



**PalmSecure® F-Pro
PalmSecure® SDK V02
DEA EPCS Biometric Subsystem
Certification Test Report**

Prepared for:
Fujitsu Frontech North America Inc.
27121 Towne Centre Drive, Suite 100
Foothill Ranch, CA 92610

Version 1.0
16 April 2018
Report #180416-iBetaBTR-v1.0

Trace to Standards
21 CFR Part 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:
April – 16 – 2018**

*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:
April – 16 – 2020**

*Copyright © iBeta Quality Assurance, all right reserved.
No portion of this report may be reproduced without written permission from iBeta*

*PalmSecure® is a registered brand mark of Fujitsu Frontech North American for use in North America.
Elsewhere in the world, PalmSecure™ may be trademarked awaiting registration.*

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

Version History

Ver #	Description of Change	Author	Approved by	Date
V1.0	Certification Report	Gail Audette	Dr. Kevin Wilson	16 April 2018

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	4
1.1	BIOMETRIC SUBSYSTEM IDENTIFICATION	4
1.2	DISCLOSURE.....	4
2	INTRODUCTION	5
2.1	INTERNAL DOCUMENTATION.....	5
	Table 2-1 Internal Document	5
2.2	EXTERNAL DOCUMENTATION.....	6
	Table 2-2 External Documents	6
2.3	TECHNICAL DOCUMENTS	6
2.4	TEST REPORT CONTENTS.....	7
3	CERTIFICATION TEST BACKGROUND	8
3.1	TERMS AND DEFINITIONS	8
	Table 3-1 Terms and Definitions.....	8
3.2	DEA-EPCS CERTIFICATION	10
3.2.1	<i>Definition of Test Criteria</i>	10
3.2.2	<i>Test Environment Setup</i>	10
	Picture 3-1: PalmSecure Application	11
	Picture 3-2: Biometric Acquisition with the PalmSecure Application and Device	11
	Table 3-2 Claimed versus Measured Error Rates.....	12
3.2.3	<i>Test Execution</i>	13
4	BIOMETRICS SYSTEM IDENTIFICATION	13
4.1	SUBMITTED BIOMETRICS SYSTEM IDENTIFICATION	13
	Table 4-1 Biometrics System Name and Version	14
	Table 4-2 Biometric System Software -- Hash of the delivered files.....	14
4.2	BIOMETRICS SYSTEM TEST ENVIRONMENT	14
	Table 4-3 Biometrics System Test Hardware	14
	Table 4-4 Biometrics System Test Software.....	15
	Table 4-5 Biometrics System Technical Documents	15
	Table 4-6 Other Software, Hardware and Materials	15
4.2.1	<i>Biometrics Test Environment – Technology Test</i>	16
5	BIOMETRICS SYSTEM OVERVIEW	17
6	CERTIFICATION REVIEW AND TEST RESULTS	18
6.1	LIMITATIONS.....	18
6.2	DEA BIOMETRIC SUBSYSTEM REVIEW	18
6.2.1	<i>PalmSecure Component Results</i>	18
6.3	FALSE MATCH RATE REVIEW	18
	Table 6-1 Age Demographics	19
	Table 6-2 Gender Demographics	19
	Table 6-3 Ethnicity Demographics.....	19
	Table 6-3 Numbers of Genuine and Imposter Matches	19
	Table 6-4 FMR at Thresholds	19
6.3.1	<i>Exceptions</i>	19
6.4	OTHER EPCS BIOMETRIC SUBSYSTEM REQUIREMENTS.....	19
	Table 6-5 Testing of Biometric Subsystem Requirements	19
7	OPINIONS AND RECOMMENDATIONS	22
7.1	RECOMMENDATIONS.....	22
	Table 7-1 Requirement in Compliance	22
7.1.1	<i>Limitations</i>	23
7.1.2	<i>Exceptions</i>	23
7.2	OPINIONS.....	23
7.3	RESPONSIBLE TEST LABORATORY PERSONNEL	24

1 Executive Summary

This report contains the results and conclusions of the iBeta Quality Assurance assessment that resulted in the certification of the biometric subsystem consisting of PalmSecure® F-Pro and PalmSecure® SDK V02 from Fujitsu Frontech North America Inc. The biometric subsystem was validated and certified against the applicable requirements of 21 CFR Part 1311.116 for its inclusion as a built-in subsystem in an Electronic Prescription of Controlled Substance (EPCS) Application.

The PalmSecure biometric subsystem is a palm vein recognition system. iBeta tested and certified the built-in matching algorithm.

The PalmSecure biometric subsystem was validated to operate at a 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 found that the NORMAL setting met the requirement.

The Fujitsu PalmSecure 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.

This report is publicly available and Attachment 1 is available upon request from Fujitsu Frontech North America. This report will be maintained on the iBeta website during the period of certification from the issuance of this report (16 April 2018) through the certification expiration date (16 April 2020).

