

**Biometric Authentication
Reader Approval Procedure**
VERSION 4.0.0

April Giles
Nabil Ghadiali



FIPS 201 EVALUATION PROGRAM

April 15, 2010

Office of Governmentwide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	7/9/2008	Document creation	Public
Approved	2.0.0	5/15/2009	Requirement R-BIO-A.20 updated along with the approval mechanism	Public
Approved	3.0.0	01/26/2009	Updated the procedure to be consistent with the Biometric Authentication System category. Updated R-BIO-A.20 requirement and vendor documentation requirement	Public
Approved	4.0.0	04/15/10	Included support for key size and algorithm support based on SP 800-78-2 for signature verification.	Public

Table of Contents

1	Introduction.....	1
1.1	Overview.....	1
1.2	Category Description	1
1.3	Purpose.....	1
2	Application Package Contents	2
2.1	Compatibility Acknowledgement	2
3	Evaluation Procedure for Biometric Authentication Reader	3
3.1	Requirements	3
3.2	Approval Mechanism Matrix.....	7
3.3	Evaluation Criteria	7
3.3.1	Vendor Test Data Report	7
3.3.1.1	R-BIO-A.3	7
3.3.1.2	R-BIO-A.4	8
3.3.1.3	R-BIO-A.5	8
3.3.1.4	R-BIO-A.6	9
3.3.1.5	R-BIO-A.7	9
3.3.1.6	R-BIO-A.12	10
3.3.1.7	R-BIO-A.13	10
3.3.1.8	R-BIO-A.14 and R-BIO-A.19.....	10
3.3.1.9	R-BIO-A.15	11
3.3.1.10	R-BIO-A.16	11
3.3.1.11	R-BIO-A.20	12
3.3.2	Vendor Documentation Review.....	12
3.3.3	Certification	13
3.3.4	Lab Test Data Report	15
3.3.5	Attestation.....	15
	Attachment A: Card/Reader Interoperability, Electronic Authentication and Security Requirements.....	17

List of Tables

Table 1 - Applicable Requirements	6
Table 2 - Approval Mechanism Matrix	7

1 Introduction

1.1 Overview

The FIPS 201 Evaluation Program (EP) is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency. The goal of the FIPS 201 Evaluation Program (EP) is to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. In addition to derived test requirements developed to test conformance to the National Institute of Standards and Technology (NIST) Standard, GSA has also established interoperability and performance metrics to further determine product suitability. A set of approval and test procedures have been developed which outline the evaluation criteria, approval mechanisms and test process employed by the Laboratory during their evaluation of a Supplier's product or service against the requirements for that category.

A Supplier submitting a Biometric Authentication Reader (hereafter referred to as the Product) for evaluation must follow the Suppliers Policies and Procedures Handbook. In addition to this handbook, the Supplier also needs to refer to this Approval Procedure which provides the necessary category-specific details in order to have a Supplier's Product evaluated by the EP and placed on the Approved Products List (APL).

1.2 Category Description

The *Biometric Authentication Reader* is a combination reader consisting of both a contact smart card reader and a fingerprint capture device. The Card Reader Biometric authenticates a PIV Cardholder by extracting one (or both) fingerprint biometric(s) stored on the card and matching it (them) with live fingerprint(s) biometric samples presented by the cardholder at the fingerprint capture device. The product also ensures the digital signature used for signing the biometric data was signed by a trusted source and is unaltered.

1.3 Purpose

The purpose of this document is to provide the following information:

- (i) Provide a list of the artifacts and/or documentation that needs to be submitted to the Evaluation Lab as part of the application package submission.
- (ii) Document the list of the requirements that apply to this category
- (iii) Specify the evaluation criteria along with their approval mechanisms that will be used by Evaluation Labs to verify compliance of the Product against the requirements that apply to this category.

2 Application Package Contents

The Application Package Contents include the artifacts, documentation and in some cases the product itself that needs to be submitted to the Evaluation Lab so that evaluation can be performed. The Application Package Contents for this category include the following:

