



Redrock PalmID

DEA EPCS Biometric Subsystem Certification Test Report

Prepared for:
Redrock Biometrics, Inc.
90 S. Spruce Ave, Suite H
South San Francisco, CA 94080

Version 1.0
6 June 2016
Report #160606-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:
June – 06 – 2016

*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 – 06 – 2018

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

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 Redrock Biometrics	Gail Audette	Dr. Kevin Wilson	June 6, 2016

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 7

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 *Definition of Test Criteria* 10

 3.2.2 *Test Environment Setup* 10

 Picture 3-1: Biometric Acquisition with the Test Environment..... 11

 Picture 3-2: Biometric Acquisition with the PalmID Application..... 11

 Table 3-2 Claimed versus Measured Error Rates..... 12

 3.2.3 *Test Execution* 13

4 BIOMETRICS SYSTEM IDENTIFICATION 15

4.1 SUBMITTED BIOMETRICS SYSTEM IDENTIFICATION 15

 Table 4-1 Biometrics System Name and Version 15

 Table 4-2 Biometric System Software -- Hash of the PalmID delivered file 15

4.2 BIOMETRICS SYSTEM TEST ENVIRONMENT 15

 Table 4-3 Biometrics System Test Hardware 15

 Table 4-4 Biometrics System Test Software..... 16

 Table 4-5 Biometrics System Technical Documents 16

 Table 4-6 Other Software, Hardware and Materials 16

 4.2.1 *Biometrics Test Environment – Technology Test*..... 17

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 *PalmID Component Results* 18

6.3 FALSE MATCH RATE REVIEW 18

 Table 6-1 Age Demographics 19

 Table 6-2 Gender Demographics 19

 6.3.1 *Camera Definition* 19

 Table 6-3 SFR and Distortion Data..... 19

 6.3.2 *Exceptions* 20

6.4 OTHER EPCS BIOMETRIC SUBSYSTEM REQUIREMENTS..... 20

 Table 6-3 Testing of Biometric Subsystem Requirements 20

7 OPINIONS AND RECOMMENDATIONS 22

7.1 RECOMMENDATIONS..... 22

 Table 7-1 Requirement in Compliance 22

 7.1.1 *Limitations*..... 23

 7.1.2 *Exceptions* 23

7.2 OPINIONS..... 23

7.3 RESPONSIBLE TEST LABORATORY PERSONNEL 23

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 PalmID from Redrock Biometrics. 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 PalmID biometric subsystem is a palm print recognition system. iBeta tested and certified the built-in matching algorithm.

The PalmID 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 utilizing the mid-level setting of the operating point threshold of 20.

The Redrock Biometrics PalmID 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 Redrock Biometrics. This report will be maintained on the iBeta website during the period of certification from the issuance of this report (6 June 2016) through the certification expiration date (6 June 2018).

1.1 *Biometric Subsystem Identification*

The RedRock Biometrics PalmID Version 3 core acquisition components are described in Section 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric Subsystem Test Environment. Two applications were provided by RedRock Biometrics – a collection batch file and a match batch file.

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 Redrock Biometrics PalmID application to the 21 CFR 1311.116 regulations. The results were generalized by running the FMR tests on a single test platform.

The Redrock Biometrics PalmID application 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 11 November 2015 (approval #15-395) for the following:

- Test Protocol Version 1.0 dated 20 October 2015, revised Version 2.0 on 21 April 2016
- Biometrics Security Procedures (Version 3.0) dated 5/20/13
- 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.)
01	Mutual Confidential Disclosure Agreement	NDA	10/5/15	iBeta Quality Assurance
01	Agreement for EPCS Pre-Certification Testing Services	MSA	10/12/15	iBeta Quality Assurance
01	Agreement for Biometric Subsystem Certification Testing Services	Contract	3/25/16	iBeta Quality Assurance
iBeta Procedures				
1.0	Biometric Deliverable Receipt Procedure		6/1/11	iBeta Quality Assurance

