Lumidigm V-Series Fingerprint Sensors

DEA EPCS Biometric Subsystem Certification Test Report

Prepared for:
Lumidigm, Inc.
801 University Blvd SE, Ste 302
Albuquerque, NM 87106

Version 2.0
05 August 2013
Report #130725-iBetaBTR-v2.0

Trace to Standards
21 CFR Part 1311.116

Test Results in this report apply to the biometric subsystem configuration tested. Testing of biometric subsystems 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:
August–05–2013

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

Date of expiration:
August-05-2015

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

Version History				
Ver #	Description of Change	Author	Approved by	Date
v1.0	Initial Draft Certification Report for V-Series	Dr. Kevin Wilson	Gail Audette	25 July 2013
v2.0	Final Certification Report for V-Series	Gail Audette	Dr. Kevin Wilson	05 August 2013

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 V3xx Series from Lumidigm, Inc. The biometric subsystem was validated and certified against the applicable requirements of 21 CFR Part 1311.116 for its inclusion as a built-in subsystem into an Electronic Prescription of Controlled Substances System (EPCS).

The Lumidigm V3xx Series 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.

The Lumidigm V3xx Series biometric subsystem is a single-finger impression device. iBeta tested and certified the built-in matching algorithm.

The Lumidigm V3xx Series consists of the following devices. Devices not listed are not subject to this certification.

Table 1-1 Devices in the V3xx Series Certified

Device/Model
V311-00
V310-00
V300-02
V302-02

For the False Match Rate requirement of 0.001 or lower as cited in 1311.116(b), iBeta found an operating point threshold of 25,501 or greater corresponding to this requirement.

iBeta tested both the 32-bit and 64-bit versions of the API used to interface to a V3xx Series devices. The results of the testing for both versions were identical.

The Lumidigm V3xx Series biometric subsystem was tested to the DEA EPCS regulations within 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 Lumidigm, Inc. This report will be maintained on the iBeta website during the period of certification from the issuance of this report (xx July 2013) through the certification expiration date of (xx July 2015).

1.1 *Biometric Subsystem Identification*

The Lumidigm V3xx Series Fingerprint Sensor and core acquisition components are described in Sections 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric Subsystem Test Environment. Three V311 devices were received by iBeta on 14 May 2013 and the Software Development Kit (SDK) installs were downloaded from Lumidigm on 16 May 2013.

Additional devices were received on 16-Jul-2013 (V310) and 20-Jul-2013 (V302 and V300). The non-streaming drivers were downloaded from Lumidigm on 17-Jul-2013.

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 http://www.ibeta.com/our-services/biometrics/epcs/reports/.

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 includes:
- Technology Test data used to determine the operating point and 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 addressed the testing of the Lumidigm V311fingerprint sensor to the 21 CFR 1311.116 regulations. The results were generalized to the V3xx Series by rerunning the FMR tests on those devices and validating that the optical subsystem of each device in the series is equivalent to the V311. The V311 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 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 Copernicus Group Independent Review Board (CGIRB) reviewed iBeta DEA-EPCS Biometric Test Protocol application and granted unconditional approval on 14 June 2013 (approval: IBE-113-187) for the following:
- Protocol Version 1.0 dated 21 May 2013
- 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 (Form A)

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 Documents

Version #	Title	Abbreviation	Date	Author (Org.)
	Mutual Confidential Disclosure Agreement	NDA	April 04, 2013	iBeta Quality Assurance
03	Agreement for EPCS Pre-Certification and Certification Testing Services	MSA	May 06, 2013	iBeta Quality Assurance
iBeta ITL Procedures				
1.0	Biometric Deliverable Receipt Procedure		6/1/11	iBeta Quality Assurance
3.0	Biometric Security Procedure		5/20/13	iBeta Quality Assurance
1.0	Biometrics Configuration Management Procedure		6/9/11	iBeta Quality Assurance
4.0	DEA-EPCS Biometric Assessment Procedure		21 May 2013	iBeta Quality Assurance
1.0	Biometric Training and Training Records Procedure		6/1/11	iBeta Quality Assurance
iBeta Project Documents				
	DEA-EPCS-Biometric-		5/15/13	iBeta Quality Assurance

Version #	Title	Abbreviation	Date	Author (Org.)
	Assessment-Lumidigm			
1.0	Lumidigm V311 DEA EPCS Pre-Certification Test Letter		5/17/13	iBeta Quality Assurance
1.0	DEA-EPCS Technology Checklist-Lumidigm V311		6/14/13	iBeta Quality Assurance
	DEA-EPCS-TC-21 CFR 1311.116-Lumidigm V311		6/12/13	iBeta Quality Assurance
	Document and Equipment Receipt Lumidigm		7/24/13	iBeta Quality Assurance
	Drawing Review for V-Series Lumidigm		7/24/13	iBeta Quality Assurance

2.2 *External Documentation*

The documents identified below are external resources used in this 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

2.3 *Technical Documents*

The Technical Documents submitted by Lumidigm Inc. 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.