- The Product itself. This should be delivered to the lab (address can be found at <http://fips201ep.cio.gov/labs.php>) using a reliable method of delivery that requires acknowledgement of receipt (e.g., FedEx, UPS, hand delivery).
- Completed Application Form, provided on the Evaluation Program website. (This form will be available through the web interface once users have been assigned a login credential.);
- Completed and signed Lab Service Agreement (found in the application submission package ZIP file). The Lab Service Agreement should be completed and scanned into a document to be uploaded to Evaluation Program website;
- Completed and signed Attestation Form (found in the application submission package ZIP file). The Attestation Form should be completed and scanned into a document to be uploaded to Evaluation Program website;
- Completed Supplier VDR-VTDR justification worksheet (found in the application submission package ZIP file);
- A Vendor Test Data Report, which provides test results showing that the Product complies with the requirements for this category. In this regard, the Supplier is expected to develop and document the test procedures used to determine how the Product was tested to arrive at the conclusion that it met all necessary requirements. The VTDR must typically contain information as stated in the Supplier's Handbook. Wherever possible, information to be supplied as part of this Vendor Test Data Report has been described in Section 3.3.1; and
- Official Certification documentation from the appropriate entity (e.g., NIST) showing conformance of the Product to the tested requirements of FIPS 201. Specific reference to the exact type of certification necessary can be found in Section 3.3.3.

For requirements that have an approval mechanism as Lab Test Data Report, the Supplier must be able to demonstrate product's capability of meeting these requirements from Section 3.0.

2.1 Compatibility Acknowledgement

For a Product to be submitted under this category, it needs to meet all requirements as stated in Section 3.1. However, in the event that the Supplier's Product interfaces with another product/service (specifically to meet R-BIO-A.16) to implement the required functionality, the Supplier needs to perform the following activities:

3 Evaluation Procedure for Biometric Authentication Reader

3.1 Requirements

In order to approve the Product as conformant to the requirements of PIV, it at a minimum, must comply with all the requirements listed below. The approval mechanism column describes the technique utilized by the Lab to evaluate compliance to that particular requirement.

Identifier #	Requirement Description	Source	Reqt. #	Approval Mechanism
R-BIO-A.1	Contact card readers shall conform to the ISO 7816 standard for the card-to-reader interface.	FIPS 201-1, Section 4.5.1 Para 1 pg.37	1.1-147	Vendor Documentation Review
R-BIO-A.2	{ Logical contact card } readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification for the reader-to-host system interface in general desktop computing environment.	FIPS 201-1, Section 4.5.1 Para 1 pg.37	1.1-151	Vendor Documentation Review
R-BIO-A.3	PIV readers shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.	Card /Card Reader Interoperability Requirements, Section 2.2.2.1 Para 1 pg.3	3-9	Vendor Test Data Report
R-BIO-A.4	The contact interface of the reader shall support both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997.	Card /Card Reader Interoperability Requirements, Section 2.2.2.2 Para 1 pg.3	3-10	Lab Test Data Report Vendor Test Data Report
R-BIO-A.5	PIV readers shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997	Card /Card Reader Interoperability Requirements, Section 3.2.3.1 Para 1 pg.4	3-19	Vendor Test Data Report
R-BIO-A.6	PIV Readers shall { not generate a Programming Voltage. }	Card /Card Reader Interoperability Requirements,	3-8	Vendor Test Data Report

		Section 2.1.1.1		
R-BIO-A.7	PIV Readers shall support implicit protocol and parameter selections as defined in ISO/IEC 7816-3:1997.	Card /Card Reader Interoperability Requirements, Section 2.2.2.3 Para 1 pg.1	3-11	Vendor Test Data Report
R-BIO-A.8	The reader buffer size shall be no less than 256 bytes.	Card /Card Reader Interoperability Requirements, Section 3.2.1.1 Para 1 pg.4	3-16	Vendor Documentation Review
R-BIO-A.9	{Fingerprint sensors used for PIV authentication shall conform to FBI specification (FBI PIV Spec 071006).}	Derived	10-6	Certification
R-BIO-A.10	{Devices shall be capable of imaging an area of at least 12.8 millimeters horizontally x 16.5 millimeters vertically.} The native scanning resolution of the device shall be at least 197 pixels per centimeter (500 pixels per inch) {in each direction.}	SP 800-76-1, Section 3.3 Para 2 pg.5	2.1-7	Certification
R-BIO-A.11	{Devices shall contain embedded fingerprint template generators and matchers on the device that have been certified by NIST as conformant to FIPS 201 and related documents.}	Derived	10-7	Certification
R-BIO-A.12	{The reader shall be able to read data from the CHUID buffer on the PIV Card.}	FIPS 201-1, Section 6.2.2 Para 1 pg.48	1.1-212	Vendor Test Data Report Lab Test Data Report
R-BIO-A.13	{The reader shall be able to compare the CHUID expiration date to the current date and determine card expiry.}	FIPS 201-1, Section 6.2.2 Para 1 pg.48	1.1-212	Vendor Test Data Report Lab Test Data Report

