

# **FIPS 201 Evaluation Program - Biometric Reader Approval Procedure**

Version 9.0.0  
February 25, 2008



## Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	03/21/06	Document creation	Limited
Draft	0.1.0	03/21/06	Submitted to GSA for approval.	GSA
Draft	0.1.1	04/10/06	Updated based on feedback from GSA.	Limited
Draft	0.2.0	04/11/06	Submitted to GSA for approval	GSA
Draft	0.2.1	04/20/06	Updated based on feedback from GSA	Limited
Draft	0.3.0	04/20/06	Submitted to GSA for approval	GSA
Draft	0.3.1	05/18/06	Updated based on feedback from GSA	Limited
Draft	0.3.2	05/19/06	Updated based on feedback from GSA	Limited
Draft	0.4.0	05/22/06	Submitted to GSA for approval	GSA
Approved	1.0.0	05/22/06	Approved by GSA	Public
Revision	1.0.1	06/29/06	Updated based on feedback from GSA	Limited
Revision	1.1.0	06/29/06	Submitted to GSA for approval	GSA
Revision	1.1.1	06/30/06	Updated based on feedback from GSA	Limited
Revision	1.2.0	06/30/06	Submitted to GSA for approval	GSA
Approved	2.0.0	06/30/06	Approved by GSA	Public
Revision	2.0.1	09/25/06	Updated reference to NIST certification	Limited
Revision	2.1.0	09/25/06	Submitted to GSA for approval	Limited
Approved	3.0.0	09/25/06	Approved by GSA	Public
Revision	3.0.1	10/02/06	Updated based on feedback from GSA	Limited
Revision	3.1.0	10/03/06	Submitted to GSA for approval	Limited
Revision	3.2.0	04/09/07	Updated based on feedback from GSA	Limited
Approved	4.0.0	04/09/07	Approved by GSA	Public
Approved	5.0.0	04/26/07	Updated with details for the upgrade process.	Public
Approved	6.0.0	07/03/07	Updated with details of the biometric authentication use case.	Public
Approved	7.0.0	07/18/07	Updated FIPS 140-2 validation requirement	Public
Approved	8.0.0	10/31/07	Updated to split approval processes from document. Processes can now be found in Suppliers Handbook.	Public
Approved	9.0.0	02/25/08	Updated and Approved based on feedback from GSA	Public

## Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	Overview.....	1
1.2	Category Description .....	1
1.3	Purpose.....	1
<b>2</b>	<b>Application Package Contents.....</b>	<b>2</b>
<b>3</b>	<b>Evaluation Procedure for a Biometric Reader.....</b>	<b>3</b>
3.1	Requirements .....	3
3.2	Approval Mechanism Matrix.....	6
3.3	Evaluation Criteria.....	6
3.3.1	Vendor Test Data Report .....	6
3.3.1.1	R-BIO.3.....	6
3.3.1.2	R-BIO.4.....	7
3.3.1.3	R-BIO.5.....	7
3.3.1.4	R-BIO.6.....	8
3.3.1.5	R-BIO.7.....	8
3.3.1.6	R-BIO.12.....	9
3.3.1.7	R-BIO.13.....	9
3.3.1.8	R-BIO.14 and R-BIO.17 .....	9
3.3.1.9	R-BIO.15.....	10
3.3.1.10	R-BIO.18.....	10
3.3.1.11	R-BIO.20.....	11
3.3.2	Vendor Documentation Review.....	11
3.3.3	Certification .....	12
3.3.4	Lab Test Data Report .....	13
3.3.5	Attestation .....	13
<b>Attachment A: Card/Reader Interoperability, Electronic Authentication and Security Requirements.....</b>		<b>15</b>

## List of Tables

Table 1 - Applicable Requirements .....	5
Table 2 - Approval Mechanism Matrix .....	6

## 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 desiring to submit a Biometric Reader (hereafter referred to as the Product) for evaluation must follow the Suppliers Policies and Procedures Handbook. In addition to this handbook, Supplier also need 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 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.

### 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 Section 3.2. Wherever possible, information to be supplied as part of this Vendor Test Data Report has been described in Section 4.3; 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 4.3.