Version #	Title	Abbreviation	Date	Author (Org.)
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		21 May 2013	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-Redrock Biometrics		5/11/2016	iBeta Quality Assurance
1.0	Redrock Biometrics DEA EPCS Pre-Certification Letter		1/19/16	iBeta Quality Assurance
1.0	DEA-EPCS-Test-Cases-Redrock Biometrics		5/31/16	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
2014	ISO 12233 Photography — Electronic still picture imaging — Resolution and spatial frequency responses	ISO 12233	2104-02-15	ISO

Version #	Title	Abbreviation	Date	Author (Org.)
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 Redrock Biometrics 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 Redrock Biometrics PalmID Biometric Subsystem included Security Assessment and Operating Point to provide 0.001 false match rate or better. Weekly status reports were sent to Redrock Biometrics. 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 Redrock Biometrics PalmID 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.

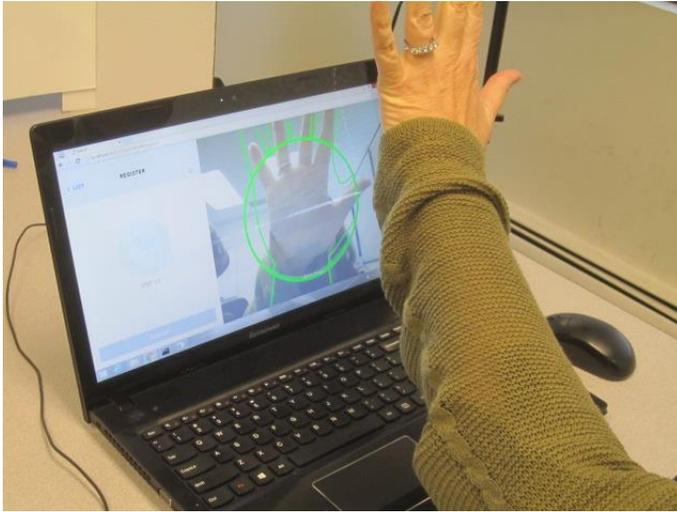
As necessary to test the system, iBeta generated a semi-automated Conformance Test Software (CTS) to enroll and challenge the biometric subsystem with biometric data and record the results.

3.2.2 Test Environment Setup

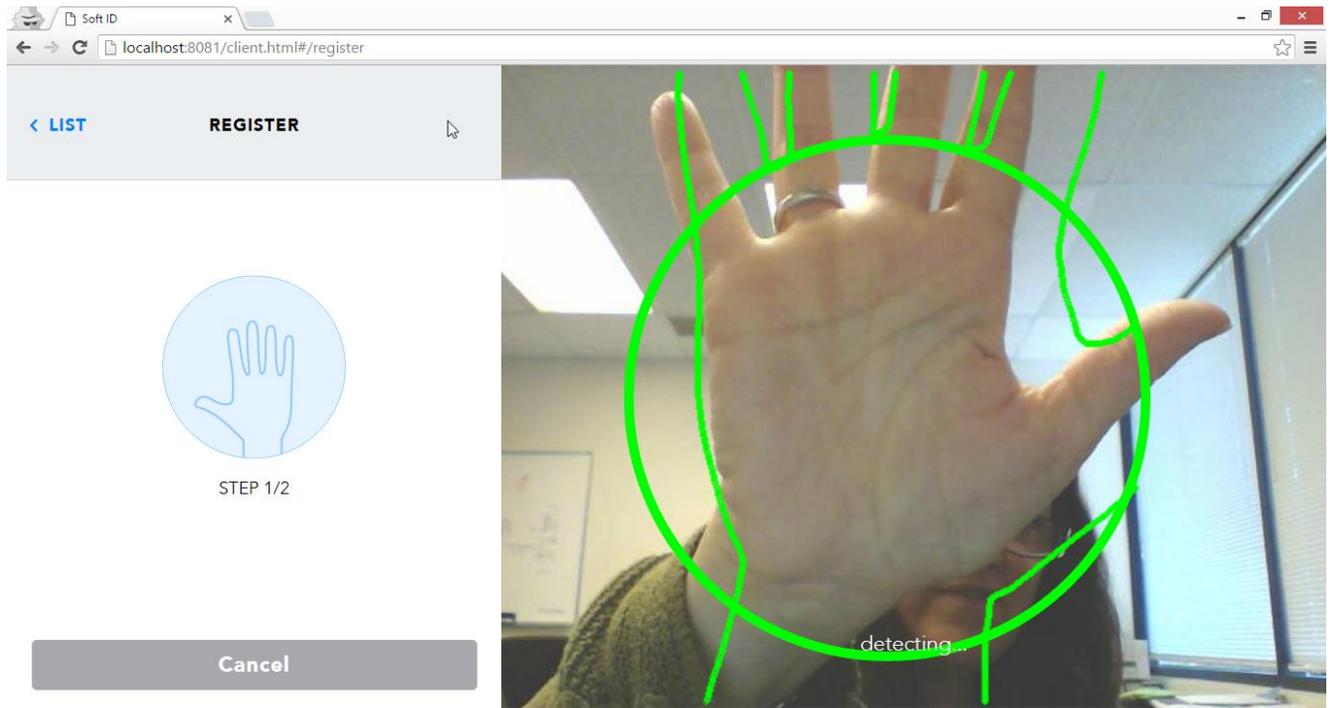
For this test effort, iBeta located all equipment in the Biometrics Lab of the iBeta facility.