R-BIO-A.14	{ The reader shall be able to parse the FASC-N from the CHUID. }	FIPS 201-1, Section 6.2.3.1	1.1-212	Vendor Test Data Report Lab Test Data Report
R-BIO-A.15	{ The reader shall be able to provide the personal identification number (PIN) to the card to access the biometric stored on the PIV Card. }	Derived	10-8	Vendor Test Data Report
R-BIO-A.16	The digital signature on the biometric is checked {based on signature algorithms and key sizes specified in Table 3-3 of SP 800-78-2} to ensure the biometric was signed by a trusted source and is unaltered.	FIPS 201-1, Section 6.2.2 Para 1 pg.48	1.1-212	Lab Test Data Report Vendor Test Data Report Vendor Documentation Review Certification ¹
R-BIO-A.17	{ If the Product interfaces with a Certificate Validator to perform certificate path discovery and validation, it uses a GSA FIPS 201 EP approved SCVP client. }	Derived	10-9	Certification
R-BIO-A.18	{ If the intended purpose of the reader is for physical access, } then the reader shall contain an integrated PIN input device.	FIPS 201-1, Section 4.5.3 Para 1 pg.37	1.1-153	Vendor Documentation Review
R-BIO-A.19	{ The reader shall be able to extract the FASC-N in the Signed Attributes field of the biometric signature block and compare to the FASC-N found in the CHUID. }	FIPS 201-1, Section 6.2.3.1 Para 1 pg.48	1.1-213	Vendor Test Data Report Lab Test Data Report
R-BIO-A.20	One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.	FIPS 201-1, Section 6.2.3.1 Para 1 pg.48	1.1-212	Vendor Test Data Report Vendor Documentation Review

¹ This approval mechanism is necessary only if the Product internally performs path discovery and validation.

R-BIO-A.21	{For externally-facing readers ² , the reader's cryptographic module shall be FIPS 140-2 validated with an overall Security Level 2 (or higher). If not externally-facing, the reader's cryptographic module shall be FIPS 140-2 validated with an overall Security Level 1.}	Derived	10-10	Vendor Documentation Review Certification
R-BIO-A.22	The biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card (i.e. the reader performs a 1:1 biometric match).	FIPS 201-1, Section 6.2.3.1 Para 1 pg.48	1.1-213	Vendor Test Data Report Lab Test Data Report

Table 1 - Applicable Requirements

² Readers are considered to be externally-facing if they are designed for placement and use on doors that are provide entry to a building or facility. Such readers are considered more susceptible to vandalism, tampering and electrical compromise.

3.2 Approval Mechanism Matrix

The table below provides an indication of the total number of requirements applicable for the Product and identifies the approval mechanisms that will be used during the evaluation by the Lab.

Total Requirements	Approval Mechanisms					
	SV	VTDR	LTDR	VDR	C	A
22	N/A	✓	✓	✓	✓	✓
Legend: SV – Site Visit; VTDR – Vendor Test Data Report; LTDR – Lab Test Data Report; VDR – Vendor Doc. Review; C – Certification; A – Attestation						

Table 2 - Approval Mechanism Matrix

3.3 Evaluation Criteria

This section provides details on the process employed by the Lab for evaluating the Product against the requirements enumerated above.

3.3.1 Vendor Test Data Report

The Lab will update the status in the Web-Enabled Tool to “VTDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide.

3.3.1.1 R-BIO-A.3

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> PIV readers shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Populate the CHUID container with valid data on a reference smart card³ that only supports Class A operating conditions Present the Class A only reference smart card to Reader and perform a GET_DATA request for the CHUID container Output the expected CHUID data container Output the CHUID data container read from the Reader Verify that the data read from the Reader matches the expected data.
Expected Results:	The CHUID data read off the reference smart cards matches the expected data values.

³ Reference smart cards used for Supplier testing and reporting must be validated under NPIVP (<http://csrc.nist.gov/npivp/>)

3.3.1.2 R-BIO-A.4

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> The contact interface of the reader shall support both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Populate the CHUID container with valid data on a reference smart card⁴ that only supports the T=0 protocol Present T=0 reference smart card to Reader and perform a GET_DATA request for the CHUID container Output the expected CHUID data container Output the CHUID data container read from the Reader Verify that the data read from the Reader matches the expected data. Repeat steps a-e using a reference smart card that only supports the T=1 protocol.
Expected Results:	The CHUID data read off the reference smart cards matches the expected data values.