130725-iBetaBTR-v2.0

- 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 5.

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 Lumidigm V3xx Series included a matching threshold to provide 0.001 False Match Rate (FMR) 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 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 Image Discrimination	BID	The statistical analysis 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
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.
Copernicus Group Independent Review	CGIRB Copernicus Group	An independent institutional review board, ensuring the rights and welfare of research study

Term	Abbreviation	Definition
Board	IRB	participants
Drug Enforcement Agency	DEA	The rate at which an impostor's biometric is falsely accepted as being that of an authorized user. It is one of the statistics used to measure biometric performance when operating in the verification or authentication task. The false match rate is similar to the false accept (or acceptance) rate.
Detection Error Trade-off	DET	A graphical plot of error rates for binary classification systems, plotting false reject rate vs. false accept rate
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 (govern 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.
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

Term	Abbreviation	Definition
		records; education; financial transactions; medical history; criminal or employment history; and information which can be used to distinguish or trace an individual's identity
PDF file	PDF	File format for all releases of the Report
Software Development Kit	SDK	Set of software development tools which allows for the creation of application for a software package
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*

During the test execution and subsystem certification effort, weekly status reports were sent to the Lumidigm certification management staff. These reports included project activity status, issues, and other relevant information.

3.2.1 Definition of Test Criteria

The test criteria determined the configuration and test cases for execution. The Lumidigm V311 fingerprint sensor configuration was established in collaboration with the vendor. For technology testing, the Lumidigm V3xx Series fingerprint sensor configuration was established in collaboration with the vendor.

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

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

3.2.2 Test Environment Setup

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

For device communications, the Lumidigm V3xx Series Fingerprint Reader device driver version 3.4.2.0 (10/8/2010) was installed on a test computer using LumiDvcSvc_4.50 as listed in Table 4-2.
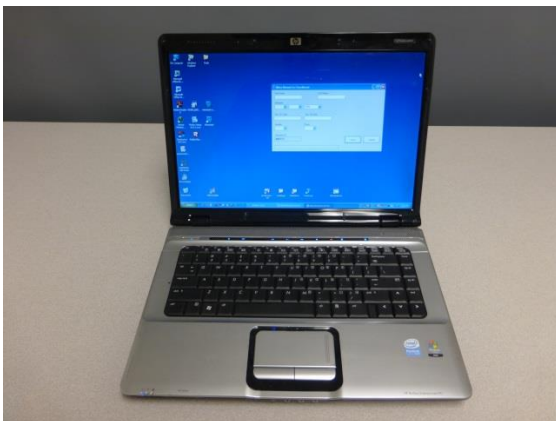
Biographical Enrollment

Biometric Acquire

Subjects were enrolled using iBetaBioEnroll (Table 4-4) which incorporated the Lumidigm SDK 4.50.31 as listed in Table 4-2. This test tool version was validated on 10 June 2013 by completing a dry run of the subject enrollment process and verifying the results manually. iBeta utilized C# and the Lumidigm supplied C# demo interface SDKBiometrics and SDKWrapper for this and other interfacing software.

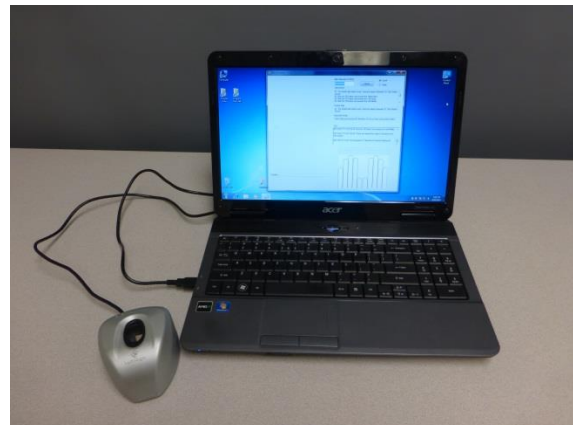Also as listed in Table 4-4, the technology test utilized iBetaBioAcqLd (32-bit) and iBetaBioAcqLd64 (64-bit), which were built from the Lumidigm SDK 4.50.31 (Table 4-2). This test tool version was validated on 10 June 2013 by acquiring seven sets of data and verifying the data collection. The as-run technology test and source code have been archived on a secure repository server.

