# VeridiumID™ V1.2.1

# DEA EPCS Biometric Subsystem Certification Test Report

**Prepared for:**
**Veridium IP Ltd**
**Chalfont Park Building 1**
**Gerrards Cross SL90BG**
**United Kingdom**

**Version 1.0**
**1 December 2017**
**Report #171201-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:**
**December– 01 – 2017**

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

**Date of expiration:**
**December– 01 – 2019**

*Copyright © iBeta Quality Assurance, all rights 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 | Gail Audette | Dr. Kevin Wilson | 15 December 2017 |

**TABLE OF CONTENTS**

# 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 VeridiumID™ V1.2.1 from Veridium IP Ltd. 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 VeridiumID™ biometric subsystem is a contactless fingerprint recognition system. iBeta tested and certified the built-in matching algorithm.

The VeridiumID™ 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 an overall setting of a threshold of 166 for both devices tested.

The Veridium IP Ltd VeridiumID™ 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 Attachments 1, 2, 3, and 4 are available upon request from Veridium IP Ltd. This report will be maintained on the iBeta website during the period of certification from the issuance of this report (1 December 2017) through the certification expiration date (1 December 2019).

## 1.1 *Biometric Subsystem Identification*

The VeridiumID™ acquisition and matching components are described in Section 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric Subsystem Test Environment. Three applications were provided by Veridium – a data collection program for iOS and Android and a matching algorithm tested in a MobyLinux virtual machine on Windows.

## 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 Legacy System Comparison Results
- Attachment 2: Detailed Technology Assessment Results
- Attachment 3: Detailed Technology Assessment Timing Results
- Attachment 4: Detailed Technology Assessment 500 ppi 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 Veridium IP Ltd. VeridiumID™ applications to the 21 CFR 1311.116 regulations. The results were generalized by running the FMR tests from data acquired on two test platforms – an iPhone 6S and a Samsung Galaxy S6.

The VeridiumID™ 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 15 September 2016 (approval: #120160885) for the following:

- Test Protocol Version 1.0 dated 19 August 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 | Confidentiality Agreement | NDA | August 2017 | Veridium IP Ltd. |
| 01 | Agreement for DEA EPCS Certification and Scenario Testing Services | Contract | 10/5/17 | iBeta Quality Assurance |
| iBeta Procedures | | | | |
| 1.0 | Biometric Deliverable Receipt Procedure | | 6/1/11 | iBeta Quality Assurance |
| 3.0 | Biometric Security Procedure | | 5/20/13 | iBeta Quality Assurance |
| 1.0 | Biometrics Configuration Management Procedure | | 6/9/11 | iBeta Quality Assurance |

| Version # | Title | Abbreviation | Date | Author (Org.) |
|---|---|---|---|---|
| 4.0 | DEA-EPCS Biometric Assessment Procedure | | 5/21/13 | iBeta Quality Assurance |
| 1.0 | Biometric Training and Training Records Procedure | | 6/1/11 | iBeta Quality Assurance |
| iBeta Project Documents | | | | |
| 1.0 | DEA-EPCS-Biometric-Assessment-Veridium | | 11/6/17 | iBeta Quality Assurance |
| 1.0 | DEA-EPCS-Test-Cases-Veridium | | 11/29/17 | 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 Veridium IP Ltd 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 2: 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 Veridium IP Ltd VeridiumID™ Biometric Subsystem included Security Assessment and Operating Point to provide 0.001 false match rate or better. Weekly status reports were sent to Veridium IP Ltd. 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 Veridium IP Ltd. VeridiumID™ 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.