3.3.1.3 R-BIO-A.5

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> PIV readers shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997 <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> A contact reference smart card² supporting both T=0 and T=1 protocols must be used for this test. Reset the card using the reader and record the ATR value. Initiate the PPS by issuing a warm reset. Record the resulting ATR value. Change the protocol from T=0 to T=1 and the values of F and D (if possible) by issuing a correctly formatted PPS command. Record the PPS response from the card & the ATR output from the card after a successful PPS exchange. Issue any APDU to the card and output the status words. Record the APDU command resulting card response.
------------------------------	---

⁴ Reference smart cards used for Supplier testing and reporting must be validated under NPIVP (<http://csrc.nist.gov/npivp/>)

Expected Results:	<ol style="list-style-type: none"> 1. The Product can successfully change the transmission protocol from T=0 to T=1. 2. The Product can successfully change serial transmission characters F & D.
--------------------------	---

3.3.1.4 R-BIO-A.6

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • PIV Readers shall not generate a Programming Voltage. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> a. Populate the CHUID container with valid data on a reference smart card. b. Create a test harness that will allow monitoring of the V_{pp} pin of the reader/smart card c. Begin monitoring of the V_{pp} pin voltage level d. Present the reference smart card to the Reader and perform a GET_DATA on each of the containers e. End monitoring of V_{pp} pin.
Expected Results:	Results of the V_{pp} log shall show that no voltage is applied during operation of the GET_DATA command.

3.3.1.5 R-BIO-A.7

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • PIV Readers shall support implicit protocol and parameter selections as defined in ISO/IEC 7816-3:1997. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> a. A reference smart card with an implicit value for protocol and parameters (Bit 5 of interface byte TA(2) returned by ATR is 1) must be used for this test b. Reset the card using the reader and obtain an ATR value. Record the ATR value. c. Send an APDU to the card and output the status words. Record the APDU command resulting card response.
Expected Results:	The Product is able to support implicit protocol and parameters selection and communicate with a card that does not offer explicit selection.

3.3.1.6 R-BIO-A.12

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • The reader shall be able to read the CHUID buffer on the PIV Card. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> a. Perform same test scenario for R-BIO-A.4
Expected Results:	See expected test results for R-BIO-A.4

3.3.1.7 R-BIO-A.13

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • The authentication process compares the expiration date from the CHUID, located on the card, to the current date to ensure the card has not expired. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> a. Create a CHUID container that contains valid data for all fields except the expiration date. The expiration date should be set to a date in the past. b. Populate the CHUID container on a T=0 or T=1 reference smart card c. Present reference smart card to Reader and perform a GET_DATA request for the CHUID container
Expected Results:	The Product shall not grant access to the cardholder based on the invalid expiration date. The Product must return an error indicator or simply denies access.

3.3.1.8 R-BIO-A.14 and R-BIO-A.19

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • The reader shall be able to parse the FASC-N from the CHUID. • The reader shall be able to extract the FASC-N in the Signed Attributes field of the biometric signature block and compare to the FASC-N found in the CHUID <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> a. Create a digitally signed biometric fingerprint data object, which is conformant to FIPS 201 b. Create a CHUID data object with a FASC-N which doesn't match
------------------------------	---

	<p>the FASC-N in the signed attributes of the biometric data object created in step a.</p> <ol style="list-style-type: none"> Load both data objects to a T=0 or T=1 reference smart card Present reference smart card to Reader Enter the PIN for the card
Expected Results:	The Product shall not grant access to the cardholder based on the FASC-N being different in the Signed Attributes of the biometric signature block and the CHUID data element. The Product must return an error indicator or simply deny access.

3.3.1.9 R-BIO-A.15

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> The biometric reader prompts the cardholder to provide a PIN to access the biometric stored on the card. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Create a biometric fingerprint container on a T=0 or T=1 reference smart card Present reference smart card to Reader Enter an incorrect PIN for the card
Expected Results:	The Product shall not grant access to the cardholder based on the invalid PIN provided. The Product must return an error indicator or simply deny access.

3.3.1.10 R-BIO-A.16

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> The digital signature on the biometric is checked to ensure the biometric was signed by a trusted source and is unaltered. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Populate test PIV Cards (T=0 or T=1) with following types of fingerprint biometric configurations: <ol style="list-style-type: none"> An invalid fingerprint biometric (invalid signature⁵) A valid⁶ fingerprint biometric whose signer is not trusted A valid fingerprint biometric whose signer's certificate path has a revoked/expired certificate
------------------------------	--

⁵ VTDRs demonstrating support for RSA and ECDSA signatures need to be provided if the Product supports both of these algorithms.

