EyeLock ID™ V1.2.1.0

DEA EPCS Biometric Subsystem Certification Test Report

Prepared for:
EyeLock, LLC
5113 Southwest Parkway
Austin, TX 78735

Version 2.0
23 November 2020
Report #201117-iBetaBTR-v2.0

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:
November 23, 2020

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:
November 23, 2022

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

Version History				
Ver #	**Description of Change**	**Author**	**Approved by**	**Date**
V1.0	Certification Report	Ryan Borgstrom	Gail Audette	17 November 2020
V2.0	Certification Report updated based on EyeLock review	Ryan Borgstrom	Gail Audette	22 November 2020

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 EyeLock ID® V1.2.1.0 from EyeLock, LLC. 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 EyeLock Iris biometric system is video-based technology that acquires iris images, converts the images using an EyeLock proprietary algorithm, and matches those images to their reference (enrollment) templates to be tested.

The EyeLock Iris biometric subsystem was validated to operate at a False Match Rate (FMR) of 0.001 or lower. The operating point corresponding with the False Match Rate described in 1311.116(b) was tested so that there was at least 95% confidence that the False Match Rate was equal to or less than the required value. To validate the False Match Rate requirement of 0.001 or lower as cited in 1311.116(b), iBeta found that the High Secure setting met the requirement.

The EyeLock 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 EyeLock, LLC. This report will be maintained on the iBeta website during the period of certification from the issuance of this report (17 November 2020) through the certification expiration date (17 November 2022).

1.1 *Biometric Subsystem Identification*

The EyeLock Core Demo App acquisition components are described in Section 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric Subsystem Test Environment. Two applications were provided by EyeLock – a data collection program for Windows OS and a matching algorithm tested on a Windows OS.

1.2 *Disclosure*

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

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

- Attachment 1: Detailed Technology Assessment Results

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

- Technology Test data used to determine the FMR;
- Test Design Procedures; and
- Test Case templates and as-run Test Cases.

2 Introduction

This report was generated to document iBeta Quality Assurance's assessment and testing of a biometric subsystem for the purpose of that subsystems' inclusion in an Electronic Prescription of Controlled Substances (EPCS) system. This report addresses the testing of the EyeLock applications to the 21 CFR 1311.116 regulations. The results were for the EyeLock Iris Biometric System that was connected to a Windows OS. The EyeLock provided matching algorithm (which is thread-safe) was used to perform matching.

A modified sample-code EyeLock Demo Core App 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 2019 (approval: #120160885) for the following:

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

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

The requirement of 21 CFR 1311.116(b) is that the biometric subsystem operate at a False Match Rate (FMR) of 0.001 or lower. Technology testing for the FMR requirement was performed using ISO/IEC 19795-1 and ISO/IEC 19795-2 as guidance documents in the generation and execution of test cases.

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

2.1 *Internal Documentation*

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

Table 2-1 Internal Document

Version #	Title	Abbreviation	Date	Author (Org.)
03	DEA EPCS Biometric Pre-Certification and Certification Proposal Eyelock v4	Contract	8/19/2019	iBeta Quality Assurance
iBeta Procedures				
2.0	Biometric Deliverable Receipt Procedure		2/21/20	iBeta Quality Assurance
4.0	Biometric Security Procedure		8/16/13	iBeta Quality Assurance
1.0	Biometrics Configuration Management Procedure		6/9/11	iBeta Quality Assurance

Version #	Title	Abbreviation	Date	Author (Org.)
1.0	DEA-EPCS Biometric Assessment Procedure		5/21/13	iBeta Quality Assurance
1.0	Biometric Training and Training Records Procedure		6/1/11	iBeta Quality Assurance
iBeta Project Documents				
2.0	DEA-EPCS-Biometric-Assessment-EyeLock		2/26/2020	iBeta Quality Assurance
1.0	DEA-EPCS-Test-Cases-EyeLock		6/5/2020	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 *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 EyeLock Iris Biometric Subsystem included Security Assessment and Operating Point to provide 0.001 false match rate or better.

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 Control specifically handles the regulations discussed in this report.

Term	Abbreviation	Definition
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 information which can be used to distinguish or trace an individual's identity

Term	Abbreviation	Definition
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 EyeLock 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.

iBeta utilized a matching engine produced by EyeLock that allowed iBeta to input files through this modified version of the EyeLock Core Demo App. The matching was conducted on a 64-bit Windows environment. The matching engine produced pass/fail results.