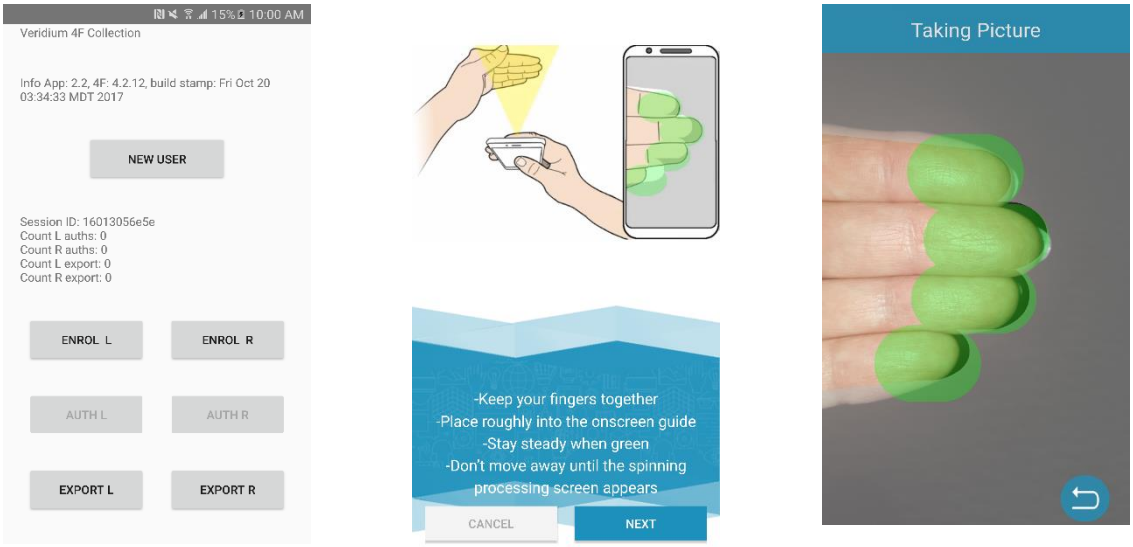
As necessary to test the system, iBeta utilized apps on the mobile devices that had been prepared by Veridium to collect images of enrollment and challenge. iBeta utilized a black-box matching engine produced by Veridium that operated on a MobyLinux VM under Windows 10. The matching engine produced scores based on the obfuscated enrollment and challenge images presented and recorded the resulting score. Fusion of the four-fingers index through pinkie were used as the biometric of interest.

### 3.2.2 Test Environment Setup

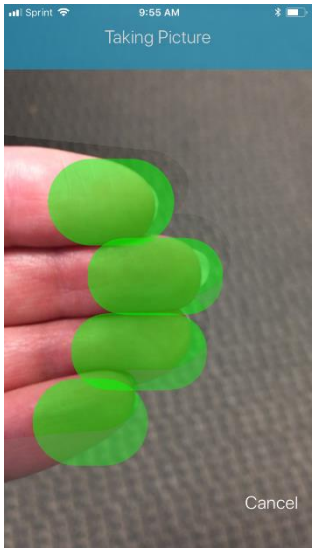
For this test effort, iBeta located all equipment in the Biometrics Lab of the iBeta facility.

A test dry run was conducted prior to full data collection. On 1 November 2017, ten 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 both an Apple iPhone 6S and a Samsung Galaxy S6. The test environment for PII collection with the VeridiumID™ Suite application on the Galaxy S6 and iPhone 6S are provided below in Pictures 3-1 and 3-2.




**Picture 3-1: Biometric Acquisition with the Samsung Galaxy S6 Test Environment and VeridiumID™ Application**




**Picture 3-2: Biometric Acquisition with the VeridiumID™ Application on the iPhone 6S**

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. The mobile-device apps generated a unique ID for each subject, which iBeta correlated with the iBeta BID. The unique ID from the Samsung device was a 12 digit hex value. The unique ID from the iPhone was an 8 digit value.

During this data collection, iBeta experienced a single Failure to Enrol (FTE) on the iPhone 6S. The subject was an older female not familiar with the iOS and iBeta determined that the FTE was due to the subject and not caused by the application.

An encrypted database was created using TrueCrypt as listed in Table 4-7. The database of 100 biometric data samples (consisting of 10 biometric data records per each of 100 individuals) was used in the technology testing. Of these 100 data records, 100 were enrolled into each of the smartphone technology test databases using 3 images for each enrollment (i.e. used as a biometric reference, genuine) into the system when the system accepted their fingerprint image as presented. The 1st, 2nd and 3rd samples were used as a challenge or biometric probe. A total of 10,100 sets of challenges were made for the 100 enrolled subjects. Of those, at least 400 were expected to match and over 10,000 were expected to not match.

The VeridiumID™ matcher 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.

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

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 Veridium provided VeridiumID™ Suite application to acquire 6 samples per subject (3 as enrollment (genuine) and 3 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 Veridium 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 Veridium matcher provided a matrix of scores 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 1 November through 15 November 2017. Test execution was conducted in the timeframe of 15 November through November 29, 2017 and the detailed results are listed in Attachments 1, 2, 3, and 4.

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 VeridiumID™ 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 VeridiumID™ applications.

**Table 4-1 Biometrics System Name and Version**

| Biometric System Name | Version |
|---|---|
| VeridiumID™ Suite | V1.2.1 |
| VeridiumID™ S - Veridium VeridiumID Library | Version 6.5.1 r113746 |

The Biometrics System as delivered and certified is documented in Table 4-2. The VeridiumID™ Suite was used to enroll and produce scores of probe images prepopulated into folders. It produced a tab-delimited file of probe image, enrollment folder, and the matching score.

