ZoOm® 3D Face Login SDK v5.1.1

DEA EPCS Biometric Subsystem Certification Test Report

Prepared for:
FaceTec, Inc.
1707 Village Center Cir, Suite 200,
Summerlin, NV 89134 USA

Version 1.0
23 June 2017
Report #170623-iBetaBTR-v1.0

Trace to Standards
21 CFR Parts 1311.116

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 DEA approved for Biometric System Testing:

Date of publication:
06 – 23 – 2017

This report is made public as of the above date.
It will be maintained at http://www.ibeta.com for a period of 2 years from that date.

Date of expiration:
June – 23 – 2019

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

Version History				
Ver #	**Description of Change**	**Author**	**Approved by**	**Date**
V1.0	Initial Certification Report for FaceTec Inc.'s ZoOm - 3D Face Login SDK, Version 5.1.1	*Dr. Kevin Wilson*	*Gail Audette*	*23 June 2017*

TABLE OF CONTENTS

1 Executive Summary

This report contains the results, conclusions and recommendations of iBeta Quality Assurance assessment of the biometric subsystem named ZoOm 3D Face Login version 5.1.1 from FaceTec performed from 31 May 2017 to 16 June 2017 to validate the applicable requirements of 21 CFR Part 1311 for its inclusion in an Electronic Prescription of Controlled Substances System (EPCS).

The ZoOm 3D Face Login application was tested on mobile devices, Apple iPhone 7 Plus and Samsung Galaxy S8 using the front-facing camera for user authentication. iBeta tested the application to meet the Drug Enforcement Agency (DEA) EPCS False Match Rate (FMR) of 0.001 or lower. The operating point corresponding with the False Match Rate described in 1311.116(b) was tested so that there was at least 95% confidence that the False Match Rate was equal to or less than the required value. To validate the False Match Rate requirement of 0.001 or lower as cited in 1311.116(b), iBeta used the vendor-supplied threshold of 4.0070.

The ZoOm 3D Face Login biometric subsystem was tested to the DEA EPCS regulations with 21 CFR Part 1311.116. All other EPCS requirements are out of scope of this report. Requirements of 1311.116 which were out-of-scope because they were not testable for the given subsystem are shown in Table 7-1.

This report is publicly available and Attachments 1, 2 and 3 are available upon request from FaceTec. This report will be maintained on the iBeta website during the period of certification from the issuance of this report (23 June 2017) through the certification expiration date (23 June 2019).

1.1 *Biometric Subsystem Identification*

The ZoOm 3D Face Login application is an app SDK that can operate on iPhone iOS and Android mobile devices. ZoOm 3D core acquisition components are described in Section 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric Subsystem Test Environment. A single application for each operating system (OS) was provided by FaceTec. The application acquired enrollment (gallery) and authentication (probe) samples and produced scores for matches between the two repositories.

1.2 *Disclosure*

This report consists of the test results as contracted by an agreement between the independent test organization, iBeta Quality Assurance LLC and the client, FaceTec. This report is made public to meet DEA requirements.

Additional results are proprietary and not made public but disclosed to the vendor:
- Attachment 1: Detailed Technology Assessment Results
- Attachment 2: Additional Technology Assessment Results - Effect of Glasses and Identical Twins
- Attachment 3: Additional Technology Assessment Results - Camera Spatial Frequency Response and Distortion

Information and data not disclosed to the vendor or any party outside of the testing lab includes
- Technology test data used to determine the FMR;
- Test Design Procedures; and
- Test case templates and as-run Test Cases.

2 Introduction

This report was generated to document the iBeta Quality Assurance's assessment and testing of a biometric subsystem for the purpose of that subsystems' inclusion in and Electronic Prescribing of Controlled Substances (EPS)) system. This report address the testing of theZoOm 3D Face Login application for user authentication on a mobile device using the selfie or front-facing camera to 21 CFR 1311.116 regulations. iBeta utilized a FaceTec generated data acquisition app on the mobile devices.

iBeta tested the application utilizing the Apple iPhone 7 Plus running on iOS 10.3.2 and Samsung Galaxy S8 running on Android 7.0. The methodology for obtaining these metrics was to collect 100 subjects' data with an enrolment (gallery) and then 2 authentication or verification templates (probe).

The target accuracy for the application established within the Statement of Work (SOW) was to calculate the FAR (FMR) at or better than 0.1% at a 95% confidence.

The FaceTec special application was used to acquire the dataset used to evaluate the FMR and FMNR results. The purpose of this document is to report the testing and findings. The complete list of the system names, major subsystems, version numbers and any interfacing devices is contained in Section 4 – Biometric System Identification. Additional details of the design, structure, and processing capabilities are identified in Section 5 – Biometric System Overview.

Testing was conducted at iBeta Quality Assurance facility in Aurora, Colorado.

Certification testing was performed in compliance with the requirements of 21 CFR Parts 1300, 1304, 1306 and 1311 as applicable. The test record included all test executions and reviews. All test executions and reviews included the record of requirements that were satisfactorily and unsatisfactorily completed, deficiencies noted, reports to FaceTec, software and manufacturing resolutions, validations of resolutions and documentation of incorporation of resolutions into the biometric system.

The New England Independent Review Board (NEIRB) reviewed iBeta Biometric Test Protocol application and granted unconditional approval on 15 September 2016 (approval: #120160885) for the following):
- Test Protocol Version 2.0 dated 19 August 2016
- Biometrics Security Procedures (Version 3.0) dated 20 may 2013
- Biometric Subsystem Assessment Procedure (Version 4.0) dated 21 May 2013
- Biometrics Testing Disclaimer (Version 1.0)
- Brochure - 'Biometrics Testing Lab'
- Informed Consent Form (Form A)

The test effort was conducted in full compliance with the IRB approved study protocol.

The requirements in the 21 CFR 1311 is that the biometric subsystem operates at a FMR of 0.001 (0.1%) or lower. Technology testing was for the FMR requirement was performed using ISO/IEC 19795-1 and ISO/IEC 19795-2 as guidance documents in the generation and execution of test cases.