The Technology Test was implemented using Lumidigm's demo that emulates a 3rd Party authentication system. iBeta assessed the demo for use in the Technology Testing and Lumidigm provided source code for the demo as specified in Table 4-2.

An encrypted database was created using TrueCrypt as listed in Table 4-6. The database of 156 biometric data sets (consisting of 2 biometric samples per individual) was used in the technology testing. Of these 156 sets, 78 were enrolled into the system using the 1st sample in the set. The 2nd sample was used as a challenge. A total of 3081 sets of challenges were made for the 78 enrolled subjects. Of those, 78 were expected to match and 3003 were expected to not match.

The Lumidigm V311 produced a similarity score for each attempted matching. The simulated overall system was configured to reject an authentication attempt if the similarity score did not exceed the threshold. Therefore, using the reported similarity index, iBeta calculated whether the system would match the challenge at that operating point. Over a series of simulated operating points, and based on this calculation, 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 per operating point 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.

$$FMR = \frac{\sum_{i=1}^{N} fm_i}{N} \hspace{3cm} (3.2.3-1)$$

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 or threshold 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).

Table 3-2 Claimed versus Measured Error Rates

N * Observed Error Rate	N * Claimed Error Rate	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 following code from the V311 API.

```
LumiQueryNumberDevices(ref nNumDevices, _ipAddress);
LumiQueryDevice(0, ref dev);
LumiInit(dev.hDevHandle, ref tmpHandle);
LumiGetConfig(_hHandle, ref config);
...
LumiCaptureEx(_hHandle, pImage, pTemplate1, ref tlen, ref nSpoof, null);
```

Although pImage was captured, iBeta did not use pImage in any further testing.

The subject templates were tested using the following code from the V3xx Series API. The matching score for the challenge was output to a csv (comma separated values) file which could be read by MS Excel. A

```
LumiQueryNumberDevices(ref nNumDevices, _ipAddress);
LumiQueryDevice(0, ref dev);
LumiInit(dev.hDevHandle, ref tmpHandle);
LumiGetConfig(_hHandle, ref config);
...
LumiCaptureEx(_hHandle, pImage, pTemplate2, ref tlen, ref nSpoof, null);
…
LumiMatch(_hHandle, pTemplate1, ref plen, pTemplate2, ref elen, ref nMatchScore, ref nSpoofScore);
```

program cycled through a set of possible threshold values that produced error rates in the range of below 0.001 to 0.008. A Detection Error Trade-off (DET) plot of a subset of the results is shown in Attachment 1 (not publicly available). By inspection, iBeta could determine the threshold required to produce a 95% Confidence Interval for an FMR of 0.001.

In the above code, the nSpoofScore was not used by iBeta because that score is not relevant to the FMR of the device. However, this certification does not prevent the use of that score in an installed system to further restrict an attempted authentication as long as the matching score threshold is met.

As described above, the technology test was repeated for each of the other models in the series. The FMR was calculated with 95% confidence interval.
The configuration returned by the V311 and V310 devices is shown below. In general, this is the default configuration of the device and API.

```
Version Info SDK(4500) FW(15330) PROC(6000) CONF(61)
*** Device Caps ***
bImageCapture:          1
bExtract:               1
bMatch:                 1
bIdentify:                        0
bSpoof:                 1
eTemplate:              CONF_TPL_ANSI378
eTransInfo:             5
Width:                  352
Height:                 544
DPI:                    500
Image Format:           0
eProcessLocation:       LUMI_PROCESS_SENSOR
Width: 352 Height: 544
BPP: 8 DPI: 500
```

The configuration returned by the V302 and V300 devices is shown below. As described above, this is the default configuration of the device and API.

```
Version Info SDK(4500) FW(9538) PROC(6000) CONF(60)
[2013-07-22T11:06:45] *** Device Caps ***
bImageCapture:          1
bExtract:               1
bMatch:                 1
bIdentify:                          0
bSpoof:                 1
eTemplate:              CONF_TPL_ANSI378
eTransInfo:             5
Width:                  352
Height:                 544
DPI:                    500
Image Format:           0
eProcessLocation:       LUMI_PROCESS_PC
Width: 352 Height: 544
BPP: 8 DPI: 500
```

Notice that the configurations differ by the following:
- The V31x has firmware FW(15330), whereas the V30x has firmware FW(9538).
- V31x performs matching on the sensor, LUMI_PROCESS_SENSOR, but the V30x performs matching in the API, LUMI_PROCESS_PC.