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

| System and Name | Version | size (bytes) | SHA-256 hash |
|---|---|---|---|
| MAC (matcher) | | | |
| libffid_dynamic.dylib | 4.2.12 | 3180164 | 99d73f3d45e14b04637f7745ed471d3dc522d2fe552ae63550b39263ff69326e |
| libffid_static.a | 4.2.12 | 9682248 | 0e426b81bf1c539ace56a3943208448067d5d44558cfd970a800d4b73b45c434 |
| Linux (matcher) | | | |
| libffid_dynamic.so | 4.2.12 | 5462448 | f9b2fde596e78eac8c9a721a8fd42ec175090a6db6b35e913a0291f3da0cef34 |
| libffid_static.a | 4.2.12 | 11086944 | 7b14d7824fdf8a0facebce24ca99214c4f67f8677ad5ab975ee4486d2577edcd |
| Android - Samsung | | | |
| arm64-v8a/libffid_dynamic.so | 4.2.12 | 12292976 | 97c2fdfc6882e68d6afef1804cc6dac4a153c52d465b4f6912bb92598ae94423 |
| armeabi-v7a/libffid_dynamic.so | 4.2.12 | 7769144 | 750f12cc9bb27f1016adfe163680b64203c9f02e224751dca5e4becaa0beff83 |
| iOS - iPhone | | | |
| Versions/A/libffid | 4.2.12 | 8723072 | 794b542b69fc3252bb467a70da78b74d5fb1c373d19cf52c75e66aa980b4e520 |

## 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. No other hardware test environment was utilized.

iBeta enrolled all subjects using the two smartphones – an iPhone 6S and a Samsung Galaxy S6. The technology portion of the test was performed on desktop PCs.

The photo or rear-facing cameras were built into the smartphone provided by iBeta for this testing. Like most cameras, the camera captured JPEG images. Images were stored by the Veridium system and by iBeta in JPG format when they were captured.

**Table 4-3 Biometrics System Test Hardware**

| Hardware | OS or Version | Manufacturer | Description |
|---|---|---|---|
| iPhone 6S | iOS 11.0.3 | Apple<br>SN: C7JQH5N3GRY6<br>Model: MKT82LL/A | Data Collection Platform |
| Samsung Galaxy S6 | Android Version 6.0.1 | Samsung Model Number: SM-G920T | Data Collection Platform |
| HP Envy 700-214<br>Intel® Core™ i5-4440 CPU @ 3.10 GHz | Windows 10 Pro 64 bit | Hewlett-Packard Company | Used to calculate FMR and FNMR |
| Dell OptiPlex 790 DesktopIntel Core i7-2600K @ 3.4GHz | Windows 10 Pro 64 bit | Dell Inc. | Used for MobyLinux/Docker VMs to perform Linux matching. |

**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 |
| Beyond Compare 4 | 4.1.9 | Scooter Software | All PC's and laptops |
| iTunes | 12.7.1 | Apple | All PC's and laptops |

For the test effort, Veridium provided documentation on system setup and use. Images within album folders were available through the Windows Explorer for the Android device. Beyond Compare was used to obtain images from the Samsung device without altering the windows-reported date of the file.

**Table 4-5 Biometrics System Technical Documents**

| Version # | Title | Date | Author (Org.) |
|---|---|---|---|
| | Veridium TouchlessID Data Collection App v2.0 | 17 Oct 2017 | Veridium IP Ltd |

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 Test |
|---|---|---|
| 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 |
| 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. Two devices were used for test coverage. On each device, a total of at least seven (7) images was collected, and typically eleven

(11). Three of these images were obtained as enrollments. The additional images were obfuscated and used as probes.

A batch file containing the names of the three enrollments and the challenge image was submitted to a python script which in turn submitted that to the matching engine to produce a score. Results were output in a JSON formatted text file with the batch file row as the variable name. Each match took approximately 1 second on the i7 PC.

#### 4.2.1.1 *Processing and Post-processing*

An iBeta program (Veridium.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 VeridiumID™ consisted of a data collection application that drove the camera for image capture and the VeridiumID™ 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 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 images were stored in the filesystem as JPEG formatted images on the iPhone and as JPEG images on the Android 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 2 (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 Veridium IP Ltd 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 VeridiumID™ biometric subsystem using images acquired using the VeridiumID™ system. The evaluation and testing certifies that the VeridiumID™ 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 VeridiumID™ 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 2 (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 10,500 attempted matches of 100 enrolled subjects. Of those matches, at least 400 were expected to match and the remaining 10,000 were expected non-matches. These values include an additional 400 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), 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 | 52 | 51.0% |
| 36 – 52 | 30 | 29.4% |
| 53 - 70 | 20 | 19.6% |
| 70> | 0 | 0.0% |