During all phases of the certification testing iBeta provided FaceTec with regular status reports.

iBeta Quality Assurance, a limited liability company, is located in Aurora, Colorado. The company is a full service software testing laboratory providing Quality Assurance and Software Testing for the business and interactive entertainment communities.

2.1 *Internal Documentation*

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

Table 2-1 Internal Documents

Version #	Title	Abbreviation	Date	Author (Org.)
	Mutual Confidential Disclosure Agreement	NDA		iBeta Quality Assurance

Version #	Title	Abbreviation	Date	Author (Org.)
Version 2.0	Agreement for DEA EPCS Pre-Certification Testing Services	MSA	April 27, 2016	iBeta Quality Assurance
Version 2.0	Agreement for DEA EPCS Pre-Certification Testing Services	Contract	May 26, 2017	iBeta Quality Assurance
iBeta 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
4.0	DEA-EPCS Biometric Assessment Procedure		5/21/13	iBeta Quality Assurance
1.0	Biometric Training and Training Records Procedure		6/1/11	iBeta Quality Assurance
iBeta Project Documents				
1.0	DEA-EPCS-Biometric-Assessment-FaceTec		6/8/17	iBeta Quality Assurance
1.0	FaceTec DEA EPCS Pre-Certification Letter		5/24/17	iBeta Quality Assurance
1.0	DEA-EPCS-Test-Cases-FaceTec		6/16/17	iBeta Quality Assurance

2.2 External Documentation

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

Table 2-2 External Documents

Version #	Title	Abbreviation	Date	Author (Org.)
2005	ISO/IEC 17025: 2005 – General requirements for the competence of testing and calibration laboratories	ISO/IEC 17025: 2005	2005-05-15	ISO/IEC
2010	ISO/IEC 17043:2010 – International Standard: Conformity assessment – General requirements for proficiency testing	ISO/IEC 17043:2010	2010-02-01	ISO/IEC
2006	ISO/IEC 19795-1:2006 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework	ISO 19795-1 Or 19795-1	Aug 17, 2007 (ANSI adoption)	ANSI ISO
2006	ISO/IEC 19795-2:2006 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation	ISO 19795-2 Or 19795-2	Feb 01, 2007 (ANSI adoption)	ANSI ISO

Version #	Title	Abbreviation	Date	Author (Org.)
1	Evaluation of measurement data — Guide to the expression of uncertainty in measurement	JCGM:100	September, 2008	JCGM (Joint Committee for Guides in Metrology)
31 Mar 2010	21 CFR Part 1311.116 Additional Requirements for Biometrics	Regulations	31 Mar 2010	Drug Enforcement Administration (DEA) Department of Justice, Office of Diversion Control
31 Mar 2010	21 CFR Parts 1300, 1304, 1306, and 1311 Electronic Prescriptions of Controlled Substances	Interim Final Rule	Effective Date 1 June 2010	Drug Enforcement Administration (DEA) Department of Justice, Office of Diversion Control
19 Oct, 2011	Docket No. DEA-360 Clarification and Notification		19 Oct, 2011	DEA Office of Diversion Control
1472G	MIL-STD-1472G Department of Defense Design Criteria Standard Human Engineering		11 January 2012	Department of Defense
R2014	INCITS 385-2004[R2014] Face Recognition Format for Data Interchange	INCITS 385	2014	ANSI INCITS
2014	ISO 12233 Photography – Electronic still picture imaging – Resolution and spatial frequency responses	ISO 12233	2014-02-15	ISO
2009	ISO 14524 Photography – Electronic still-picture cameras – Methods for measuring optoelectronic conversion functions (OECFs)	ISO 14524	2009-02-15	ISO

2.3 Technical Documents

The Technical Documents submitted by FaceTec for this certification test effort are listed in Section 4 – Biometric Subsystem Identification.

2.4 Test Report Contents

The contents of this Test Report include:
- Section 1: The Executive Summary identifies a brief summary of results and conclusions of the accuracy testing.
- Section 2: The Introduction identifies the scope of accuracy testing.
- Section 3: The Test Background identifies the process for accuracy testing.
- Section 4: The Biometric Subsystem Identification identifies the system configuration including hardware, software and the technical documentation.
- Section 5: The Biometric Subsystem Overview identifies the subsystem functionality capabilities.
- Section 6: The Certification Review and Test Results are the methods and results of the testing effort.
- Section 7: The Opinions and Recommendations section identifies the certification and limitations of that certification based upon the results of Section 6.

Detailed Results and Data Analysis are in Attachments 1, 2 and 3: Detailed Technology Assessment Results.

3 Certification Test Background

As a background for this biometric subsystem certification, under 21 CFR 1300, 1304, 1306 and 1311, the DEA Office of Diversion Control specifies and regulates the operation of Electronic Prescription of Controlled Substances (EPCS) applications. The regulations require 2-factor authentication of individuals to a system that electronically prescribes controlled substances. The regulations allow for two of three factors to be used for authentication. One of those factors may include a biometric from the individual claiming an identity.

Certification testing of the ZoOm 3D Face Login biometric subsystem included Security Assessment and Operating Point to provide 0.001 false match rate or better (0.1%). Weekly status reports were sent to FaceTec. These reports included project activity status, issues, and other relevant information.