3.2.3 Document and Drawing Review

iBeta reviewed the configuration controlled engineering drawings, bill of materials, and Engineering Change Request (ECR) provided by Lumidigm to assess that the V300, V302, and V310 contain the same assembly or sub-assembly as the V311 that was utilized for the biometric acquisition. The list of documents review is contained in Table 4-6. iBeta concluded that the V3xx device series is technically identical as the devices have identical optical and mechanical construction, use the same APIs, and contain the same code base for biometrics. Based on this assessment, iBeta was able to proceed with the execution of the technology test on the V300, V302, and V310 devices with the same database of V311 acquired fingerprints.

3.2.4 Test Execution

For the baseline device, the V311, test enrollment and execution was conducted during the June 12 through 21, 2013 timeframe and the results are listed in Attachment 1.

Additional devices, V311, V310, V302, and V300, were tested during the period July 17 through July 21, 2013.

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 Copernicus Group Independent Review Board on 14 June 2013, approval: IBE-113-187.

Subject biographical data was acquired on a stand-alone laptop (separate from the biometric data laptop) as described in Table 4-3 using iBetaBioEnroll testing software as described in Table 4-4. Only an identifier, the Biometric ID (BID), connected the subject biographical data to the acquired biometric data. As of the publication of this report the biographical data collected for this study has been destroyed.

A USB flash drive was used to transfer the encrypted biometric data to the Technology Testing computer as per iBeta security procedures. iBeta simulated enrolling each user into the system using the acquired enrollment records. A Failure to Enroll Rate not to exceed 15% was assumed. There were no subjects that failed to enroll. Acquisition of Technology Testing corpus data was acquired in an office type of environment consistent with the expected environment for prescribing practitioners.

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.

During this test effort, iBeta experienced no Failure to Acquire (FTA) instances using the maximum of 4 attempts as specified by NIST SP800-76-1 standards.

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

3.2.4.1 *Deviations and Exclusions*

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 Biometric Subsystem Identification

The Biometric Subsystem Identification documents the Lumidigm V3xx Series fingerprint sensor submitted for certification and the hardware, software and the documentation utilized during the certification test effort.

4.1 *Submitted Biometric Subsystem Identification*

Table 4-1 contains the elements of the LUMI_VERSION, sdkVersion, fwrVersion, prcVersion, and tnsVersion. Table 4-1 shows the values as they are formatted by Lumidigm sample code.

The models submitted and certified in this report capture and process an 8-bit grayscale image of 352 x 544 pixels (Width x Height). Because the image size processed into a template could affect the FMR, no other image size devices were certified.

Table 4-1 Biometric Subsystem Name

Biometric Subsystem Name	Version
Lumidigm V311 Fingerprint Sensor	SDK(4500) FW(15330) PROC(6000) CONF(61)
Lumidigm V310 Fingerprint Sensor	SDK(4500) FW(15330) PROC(6000) CONF(61)
Lumidigm V300 Fingerprint Sensor	SDK(4500) FW(9538) PROC(6000) CONF(60)
Lumidigm V302 Fingerprint Sensor	SDK(4500) FW(9538) PROC(6000) CONF(60)

Table 4-2 Models in the V3xx series

Device Model		Description
V311-00	Streaming	Matching and all image processing occur on the device
V310-00	Streaming	OEM version of V311, no skin
V300-02	Embedded	Raw images are formatted on the device, final image processing and matching occur on the PC
V302-02	Embedded	OEM version of V300, no skin

Table 4-3 Biometric Subsystem Software

Software Applications	Version	Function Description
LumiSDKSetup_4.50.31	4.50.31	32-bit SDK Application
LumiSDKSetup_x64_4.50.31	4.50.31	64-bit SDK Application
LumiDemoSetup_4.50.31	4.50.31	32-bit Demo SDK Application
LumiDemoSetup_x64_4.50.31	4.50.31	64-bit Demo SDK Application
LumiDvcSvc_4.50	4.50.31	V3xx Series device Service driver (version 3.4.2.0) LumiDeviceService Windows Installation 4.50.31
LumiDvcSvcDeployment_4.50	4.50.31	Silent install of V3xx Series device Service driver (version 3.4.2.0) LumiDeviceService Windows Installation 4.50.31
Lumi_NON_STR_Drivers_Setup_4.50	4.50	Installs additional device drivers for V300 and V302 non-streaming devices.

The V3xx devices interfaced to Microsoft Windows PC's through a wired USB interface.

Appendix A contains the MD5 and SHA-160 hash of the certified V3xx API and their install programs.

4.2 *Biometric Subsystem Test Environment*

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

iBeta enrolled all subjects using the V311 sensor. The technology portion of the test was performed using each sensor attached to a 32-bit OS and 64-bit OS as described in Table 4-4.