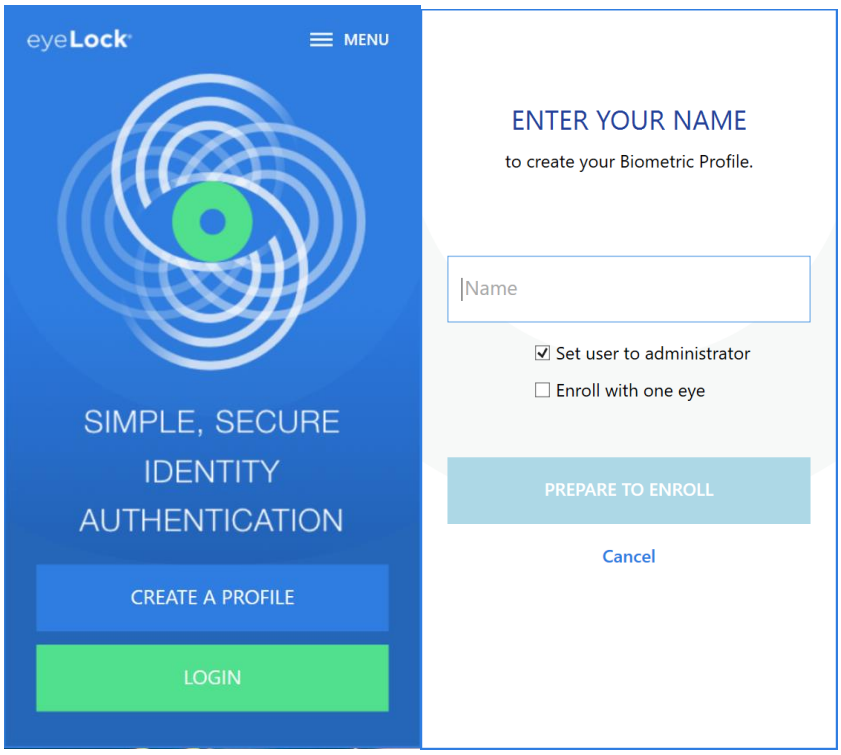
3.2.2 Test Environment Setup

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

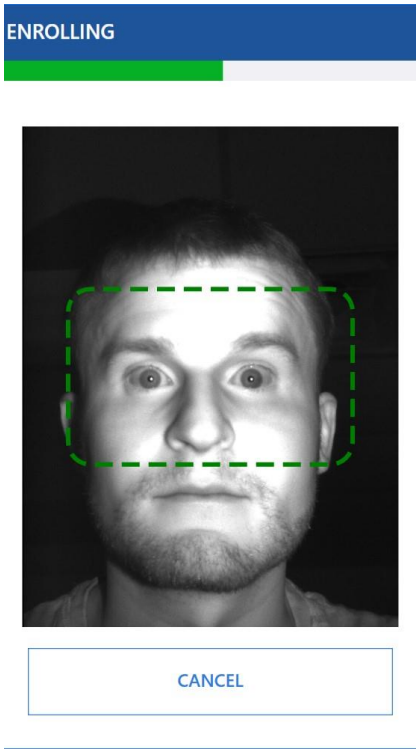
A test dry run was conducted prior to full data collection. On 18 March 2020, fourteen iBeta employees provided Personally Identifiable Information (PII) and a prototype test of the data collection test case was conducted. The enrollment data and all five samples were then used to conduct a match and cross-match test. The data analysis was conducted and the test case was adjusted as necessary.

The Technology Test was implemented using an Image Capture Device and guide to collect data as provided below in Pictures 3-1 and 3-2.

Picture 3-1: EyeLock Core Demo App



Picture 3-2: Biometric Acquisition with the EyeLock Core Demo App



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

Data collection occurred during a pandemic and the test operator was unable to communicate with the data subjects. As a result, the Failures to Enroll (FTEs) and Failure to Acquire (FTA) that were recorded are not considered valid because had the test operator been able to properly instruct the data subjects, these events may not have occurred. During this data collection, seven Failure to Enrolls (FTE), and a single Failure to Acquire were noted.

The offline database of 98 biometric data samples (consisting of 6 biometric data records per each of 98 individuals) were used in the technology testing.

The EyeLockCrossMatch-DualEye matcher produced a pass/fail result for each attempted match. At the High Security setting, 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.