3.1 Terms and Definitions

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

Table 3-1 Terms and Definitions

Term	Abbreviation	Definition
Authentication	Auth	The process whereby a claimant provides evidence to a system that the claimant is in fact the person claimed and not an imposter.
Biometric characteristic		A specific type of physical attribute associated with an individual that may be used to establish identity. Examples are fingerprint, iris, facial, hand geometry, vein pattern, gait and signature.
Biometric Sample	biometric	Information obtained from a biometric sensor, either directly or after further processing
Biometric Subsystem		As viewed from the perspective of an overall prescription signing system or application, the biometric subsystem is that portion of the system used to provide the biometric authentication when a biometric is used as one of the two factors of authentication.
Biometrics Identification	BID	The anonymous 6 digit subject identification biological characteristics.
Built-in		iBeta's DEA approved process describes a 'built-in' biometric subsystem as a subsystem that is primarily enclosed by the overall EPCS system. It therefore relies on the enclosing system to satisfy most or all of the DEA regulations for EPCS.
Claimant		Person claiming to have an identity for which the biometric subsystem will validate the claim.
Commercial Off-the-Shelf	COTS	Commercial Off-The-Shelf; an item that is both commercial and sold in substantial quantities in the commercial marketplace.
Confidence Interval	CI	Confidence intervals consist of a range of values (interval) that act as good estimates of the unknown population parameter. In the context of this report and ISO 19795, the confidence interval is purely statistical in estimation.
Conformance Test Suite	CTS	A test program utilized to provide data such as biometric data to the IUT and automatically obtain results (such as a similarity score) in response to a particular challenge.
Drug Enforcement Agency	DEA	The United States Department of Justice Drug

Term	Abbreviation	Definition
		Enforcement Agency. The Office of Diversion Control specifically handles the regulations discussed in this report.
Detection Error Trade-off	DET	A graphical plot of error rates for binary classification systems, plotting false reject rate vs. false accept rate.
Distortion		A measure of the inability of an image to reproduce parallel lines when parallel lines are presented at a target.
Electronic Medical Record	EMR	Overall system which is subject to DEA-EPCS regulations and which digitally signs and transmits electronic prescriptions
Electronic Prescription of Controlled Substances	EPCS	Program allowing physicians and their agents to electronically transmit prescriptions to a dispensary such as a pharmacy.
Enrollment		A biometric sample taken and stored as an enrollment
Factor		In authentication, one of the pieces of evidence that is used to support the identity claim of the claimant.
False Match Rate	FMR	Probability that the system incorrectly matches the input pattern to a non-matching template in the database
False Non-Match Rate	FNMR	Probability that the system fails to detect a match between the input pattern and a matching template in the database
Failure to Acquire	FTA	Failure to capture and/or extract usable information from a biometric sample.
Failure to Enroll	FTE	Failure to capture and/or extract usable information from a biometric sample.
Implementation under test	IUT	That which implements the standard(s) being tested
Imposter		An expected non-match mating of a probe (authentication) sample against an enrollment record.
Institutional Review Board	IRB	A committee that has been formally designated to approve, monitor, and review biomedical and behavioral research involving humans.
Independent Test Lab	ITL	Lab accredited by NIST to perform certification testing of biometric systems.
National Voluntary Laboratory Accreditation Program	NVLAP	Part of NIST that provides third-party accreditation to testing and calibration laboratories.
New England Independent Review Board	NEIRB	An independent institutional review board, ensuring the rights and welfare of research study participants.
Operating point		Biometric systems can utilize a variety of algorithms and techniques to reach a decision as to whether a challenge biometric matches a previously enrolled biometric. The sum of all of these configuration parameters including some similarity score cutoff corresponds to the operating point of the system.
PDF file	PDF	File format for all releases of the Report
Principal Investigator	PI	Person responsible for the oversight of their

Term	Abbreviation	Definition
		research and ultimately responsibility for the conduct of those to whom they delegate responsibility.
Personally Identifiable Information	PII	Any personal information about an individual, maintained by an agency, including, but not limited to an individual's name; social security number; date of birth; mother's maiden name; biometric records; education; financial transactions; medical history; criminal or employment history; and information which can be used to distinguish or trace an individual's identity.
Probe		A sample taken under authentication conditions.
Resolution		Used in the context of this report, refers only to the pixel width and height of a digitized image produced by a camera.
Software Development Kit	SDK	Set of software development tools which allows for the creation of application for a software package.
Spatial Frequency Response	SFR	Estimation of the spatial frequency response of an imaging device based on an image of a slanted edge and line-spread-function of that image
System under test	SUT	The computer system of hardware and software on which the implementation under test operates
Technology Testing		Refers to the acquisition of a corpus of biometric records that are used to enroll and challenge a biometric system to determine statistics such as false-match rate and false-non-match rate.
Vendor		Biometrics system manufacturer

3.2 DEA-EPCS Certification

Under 21 CFR 1300, 1304, 1306 and 1311, the DEA Office of Diversion Control specifies and regulates the operation of Electronic Prescription of Controlled Substances (EPCS). The regulations require 2-factor authentication of individuals to a system that prescribes or dispenses controlled substances. The regulations allow for any two of three factors to be used for authentication. One of those factors includes a biometric from the individual claiming an identity.

3.2.1 Definition of Test Criteria

The test criteria determined the configuration and test cases were performed. The System under Test (SUT) was the ZoOm SDK version 5.1.1 (certification candidate). For purposes of testing the SDK, the ZoOm 3D Face Login test application version 2.0 (which incorporates the ZoOm 3D Face Login SDK v5.1.1) was obtained through the intermediary TestFairy on 6 June 2017 via notification from TestFairy and FaceTec. An iOS and an Android version were released. These mobile device apps provided the enrollments and sample verifications used to test the SDK and it corresponding matching algorithm.

The security aspects of the biometric subsystem were assessed using 21 CFR 1311 requirements as guidelines along with the DEA Clarification dated 19-October-2011 to include "processing integrity" utilizing NIST SP800-53A as a guideline.

21 CFR 1311.116(b) and (h)(4) require that the biometric subsystem operate at a point with 95% confidence that the false match rate is 0.001 or lower. iBeta utilizes the test methods defined in ISO/IEC 19795-1 and ISO/IEC

19795-2 to acquire biometric data and use it to test the technology of the biometric subsystem to validate an operating point that meets the requirement.

The vendor supplied application acquired biometric samples which were stored on the mobile device file system.
- All samples consisted of a far and a near video through the front-facing camera of the device that was processed by the application and stored as a template.
- The template is based on the processing of at least 50 frames of video in near real-time.
- An enrollment sample (gallery) consisted of the acquisition of three (3) pairs of near and far samples as video.
- Two authentication samples (probes) each consisted of the acquisition of a typical pair of near and far samples as video.
- As described elsewhere each subject was assigned a six-digit Biometric Identification number (BID) by iBeta prior to interacting with the two test devices. Because FaceTec had proposed that the contract might be expanded to include more subjects to reach accuracy levels below 0.1% FMR iBeta also captured a photo of each subject associated with their BID. These photos were maintained separately from the biometric data.