Table 4-4 Biometric Subsystem Test Hardware

Hardware	Module (model)	OS or Version	Manufacturer	Description (including functional purpose)
Lumidigm Test Hardware				
Lumidigm V311-00	001155C	SN 009155	Lumidigm	Biometric fingerprint sensor for acquisitions, and Technology Testing in 32 and 64-bit architectures
Lumidigm V311-00	001155C	SN 011820	Lumidigm	Biometric fingerprint sensor for use in iBeta CTS development
Lumidigm V311-00	001155C	SN 008919	Lumidigm	Biometric fingerprint sensor for enrollment in 32-bit architecture
Lumidigm V311-00	001155C	SN 003792	Lumidgm	Biometric Technology Testing in 32 and 64-bit architectures
Lumidigm V310-00	001155A	SN 002338	Lumidigm	Used in technology testing (FMR) as a sample device type
Lumidigm V300-02	000790J	SN 139309	Lumidigm	Used in technology testing (FMR) as a sample device type
Lumidigm V302-02	000790J	SN 060433	Lumidigm	Used in technology testing (FMR) as a sample device type
iBeta Test Hardware				
PC: Laptop Pavilion DV6000 Intel 1.60 GHz; 760 MB RAM		Windows XP Pro SP3 32-bit	Hewlet-Packard	COTS System for subject biographical check-in with mounted TrueCrypt encrypted 2GB database volume
PC: Laptop Aspire AMD Athlon 2.00 GHz; 3 GB RAM		Windows 7 Home Premium SP1 64-bit	Acer	COTS System to test 64-bit Lumidigm SDK v4.50 with Lumidigm V3xx fingerprint scanners with mounted TrueCrypt encrypted 2GB database volume
HP Compaq DC7800P Intel Core2 2.33GHz; 2.00 GB RAM		Windows 7 Home Premium SP1 32-bit	Hewlet-Packard	COTS System for subject enrollment of biographical data with mounted TrueCrypt encrypted 1GB database volume

Table 4-5 Biometric Subsystem Test Software

Software	Version	Manufacturer	Identify Hardware
iBetaBioEnroll	0.1	iBeta (built using Lumidigm SDK 4.50.31 32-bit API)	Subject enrollment on Pavilion DV6000
iBetaBioAcqLd64	0.4	iBeta (built using Lumidigm SDK 4.50.31 64-bit API)	Subject fingerprint acquirement on AMD Athlon
LdXRef	0.6	iBeta (built using Lumidigm SDK 4.50.31 32-bit API)	Technology Test on HP Compaq DC7800P
LdXRef64	0.6	iBeta (built using Lumidigm SDK 4.50.31 64-bit API)	Technology Test on AMD Athlon

Table 4-6 Biometric Subsystem Technical Documents

Version #	Title	Abbreviation	Date	Author (Org.)
4.50	Interoperability API	Lumidigm InOpAPI v4.50	04/23/2013	Lumidigm, Inc.
4.50	Lumidigm Framework Matrix	Lumidigm Framework Matrix v4.50	None	Lumidigm, Inc.
4.50	Software Development Kit	Lumidigm SDK v4.50	03/19/2013	Lumidigm, Inc.
4.50	Install Guide for SDK and Demo Release 4.50	Lumidigm Install Guide v4.50	None	Lumidigm, Inc.
4.50	Lumidigm User Configuration Manager v4.50	Lumidigm User Config Manager v4.50	None	Lumidigm, Inc.
4.50	V-Series Biometric Performance and Thresholds	Lumidigm Biometric Performance 4.50 - V-Series	None	Lumidigm, Inc.
4.50	Demo Documentation	Lumidigm Demo v4.50	None	Lumidigm, Inc.
4.50	Lumidigm Drivers Install Guide v4.50.pdf	Lumidigm Drivers Install Guide v4.50	2013	Lumidigm, Inc.
4.50	Lumidigm Non-Stream Drivers	Lumi_NON_STR_Drivers_Setup_4.50	None	Lumidigm, Inc.
1.7	Lumidigm V-Series Fingerprint Sensor Specification	Lumidigm_V-Series_Specs_1.7	None	Lumidigm, Inc
1.11	Lumidigm V-Series Multispectral Fingerprint Sensors	Lumidigm_V-Series_Sensors_Datasheet_v1.11	None	Lumidigm, Inc.
C	000790-DWG Venus OEM Assembly	000790C-DWG.pdf	6/27/2012	Lumidigm, Inc.
J	000790-BOM Venus Gen 2 Cam Brd w Lens	000790J-BOM.pdf	6/19/2012	Lumidigm, Inc.
C	000792-DWG Venus IP65 Assembly Gen 2	000792C-DWG.pdf	5/9/2012	Lumidigm, Inc.
J	000792-BOM Venus IP65 Assy with Gen2 Cam Brd	000792J-BOM.pdf	6/29/2012	Lumidigm, Inc.
H	000801-BOM Venus Gen2 Cam Brd w Lens Assy	000801H-BOM.pdf	6/29/2012	Lumidigm, Inc.
C	001154-BOM V31X Camera Brd w Lens	001154C-BOM.pdf	3/14/2013	Lumidigm, Inc.
B	001155-DWG V31X OEM Assembly	001155B-DWG.pdf	6/28/2012	Lumidigm, Inc.
D	001155-BOM V31X OEM Assembly	001155D-BOM.pdf	3/14/2013	Lumidigm, Inc.
A	001229-DWG V31X IP65 Assembly	001229A-DWG.pdf	3/8/2011	Lumidigm, Inc.
D	001229-BOM V311 IP65 Assy	001229D-BOM.pdf	3/14/2013	Lumidigm, Inc.
FRM0001 Rev 02	Engineering Change Request (ECR) 158	ECR #158 scan.pdf	3/8/2013	Lumidigm, Inc.
F	000900-BOM Assembly, Venus Top Half w Conn	000900F-BOM.pdf	6/29/2012	Lumidigm, Inc.
B	001153-BOM V31X Camera Board	001153B-BOM.pdf	5/23/2013	Lumidigm, Inc.
H	000761-BOM PWA Camera Board Gen2	00761H-BOM.pdf	2/18/2011	Lumidigm, Inc.