⁶ Valid in this context implies that the data object is formatted correctly and individual fields contain values as specified within the standard. 1:1 biometric match should also conclude with successfully.

	<p>iv. A valid fingerprint biometric whose signer's certificate path can be built successfully.</p> <p>b. Attempt to present the above-configured PIV Cards to the Product and note the results.</p>
Expected Results:	The Product successfully verifies the digital signature on the Biometric and is capable of performing a path validation on the Biometric signer's certificate to determine authenticity of the Biometric. All cases except the last result in access being denied.

3.3.1.11 R-BIO-A.20

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> The reader is able to use the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) for the purpose of access control. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <p>a. A report generated as a result of testing which shows the Product either (i) transmitting the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) to the PACS for the authorization decision or (ii) making the decision based on access decision logic stored within the Product.</p>
Expected Results:	The Product is capable of using the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) for the purpose of access control.

The Lab will update the status in the Web-Enabled Tool to "VTDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.

3.3.2 Vendor Documentation Review

Reference(s):	R-BIO-A.1, R-BIO-A.2, R-BIO-A.8, R-BIO-A.16, R-BIO-A.18, R-BIO-A.20, R-BIO-A.21
Evaluation Procedure:	<ol style="list-style-type: none"> The Lab will update the status in the Web-Enabled Tool to "VDR Begun" as instructed in the Web-enabled Tool Laboratory User Guide. The Lab will review the documentation submitted by the Supplier to ascertain the following: <ol style="list-style-type: none"> <i>ISO7816 Conformance (R-BIO-A.1)</i> <ul style="list-style-type: none"> The card-to-reader interface is compliant with the specifications of ISO7816. The tester shall verify that the documentation provided by the Supplier clearly shows that the reader conforms to all parts of ISO7816. <i>PC/SC Specifications (R-BIO-A.2)</i> <ul style="list-style-type: none"> For logical readers, the tester shall verify that the documentation provided clearly shows that the contactless card reader conforms to

	<p>the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface.</p> <p>c. <i>Buffer Size (R-BIO-A.8)</i></p> <ul style="list-style-type: none"> The reader buffer size is not less than 256 bytes. <p>d. <i>Validation of the Biometric Signer's Certificate (R-BIO-A.16)</i></p> <ul style="list-style-type: none"> The FIPS 140-2 approved algorithms supported by the reader for signature verification. Evidence shall be demonstrated using the Security Policy of the cryptographic module being used. The Product's capability to (i) perform standards-complaint path validation internally, (ii) to interface with an approved certificate validator (an EP category), (iii) to interface with an approved cached status proxy (an EP category). In case of option (i), follow steps from Section 3.3.3. In case of options (ii) and (iii), review the letter from the Suppliers with which the Product is capable of interfacing. <p>e. <i>Basis for Access Control Decision(R-BIO-A.20)</i></p> <ul style="list-style-type: none"> The Product's can either (i) transmit the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) to the PACS for the authorization decision or (ii) make the decision based on access decision logic stored within the Product. <p>f. <i>Intended Purpose (R-BIO-A.18, R-BIO-A.21)</i></p> <ul style="list-style-type: none"> The intended purpose of the reader, physical or logical access. If it is physical, then the reader needs to contain an integrated PIN input device and whether it is designed for external use or not. <p>3. The Lab will update the status to "VDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.</p>
Expected Result:	<ol style="list-style-type: none"> The Product conforms to the specifications of ISO 7816 The Product conforms to the Personal Computer/Smart Card (PC/SC) Specification for the reader-to-host system interface. The reader buffer size is at least 256 bytes The Product is capable of performing biometric signer certificate validation using one or more of the methods identified. The Product is capable of either (i) transmitting the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) to the PACS for the authorization decision or (ii) making the decision based on access decision logic stored within the Product. The intended use (externally-facing or not) of the Product has been specified in the Vendor Documentation. For physical readers, the PIN input device is integrated in the Product.