A test dry run was conducted prior to full data collection. On 27 April 2016, eight iBeta employees provided PII and a prototype test of the date 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 PalmID's collection.bat and the match.bat. The test environment for PII collection with the PalmID application is provided below in Pictures 3-1 and 3-2.



Picture 3-1: Biometric Acquisition with the Test Environment



Picture 3-2: Biometric Acquisition with the PalmID Application

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 that stated that she had spinal cord injuries and could not steady her hand. A single Failure to Acquire (FTA) was also noted on a subject who was able to record her enrolment and first verification data but could not record a second verification data point. iBeta used the maximum of 4 attempts as specified by NIST SP800-76-1 standards before declaring the FTA.

An encrypted database was created using TrueCrypt as listed in Table 4-7. The database of 116 biometric data samples (consisting of 2-3 biometric data records per each of 116 individuals) was used in the technology testing. Of these 116 data records, 116 were enrolled (i.e. used as a biometric reference, genuine) into the system when the system accepted their palm image as presented. The 2nd sample was used as a challenge or biometric probe. Additionally, for genuine comparisons only, the third sample was used. A total of 6901 sets of challenges were made for the 116 enrolled subjects. Of those, 231 were expected to match and 6670 were expected to not match.

The PalmID API produced a score result for each attempted match. At a given threshold, 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. However the matching of I x J was not repeated for the dependent 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)/2 expected non matches and 2*n expected matches if every reference has a corresponding probe associated with it. One FTA of the second sample taken resulted in only 231 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 Redrock provided PalmID application to acquire 3 samples per subject (1 as enrollment (genuine) and 2 as verification samples). Because the matcher was operating as a black box to iBeta, the BIDs of all the verification samples were scrambled using a random-number generator. After the Redrock 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 two verification samples and the methods of ISO 19795-1 B.2.3.2 were used to determine the FNMR at 95% CI.

The Redrock matcher provided a matrix of scores of all samples against all samples. For most runs, only the first verification sample was used for those runs and only the upper triangle of the enrollment vs. first verification was used for further analysis. A separate additional run was performed for the diagonal (expected match scores) only of the enrollment vs. second verification sample.

iBeta observed that the scores produced contained some variability, which Redrock affirmed was expected behavior. However, to validate that this randomness was not producing a change in the threshold, iBeta performed five sets of matches. Within the five sets of matches, iBeta did not observe any scores that altered the FMR provided in this report.