Table 4-7 Other Software, Hardware and Materials

Material	Material Description	Use in the Biometric Subsystem
Hand sanitizer	COTS Hand sanitizer	Subject hand cleaning (COTS)
Alcohol swabs	COTS Alcohol swabs	Platen cleaning (COTS)
Microfiber Cloth	COTS Microfiber Cloth	Platen cleaning (COTS)

Material	Material Description	Use in the Biometric Subsystem
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
Microsoft Visual Studio 2008 Version 9.0.21022.8 RTM	Build and source code Integrated Development Environment	Supplied by iBeta: View source code
Beyond Compare 2 v.2.4.3 (Scooter Software)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
Hash.exe v.7.08.10.07.12 (Maresware)	Hash creation utility	Supplied by iBeta: used to generate hash signatures for files/data
TrueCrypt	Encryption software for encrypting subject PII biometric data.	Supplied by iBeta: open-source disk encryption software http://www.truecrypt.org
Sysinternals SDelete v1.61	Subject PII biometric data logical shredding utility	Supplied by iBeta: used to destroy biometric PII data as per iBeta security procedures http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

4.2.1 Biometrics Test Environment – Technology Test

The seven devices listed in Table 4-4 indicate their functional purpose in the test effort. All seven devices were used for test coverage. The V311 S/N 003792 was not tested on the 64-bit operating system.

Technology testing interface LdXRef (32-bit) and LdXRef64 (64-bit) was created by iBeta with the use of Lumidigm SDK 4.50.31 API. The testing interface consisted of using the Lumidigm V3xx device service driver v4.50 for device communications.

The V300 and V302 devices require additional non-streaming drivers (Lumi_NON_STR_Drivers_Setup_4.50). These drivers are not necessary and were not installed for some V311 devices tested. The setup program contains both the 32-bit and 64-bit drivers.

4.2.1.1 *Processing and Post-processing*

After enrollment was completed, the iBeta CTS challenged the biometric subsystem with biometric data, processing and post-processing to produce data analysis spreadsheets and log files.

5 Biometric Subsystem Overview

The Lumidigm V3xx consists of a fingerprint sensor based on Lumidigm's multispectral imaging technology and is designed for use in a wide range of products and applications including automated teller machines (ATM), access control terminals, civil identity applications, logical access in healthcare and banking, and time and attendance terminals.

System functions:
- 0.7" x 1.1" ellipse platen
- Dynamic presence detection

- Multispectral imaging
- Image processing
- Image output
- Liveness detection
- Continuous scan for a properly placed finger
- Produces 500 dpi (352 x 544 pixels) ANSI 381 image and a spoof score
- ANSI-INCITS 381 image format
- Image can be passed to any extraction/matching fingerprint algorithm for further processing and authentication – not certified functionality
- Supported: USB 2.0, RS-232
- ANSI 378 / MINEX-certified biometric templates
- ANSI-INCITS 378 and ISO/IEC 19794-2:2005 template format
- USB 2.0 (480 Mbps) interface

Biometric matching functions:
- Feature extraction
- Biometric template generation
- 1:1 matching or verification with template storage (up to 1,000 users)
- 1:N identification (up to groups of 10,000 fingers) on V31X – not certified functionality
- Image bit depth: 8bit, 256 grayscale
- MINEX certified

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 Lumidigm to provide iBeta with systems and devices 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 V3xx Series operate in a built-in mode in that the device is connected by a wire. The interface is an API which depends on the EPCS system to meet the DEA regulations for both physical and logical security.