### 3 Evaluation Procedure for a Biometric 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.1	Contact card readers shall conform to the ISO7816 standard for the card-to-reader interface.	FIPS 201, Section 4.5.1	1.1-147	Vendor Documentation Review
R-BIO.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, Section 4.5.1	1.1-151	Vendor Documentation Review
R-BIO.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 2.2.2.2	3-9	Lab Test Data Report Vendor Test Data Report
R-BIO.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 2.2.2.3	3-10	Lab Test Data Report Vendor Test Data Report
R-BIO.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	3-19	Vendor Test Data Report
R-BIO.6	PIV Readers shall not generate a Programming Voltage.	Card /Card Reader Interoperability Requirements, Section 2.2.2.1	3-8	Vendor Test Data Report
R-BIO.7	PIV Readers shall support implicit protocol and parameter selections as defined in	Card /Card Reader Interoperability	3-11	Vendor Test Data Report

	ISO/IEC 7816-3:1997.	Requirements, Section 2.2.2.4		
R-BIO.8	The reader buffer size shall be no less than 256 bytes.	Card /Card Reader Interoperability Requirements, Section 3.2.1.1	3-16	Vendor Documentation Review
R-BIO.9	Fingerprint sensors used for PIV authentication shall conform to FBI specification ( <a href="#">FBI PIV Spec 071006</a> ) .	Derived	N/A	Certification
R-BIO.10	Devices shall be capable of imaging an area of at least 12.8 millimeters horizontally x 16.5 millimeters vertically at a native resolution of at least 197 pixels per centimeter in each direction.	SP 800-76-1, Section 3.3	2.1-7	Certification
R-BIO.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	N/A	Certification
R-BIO.12	The reader shall be able to read data from the CHUID buffer on the PIV Card.	FIPS 201-1, Section 6.2.2	1.1-212	Vendor Test Data Report Lab Test Data Report
R-BIO.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	1.1-212	Vendor Test Data Report Lab Test Data Report
R-BIO.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.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	N/A	Vendor Test Data Report

R-BIO.16	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	1.1-153	Vendor Documentation Review
R-BIO.17	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	1.1-213	Vendor Test Data Report Lab Test Data Report
R-BIO.18	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	1.1-212	Vendor Test Data Report Lab Test Data Report
R-BIO.19	The reader's cryptographic module shall be FIPS 140-2 validated with an overall Security Level 2 (or higher).	Derived	N/A	Certification
R-BIO.20	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	1.1-212	Vendor Test Data Report Lab Test Data Report

Table 1 - Applicable Requirements



### 3.2 Approval Mechanism Matrix

The table below provides an indication of the total number of requirements applicable for the Product and provides a breakup of how the evaluation will be conducted based on the different approval mechanisms available to the Lab.

Total Requirements	Approval Mechanisms					
	SV	VTDR	LTDR	VDR	C	A
20	N/A	12	8	4	4	1
<b>Legend:</b> 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.3

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

<sup>1</sup> 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.4

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>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.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>Populate the CHUID container with valid data on a reference smart card<sup>2</sup> that only supports the T=0 protocol</li> <li>Present T=0 reference smart card to Reader and perform a GET_DATA request for the CHUID container</li> <li>Output the expected CHUID data container</li> <li>Output the CHUID data container read from the Reader</li> <li>Verify that the data read from the Reader matches the expected data.</li> <li>Repeat steps a-e using a reference smart card that only supports the T=1 protocol.</li> </ol>
<b>Expected Results:</b>	The CHUID data read off the reference smart cards matches the expected data values.

## 3.3.1.3 R-BIO.5

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>PIV readers shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>A contact reference smart card<sup>2</sup> 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.</li> <li>Initiate the PPS by issuing a warm reset. Record the resulting ATR value.</li> <li>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.</li> <li>Record the PPS response from the card &amp; the ATR output from the card after a successful PPS exchange.</li> <li>Issue any APDU to the card and output the status words. Record the APDU command resulting card response.</li> </ol>
------------------------------	---

<sup>2</sup> Reference smart cards used for Supplier testing and reporting must be validated under NPIVP (<http://csrc.nist.gov/npivp/>)

