FIPS 201 Evaluation Program - Authentication Key Reader Approval Procedure

Version 8.0.0
October 31, 2007

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	04/21/06	Updated based on feedback from GSA	Limited
Draft	0.3.0	04/21/06	Submitted to GSA for approval	GSA
Draft	0.3.1	05/15/06	Updated based on feedback from GSA	Limited
Draft	0.3.2	05/19/06	Updated based on feedback from GSA	Limited
Draft	0.3.3	05/22/06	Updated based on feedback from GSA	Limited
Approved	1.0.0	05/23/06	Approved by GSA	Public
Revision	1.0.1	06/28/06	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
Approved	3.0.0	10/18/06	Approved by GSA	Public
Approved	4.0.0	02/09/07	Updated to include process for product updates, resubmissions and evaluation fees	Public
Approved	5.0.0	04/02/07	Updated with details for the evaluation fees.	Public
Approved	6.0.0	04/26/07	Updated with details for the upgrade process.	Public
Approved	7.0.0	07/11/07	Added the PKI path validation and revocation checking requirements.	Public
Approved	8.0.0	10/31/07	Updated to split approval processes from document. Processes can now be found in Suppliers Handbook.	Public

Table of Contents

List of Tables

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 an Authentication Key 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 *Authentication Key Reader* is a contact smart card reader that includes the capability to authenticate a PIV Card by accessing the public key certificate for PIV Authentication Key and applying cryptographic operations.

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 secure delivery method 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 3.3;
- 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 the Section 3.3; and
- All necessary Supplier documentation providing proof that the Product complies with the subset of requirements (as outlined in Section 3.1) for this category which has Supplier documentation review as its approval mechanism. Examples of specific documentation would include: user guides, technical specifications, white papers, line cards, etc.

3 Evaluation Procedure for an Authentication Key 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-AUK.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-AUK.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-AUK.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-AUK.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-AUK.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-AUK.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-AUK.7	PIV Readers shall support implicit protocol and	Card /Card Reader	3-11	Vendor Test Data Report

	parameter selections as defined in ISO/IEC 7816-3:1997.	Interoperability Requirements, Section 2.2.2.4		
R-AUK.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-AUK.9	The reader shall be able to read the PIV Authentication buffer on the PIV Card.	Derived	N/A	Lab Test Data Report Vendor Test Data Report
R-AUK.10	The reader shall be able to generate and send a cryptographic challenge to the PIV Card.	FIPS 201 Section 6.2.4	1.1-215	Lab Test Data Report Vendor Test Data Report
R-AUK.11	The reader shall be able to decrypt and match the cryptographic response from the PIV Card.	FIPS 201 Section 6.2.4	1.1-215	Lab Test Data Report Vendor Test Data Report
R-AUK.12	The reader shall be able to provide the personal identification number (PIN) to the card to access the PIV Authentication Key stored on the PIV Card.	Derived	N/A	Vendor Documentation Review
R-AUK.13	The reader shall be able to conduct a standards-compliant PKI path validation on the PIV Authentication Certificate. The related digital certificate is checked to ensure that it is from a trusted source.	FIPS 201 Section 6.2.4	1.1-215	Lab Test Data Report Vendor Test Data Report
R-AUK.14	The revocation status of the certificate is checked to ensure current validity	FIPS 201 Section 6.2.4	1.1-215	Lab Test Data Report Vendor Test Data Report
R-AUK.15	If the intended purpose for the reader is for physical access, then the reader shall contain an	FIPS 201, Section 4.5.3	1.1-152	Vendor Documentation Review

	integrated PIN input device.			
R-AUK.16	The reader shall be able to parse the PIV Authentication Certificate to extract relevant fields (signer DN, FASC-N) for the purpose of access control.	FIPS 201 Section 6.2.4	1.1-215	Lab Test Data Report Vendor Test Data Report
R-AUK.17	If the reader contains a cryptographic module, it shall be validated to FIPS 140-2 with an overall Security Level 2 (or higher).	Derived	N/A	Certification

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
17	N/A	11	8	5	1	1
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 Documentation Review

Reference(s):	R-AUK.1, R-AUK.2, R.AUK.8, R-AUK.12, R-AUK.15
Evaluation Procedure:	1. The Lab will update the status in the Web-Enabled Tool to “VDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide. 2. The Lab will review the test data report submitted by the Supplier to ascertain the following: a. *ISO7816 Conformance (R-AUK.1)* • The card-to-reader interface is compliant with the specifications of ISO7816 b. *PC/SC Specifications (R-AUK.2)* • Contact card readers conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface. c. *Buffer Size (R-AUK.8)* • The reader buffer size is not less than 256 bytes. d. *PIN Provisioning (R-AUK.12, R-AUK.15)* • The reader is able to provide the PIN to the PIV Card to access the PIV Authentication Key. • Readers that are intended to be used for physical access contain an integrated PIN input device. 3. The Lab will update the status to “VDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	1. The reader is able to provide the PIN to the PIV Card to access the PIV Authentication Key. 2. Readers intended for use in physical access environments contain an

	integrated PIN input device. 3. The PIV Authentication certificate can be parsed to extract the relevant fields for access control.

3.3.2 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.

3.3.2.1 R-AUK.3

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • 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. At a minimum, the following test scenario must be performed to confirm compliance: a. Populate the PIV Authentication Certificate container with valid data on a reference smart card[1] that only supports Class A operating conditions b. Present Class A only reference smart card to Reader and perform a GET_DATA request for the PIV Authentication Certificate container c. Output the expected PIV Authentication Certificate data container d. Output the PIV Authentication Certificate data container read from the Reader e. Verify that the data read from the Reader matches the expected data.
Expected Result:	The PIV Authentication Certificate data read off the reference smart cards matches the expected data values.