1.1 *Biometric Subsystem Identification*

The PalmSecure acquisition and matching components are described in Section 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric Subsystem Test Environment. Two application programming interfaces and sample code in C-Sharp were provided by Fujitsu – a data collection program for Windows OS and a matching algorithm tested on a Windows OS.

1.2 *Disclosure*

This report consists of the publicly available assessment and test results made between the independent test organization, iBeta Quality Assurance LLC and the vendor. This report is made public in accordance with DEA requirements and is located at www.ibeta.com.

Additional results are proprietary and not made public but disclosed to the vendor:

- Attachment 1: Detailed Technology Assessment Results

Information and data not disclosed outside of the testing lab include:

- 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 iBeta Quality Assurance's assessment and testing of a biometric subsystem for the purpose of that subsystems' inclusion in an Electronic Prescription of Controlled Substances (EPCS) system. This report addresses the testing of the Fujitsu PalmSecure applications to the 21 CFR 1311.116 regulations. The results were for a representative F-Pro with U-Guide connected to a Windows OS application. The Enterprise Edition API matching algorithm (which is thread-safe) was used to perform matching.

A modified sample-code PalmSecure application using the Profession Edition API was used to acquire the dataset used to evaluate the FMR results. The purpose of this document is to provide an overview of the certification testing and findings. The complete list of the systems 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 the Section 5 - Biometric System Overview.

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

Certification testing was performed in compliance with the requirements of 21 CFR 1311.116. All test executions and reviews included the record of requirements that were satisfactorily and unsatisfactorily completed. No deficiencies were noted during the test effort.

The New England Independent Review Board (NEIRB) reviewed the iBeta DEA-EPCS Biometric Test Protocol application and granted unconditional approval on 15 September 2016 (approval: #120160885) for the following:

- Test Protocol Version 1.0 dated 19 August 2016
- Biometrics Security Procedures (Version 3.0) dated 20 May 2013
- DEA-EPCS Biometric Subsystem Assessment Procedure (Version 4.0) dated 21 May 2013
- Biometrics Testing Disclaimer (Version 1.0)
- Brochure - 'Biometrics Testing Lab'
- Informed Consent Form (NEIRB Version 1.0)

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

The requirement of 21 CFR 1311.116(b) is that the biometric subsystem operate at a False Match Rate (FMR) of 0.001 or lower. Technology testing 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.

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 Document

Version #	Title	Abbreviation	Date	Author (Org.)
03	Agreement for PalmSecure® F-Pro U-Guide DEA EPCS Certification and Scenario Testing Services	Contract	1/8/2018	iBeta Quality Assurance
iBeta Procedures				
2.0	Biometric Deliverable Receipt Procedure		4/12/17	iBeta Quality Assurance

Version #	Title	Abbreviation	Date	Author (Org.)
4.0	Biometric Security Procedure		8/16/13	iBeta Quality Assurance
1.0	Biometrics Configuration Management Procedure		6/9/11	iBeta Quality Assurance
1.0	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				
2.0	DEA-EPCS-Biometric-Assessment-Fujitsu		2/21/18	iBeta Quality Assurance
1.0	DEA-EPCS-Test-Cases-Fujitsu		3/16/18	iBeta Quality Assurance

2.2 External Documentation

The documents identified below are external resources used to 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
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

2.3 Technical Documents

The Technical Documents submitted by Fujitsu 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 certification testing.
- Section 2: The Introduction identifies the scope of certification testing.
- Section 3: The Certification Test Background identifies the process for certification 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 Attachment 1: 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 PalmSecure Biometric Subsystem included Security Assessment and Operating Point to provide 0.001 false match rate or better. Weekly status reports were sent to Fujitsu. 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 print, 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 of 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 Software	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 Enforcement Agency. The Office of Diversion

Term	Abbreviation	Definition
		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.
Enrollee		Person enrolling in the EMR
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 create a proper template from an input for a number of specified attempts (governed by NIST SP800-76-1)
Implementation under test	IUT	That which implements the standard(s) being tested
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.
Logically Shred		To overwrite data in memory or disk locations enough times to mitigate the probability that the information can be retrieved by unauthorized persons
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.
Principal Investigator	PI	Person responsible for the oversight of their 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

Term	Abbreviation	Definition
		information which can be used to distinguish or trace an individual's identity
PDF file	PDF	File format for all releases of the Report
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		Biometric subsystem manufacturer

3.2 DEA-EPCS Certification

3.2.1 Definition of Test Criteria

The test criteria determined the configuration and test cases for execution. The Fujitsu PalmSecure biometric application configurations were established in collaboration with the vendor.

The test requirements are established in the DEA Final Interim Rule specifically in 21 CFR 1311.116(b) and (h)(4) that require that the biometric subsystem operate at a point with 95% confidence that the false match rate is 0.001 or lower. iBeta utilized the test methods defined in ISO/IEC 19795-1 and ISO/IEC 19795-2 to acquire biometric data and used it to test the technology of the biometric subsystem to validate an operating point that met this requirement.