3.2.2.1 Camera Definition

Because the test by design and contractual stipulation was with only one camera, iBeta proposed to perform some testing to define the camera capabilities. iBeta used the following to quantify the accuracy of the camera tested (which was built into the laptop). The camera operated at 640 x 480 (W x H) resolution during the testing; however, camera resolution does not specifically quantify how accurate a camera might be. At any given resolution and distance, the camera might produce other artifacts such as distortion, fuzziness, defocus, or noise.

1. Spatial Frequency Response (SFR) As described in ISO 12233, a photo of a slanted edge was used to determine the spatial frequency response. iBeta used the publicly available MITRE SFR application source code compiled for Windows to analyze the slanted edge photos. The MITRE software and SFR technique is used by MITRE and the FBI to perform Appendix F certification of fingerprint sensors.
2. Distortion. Distortion was measured in the sense of barrel or pincushion type of distortion and reported in percentage $\Delta H/H$. iBeta used a NIST certified ruler to measure the accuracy of the grid-lines used for this test on the target to approximately 0.14% accuracy.

3.2.3 Test Execution

Test enrollment or data collection was conducted April 29 through May 13, 2016. Test execution was conducted in the timeframe of May 16 through May 27, 2016 and the detailed results are listed in Attachment 1.

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. As of the publication of this report, the biographical data collected for this study has been destroyed except for the aggregate data reported herein.

The scrambling of the BIDS was performed on the same laptop used to acquire the data. Likewise, the matching was performed on the same laptop where the data had been acquired. 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.

For SFR measurements, the MITRE SFR takes the image pixel density as an input. iBeta always supplied the ppi value of 500 for this input. When analyzing the results, iBeta converted the cy/mm output to cy/pixel based on the fact that there are 19.68 pixels/mm at 500 dpi. As described below, cy/pixel could be converted to cy/degree to compare different cameras under otherwise similar

conditions where $cy/degree$ is relative to the view angle of each pixel. The laptop camera (as are most web-cams) had a fixed focus, fixed aperture, and fixed f-number. During capture the camera auto-adjusted gain and/or "shutter speed." Shutter speed as used here may actually be a video frame rate from which the capture method acquired a frame from.

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 PalmID application 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 Redrock Biometrics PalmID application. The Redrock Biometrics PalmID Test user Guide stipulated that minimum system requirements as:

- Windows PC: Either a desktop or laptop may be used. (If a laptop is used, it is recommended to set the power plan to High Performance for faster speed).
- OS: Windows 7, 8, or 10 64 bit.
- Webcam: embedded or connected with an USB.
- Processor: Intel CPU i5 or higher.
- Monitor: 1366 x 768 pixels or higher.
- Hard drive: 50 MB free space (not including the size of data samples).
- RAM: 300 MB free ram at the start of the program (excluding system and other applications).
- Browser: Google Chrome version 47.0.2526 or later.
- Node.js: node.js is required to run the web GUI of the data collection program.

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
PalmID	V3

The Biometrics System as delivered and certified is documented in Table 4-2/

Table 4-2 Biometric System Software -- Hash of the PalmID delivered file

System	DLL Name	Version	size (bytes)	SHA-256 hash
64-bit DLLs				
	PalmAPI.DLL	3.0	19,416,576	d161c6f40a7a259afedab31a94510cdafe7ef974a5bd59df3aed6f4af5357713
32-bit DLLs				
No 32-bit DLL's were provided for testing				

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 same laptop and associated webcam. The technology portion of the test was performed on the single test laptop.

The webcam was built into the laptop provided by iBeta for this testing. Like most webcams, the camera operated in video type of format and iBeta does not know if any (lossless or lossy) compression of this feed was done prior to capturing an image. Images were stored by the PalmID system and by iBeta in PNG format when they were captured.