Following each group of data acquisition days, the enrollment and authentication samples were copied from the test devices and placed into the iBeta biometric storage per PII security procedures.

Included with the FaceTec supplied data acquisition system was a matching algorithm that matched all enrollment samples against all authentication samples and produced a score. A lower score indicated a better match (i.e. similar to a distance measurement). Prior to placing the set of enrollments and authentications onto the test device, the filenames and timestamp of the files were obfuscated by iBeta so that the filename did not contain information about whether or not the samples should match.

As necessary to test the system, iBeta generated automated Conformance Test Software (CTS) to collect, de-obfuscate the results, and count the number of false match and false non-match errors at a given threshold. From this, iBeta produced the threshold required for the system to operate at better than a FAR (FMR) or 0.1% to meet the DEA requirement.

3.2.2 Test Environment Setup

A test dry run was conducted prior to full data collection. On 7 June 2017, ten iBeta employees provided PII and a prototype test of the data collection test case was conducted. The enrolment data and both verification samples were then used to conduct a match and cross-match test. The data analysis was conducted and the test case was adjusted as necessary.

The Technology Test was implemented using the FaceTec matcher: ZoOm 3D Face Login v2.0 (which implements the ZoOm 3D Face Login SDK v5.1.1) to produce the matching scores. The test environment for PII collection with the FaceTec application is provided below in Pictures 3-1 and 3-2.

Subjects' data collection was only associated with anonymous Biometric Identification (BID) 6 digit number. Each subject provided their self-declared ethnicity, their birthday month and year, and gender.

During this data collection, iBeta experienced a single Failure to Enrol (FTE) on a subject who could not capture at the closest position to the face. The testers attempted to also hold the phone as it was perceived that the subject could not steady her hand; however, one subject could not enroll on either the iPhone 7 Plus or the Samsung Galaxy S8 with and without tester assistance. The subject was a 57 year old, white female. iBeta used the maximum of 4 attempts as specified by NIST SP800-76-1 standards before declaring the FTE.
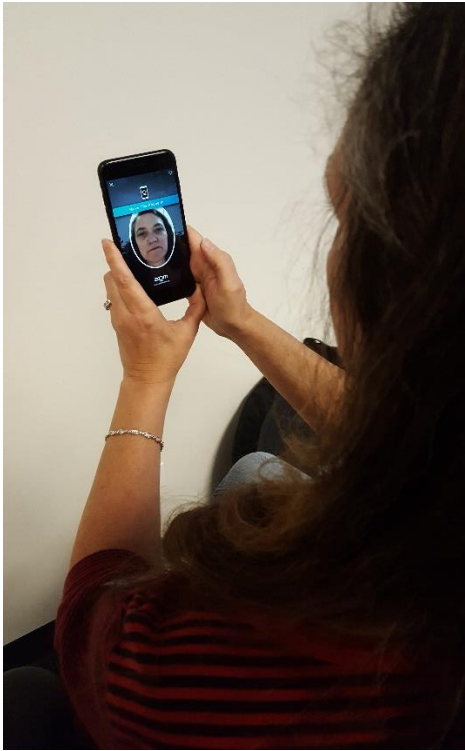
Picture 3-1: Biometric Acquisition example with the iPhone 7 Plus
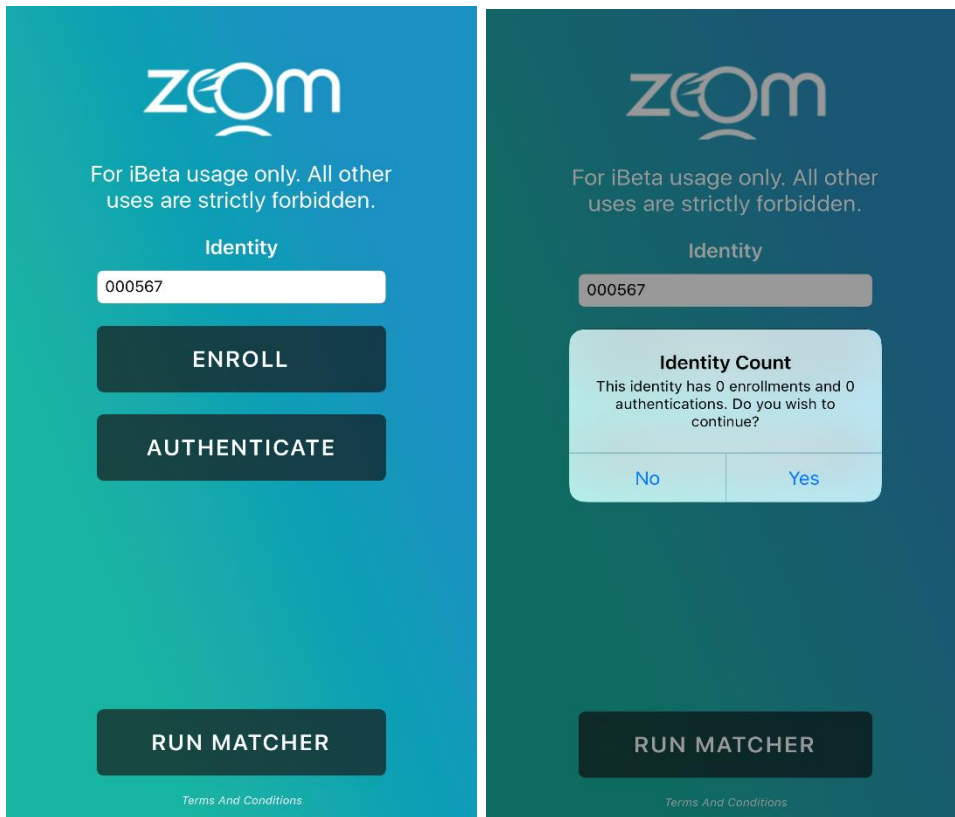
Picture 3-2: Biometric Acquisition with the ZoOm data collection SDK

For data collection, if a subject presented with eye glasses, they were instructed to either keep the eye glasses on for the entire data collection process or remove them. The tester noted on the test data sheet the subject BID number if wearing glasses for the data collection. The tester also noted any other facial constraints such as a beard or moustache. Subjects that presented with hats were asked to remove them for the data collection. No subjects presented with an eye patch, facial tattoos, or a bandage.