The V3xx Series was tested in verification mode (1:1), which is the only mode applicable to the DEA EPCS regulations. Operation in identification mode was not certified. Verification mode means that the V3xx returns a matching score against a single other fingerprint template that is associated with the identity claimed.

The scope of this iBeta report and certification is solely for the Lumidigm V3xx Series biometric subsystem as listed in Table 1-1. The evaluation and testing certifies that the Lumidigm V3xx Series 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 **Lumidigm V3xx Series Component Results**

There were neither deviations from the DEA approved test method nor any test setup that varied from the standard protocol. The results for all devices tested were identical, so only the V311 results are reported in detail in Amendment-1 (not publicly available) to this report.

Regardless of where the matching was performed, LUMI_PROCESS_SENSOR or LUMI_PROCESS_PC, the API would not initialize and therefore could not perform a LumiMatch operation unless a device was attached to the PC and the appropriate drivers had been installed.

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 3,081 attempted matches of 78 enrolled subjects.

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

Table 6-1 Age Demographics

Age (Years)	Count	Percentage
<18	0	0.0%
18 - 30	21	26.9%
31 - 50	36	46.2%
51 - 70	21	26.9%
70>	0	0.0%

Table 6-2 Gender Demographics

Gender	Count	Percentage
Male	44	56.4%
Female	34	43.6%
Undisclosed	0	0.0%

iBeta found that at an operating point of 25,501 or above, the biometric subsystem meets or exceeds an FMR of 0.001 with a 95% confidence interval.

In other words, the API method, LumiMatch, when provided a challenge fingerprint, pProbeTemplate, and an enrolled template, pGalleryTemplate, returns a score, nScore. The enclosing EPCS system must validate that the returned score, nScore, is equal to or exceeds 25,501.

6.3.1 **Exceptions**

The Lumidigm V3xx Series 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.

7 Opinions and Recommendations

7.1 *Recommendations*

iBeta Quality Assurance has completed the testing of the Lumidigm V3xx Series 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 Lumidigm V3xx Series fingerprint sensor 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.

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).	☑
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

(b) This requirement is met only if the overall system uses a threshold of 25501 or greater to implement the verification of a single practitioner.

(c) iBeta is a DEA-approved laboratory for testing and EPCS Biometric subsystem.

(e) The tested biometric subsystem has the capability to meet this requirement but it must be tested for the overall system.

(f) The tested biometric subsystem has the capability to meet this requirement, but it must be implemented and tested for the overall system. The API call LumiQueryDevice returns a LUMI_DEVICE structure which contains a string, strIdentifier. This string is unique to a device. The first two characters of the string correspond to the Product ID of the device (33 in the case of the V311) and the remaining 5 characters of the string correspond to the Serial Number, S/N, that is also printed on the bottom of the device. A typical strIdentifier for each model device is given in Table 7-2.

Table 7-2 A typical LumiQueryDevice strIdentifier

Device Model	strIdentifier returned by LumiQueryDevice
V311	333792
V310	332338
V300	13348139309
V302	1334860433

(g) The tested biometric subsystem is capable of performing the match to an enrolled template locally and was tested in this configuration. The overall system implementation must be tested to verify that this requirement is met or is not applicable.

(h) iBeta's processes and procedures for certifying a biometric subsystem have been approved by the DEA-EPCS and iBeta affirms that these requirements were met during testing.

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 or such devices configured to acquire image sizes other than 352 x 544.

7.1.2 Exceptions

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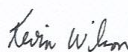
7.2 *Opinions*

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

The Lumidigm V3xx Series fingerprint sensors operated as expected.

7.3 *Responsible Test Laboratory Personnel*

The contact information for the Copernicus Group IRB appointed Principal Investigator for this test effort:

Dr. Kevin Wilson
Director of Biometrics
kwilson at ibeta.com
303-627-1110 extension 177