**Table 6-2 Gender Demographics**

| Gender | Count | Percentage |
|---|---|---|
| Male | 54 | 52.9% |
| Female | 48 | 47.1% |
| Undisclosed | 0 | 0.0% |

**Table 6-3 Ethnicity Demographics**

| | Count | Percentage |
|---|---|---|
| White | 84 | 82.4% |
| Asian | 2 | 2.0% |
| Hispanic | 10 | 9.8% |
| African American | 6 | 5.9% |
| Other | 0 | 0.0% |

Table 6-3 delineates the number of genuine and imposter matches for the test. Table 6-4 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 as well as the case for the Galaxy S6 at the passing threshold for the iPhone 6S.

**Table 6-3 Numbers of Genuine and Imposter Matches**

| Device | Genuine (expected match) | Imposter (expected non-match) |
|---|---|---|
| ISO 19795-1 Annex B-1 | | |
| iPhone 6S | 404 | 10100 |
| Galaxy S6 | 412 | 10506 |

**Table 6-4 FMR at Thresholds**

| Threshold | FM count | FMR (obs) | FMR (95% CI) |
|---|---|---|---|
| iPhone 6S | | | |
| 147 | 18 | 0.001782 | 0.002644 |
| 164 | 5 | 0.000495 | 0.001050 |
| 166 | 4 | 0.000396 | 0.000921 |
| 168 | 3 | 0.000297 | 0.000782 |
| 171 | 3 | 0.000297 | 0.000782 |
| 173 | 2 | 0.000198 | 0.000634 |
| 179 | 1 | 0.000099 | 0.000475 |
| 183 | 1 | 0.000099 | 0.000475 |
| 184 | 1 | 0.000099 | 0.000475 |
| 185 | 1 | 0.000099 | 0.000475 |
| 189 | 0 | 0.000000 | 0.000297 |
| Galaxy 6S | | | |
| 147 | 5 | 0.000476 | 0.001009 |
| 148 | 4 | 0.000381 | 0.000885 |
| 149 | 2 | 0.000190 | 0.000609 |
| 152 | 2 | 0.000190 | 0.000609 |
| 155 | 1 | 0.000095 | 0.000457 |
| 156 | 1 | 0.000095 | 0.000457 |
| 160 | 0 | 0.000000 | 0.000286 |
| 168 | 0 | 0.000000 | 0.000286 |

As shown in Table 6-4, a threshold of 166 met the requirement on both the iPhone 6S and the Galaxy S6. The Galaxy S6 performed better than the iPhone and a threshold of 148 would meet the requirement for

that device. No scores of 166 were observed on the Galaxy S6 but it met the requirement for the scores of 160 and 168.

### 6.3.1 Exceptions

The VeridiumID™ 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. | ☑ |
| 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. | ☑ |
| 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. | ☑ |
| 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. | ☑ |
| 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. | ☐ |
| 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. | ☐ |
| 1311.116(g) | The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results | Authentication is local in that the enrollment or reference records reside in a folder on the device. | ☐ |

| Requirement Reference | Requirement | Details of level of iBeta Assessment | ✓ |
|---|---|---|---|
| | 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:<br>(1) Cryptographically source authenticated;<br>(2) Combined with a random challenge, a nonce, or a time stamp to prevent replay;<br>(3) Cryptographically protected for integrity and confidentiality; and<br>(4) Sent only to authorized systems. | 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.<br><br>This requirement may need to be fully tested in the overall system. | |
| 1311.116(h) | Testing of the biometric subsystem must have the following characteristics:<br><br>(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.<br><br>(2) Test data are sequestered.<br><br>(3) Algorithms are provided to the testing laboratory (as opposed to scores or other information).<br><br>(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.<br><br>(5) Results of the testing are made publicly available. | (1) iBeta is independent of Veridium and does not have an interest in the outcome of the performance of this testing.<br><br>(2) Test data were destroyed at the conclusion of testing and test data were not provided to the vendor during testing.<br><br>(3) Algorithm was provided in the form of a .bat file and a black box executable that were used during testing.<br><br>(4) iBeta's process and procedures to test the FMR at 95% confidence have been approved by the DEA.<br><br>(5) This report is available at http://www.ibeta.com/our-software-quality-services/epcs/reports/ | ☑ |

#### 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 VeridiumID™ 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 VeridiumID™ 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)<br>1311.116(g)(2)<br>1311.116(g)(3)<br>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:<br>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. | ☑ |

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.

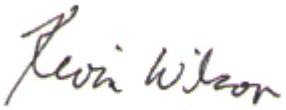
## 7.2 *Opinions*

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

The VeridiumID™ 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