As necessary to test the system, iBeta modified the PalmSecureSample_cs demo Windows application to collect data. Fujitsu provided an attestation declaring that the PalmSecure authentication algorithm used in the Professional Edition (for client device usage) and Enterprise Edition (for server usage) are identical regardless of the supported operating systems. The supported operating systems identified by Fujitsu are Windows 7 SP1 (x86 and x64), Windows 8.1 Update (x86 and x64), Windows 10 Version 1703 (x86 and x64), and Linux (x64) (kernel 2.6.32 or later). The attestation is provided in Attachment 1 (not publicly available).

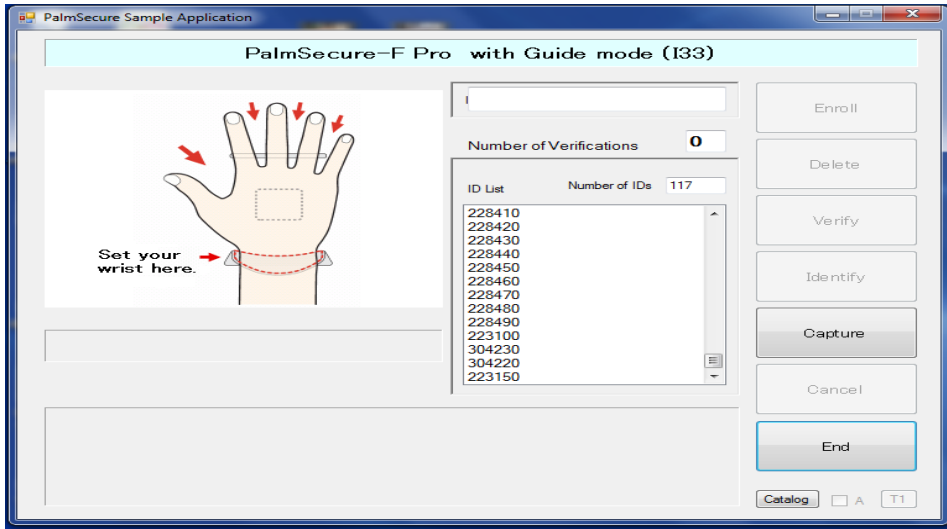
iBeta utilized a matching engine produced by Fujitsu that iBeta provided input files through modified version of the Fujitsu server version of the application. The matching was conducted on a 64-bit Windows environment. The matching engine produced pass/fail results. Because the results were provided in only the pass/fail format, iBeta ran the matching/cross-matching 5 times – once at each of the sensitivity settings.

3.2.2 Test Environment Setup

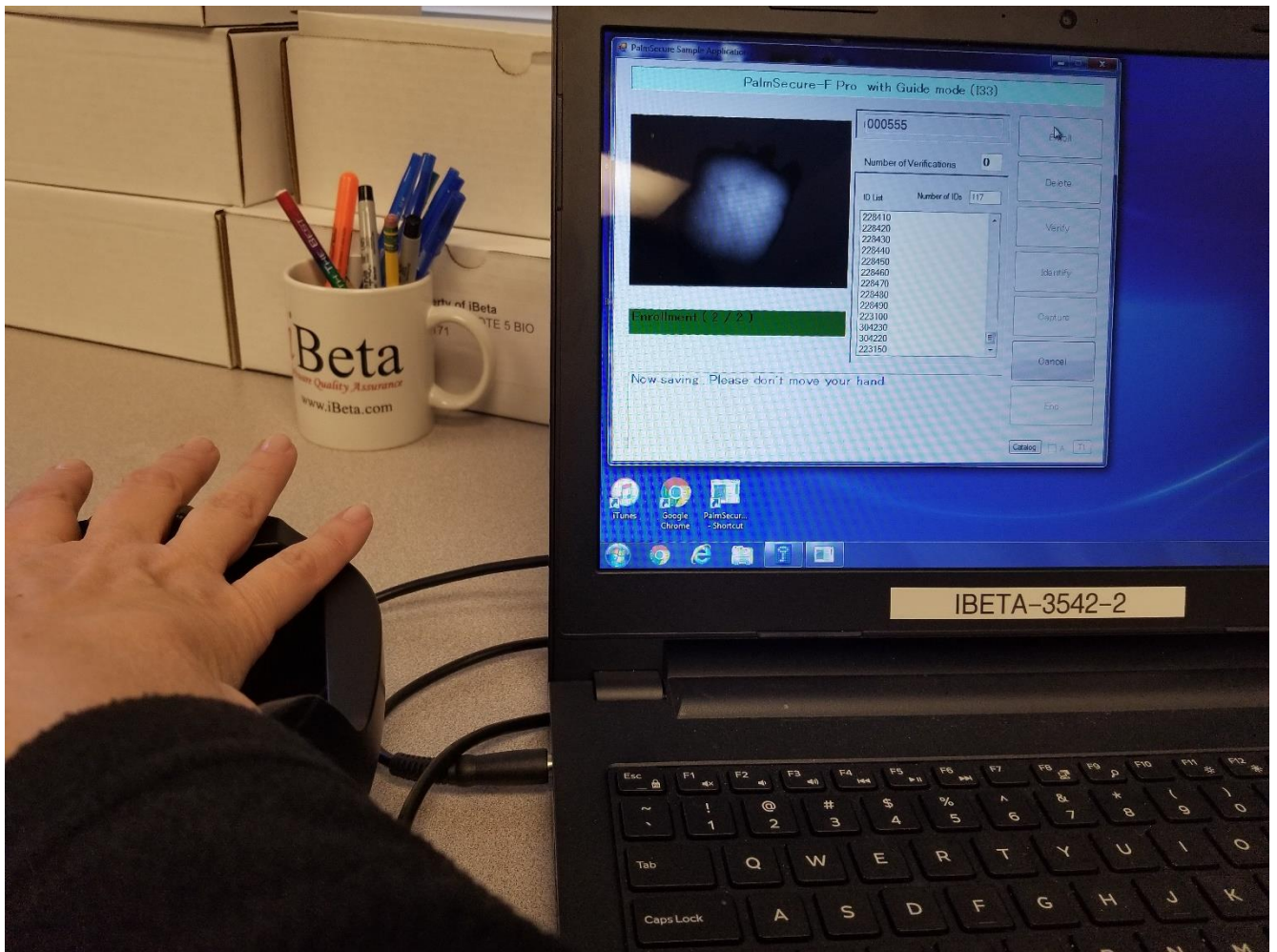
For this test effort, iBeta located all equipment in the Biometrics Lab of the iBeta facility.