3.3.3 Certification

Reference(s):	R-BIO-A.9 to R-BIO-A.11, R-BIO-A.16, R-BIO-A.17, R-BIO-A.21
----------------------	---

Evaluation Procedure:	<ol style="list-style-type: none"> 1. The Lab will update the status in the Web-Enabled Tool to “C Begun” as instructed in the Web-enabled Tool Laboratory User Guide. 2. The Lab will perform the following activities in order to determine certification status of the Product with the FBI PIV Spec 071006: <ul style="list-style-type: none"> ▪ Examine the certification statement to see if it provided by the FBI and that it is still current i.e. valid; ▪ Review the list of certified fingerprint sensors to determine inclusion of the Product on the FBI’s Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications website located at : - http://www.fbi.gov/hq/cjisd/iafis/cert.htm 3. The Lab will perform the following activities for the embedded Template Matcher, if necessary, in order to determine certification status of the Product with SP 800-76 requirements: <ul style="list-style-type: none"> ▪ Review the list of Template Generators and Matchers to determine their inclusion of the Product. The list is available on the website located at: http://fingerprint.nist.gov/MINEX/QPL.html ▪ Optionally, if provided, examine the certification statement for authenticity (i.e. see if it provided by NIST) and that it is still current i.e. valid. 4. The Lab will perform the following activities for the Cryptographic Module in order to determine certification status of the Product with FIPS 140-2 requirements: <ul style="list-style-type: none"> ▪ Examine the certification statement to see if it was provided by the NIST/CSE and that it is still current i.e. valid; ▪ Verify the authenticity of this certification provided by the NIST/CSE; ▪ If product has been updated and re-evaluated, check the website to determine the correct version of approved products. The list is available on the website located at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm 5. The Lab will perform the following activities to determine the Product’s ability to perform Path Discovery and Validation (PD-VAL). This is required if the Product performs PD-VAL functions internally. <ul style="list-style-type: none"> ▪ Review the list of products approved by the Federal PKI Policy Authority for use by Federal agencies in implementing PD-VAL in a Bridge-enabled environment. The list is available on the website located at: http://www.idmanagement.gov/fpkia/validation_solutions.cfm 6. The Lab will perform the following activities in order to determine status of the SCVP client used by the Product (if applicable): <ul style="list-style-type: none"> ▪ Review the FIPS 201 EP APL to determine inclusion of the SCVP Client used by the Product. The list is available on the website located at: http://fips201ep.cio.gov/apl.php
------------------------------	--

	7. The Lab will update the status to “C Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	<ol style="list-style-type: none"> 1. The fingerprint sensor/biometric reader is certified by the FBI in accordance to the FBI PIV Spec 071006 located at: http://fips201ep.cio.gov/index.php, on the Supporting Documents link 2. The Product is certified by NIST as conforming to the certification criteria for Template Generators and Matchers as specified in SP 800-76. 3. The Cryptographic Module is certified by NIST/CSE at FIPS 140-2 Level 1 or higher depending on whether the reader is externally-facing or not. 4. The Product is on the Qualified Validation List (QVL) and is approved by the Federal PKI Policy Authority for use by Federal agencies in implementing PD-VAL in a Bridge-enabled environment. 5. The Product uses approved SCVP Client to interface with a certificate validator to obtain certificate status information.

3.3.4 Lab Test Data Report

Reference(s):	R-BIO-A.4, R-BIO-A.12 - R-BIO-A.14, R-BIO-A.16, R-BIO-A.19, R-BIO-A.22
Test Procedure:	<ol style="list-style-type: none"> 1. The Lab will update the status in the Web-Enabled Tool to “LTDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide. 2. The Lab will execute test procedures for this category in accordance with the “<i>Biometric Authentication Reader Test Procedure</i>”. 3. The Lab will update the status to “LTDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	The Product successfully passes all the test cases documented within the test procedure.

3.3.5 Attestation

Reference(s):	N/A
Evaluation Procedure:	<ol style="list-style-type: none"> 1. The Lab will update the status in the Web-Enabled Tool to “A Begun” as instructed in the Web-enabled Tool Laboratory User Guide. 2. Review the Attestation Form provided by the Supplier, confirming that the Product to the best of their knowledge, conforms to all the necessary requirements of the category under which the Product applies. Verify that person signing this Attestation Form has the authority to do so (a minimum “C” level [e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner]). 3. The Lab will update the status in the Web-Enabled Tool to “A Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	The Attestation Form has been signed by an authorized individual (e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner).

Appendix A—Document Release Summary of Changes

Identifier #	Reference	Description of Change
R-BIO-A.16	Section 3.1, pg. 5	Updated requirement to include key size and algorithm support based on SP 800-78-2.

Attachment A: Card/Reader Interoperability, Electronic Authentication and Security Requirements

Card/Reader Interoperability, Electronic Authentication and Security Requirements, v4.0,
May 15, 2006.