The iBeta created CTS utilized during the testing was named FaceTecA and was version v2.1.2. This version was validated on 8-Jun-2017 and during test execution through 13-Jun-2017. The as-run CTS and source code have been archived at iBeta SVN repository, dev\FaceTecA.

The technology test was implemented using a database of Z biometric data sets consisting of N biometric samples per individual. Of these Z sets, X were enrolled into the system using the first of the N in the set. The remainder were used as a challenge. (N-1)* Z sets of challenges were made for each of the X enrolled subjects for a total of X * (N-1) * Z challenges. Of these, (N-1)*X were expected to match and (N-1)*X*(Z-1) were expected to not match.

The biometric subsystem was configured to produce a similarity index for each attempted matching. The biometric system normally accepts a match only when the similarity index is lower than the operating point index. Therefore using the reported similarity index, iBeta calculated whether the challenge would be matched by the system at that operating point or not. Over a series of simulated operating points, and based on this calculation, each challenge was reported as a true accept (ta_i), true reject (tr_i), false accept (fa_i) or false reject (fr_i). If there were then M total challenges per operating point, a pair of numbers can be calculated. In each case, a challenge was considered to be a transaction with one of the results above reported. These results and calculations do not include the concept of allowing multiple attempts per transaction.

$$FMR = \frac{\sum_{i=1}^{M} fa_i}{M}$$

And

$$FNMR = \frac{\sum_{i=1}^{M} ta_i}{M} = \frac{\sum_{i=1}^{M} fr_i}{M}$$

A log-log plot of FNMR versus FMR is then provided and the FNMR for the operating point with a FMR at or below 0.001 is included in the results section.

Using methods and formulas documented in ISO/IEC 19795-1:2006, the variances of the above rates can be calculated.

The integer points of the Claim-Supported line of Figure B-1 of ISO/IEC 19795-1 Annex B were determined and are given in Table 3-2.

Table 3-2 Claimed Value for Measured Value integers from Figure B-1 of ISO 19795-1

Measured Value	Claimed Value
0	3
1	4.8
2	6.4
3	7.9
4	9.3
5	10.6
6	11.9
7	13.2
8	14.5

3.2.3 Readiness Review

Per the executed contract, iBeta initiated the DEA EPCS Certification test effort with a readiness review to determine and document the test plan prior to data collection. This readiness review also identified the hardware to be tested and the environmental conditions. For the iOS SDK from FaceTec, iBeta performed the following tasks that were delineated and documented in the FaceTec DEA EPCS Biometric Subsystem Pre-Certification Test Letter, Revision A, dated 24 May 2017:

- Kick-off meeting with FaceTec's ZoOm Biometrics (8/16/16)
- Creation of an initial assessment matrix (8/22/16)
- Pre-Certification restart with FaceTec (3/3/17)
- Obtained SDK and reviewed White Paper (5/22/17)
- Conducted the Pre-Certification Tasks (5/22/17)
  - ✓ Obtained an iPhone 7 Plus with iOS 10.3.1 and downloaded the SDK.
  - ✓ Assessed how the FMR test will be conducted. This was accomplished by collecting two subject's data with a 6 digit biometric identification number. Ran the matcher program (from the 'Generate CSV' button and exported the CSV file. Some of the data was obfuscated as we ran the test with the data collected from both deliveries of the SDK.
  - ✓ Assessed the capability of the proposed biometric subsystem to meet other DEA EPCS requirements including those in 1311.116.
  - ✓ Established the lighting for data collection as:
    - o Office Environment (450-750 lux)
- Issuance of the pre-certification letter (5/24/17).

iBeta then proceeded to the Certification phase of the project. Results are provided in Section 6.

3.2.4 Test Execution

Test execution was conducted beginning on 8 June 2017, with additional data collection performed from 8 June 2017 through 13 June 2017. Data analysis was performed through 15 June 2017. The detailed results are listed in Attachments 1, 2, and 3.

No issues were identified in the review.

No model, approximation or prediction of verification or identification performance was used. False-match rates provided in tables and shown as points in plots were obtained from actual data. Lines between points in plots are suggestions of linear or curvilinear relationship between the points and indicated for clarity in plot representation. Interpolation or extrapolation of the results outside of the points tested is outside of the scope of this report.

3.2.4.1 *Deviations and Exclusions*

Any deviations from or exclusions to the test method are documented, technically justified, authorized and accepted by the customer and are documented as such in Attachments 1, 2, and 3.

The ZoOm 3D Face Login application acquires facial video images but does not store facial images for use in tokens (badges) or for use in a facial database that is non-proprietary to FaceTec. The facial login works in part by utilizing the distortion caused by the lens at near and far focal distances. Thus the technique is not standard facial identification using a single flat image taken at a far focal distance. The video images acquired by the system are consistent with the minimal resolution requirements of SP800-76 even at the far distance.

There were no other deviations or omissions from the standards.

4 Biometrics System Identification

The System Identification stipulates the ZoOm 3D Face Login mobile device application submitted for certification and the hardware, software and the documentation used in testing.

4.1 *Submitted Biometrics System Identification*

Table 4-1 Biometrics System Name and Version

Biometric System Name	Version
ZoOm SDK (Certification Candidate)	5.1.1

Table 4-2 Biometrics System Components

Hardware	Firmware & Version	Description
Apple iPhone 7 Plus	iOS 10.3.2	F2MSG0PGHG04
Samsung Galaxy S8	Android 7.0	R38J30FTQDP

Table 4-3 Biometrics System Software and Documentation

Software Applications	Version	Function Description
ZoOm 3D Face Login data collection and matching application	2.0.0	Test app to acquire gallery and probes.
Matching software was same as above	2.0.0	Test app to produce scores of gallery x probes

The submitted FaceTec sampling application also produced scores of the match between two files. This score corresponds to a distance-like score in that a smaller value indicated a better match.