A test dry run was conducted prior to full data collection. On 12 February 2018, five iBeta employees provided PII and a prototype test of the data collection test case was conducted. The enrolment data and first verification sample 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 a single sensor and guide to collect data as provided below in Pictures 3-1 and 3-2.



Picture 3-1: PalmSecure Application



Picture 3-2: Biometric Acquisition with the PalmSecure Application and Device

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 no Failure to Enrol (FTE); however, the system failed to store an enrollment sample. That subject did acquire verification samples successfully therefore there were 100 sets of verifications but only 99 enrollments.

No Failure to Acquires (FTAs) were noted.

An encrypted database was created using TrueCrypt as listed in Table 4-7. The database of 100 biometric data samples (consisting of 8 biometric data records per each of 100 individuals) was used in the technology testing.

The PalmSecure matcher produced a score and/or pass/fail result for each attempted match. At a given sensitivity settings, each challenge was reported as a true match (tm_i), true non-match (tn_i), false match (fm_i) or false non-match (fn_i). If there were then M challenges that were expected to not match, 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.

$$FMR = \frac{\sum_{i=1}^N fm_i}{N} \quad (3.2.3 - 1)$$

Equation 3.2.3-1 is the calculated (or observed) FMR; however, the DEA EPCS regulations require a statistical 95% Confidence Interval for the operating point of the system. Table 3-2 shows the values taken from Figure B.1 of INCITS/ISO/IEC 19795-1:2006[2007], which plots O/N = the Observed Error Rate and C/N = the Claimed Error Rate where N is the number of comparisons made. Here, O is the observed number of errors for the given N and C is the virtual number of errors that fall within the 95% confidence interval of the hypothesis that the FMR is 0.001 or better. While Figure B.1 of ISO 19795-1 has observed error rates as high as 30/N, iBeta chose to use smaller values of N to lower the cost of testing (for any given claimed error rate).

To obtain the matches, iBeta challenged all enrollment (reference) records against all verify (probe) records. The matching of I x J was repeated for the case of J x I where the first record is the enrollment (reference) and the second record is the verification (probe) record. Thus there are approximately N = n*(n-1) expected non matches and 7*n expected matches if every reference has a corresponding probe associated with it. One FTA of the second sample taken resulted in only 695 expected matches.

Table 3-2 Claimed versus Measured Error Rates

N x Observed Error Rate	N x Claimed Error Rate	Minimum N for an Error Rate of 0.001
0	3.0	3000
1	4.8	4800
2	6.4	6400
3	7.9	7900
4	9.3	9300
5	10.6	10600
6	11.9	11900

Using methods and formulas documented in ISO/IEC 19795-1:2006, the variances of the above rates were calculated using Table 3-2.

As described above, the subjects were enrolled using the Fujitsu provided PalmSecure SDK V02L02 application to enroll and then acquire 11 samples per subject (2 enrollments, then two enrollment verifications and finally 7 as verification samples were captured). The matcher used during the enrollment

process to verify the quality of the enrollment templates was the Professional Edition (PE) matcher which is the same algorithm in the Enterprise Edition (EE) matcher but run locally on the enrolment platform.