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

### 3.3.1.4 R-BIO.6

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

### 3.3.1.5 R-BIO.7

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• PIV Readers shall support implicit protocol and parameter selections as defined in ISO/IEC 7816-3:1997.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>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</li> <li>b. Reset the card using the reader and obtain an ATR value. Record the ATR value.</li> <li>c. Send an APDU to the card and output the status words. Record the APDU command resulting card response.</li> </ol>
<b>Expected Results:</b>	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.12

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

## 3.3.1.7 R-BIO.13

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>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.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>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.</li> <li>Populate the CHUID container on a T=0 or T=1 reference smart card</li> <li>Present reference smart card to Reader and perform a GET_DATA request for the CHUID container</li> </ol>
<b>Expected Results:</b>	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.14 and R-BIO.17

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>The reader shall be able to parse the FASC-N from the CHUID.</li> <li>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</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>Create a digitally signed biometric fingerprint data object, which is conformant to FIPS 201</li> </ol>
------------------------------	---

	<ul style="list-style-type: none"> <li>b. Create a CHUID data object with a FASC-N which doesn't match the FASC-N in the signed attributes of the biometric data object created in step a.</li> <li>c. Load both data objects to a T=0 or T=1 reference smart card</li> <li>d. Present reference smart card to Reader</li> <li>e. Enter the PIN for the card</li> </ul>
<b>Expected Results:</b>	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.15

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• The biometric reader prompts the cardholder to provide a PIN to access the biometric stored on the card.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ul style="list-style-type: none"> <li>a. Create a biometric fingerprint container on a T=0 or T=1 reference smart card</li> <li>b. Present reference smart card to Reader</li> <li>c. Enter an incorrect PIN for the card</li> </ul>
<b>Expected Results:</b>	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.18

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• The reader is able to extract CHUID data elements, such as FASC-N and Agency Code, to determine whether the cardholder should be granted access.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ul style="list-style-type: none"> <li>a. Create a CHUID container that contains valid data for all fields except any one field which the Reader supports verification of. For example, if the Reader supports FASC-N verification, the FASC-N shall be set to a value that the reader will reject.</li> <li>b. Provide CHUID container value created in VTDR</li> <li>c. Populate the CHUID container on a T=0 or T=1 reference smart card</li> <li>d. Execute the biometric authentication use case.</li> <li>e. Repeat steps a-c for each additional CHUID data element that the</li> </ul>
------------------------------	--

	Reader verifies (as documented by the Supplier)
<b>Expected Results:</b>	For test scenarios executed, the Product may or may not grant access to the cardholder based on the CHUID data elements. In case of invalid data elements, the Product must return an error indicator or simply deny access.

### 3.3.1.11 R-BIO.20

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>The reader is able to match the biometric stored on the PIV Card to the live biometric captured at the time of authentication attempt.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>Create a biometric fingerprint template in accordance with ANSI 378 wrapped in a CBEFF header and signature. Ensure the validity of the encoding of this data object by testing it against the specific tests case found in the NIST SP 800-85b test tool.</li> <li>Populate the biometric container on a T=0 or T=1 reference smart card.</li> <li>Perform an authentication attempt using the live fingerprint used for creating the data in Step a.</li> <li>Perform an authentication attempt using a non-valid fingerprint.</li> </ol>
<b>Expected Results:</b>	<p>The reader demonstrates successful authentication of the fingerprint when using the correct fingerprint during the authentication attempt.</p> <p>The reader demonstrates successful rejection of the fingerprint that is not the fingerprint that was created for the biometric data container.</p>

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

<b>Reference(s):</b>	R-BIO.1, R-BIO.2, R-BIO.8, R-BIO.16
<b>Evaluation Procedure:</b>	<ol style="list-style-type: none"> <li>The Lab will update the status in the Web-Enabled Tool to “VDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>The Lab will review the documentation submitted by the Supplier to ascertain the following: <ol style="list-style-type: none"> <li><i>ISO7816 Conformance (R-BIO.1)</i> <ul style="list-style-type: none"> <li>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.</li> </ul> </li> <li><i>PC/SC Specifications (R-BIO.2)</i> <ul style="list-style-type: none"> <li>For logical readers, the tester shall verify that the documentation</li> </ul> </li> </ol> </li> </ol>