4.2 *Biometrics System Test Environment*

The Biometric Subsystem Test Environment identifies the specific hardware and software that was used in the test environment.

iBeta enrolled and verified all subjects using the each smartphone and associated application. Throughout the data collection, no application upgrades were introduced and no smartphone hardware failures occurred to prompt any change to the hardware.

Table 4-4 Biometrics System Test Hardware

Hardware	OS or Version	Manufacturer	Description (include functional purpose and condition of the equipment)
Gateway DX4860 Intel Core i5	Windows 7 Home Premium	Gateway/Acer	Generic PC
HP-Envy Intel Core i5	Windows 10 Home	Hewlett Packard	Generic PC

Table 4-5 Biometrics System Test Software

Software	Version	Manufacturer	Identify Hardware
TrueCrypt	7.1.a	TrueCrypt	All PC's and laptops
SDelete	1.61	Microsoft	All PC's and laptops
iTunes	12.5.1.21	Apple	All PC's and laptops
Andro Shredder	1.19	Apparillos.com	Android devices

Table 4-6 Other Software, Hardware and Materials

Material	Material Description	Use in the Biometrics System
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 and results
Repository servers	Separate servers for storage of	Supplied by iBeta: Documents are

Material	Material Description	Use in the Biometrics System
	test documents and source code, running industry standards operating systems, security and back up utilities	maintained on a secure network server. Source code is maintained on a separate data disk on a restricted server
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
Visual Studio 2013 v.12.0.2.1005.1 (Microsoft)	Build and source code Integrated Development Environment	Supplied by iBeta: View source code
Beyond Compare 3 v.3.2.4 (Scooter Software)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
WinDiff 5.1 (Microsoft)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
Md5deep v4.4	Open Source	Hashing of executable code
Extech Easy View 30 Light Meter	Ambient light meter	Ambient light measurements were taken prior to biometric data acquisition on a per day basis or when conditions change

The camera specifications are given in Table 4-7. The ZoOm 3D app acquired video at approximately the distances shown, which is the distance from the bridge of the nose to the surface of the mobile device.

Table 4-7 Front-Facing Camera Specification

Device	Mega-pixels	Image size (Width x Height)	f/#	Approx Distance (in)	Source
Apple iPhone 7 Plus	7.0	2320 x 3088	f/2.2	7, 13	apple.com
Samsung Galaxy S8	8.0	2448 x 3264	F/1.7	8, 12	samsung.com

4.2.1 Biometrics Test Environment – Data Acquisition

The test environment consisted of a data-acquisition mobile app provided by FaceTec. The app accepted a Biometric ID (BID) and executed an enrollment (gallery) when the user pressed the Enrollment button, and executed an authentication sample (probe) when the user pressed the Authenticate button. Enrollment templates consisted of three pairs of near and far video. Authentication templates consisted of a single pair of near and far video. An enrollment and an authentication sample resulted in a single file for each unit operation.

As described above, the enrollment and authentication samples were not stored as videos, but stored in a proprietary format. The samples were stored in the app sandbox on the iPhone 7 Plus where they could be acquired using iTunes. The samples were stored on the Samsung Galaxy S8 in the app sandbox where they could be acquired using a Windows browser.

Enrollment and authentication samples were stored using the nomenclature
XXXXXX_aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa_yyy
Where
XXXXXX is the iBeta assigned BID
aaaa is a random 32 digit lower case hex value
yyy is either enrollment or authentication
On the Android version of the app, the last '_' consisted of two characters '__'.

4.2.2 Biometrics Test Environment – Technology Test

The same mobile app that acquired the data also had a button marked 'Perform Matching,' which executed a full set of matches for all files in the appropriate folder. The app produced a matching score for each file matched against each other file and output the results into a csv file in the same folder as the data.

Prior to performing matching, iBeta offloaded all the files from the mobile device. iBeta obfuscated the XXXXXX and aaa values with randomly produced numbers or hex values so that the filename could not indicate whether the BID of one file should be expected to match the BID of another file. After obtaining the resulting csv file, iBeta replaced the vendor-produced filenames with the associated original filenames to determine what should or should not match.

Data from the mobile devices was collected and stored per IRB requirements in an encrypted drive, and subsequent calculations were performed on that drive when user PII were involved. After obtaining and de-obfuscating the results, an iBeta program customized for the FaceTec study performed the calculations to determine the FMR and FNMR at the default threshold.

5   Biometrics System Overview

The ZoOm 3D Face Login utilizes the front-facing camera of a mobile device to acquire facial enrollment and authentication video. The data-acquisition apps consisted of FaceTec generated apps to acquire enrollment and authentication samples associated with the attendant input BID.

The enrollment phase consisted of acquiring three pairs of videos producing a single enrolment template. An overlay to the displayed selfie image appeared with a frame of the expected size of the subject face. This frame corresponded to a small (far) facial video and a large (near) facial video. When the user had moved the camera to obtain the appropriate selfie video, the boundary of the oval template rotated with a green color and the sample was acquired.

Image or videos were not stored. The average template size for enrollment was 3.4 MB, and the average template for authentication was 1.0 MB.

iBeta only reviewed the functionality of this system as it relates to the DEA EPCS regulations as it pertained to those described in this report and specifically to the 1311.116 section.

Additional details of the biometrics system are contained in section 3.2.2 Test Environment Setup.

6   Certification Review and Test Results

The results and evaluations of the certification are identified below.   Detailed data regarding the Acceptance/Rejection criteria, reviews and tests for FMR are found in Attachments 1 and 2 (not released publicly).

6.1 *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 IUT/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 IUT/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.

During pre-engagement and pre-assessment analyses, iBeta determined that the subsystem is to be built into the local EPCS system. The interface to the device is an API, but the test system provided to iBeta used a vendor-supplied mobile device app to acquire data. Much of this configuration could vary in a final EPCS implementation. The interface to the file system of enrollment records also depends on physical and logical security of the overall system.