Kevin Wilson Ph.D.
Director of Biometrics

Appendix A: SHA hash of certified Lumidigm V3xx Series API

MD5 and SHA-160 hash of certified V3xx Series API

PATH	MD5	SHA-160	SIZE
Lumidigm\x64\plugin\AlgoDvc.dll	9CB2A1D8B6AA90D48B22C51C10808916	509DCA49F50CA969E93DB55203A056070B1F8ECE	164352
Lumidigm\x64\plugin\IEngine_Plus.dll	A9EA1EB31BD8059B159D0B7D1382A5D5	BBE24AACDA10FC728FB196A06628177949E69F63	119296
Lumidigm\x64\plugin\MercuryDvc.dll	7C2A80D372A48CC28495F94DC6363EF1	1508DBC2FD7E4A28A79E960BA69D5FB38CAE6E03	286208
Lumidigm\x64\plugin\PreProcV31_INT16.dll	79F2761B7F8DC7129F26CE531E1180A2	34A53C1438F87A53A005B3ABDEB36675B576F4E3	380928
Lumidigm\x64\plugin\SDvc.dll	790B70013AFE6DAD3C0BA77EF46CAAA4	56C016F4A35A88C8C8219882812846D07813C251	229376
Lumidigm\x64\plugin\VenusDvc.dll	F66D5EA8727A2FC50C2D71BB19D31417	481C6D8D50646274CCE194B5F88F6B1F0F154979	302592
Lumidigm\x64\SPM\eSPM_1.bin	67AD7406183A8702BAED739D51E3191C	758A2E117237CF3D561227F2203B1BDB9A381699	4076
Lumidigm\x64\LumiAPI.dll	5BADCB12E155DD5C0192827D5D64212D	B46C707DEB45D5CD9520108F2E5371CF675056A3	44032
Lumidigm\x64\LumiCore.dll	03D23A4BD171BE40043060DCA4440C93	1A79E530FED65CE8DC2582EE64BC690F5BB9094B	145920
Lumidigm\x64\LumiInOpAPI.dll	6B1C8AD24C5C9578A662C6A78965C140	18A9922304A626349F12664243B4E5D2978CB86A	381952
Lumidigm\x86\plugin\AlgoDvc.dll	A214AF9B6A6CC5E7DDBCD613A0ED4828	6F7556398EA805B79E280229EEA502A8D3406179	155648
Lumidigm\x86\plugin\IEngine_Plus.dll	1F82DF48A57951606A5459F0B105169E	7DB1E113268ABBB34048876EA8F8DD957E8C0C58	106496
Lumidigm\x86\plugin\MercuryDvc.dll	EE07A5EDCF570C950AA0E5538F1E396E	1E889F4FD3D90CE1C0E358ECEAC80120EAE57A42	192512
Lumidigm\x86\plugin\PreProcV31_INT16.dll	287E1673F6A520E5C3698DC905388C01	DA6BC690997AE136870D4B5AA0C4D3EF61D1E9D4	303104
Lumidigm\x86\plugin\SDvc.dll	EDA673D5433CD8DCC0F911412174AFEE	4706FB70BD861735C7D02EAC4FFB496C7A262855	229376
Lumidigm\x86\plugin\VenusDvc.dll	7B19AED346883D15126354039A289058	949FD8A9EC8D7DE4391C2AB6A02004F298413F01	204800
Lumidigm\x86\SPM\eSPM_1.bin	67AD7406183A8702BAED739D51E3191C	758A2E117237CF3D561227F2203B1BDB9A381699	4076
Lumidigm\x86\LumiAPI.dll	E33B77F0A986CC2331B24865F148264E	C50FF5056AFA3F14690FE3B264018277B943C6E7	28160
Lumidigm\x86\LumiCore.dll	70A62A73C3ABCD05AFAB684F4EF9EDB7	561A55153930AE4DEF9B59E822B3BC040E724D9B	98304
Lumidigm\x86\LumiInOpAPI.dll	0EEA476CC65F83A849E9268983BC0CE5	052233452E0DC3281E8759C979D6DA2C793835D6	413696

MD5 and SHA-160 hashes of Lumidigm API Installers

PATH	MD5	SHA-160	SIZE
32bit\LumiDemoSetup_4.50.31.exe	E1C15F6419E859980385DA818532C39D	412913FBBC7E49CF96373EFC29132BE861E1EB26	13750188
32bit\LumiSDKSetup_4.50.31.exe	460C9F01DCE6487C5A0FDFA4BCAAA672	A3E902F16B175B8B76564A96EFBC138326F9BCD8	11449243
64bit\LumiDemoSetup_x64_4.50.31.exe	9C71CE183DA67E9572D8329A0426759C	AD1EC62289A54673B89E2E7EE80F4C17E0EF1147	14279094
64bit\LumiSDKSetup_x64_4.50.31.exe	F0B1D76F634F0D074DD118730FCF420A	B36864645511DA8A5DE7EBCE7BCD0094FA8E08C4	11032272
LumiDeviceService Windows Installation.zip	181F2630B342C0F65DA0502524223608	8BEF59F42BE3CDF1858A6564CA7EAF6EA0389FF6	57909188
Lumi_NON_STR_Drivers_Setup_4.50.exe	D7BB27E41A7FBE1EB988A3EF44C4CA7B	6B3E4DC560CCD4C21147DE14FB0FE8A3BF17B623	4577283