Table 4-3 Biometrics System Test Hardware

Hardware	OS or Version	Manufacturer	Description (include functional purpose and condition of the equipment)
Lenovo G500 Intel® Core™ i5-3230M @2.60 GHz	Windows 8.1 64-bit	Lenovo	S/N: CCAB10LP4160T6 Used for collection and matching. Power plan switched to High Performance Embedded Webcam: Fixed Focus CMOS

Hardware	OS or Version	Manufacturer	Description (include functional purpose and condition of the equipment)
			camera 1366 x 768 resolution monitor Hard Drive: 25.0 GB with 24.9 free at the start of data collection RAM: 3.90 GB with 2.1 GB free at start of data collection Browser: Google Chrome version 49.0.2623.112 m Node.js: 4.4.2
EasyCamera (built-in webcam)	6.2.9200.10240	Lenovo	Webcam situated above the monitor.
HP Envy 700-214 Intel® Core™ i5-4440 CPU @ 3.10 GHz	Windows 10 Home 64 bit	Hewlett-Packard Company	

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
WebCSharp	2015-May-02	Open Source	Lenovo for distortion and SFR image capture. Modified by iBeta to store lossless compressed PNG images
MITRE SFR	1.4.2	MITRE	Compiled from source-code for windows command line.
Node.js	4.4.2	Node JS open source TSC	Required by PalmID for image capture GUI
Google Chrome Browser	49.0.263.112	Google	Browser-based app to acquire palm biometrics.

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

Table 4-5 Biometrics System Technical Documents

Version #	Title	Date	Author (Org.)
1.0	Palm ID Test User Guide	4/6/16	Redrock Biometrics, Inc.

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
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 Compile and run mitre-sfr
Beyond Compare 3 v.3.2.4 (Scooter)	Comparison utility	Supplied by iBeta: used to compare

Material	Material Description	Use in the Biometrics System
Software)		file/folder differences
Md5deep v4.4	Open Source	Hashing of executable code
Slanted edge target	Digital Camera Resolution Chart	Used to measure camera accuracy
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. One device was used for test coverage. To acquire the enrollment and verification samples, the collect.bat method was executed. This batch file started the collect.exe program as well as the locally hosted web page which executed javascript to acquire the samples.

For the technology testing, after obfuscating the data, iBeta executed the match.bat method, which in turn executed the match.exe program with the parameter pointing to the data folder where iBeta had scrambled the acquired data folder and filenames. As described above, the output of this program was a CSV file in matrix format giving the score of the match for all enrollments and verifications found. iBeta ignored the enrollment x enrollment and verification x verification portions of the matrix and only parsed out the upper triangle of the enrollment x verification results.

4.2.1.1 Processing and Post-processing

An iBeta program (redrock.exe) which had scrambled the palm image data, was used to unscramble the results output and pull out only the upper triangle of results and present them in linear format so the results could be imported into Excel for further processing.

5 Biometrics System Overview

The PalmID consists of a data collection application that drives the camera for image capture and the PalmID matching software. This implementation used a node.js server and script to acquire the palm images for enrollment and verification.

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 API could produce an ID for the camera 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 palm images were stored in the filesystem as PNG formatted images without any protection from tampering.

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 Redrock Biometrics 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, but the test system provided to iBeta used a localhost node.js server and a browser-hosted script 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 PalmID application was tested in verification mode (1:1), which is the only mode applicable to the DEA EPCS regulations. Use of the application in identification mode (1:N) was not certified, although such methods may be available in the application. Verification mode means that the PalmID application returns a true/false result against the left-palm print that is associated with the identity claimed. A true result indicates a match to the identity claimed.

The scope of this iBeta report and certification is solely for the PalmID biometric subsystem as listed in **Error! Reference source not found.** The evaluation and testing certifies that the PalmID 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 PalmID 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 Amendment -1 (not publicly available) to this report.

As tested, the software would not initialize the application unless the PalmID was attached to the internet. Likewise, the application would not initialize and therefore could not perform a match operation unless a device was attached to the internet.

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 7,016 attempted matches of 116 enrolled subjects. Of those matches,

231 were expected to match and the remaining 6,670 were expected non-matches. These values include an additional 115 second 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) and Gender (Table 6-2) demographics reported below.