The scope of this iBeta report and certification is solely for the ZoOm biometric subsystem as listed in Section 4. The evaluation and testing certifies that the ZoOm 3D Face Login subsystem meets the DEA biometric regulations and can be incorporated into an EPCS application which can then be certified to meet the full DEA EPCS regulations.

6.2 *DEA Biometric Subsystem Review*

6.2.1 ZoOm 3D Face Login Component Results

More detailed results are reported in Attachments 1, 2 and 3 (not publicly available) to this report.

False Match Rate results are given in section 6.3.

6.2.1.1 *Exceptions*
There were no exceptions taken to the test method.

6.3 *False-Match Rate Review*

6.3.1 Population Demographics and Recorded Test Environment

As described in the Test Environment Setup Section 3.2.2 above, the False Match Rate (FMR) was calculated based on results from 4295 attempted matches of 100 enrolled subjects. Of those matches, 200 were expected to match and the remaining 4095 were expected non-matches. These values include an additional 100 second verification samples which were acquired from the subjects and were used to calculate the FNMR only for expected matches.

Each subject provided their self-declared ethnicity, their birthday month and year, and gender. Data was also collected as to whether the subjects was wearing contacts.   The iBeta Security Procedure was utilized to

maintain biographical data separately from biometric data and access to both was restricted to appropriate personnel. Collection of biographical data is used only to prevent the inclusion of duplicate crew members.

For data collection and subject recruitment, iBeta, per IRB, cannot target specific ethnic, age, or gender groups.

iBeta obtained the Age (Table 6-1), Gender (Table 6-2), and Self-Declared Ethnicity (Table 6-3) demographics as reported below.

Table 6-1 Age Demographics

Gender	Count	Percent
Male	63	63%
Female	37	37%
Undisclosed	0	0%

Table 6-2 Gender Demographics

Age (Years)	Count	Percent
<18	0	0%
18 – 35	40	40%
36 – 52	25	25%
53 - 70	35	35%
70>	0	0%

Table 6-3 Self-Declared Ethnicity

Ethnicity	Count	Percent
White	81	81%
Hispanic/Latino	10	10%
Asian	4	4%
African American	3	3%
American Indian	2	2%

In addition, all data collection was conducted in normal office (clinical and hospital) lighting environment and the illumination was recorded each day and verified to be within the Mil-Std 1472G office environment (per Table XXII stating the specific task illumination requirements for general office work to be illuminations at the preferred level of 755 lux with a minimum level of 450 lux). During data collection, all data was collected with the measured lux of between 450 and 620.

Testers noted when data collect subjects presented to the application with glasses, beard or moustache. For the 100 subjects, Table 6-3 below provides the metrics of these presented attributes.

Table 6-4 Facial Attributes

Subject Presented:	No other attribute	Moustache only	Beard and moustache	Total
Without glasses	55	1	11	77
With glasses	12	1	10	23

6.3.2 ZoOm 3D Face Login Component Results

FaceTec indicated that the threshold expected to meet the 0.1% FMR was a score of 4.0070 or less. As shown in Table 6-5, the system meets the DEA EPCS requirement for a FMR of 0.1% or less at the threshold of 4.0070 on both devices.

As described in section 3.2.2 above, the false match rate (FMR) and false non-match rate (FNMR) were calculated based on results from 4950 expected non-match values and 199 expected match values on the iPhone 7 Plus and 200 expected match values on the Samsung Galaxy S8. All subject data was utilized (subjects with glasses, beards, and moustaches). Using this methodology and for this study, the lower limit of detection of FMR is 0.00061.

Table 6-5 Thresholds for the ZoOm 3D

Device	threshold	FM	FMR 95% CI
iPhone 7 Plus	4.00575	0	0.00061
	4.0070	1	0.00097
Samsung Galaxy S8	4.0070	0	0.00061
	4.0073	1	0.00097
FM = the count of False Accepts (false match)			

6.3.2.1 *Exceptions*

There were no exceptions to the test method when calculating the FMR.

6.3.3 Camera Definition

Per 1311.116(d) the facial biometric subsystem must conform to SP-800-76 if they exist. SP-800-76 calls out the requirements of INCITS 385-2004, which are included in Table 6-6.

Table 6-6 Image requirements

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
7.2.1	Pose	The system appeared to correct for non-frontal poses by refusing to capture a template	☑
7.2.3	Expression	Facial images are not stored.	☑
7.2.4	Position	The system would not acquire a video if the face was not within the boundaries shown	☑
7.2.5	Shoulders	Shoulders did not appear within the boundaries of interest.	☑
7.2.6	Background	Facial images are not stored.	☑
7.2.7-7.2.10	Lighting, Shadows and Hot Spots	FaceTec documentation recommends even diffuse lighting.	☑
7.2.11	Glasses	Demographics of subjects wearing glasses were reported. Subjects were not instructed by iBeta personnel to remove glasses and were tested as they presented.	☑
7.2.12	Eye-patches	iBeta observed no subjects wearing eye patches. Facial images are not stored.	☑
A.2 – A.7	Photograph requirements	Facial images are not stored.	☑
A.8	Radial distortion The purpose of this requirement is to make consistent radial distortion due to focal length. For a typical photo capture system with a subject 1.5 to 2.5 meters from the camera, the focal length of the camera lens should be that of a medium telephoto lens. For 35 mm photography this means that the focal length should be between 90 mm and 130 mm. For other negative formats/sensors the recommended focal length is 2 to 3 times the diagonal of the negative/sensor.	The system relies on radial distortion and does not store facial images for other purposes of identification.	☑
	Compression	Facial images are not stored.	☑

6.3.3.1 *Exceptions*

As described in the table for Image Requirements, the ZoOm 3D biometric subsystem uses facial video but does not acquire those images, store them, or distribute them as identification images for any other purpose (such as a full-frontal-image, or token identifier).