Because the matcher was operating as a black box to iBeta, once all of the enrolment and verification samples were extracted, the BIDs of all the verification samples were scrambled using a random-number generator. After the Fujitsu EE matcher performed the matching, the dictionary of scrambled BID to actual BID was reversed so that iBeta could determine the FMR and FNMR from the expected match and mismatch by BID.

The Fujitsu matcher provided a matrix of pass/fail results of all samples against all samples. For most runs, only the first verification sample was used. A separate additional run was performed for the diagonal (expected match scores) only of the enrollment vs. all probe or verification samples.

3.2.3 Test Execution

Test enrollment or data collection was conducted 23 February through 7 March 2018. Test execution was conducted on 15 March 2018 and the detailed results are listed in Attachment 1. iBeta executed the matching/cross-matching five times to acquire the results for the sensitivity settings of lowest, low, normal, high and highest.

Following the DEA Regulations 21 CFR Part 1311, subjects were enrolled and included iBeta employees and non-employees as per the iBeta DEA-EPCS Biometric Test Protocol approved by the New England Independent Review Board.

Subject biographical data was acquired on paper. Only an identifier, the Biometric ID (BID), connected the subject biographical data to the acquired biometric data.

The scrambling of the BIDS was performed on the same PC used to analyze the data. The matching was performed on a separate computer with higher computing power. A USB flash drive was used to transfer the resulting files containing the set of match scores and the dictionary of scrambled BIDs to actual BIDS. The descrambling, FMR, and FNMR calculations were performed with that data on another desktop computer.

As per the iBeta security procedures and after completion of all testing, subject Personally Identifiable Information (PII) biographical data was logically overwritten as per a NIST SP800-88 approved method by using the Microsoft Sysinternals SDelete utility.

There were no issues that were identified in the review; therefore, there is no attached Discrepancy Report.

3.2.3.1 Deviations and Exclusions

In accordance with iBeta Standard Operating Procedures, any deviations from or exclusions to the test method are documented, technically justified, authorized and accepted by the customer.

There were no deviations or omissions from the standards.

4 Biometrics System Identification

The PalmSecure applications as specified in Table 4-1 and 4-2 were tested for this certification.

4.1 Submitted Biometrics System Identification

Table 4-1 contains the elements of the PalmSecure applications.

Table 4-2 and 4-4 lists the laptop system definition that was used for this test effort that meets the minimum requirements as listed above. No other hardware test environment was utilized.

Table 4-1 Biometrics System Name and Version

Biometric System Name	Version
PalmSecure SDK	V02
Professional Edition Authentication Libraries	V33L60-B36
Enterprise Edition Authentication Libraries	V33L61-B36

The Biometrics System as delivered and certified is documented in Table 4-2. The PalmSecure SDK was used to enroll and capture verification images. The Professional Edition matcher was used during the data collection to verify the enrollment and the Enterprise Edition matcher was used for the match/cross-match to determine FMR.

Table 4-2 Biometric System Software -- Hash of the delivered files

System and Name	Version	size (bytes)	SHA-256 hash
EE Authentication Libraries	V33L61-B36		
F3BC4BIOSV.DLL		120	5993acc033ae6ea099df4c3e281bcd9627ca4891fc2d5bdec86c06cde7c4bb64
F3BC4BSPSV.DLL		685200	fa2dd6fbaf86bb2899363bb2d0fb3e3a983a4a60fd834eadde144b7379dc0ef5
F3BC4COMSV.DLL		260760	34ec069602cd4fcd06ec68d673957a8abcd3f6f2d087964a4abddb780710e43
F3BC4DNISV.DLL		150528	44cfb6d4306c8bfb3ed4e155a67315af874a835bfdfbba8ebee25c4cc088684f
F3BC4MATSV.DLL		1049232	4a7d8318a72d4fb634edcac12f5d38ab04b83572c28ab8e6d1332499b59d866f
PalmSecure SDK (includes the PE Authentication Libraries)	V02 (V33L60-B36)		
F3BC4BIO.DLL		250960	a46a85ed10c1de064a14cff846d1e1e813b3423b48ffdb9ae7f8ed4032333fad
F3BC4DNI.DLL		150528	7935eeea65e389265ff05c030315a940c07b8b54515a4764ca9bada14802560d
F3BC4COM.DLL		261200	3a3fe2b1d2c2b01b69f4d67ecfdde0c944cb13a07eb5353f7f994521a60268a4
F3BC4BSP.DLL		68500	a9d05db9aa06880c5ca76e7504f3e48ecf4be7b3d499049d65b01b3df7c62600
F3BC4MAT.DLL		1049680	f66b2fc030f1ebde1bf9989ed35ebef5f31e92686e04539b7619c84dc66a8618
F3BC4CAP.DLL		1815120	f66c2f79317f4fa1afefdd82e5de85ef7d7cfd052db862da5e2daaebf3f806e4

4.2 Biometrics System Test Environment

The Biometric Subsystem Test Environment identifies the specific hardware and software that was used in the test environment in Tables 4-3 and 4-4, respectively.

iBeta enrolled all subjects using the a single F-Pro sensor embedded in the U-Guide. The technology portion of the test was performed on a desktop PC.