Since there were no False Matches recorded, iBeta used the Rule of 3 defined in ISO 19795-1-2006[2007]: "The Rule of 3 addresses the question "What is the lowest error rate that can be statistically established with a given number N of independent identically distributed comparisons?" This value is the error rate p for which the probability of zero errors in N trials, purely by chance, is (for example) 5%. This gives:

$$p \approx 3/N \qquad (3.2.3-2)$$

for a 95% confidence level."

As described above, the subjects were enrolled using the EyeLock provided EyeLock Demo Core App V1.2.1.0 and then acquire 5 samples per subject (1 enrollment and 5 verification samples were captured).

In some instances, there was more than one enrollment for a subject. No enrollments were deleted and all enrollment samples were included in the offline matching.

The EyeLock matcher provided a matrix of pass/fail results of all samples against all samples.

3.2.3 Test Execution

Test enrollment or data collection was conducted 18 March through 21 May 2020. Test execution was conducted on 5 June 2020 and the detailed results are listed in Attachment 1. iBeta executed the matching/cross-matching for the High Security configuration setting.

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 matching was performed on the EyeLock provided HP Elite x2 G4 computer that output a .csv file. The descrambling, FMR, and FNMR calculations were performed 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 EyeLock 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 EyeLock applications.

Table 4-2 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/SHA256 Hash/size (bytes)
EyeLock Core Demo App	Application Version: 1.2.1.0 Library Version: 2.5.7
EyeLockCrossMatch-DualEye.exe	F32FD88E6F18D981E4BF94EFAAD4D205A5637EC842555 4A9A92194CA65E57A88

The Biometrics System as delivered and certified is documented in Table 4-2. The EyeLock Demo Core App was used to enroll and capture verification images. The EyeLockCrossMatch-DualEye matcher was used for the match/cross-match to determine FMR.

Table 4-2 Biometric System Components

Hardware	Firmware, Operating System & Version	Description
HP Elite x2 G4	Windows 10 Pro v.1809 Device ID: 36F580AF-A3CE-4F3E-9F8C-621E6D62D782	Tablet with EyeLock Core installed; used for data collection
EyeLock Iris Biometric System (camera)	Board Type: Kimber Board Revision: 1.0 Imager Type: J1-5 Driver version: 10.0.17763.404	USB video device used for capturing eye crops; used for data collection

The USB-C cord supplied by EyeLock and 6-foot USB-C extension provided by iBeta was used to acquire data from the device.

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.

Table 4-3 Biometrics System Test Hardware

Hardware	OS or Version	Manufacturer	Description
EyeLock Iris Biometric	Driver version: 10.0.17763.404	EyeLock	Kimber Board

Hardware	OS or Version	Manufacturer	Description
System (camera)			
HP Elite x2 G4 Intel Core i5	Windows 10 Pro	HP	Collected data from capture device

Table 4-4 Biometrics System Test Software

Software	Version	Manufacturer	Identify Hardware
SDelete	2.02	Microsoft	All PC's and laptops

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

Table 4-5 Biometrics System Technical Documents

Version #	Title	Date	Author (Org.)
1.0	EyeLock Embedded Overview	23 October 2019	EyeLock
1.0	TN-214 Template Database	23 October 2019	EyeLock

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
Certified ruler		Used to measure grid spacing for camera accuracy

4.2.1 Biometrics Test Environment – Technology Test

The devices listed in Table 4-3 indicate their functional purpose in the test effort. A single device was used to capture all of the data for the testing. On this device, each subject completed enrollment then captured five (5) verification images. The verification images were obfuscated and used as probes.

4.2.1.1 *Processing and Post-processing*

iBeta used Excel to analyze the cross_match_output.csv file and parse through the data to find results.

5 Biometrics System Overview

EyeLock LLC provides advanced iris biometric technology for the Internet of Things (IoT) providing security through proprietary algorithms. Iris authentication is highly secure and accurate as proven by the NIST Iris Exchange studies and documented in biometric technology articles.

EyeLock solutions include more than 75 patents and patents pending and have been integrated across consumer and enterprise products and platforms, eliminating the need for PINs and passwords.

The EyeLock Embedded offer for OEM customers is to enable a path for OEMs to embed Iris Biometric technology in their equipment. This is achieved by providing:
1. Reference Design Kits, which are hardware designs that can be used to launch an OEM-specific board design. This provides the OEM with maximum flexibility to fit the design in the available volume and allows the OEM to use their superior buying power as an advantage.
2. Software Design Kit, which provides a mechanism for interaction between EyeLock Services and OEM business logic. In addition to providing sample code for OEM business logic and a sample GUI, the SDK provides two primary services:

a. Template Service — to generate both enrollment and candidate matching templates
b. Matcher Service — to provide matches for enrollment templates (stored in the OEM database) and candidate matching templates (provided by the Template Service via the OEM Client Application).