6.4 *Other EPCS Biometric Subsystem Requirements*

Table 6-7 Testing of Biometric Subsystem Requirements

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
1311.116(a)	If one of the factors used to authenticate to the electronic prescription application is a biometric as described in § 1311.115, it must comply with the following requirements.	The purpose of this report is to allow that facial biometric as obtained and described herein meets the other subsystem requirements for use in a DEA EPCS system.	☑
1311.116(b)	The biometric subsystem must operate at a false match rate of 0.001 or lower.	As describe in section 6.3, the API and device are capable of meeting this requirement when the threshold is set to 4.0070 or lower.	☑
1311.116(b)	The biometric subsystem must operate at a false match rate of 0.001 or lower.	iBeta did not test a subsystem utilizing the vendor provided threshold of 4.0070 or lower for a match. The enclosing system must validate this requirement.	☐
1311.116(c)	The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate. Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (h) of this section.	The purpose of this report is to validate the threshold required to produce a FMR or 0.001 or lower. iBeta is a DEA-approved nongovernment laboratory.	☑
1311.116(d)	The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800–76–1 as incorporated by reference in § 1311.08, if they exist for the biometric modality of choice.	As described above in Table 6-4 Image Requirements	☑
1311.116(e)	The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.	The tested biometric subsystem was tested as built-in, which means that it relies on the enclosing system to provide some or all of the security.	☐
1311.116(f)	The biometric subsystem must store device ID data at enrollment (i.e., biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.	Although the system is capable of meeting this requirement because it encrypts the enrolled template using a local key, iBeta did not specifically test this requirement for the enclosing system.	☐

Requirement Reference	Requirement	Details of level of iBeta Assessment	✔
1311.116(g)	The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be: (1) Cryptographically source authenticated; (2) Combined with a random challenge, a nonce, or a time stamp to prevent replay; (3) Cryptographically protected for integrity and confidentiality; and (4) Sent only to authorized systems.	Presumably, matching would be local to the device, and the device would meet these requirements when communicating the authentication result to the overall system.	☐
1311.116(h)	Testing of the biometric subsystem must have the following characteristics: (1) The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric. (2) Test data are sequestered. (3) Algorithms are provided to the testing laboratory (as opposed to scores or other information). (4) The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value. (5) Results of the testing are made publicly available.	iBeta's process and procedures to test the FMR at 95% confidence have been approved by the DEA. This report will be available on the iBeta website for 2 years after publication.	☑

6.4.1.1 *Exceptions*

The 21 CFR 1311.116(b), and (e) through (g) requirements were not tested as iBeta only had the matching algorithm and no means to connect that algorithm to a system that might operate like an EPCS approvable system.

7 Opinions & Recommendations

7.1 *Recommendations*

iBeta Quality Assurance has completed the testing of the ZoOm 3D Face Login biometric subsystem. In our opinion the acceptance requirements of 21 CFR Parts 1311.116 have been met as delineated in Table 6-5 and its Notes.

iBeta Quality Assurance certifies the ZoOm 3D Face Login application to the requirements of 21 CFR Parts 1311.116(b) and 1311.116(h)(4). Other requirements assessed are also included in Table 6-5 above.

The Table 7-1 summarizes the 21 CFR 1311 requirements that were found to be in compliance with the regulation. Requirements checked (☑) were found to be in compliance. Requirements not checked (☐) were not

within the scope of iBeta's certification and must be tested by the entity certifying or auditing the overall EPCS system as described in the Notes. However, in all cases, iBeta believes this system can be incorporated into an EPCS certified system to meet all requirements for that system.

Table 7-1 Requirements in Compliance

Requirement	Description	Approved
1311.116(a)	If one of the factors used to authenticate to the electronic prescription application is a biometric as described in §1311.115, it must comply with the following requirements.	☐
1311.116(b)	Biometric subsystem to operate at a false match rate of 0.001 or lower	☑
1311.116(c)	The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate. Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (h) of this section.	☑
1311.116(d)	The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800–76–1 as incorporated by reference in §1311.08, if they exist for the biometric modality of choice.	☑
1311.116(e)	The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.	☐
1311.116(f)	The biometric subsystem must store device ID data at enrollment (i.e. biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.	☐
1311.116(g)(1) 1311.116(g)(2) 1311.116(g)(3) 1311.116(g)(4)	The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be: Cryptographically source authenticated, combined with a random challenge, a nonce, or a time stamp to prevent replay, cryptographically protected for integrity and confidentiality; and sent only to authorized systems.	☐
1311.116(h)(1)	The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.	☑
1311.116(h)(2)	Test data are sequestered.	☑
1311.116(h)(3)	Algorithms are provided to the testing laboratory (as opposed to scores or other information).	☑
1311.116(h)(4)	The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value.	☑

All other 21 CFR 1311 requirements that may be applicable to an installed biometrics subsystem were outside of the scope of testing of this subsystem in the absence of its containing system. All other requirements must be tested for the overall enclosing system.

Notes on the 1311.116 requirements:
- 1311.116(a) is a rollup requirement mandating the other requirements for biometrics subsystem
- 1311.116(e): The tested biometric subsystem has the capability to meet this requirement but it must be tested for the overall system. See Table 6-7 for details.
- 1311.116(f): The tested biometric subsystem has the capability to meet this requirement, but it must be implemented and tested for the overall system. See Table 6-7 for details.
- 1311.116(g): The tested biometric subsystem has the capability to meet this requirement especially when operated locally. See Table 6-7 for details.

7.1.1 Limitations

As described in Section 6.1 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 regulations. Device or system behavior which falls outside of the scope of this testing is not certified. iBeta cannot extrapolate the results of the testing to include devices other than those listed in Table 4-2.

Because the biometric subsystem does not sign or receive electronic prescriptions, it was found to not be subject to other requirements of the 1311 such as auditing and records maintenance. These are the responsibility of the overall system since the biometric subsystem only returns a pass/fail response to one of the two factors used for authentication prior to signing a prescription.
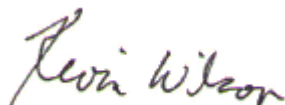
7.1.2 Exceptions

There were no exceptions other than those listed in Section 6.3.1.

7.2 *Opinions*

The vendor supplied documentation was acceptable for iBeta to collect and analyze the biometric authentication methods provided by FaceTec.

7.3 *Responsible Test Laboratory Personnel*

The responsible test laboratory person and the contact information for the New England IRB appointed Principal Investigator for this test effort:

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