Table 4-3 Biometrics System Test Hardware

Hardware	OS or Version	Manufacturer	Description
PalmSecure U-Guide	PN: FAT13FGA02	Fujitsu	Holds the sensor and positions the palm used for data collection
PalmSecure F-Pro Sensor	P/NA: FAT13FPS01 P/NO: KD4215-B001 06E KA00016739	Fujitsu	Biometric sensor used for data collection
PalmSecure U-Guide	PN: FAT13FGA02	Fujitsu	Spare - holds the sensor and positions the palm
PalmSecure F-Pro Sensor	P/NA: FAT14PR4WA P/NO: KD03986-A111 06E KA00016763	Fujitsu	Spare – biometric sensor
HP Envy 700-214	Windows 10 Pro 64 bit	Hewlett-Packard Company	Used to calculate FMR and FNMR

Hardware	OS or Version	Manufacturer	Description
Intel® Core™ i5-4440 CPU @ 3.10 GHz			
Inspiron 3542 Intel® Pentium® 3558U @1.70 GHz 64-bit OS	Windows 7 Home Premium Service Pack 1	Dell	Laptop for data collection

Table 4-4 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

For the test effort, Fujitsu provided documentation on system setup and use.

Table 4-5 Biometrics System Technical Documents

Version #	Title	Date	Author (Org.)
U1PS-LA12-04ENZ3	PalmSecure™ SDK V02 Manual Structure	Rev 4. April 2017	Fujitsu
U8PS-LG22-06ENZ3	PalmSecure™ SDK V02 How to Acquire the License File	Rev. 6 April 2017	Fujitsu
U2PS-LA22-05ENZ3	PalmSecure™ SDK V02 System Development Guide	Rev. 5 April 2017	Fujitsu
U4PS-LC32-03ENZ3	PalmSecure™ SDK V02 Authentication Library Reference Guide for I33-format Type (V33)	Rev. 3 April 2017	Fujitsu
U3PS-LB22-01ENZ3(1)	PalmSecure™ SDK V02 Authentication Accuracy Data Sheet	Rev. 1.1 April 2017	Fujitsu
U9PS-LH92-01ENZ3	PalmSecure™ SDK V02 How to Place the Hand (Standard with the Guide)	First Edition April 2017	Fujitsu
KD96017-0953	PalmSecure-F U-Guide Assembly Instructions	2017	Fujitsu
KD96016-0542	Check List for Palm Guide Design	Rev.2 Nov 2016	Fujitsu
U4PS-LC72-05ENZ3	PalmSecure™ SDK V02 Sample Interface Library for Microsoft .NET Framework Manual	Rev. 5 April 2017	Fujitsu
U4PS-LC84-04ENZ3	PalmSecure™ SDK V02 Sample Application for Microsoft .NET Framework Manual Professional Edition	Rev. 4 April 2017	Fujitsu
U4PS-LC42-03ENZ3	PalmSecure™ SDK V02 Sensor Driver Installation Guide	Rev. 3 April 2017	Fujitsu
U5PS-LD12-03ENZ3	PalmSecure™ SDK V02 Sensor Maintenance Tool Operation Guide	Rev. 4 April 2017	Fujitsu

Throughout the test effort, iBeta utilized other software, hardware and materials as warranted to support the testing, analysis and reporting.

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 test documents and source code, running industry standards operating systems, security and back up utilities	Supplied by iBeta: Documents are maintained on a secure network server. Source code is maintained on a separate data disk on a restricted server
Microsoft Office 2010	Excel and Word software and document templates	Supplied by iBeta: The software used to create and record test plans, test cases, reviews and results

Material	Material Description	Use in the Biometrics System
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
Beyond Compare 4 v.4.1.9 (Scooter Software)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
Md5deep v4.4	Open Source	Hashing of executable code
Certified ruler		Used to measure grid spacing for camera accuracy

4.2.1 Biometrics Test Environment – Technology Test

The devices listed in Table 4-4 indicate their functional purpose in the test effort. A single device was used to capture all of the data for the testing. On this device, each subject completed enrolment by capturing two enrollment images and then verified those enrollment images with two verifications. The subject then captured seven (7) verification images. The verification images were obfuscated and used as probes.

4.2.1.1 Processing and Post-processing

An iBeta program (Fujitsu.exe) which had scrambled the image data, was used to unscramble the results output and pull out only the first probe score for each enrollment-probe match and present them in linear format so the results could be imported into Excel for further processing.

5 Biometrics System Overview

The PalmSecure consisted of a data collection application that drove the sensor for image capture and the PalmSecure matching software.