EyeLock also offers flexible matching topologies; 1:1, 1:n, 1:many, local, network, and hybrid (local first, then network if needed). Additionally, a rich array of supporting documentation is available to assist during the integration phase. More information about EyeLock can be found at www.eyelock.com.

The test conducted for DEA EPCS certification consisted of an SDK-created data collection application that drove the sensor for image capture and the EyeLock 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.

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.

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 EyeLock to provide iBeta with the application 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 EyeLock biometric subsystem using images acquired using the EyeLock system. The evaluation and testing certifies that the EyeLock 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 EyeLock Component Results

There were neither deviations from the DEA approved test method nor any test setup that varied from the standard protocol. The results are reported in detail in Attachment 1 (not publicly available) to this report.

False Match Rate results are given in Section 6.3.

6.2.1.1 *Exceptions*

There were no exceptions taken to the test method.

6.3 *False Match Rate Review*

As described in the Test Environment Setup Section 3.2.2 above, the False Match Rate (FMR) was calculated based on results from approximately 9,506 attempted matches of 98 enrolled subjects. Of those matches, 98 were expected to match and the remaining 9,408 were expected non-matches. These values do not include an additional 490 additional verification samples which were acquired from the subjects and were used to calculate the FNMR only for expected matches.

iBeta obtained the Age (Table 6-1), Gender (Table 6-2), Ethnicity (Table 6-3), and Eye Color (Table 6-4) demographics reported below.

Table 6-1 Age Demographics

Age (Years)	Count	Percentage
<18	0	0.0%
18 – 35	49	50%
36 – 52	21	21.43%
53 - 70	28	28.57%
70>	0	0.0%

Table 6-2 Gender Demographics

Gender	Count	Percentage
Male	52	53.06%
Female	46	49.94%
Undisclosed	0	0.0%

Table 6-3 Ethnicity Demographics

	Count	Percentage
White	60	61.22%
Asian	14	14.29%
Hispanic	16	16.33%
African American	7	7.14%
Other Native American	1	1.02%

Table 6-4 Eye Color Demographics

Eye Color	Count	Percentage
Brown	51	52.04%
Hazel	18	18.37%
Blue	16	16.33%
Green	6	6.12%
Blue/Green	3	3.06%
Gray	2	2.04%
Green/Gray	1	1.02%
Light Blue/Green	1	1.02%

6.3.1 Exceptions

The EyeLock 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 6-3 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 application 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	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.	☑

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
	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.	The system captures the iris which is 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 is used to issue electronic prescriptions for controlled substances.	The biometric device is expected to be co-located 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. EyeLock provides the ability to output this information.	☑
1311.116(g)	The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be: (1) Cryptographically source authenticated; (2) Combined with a random challenge, a nonce, or a time stamp to prevent replay; (3) Cryptographically protected for integrity and confidentiality; and (4) Sent only to authorized systems.	Authentication is local in that the enrollment or reference records reside in a folder on the device. Depending on the implementation and integration into a larger health records systems, the storage of records, match results, and/or non-match results may be not be local; therefore, these regulations may apply. This requirement may need to be fully tested in the overall system.	☐

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
1311.116(h)	Testing of the biometric subsystem must have the following characteristics: (1) The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric. (2) Test data are sequestered. (3) Algorithms are provided to the testing laboratory (as opposed to scores or other information). (4) The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value. (5) Results of the testing are made publicly available.	(1) iBeta is independent of EyeLock and does not have an interest in the outcome of the performance of this testing. (2) Test data were destroyed at the conclusion of testing and test data were not provided to the vendor during testing. (3) Algorithm was provided as an executable that was used during testing. (4) iBeta's process and procedures to test the FMR at 95% confidence have been approved by the DEA. (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 EyeLock Iris 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 EyeLock ID 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.	☑

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 6-3 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 6-3 for details.
(g) The tested biometric subsystem has the capability to meet this requirement especially when operated locally. See Table 6-3 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 EyeLock Core Demo App 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:

Gail Audette
iBeta Quality Assurance Director of Biometrics
GAudette@ibeta.com
303.627.1110 extension 182