Table 6-1 Age Demographics

Age (Years)	Count	Percentage
<21	0	0.0%
21 - 30	44	37.9%
31 - 50	37	31.9%
51 - 70	35	30.2%
70>	0	0.0%

Table 6-2 Gender Demographics

Gender	Count	Percentage
Male	65	56.0%
Female	51	44.0%
Undisclosed	0	0.0%

At 95% confidence intervals, iBeta found that the designated system met the 0.001 FMR at a threshold of 20.

In other words, the PalmID application method, match.bat complies with the regulation if the algorithm returns with a value of 20 or greater to indicate a match.

6.3.1 Camera Definition

iBeta utilized camera distortion and SFR to quantitate the accuracy and specifications of the camera. The camera operated in 640 x 480 mode (relatively low “resolution,” and the lowest resolution available for that camera). However, as described in section 3.2.2.1, the resolution does not define the accuracy of the camera, but only the pixel width and height of its resulting canvas.

During data acquisition of palm prints, iBeta observed that the application would acquire a palm image between 5-1/2 and 10 inch. The acquisition process automatically captured the image(s) when the palm was at the appropriate distance and more-or-less within the template projected for user feedback. Most images seemed to be acquired around 8 +/- 1/2 inches. Most subjects approached the camera with their palm and the only way to measure the close distance was to start close and pull out. Therefore, few subjects found the close distance unless they were not presenting the hand perpendicular to the camera direction or had it cupped. As described above, these cases rarely resulted in an FTE or FTA because the subjects habituated (learned) quickly with some coaching from the operator.

As described in the table below, at the given resolution setting of 640 x 480, each camera pixel corresponded to an angular view of 0.086 x 0.089 degrees. The SFR was calculated as cycles/pixel, so the spatial Nyquist frequency would correspond to approximately 0.17 degrees (i.e Nyquist frequency equals two times the sampling frequency).

Table 6-3 SFR and Distortion Data

Measurement	Observed Value	Notes
Field of View		
Width	54.9 degrees	
Height	42.5 degrees	
Pixel Width	0.086 degrees	
Pixel Height	0.089 degrees	The pixels were not “square.” 3% higher than wide.
SFR		
At 0.25 cy/pixel (i.e. 4 pixel)	0.68 to 0.83	Possible effects of sharpening especially of vertical edges were observed
At 0.50 cy/pixel	0.25 to 0.53	
Distortion		
Width	-0.25%	Less than experimental error.
Height	+0.05%	Less than experimental error

6.3.2 Exceptions

The PalmID 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 6-4 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 palm print 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 API 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 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. The system certifying agency must verify that the algorithm operates at the threshold defined above.	<input checked="" type="checkbox"/>
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.	Not Applicable for the palm print modality.	<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.	The biometric subsystem has the capability to meet this requirement, and the requirement was validated; however, this requirement will need to be fully tested in the overall system.	<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	Authentication is local in that the enrollment or reference records reside in a folder on the PC. Depending on the implementation	<input type="checkbox"/>

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
	<p>over an open network, biometric data (raw data or templates), match results, and/or non-match results must be:</p> <p>(1) Cryptographically source authenticated;</p> <p>(2) Combined with a random challenge, a nonce, or a time stamp to prevent replay;</p> <p>(3) Cryptographically protected for integrity and confidentiality; and</p> <p>(4) Sent only to authorized systems.</p>	<p>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.</p> <p>This requirement may need to be fully tested in the overall system.</p>	✓
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 Redrock Biometrics 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>	☑

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 PalmID 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 PalmID application 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 6-4 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 6-4 for details.
- (g) The tested biometric subsystem has the capability to meet this requirement especially when operated locally. See Table 6-4 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

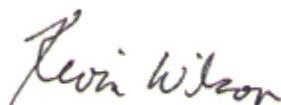
The vendor supplied documentation was acceptable for iBeta to produce a software test suite built upon the vendor's SDK.

The PalmID 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:

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



Kevin Wilson Ph.D.
 Director of Biometrics