Additional functionality of the biometric subsystem was reviewed to verify additional requirements of the DEA EPCS regulations in addition to the FMR (1311.116(b)) requirement. However, for all practical purposes, the only other requirements iBeta was able to test was that the SDK could produce an ID for the PalmSecure and could produce enrollment and/or verification images.

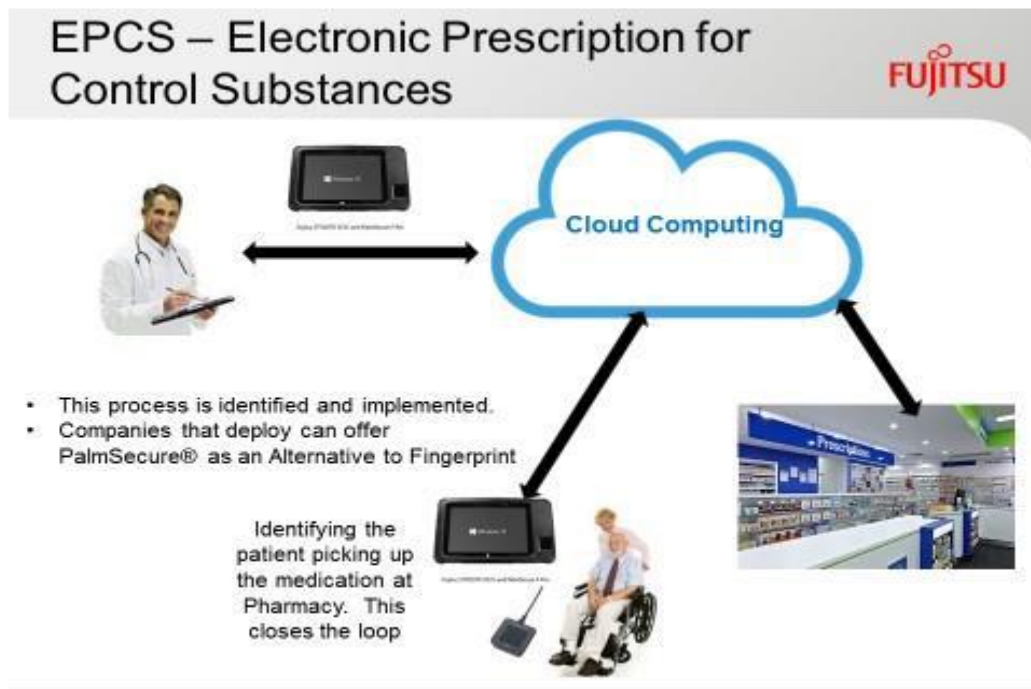
As tested, the enrollment and verification subsystem accessed the records through the filesystem. iBeta was not able to review any other functionality associated with a specific implementation of the biometric subsystem as it might interface to an EPCS certifiable system.

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.

As tested, the images were stored in the file system as bmp formatted images with templates as binary on the iBeta test laptop without any protection from tampering.

For this biometric system, Fujitsu utilized PalmSecure technology. A sensor illuminate and capture the subcutaneous veins in a palm. The number of uniqueness of veins in a human hand provide the basis for capture and comparison. During enrollment, PalmSecure registers unique palm vein characteristics that constitutes a template. A proprietary algorithm is then applied which converts the captured template into a string of numbers which are not interpretable by the naked eye to ensure privacy and protect against identity theft when transmitted. This enrollment process is completed within seconds. Blood must actively be flowing through the palm vein to successfully capture a template and perform authentication assuring subject liveness.

The diagram below (provided by Fujitsu) shows a typical application of how PalmSecure can be deployed.



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 Attachment 1 (not released publically).

6.1 Limitations

The results and conclusions of this report are limited to the specific Implementation under Test (IUT) applications and versions described in Section 1.1 and Section 4.1.

It was the responsibility of Fujitsu to provide iBeta with the SDK and documentation for certification 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 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 conforms to the regulations. Use of these results will not guarantee conformity of an implementation to the regulations; 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, however, iBeta tested the API through vendor supplied applications (apps). 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 PalmSecure biometric subsystem using images acquired using the PalmSecure system. The evaluation and testing certifies that the PalmSecure system 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 PalmSecure Component Results

There were neither deviations from the DEA approved test method nor any test setup that varied from the standard protocol. The results are reported in detail in Attachment 1 (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

As described in the Test Environment Setup Section 3.2.2 above, the False Match Rate (FMR) was calculated based on results from approximately 9,900 attempted matches of 99 enrolled subjects. Of those matches, 99 were expected to match and the remaining 9,801 were expected non-matches. These values do not include an additional 602 additional verification samples which were acquired from the subjects and were used to calculate the FNMR only for expected matches.