	<p>provided clearly shows that the contactless card reader conforms to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface.</p> <p>c. <i>Buffer Size (R-BIO.8)</i></p> <ul style="list-style-type: none"> <li>The reader buffer size is not less than 256 bytes.</li> </ul> <p>d. <i>Intended Purpose (R-BIO.16)</i></p> <ul style="list-style-type: none"> <li>Confirm 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.</li> </ul> <p>3. The Lab will update the status to “VDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.</p>
<b>Expected Result:</b>	<ol style="list-style-type: none"> <li>The Product conforms to the specifications of ISO 7816</li> <li>The Product conforms to the Personal Computer/Smart Card (PC/SC) Specification for the reader-to-host system interface.</li> <li>The reader buffer size is at least 256 bytes</li> <li>The intended use of the Product has been specified in the Vendor Documentation. For physical readers, the PIN input device is integrated in the Product.</li> </ol>

### 3.3.3 Certification

<b>Reference(s):</b>	R-BIO.9 to R-BIO.11, R-BIO.19
<b>Evaluation Procedure:</b>	<ol style="list-style-type: none"> <li>The Lab will update the status in the Web-Enabled Tool to “C Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>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"> <li>Examine the certification statement to see if it provided by the FBI and that it is still current i.e. valid;</li> <li>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 : - <a href="http://www.fbi.gov/hq/cjisd/iafis/cert.htm">http://www.fbi.gov/hq/cjisd/iafis/cert.htm</a></li> </ul> </li> <li>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"> <li>Review the list of Template Generators and Matchers to determine their inclusion of the Product. The list is available on the website located at: <a href="http://fingerprint.nist.gov/MINEX/QPL.html">http://fingerprint.nist.gov/MINEX/QPL.html</a></li> <li>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.</li> </ul> </li> </ol>

	<ol style="list-style-type: none"> <li>The Lab will perform the following activities for the Cryptographic Module in order to determine certification status of the Product with FIPS 140-2 Level 1 requirements: <ul style="list-style-type: none"> <li>Review the FIPS 140-2 Cryptographic Modules Validation List to determine inclusion of the Product and the level at which it has been certified. The list is available on the website located at: <a href="http://csrc.nist.gov/cryptval/140-1/1401val.htm">http://csrc.nist.gov/cryptval/140-1/1401val.htm</a>.</li> <li>Optionally, if provided, examine the certification statement for authenticity (i.e. see if it provided by the NIST/CSE) and that it is still current i.e. valid</li> </ul> </li> <li>The Lab will update the status to “C Complete” as instructed in the Web-enabled Tool Laboratory User Guide.</li> </ol>
<b>Expected Results:</b>	<ol style="list-style-type: none"> <li>The fingerprint sensor/biometric reader is certified by the FBI in accordance to the FBI PIV Spec 071006 located at: <a href="http://fips201ep.cio.gov/index.php">http://fips201ep.cio.gov/index.php</a>, on the Supporting Documents link</li> <li>The Product is certified by NIST as conforming to the certification criteria for Template Generators and Matchers as specified in SP 800-76.</li> <li>The Cryptographic Module is certified by NIST/CSE at FIPS 140-2 Level 2 or higher.</li> </ol>

### 3.3.4 Lab Test Data Report

<b>Reference(s):</b>	R-BIO.3, R-BIO.4, R-BIO.12 - R-BIO.14, R-BIO.17, R-BIO.18, R-BIO.20
<b>Test Procedure:</b>	<ol style="list-style-type: none"> <li>The Lab will update the status in the Web-Enabled Tool to “LTDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>The Lab will execute test procedures for this category in accordance with the “<i>Biometric Reader Test Procedure</i>”.</li> <li>The Lab will update the status to “LTDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.</li> </ol>
<b>Expected Results:</b>	The Product successfully passes all the test cases documented within the test procedure.

### 3.3.5 Attestation

<b>Reference(s):</b>	N/A
<b>Evaluation Procedure:</b>	<ol style="list-style-type: none"> <li>The Lab will update the status in the Web-Enabled Tool to “A Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>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,</li> </ol>



	<p>President, Business Partner or Owner])).</p> <p>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.</p>
<b>Expected Results:</b>	<p>1. The Attestation Form has been signed by an authorized individual (e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner).</p>

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

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