Certification Test Results – Test Case 2*