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

Table 6-1 Age Demographics

Age (Years)	Count	Percentage
<21	0	0.0%
18 – 35	49	49.0%
36 – 52	29	29.0%
53 - 70	22	22.0%
70>	0	0.0%

Table 6-2 Gender Demographics

Gender	Count	Percentage
Male	56	56%
Female	44	44%
Undisclosed	0	0.0%

Table 6-3 Ethnicity Demographics

	Count	Percentage
White	71	71%
Asian	2	2%
Hispanic	14	14%
African American	12	12%
Other Native American	1	1%

Table 6-3 shows the threshold at which a transition occurred in the false match (FM) count. These are the results as obtained using the DEA approved method which only utilizes the first sample of the non-matching subjects. The table also shows the interesting points where 0, 1, or 2 FMs were observed.

Table 6-3 Numbers of Genuine and Imposter Matches

	Genuine (expected match)	Imposter (expected non-match)
ISO 19795-1 Annex B-1		
PalmSecure	99	9,801

Table 6-4 FMR at Thresholds

Sensitivity Setting	FM count	FMR (obs)	FMR (95% CI)
Lowest	0	0.000	0.000306
Low	0	0.000	0.000306
Normal	0	0.000	0.000306
High	0	0.000	0.000306
Highest	0	0.000	0.000306

As shown in Table 6-4, the threshold set with any sensitivity setting met the requirement.

6.3.1 Exceptions

The PalmSecure biometric subsystem is certified effective on the publish date of this report. Per 21 CFR 1311.300(a)(2), this certification expires 2 years from that date. Also per that requirement, the assessments and testing for certification applies only to the subsystem tested and documented within this report. Any alterations to that subsystem invalidate this certification.

The data supporting these certification results are found in Attachment 1.

6.4 Other EPCS Biometric Subsystem Requirements

Table 6-5 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 a facial biometric as obtained and described herein meets the other subsystem requirements for use in a DEA EPCS system.	<input checked="" type="checkbox"/>
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 SDK and device meet this requirement.	<input checked="" type="checkbox"/>
1311.116(c)	The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate	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	<input checked="" type="checkbox"/>

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
	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.	nongovernment laboratory. The system certifying agency must verify that the algorithm operates at the threshold defined above.	
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.	The system captures fingerprints, but it captures the index, middle, ring and pinkie as a set, which is not a modality included in SP 800-76.	<input checked="" type="checkbox"/>
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 biometric device is expected to be collocated with the practitioner's computer.	<input type="checkbox"/>
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.	It is the responsibility of the enclosing system on the mobile device to provide this ID. The ID is available through the API but not stored with the template.	<input type="checkbox"/>
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.	Authentication is local in that the enrollment or reference records reside in a folder on the device. Depending on the implementation and integration into a larger health records systems, the storage of records, match results, and/or non-match results may be not be local; therefore, these regulations may apply. This requirement may need to be fully tested in the overall system.	<input type="checkbox"/>

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
1311.116(h)	<p>Testing of the biometric subsystem must have the following characteristics:</p> <p>(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.</p> <p>(2) Test data are sequestered.</p> <p>(3) Algorithms are provided to the testing laboratory (as opposed to scores or other information).</p> <p>(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.</p> <p>(5) Results of the testing are made publicly available.</p>	<p>(1) iBeta is independent of Fujitsu and does not have an interest in the outcome of the performance of this testing.</p> <p>(2) Test data were destroyed at the conclusion of testing and test data were not provided to the vendor during testing.</p> <p>(3) Algorithm was provided in the form of a .bat file and a black box executable that were used during testing.</p> <p>(4) iBeta's process and procedures to test the FMR at 95% confidence have been approved by the DEA.</p> <p>(5) This report is available at http://www.ibeta.com/our-software-quality-services/epcs/reports/</p>	<input checked="" type="checkbox"/>

6.4.1.1 Exceptions

The 21 CFR 1311.116(e), (f), and (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 and Recommendations

7.1 Recommendations

iBeta Quality Assurance has completed the testing of the PalmSecure biometric subsystem. In our opinion the acceptance requirements of 21 CFR Parts 1311.116 have been met as delineated in Table 7-1 and its Notes.

iBeta Quality Assurance certifies the PalmSecure to the requirements of 21 CFR Parts 1311.116(b) and 1311.116(h)(4). Other requirements assessed are also included below in Table 7-1.

The following table (Table 7-1) contains 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 Requirement 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).	☑

Requirement	Description	Approved
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.	<input checked="" type="checkbox"/>

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:

- (a) 1311.116(a) is a rollup requirement mandating the other requirements for biometrics subsystem
- (e) The tested biometric subsystem has the capability to meet this requirement but it must be tested for the overall system. See Table 6-5 for details.
- (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 6-5 for details.
- (g) The tested biometric subsystem has the capability to meet this requirement especially when operated locally. See Table 6-5 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 1-1.

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.

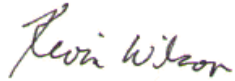
7.2 Opinions

The vendor supplied documentation was acceptable for iBeta to produce a software test suite built upon the vendor's SDK.

The PalmSecure application operated as expected.

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:

A handwritten signature in cursive script that reads "Kevin Wilson".

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