3.3.2.2 R-AUK.4 and R-AUK.9

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • 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. At a minimum, the following test scenario must be performed to confirm compliance: a. Populate the PIV Authentication Certificate container with valid data on a reference smart card[2] that only supports the T=0 protocol

---

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

	b. Present T=0 reference smart card to Reader and perform a GET_DATA request for the PIV Authentication Certificate container c. Output the expected PIV Authentication Certificate data container d. Output the PIV Authentication Certificate data container read from the Reader e. Verify that the data read from the Reader matches the expected data. f. Repeat steps a-e using a reference smart card that only supports the T=1 protocol
Expected Result:	The PIV Authentication Certificate data read off the reference smart cards matches the expected data values.

3.3.2.3 R-AUK.5

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • PIV readers shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997 At a minimum, the following test scenario must be performed to confirm compliance: a. A reference smart card 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. b. Initiate the PPS by issuing a warm reset. Record the resulting ATR value. c. 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. d. Record the PPS response from the card & the ATR output from the card after a successful PPS exchange. e. Issue any APDU to the card and output the status words. Record the APDU command resulting card response.
Expected Result:	1. The card reader can successfully change the transmission protocol from T=0 to T=1. 2. The card reader can successfully change serial transmission characters F & D.

3.3.2.4 R-AUK.6

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following:

---

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

	• PIV Readers shall not generate a Programming Voltage. At a minimum, the following test scenario must be performed to confirm compliance: a. Populate the PIV Authentication Certificate container with valid data on a reference smart card. b. Create a test harness that will allow monitoring of the Vpp pin of the reader/smart card c. Begin monitoring of the Vpp 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 Vpp pin
Expected Result:	Results of the Vpp log shall show that no voltage is applied during operation of the GET_DATA command.

3.3.2.5 R-AUK.7

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • PIV Readers shall support implicit protocol and parameter selections as defined in ISO/IEC 7816-3:1997. At a minimum, the following test scenario must be performed to confirm compliance: a. A contact 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 Result:	The reader is able to support implicit protocol and parameters selection and communicate with a card that does not offer explicit selection.

3.3.2.6 R-AUK.10

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *Cryptographic Challenge Generation*: The Product is capable of generating a cryptographic challenge and transmitting it to the PIV Card. At a minimum, the following test scenario must be performed to confirm compliance: a. A report generated as a result of testing which shows that a

	cryptographic challenge has been generated and sent to the card. The report should also show the plaintext output of the challenge that was sent to the card.
Expected Result:	The Product is capable of generating a cryptographic challenge and transmitting it to the PIV Card.

3.3.2.7 R-AUK.11

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *Response Verification*: The Product is capable of decrypting the response from the PIV Card using the certificate which corresponds to the PIV Card Authentication Key. At a minimum, the following test scenario must be performed to confirm compliance: a. A report generated as a result of testing which shows an encrypted response returned from the PIV Card. At a minimum, the report should display: • The encrypted response returned from the Card • The result of the decryption operation • The algorithm used to decrypt the data • The public key that was used to decrypt the response • The original challenge that matches the decrypted response
Expected Result:	The decrypted response from the card should match the value reported in Test Case R-AUK.10.

3.3.2.8 R-AUK.13 and R-AUK.14

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *PKI Path Validation*: The Product is capable of conducting a standards-compliant PKI path validation on the PIV Authentication Certificate. • *Certificate Revocation Status*: The Product is capable of checking the revocation status of the certificate to ensure current validity. At a minimum, the following test scenario must be performed to confirm compliance: a. The Product is capable of storing trust anchors and other intermediate certificates for the purpose of path building. b. A PIV Card with an untrusted PIV Authentication Certificate is presented to the Product. The Product returns an error or simply denies access because a path cannot be built.

	c. Next, a PIV Card that contains a PIV Authentication Certificate that is trusted (i.e. the Reader can build a valid path from the PIV Authentication to a trust anchor) is presented to the Reader. In this scenario the authentication attempt progresses successfully. d. Finally, a revoked PIV Authentication Certificate (that is trusted by the Product) is presented. The Reader performs a revocation check (by looking up CRL information) and determines the status of the PIV Authentication Certificate. In this case, the Certificate is revoked and therefore the authentication attempt concludes with the Product signaling an error or simply denying access.
Expected Result:	The Product is capable of conducting a standards-compliant PKI path validation on the PIV Authentication Certificate and determining its revocation status.

3.3.2.9 R-AUK.16

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • The reader is able to parse the PIV Authentication Certificate to extract relevant fields (signer DN, FASC-N) for the purpose of access control. At a minimum, the following test scenario must be performed to confirm compliance: a. Populate a PIV Authentication Certificate on a T=0 or T=1 reference smart card that contains valid data for all fields except any one field which the Reader supports verification of for access control decisions. For example, if the Reader supports FASC-N verification, the FASC-N shall be set to a value that the reader will reject. Note: - All other fields shall be valid and the PIV Authentication Certificate is trusted by the Reader. b. Present reference smart card to Reader and perform the authentication use case scenario. *c.* Repeat steps a-b for each additional PIV Authentication Certificate field that the Reader uses to perform access control (as documented by the Supplier)
Expected Results:	For test scenario executed, the Product shall not grant access to the cardholder based on the invalid PIV Authentication Certificate field. The Product returns an error indicator or simply denies access.

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

3.3.3 Lab Test Data Report

Reference(s):	R-AUK.3, R-AUK.4, R-AUK.9 to R-AUK.11, R-AUK.13, R-AUK.14, R-AUK.16
Test Procedure:	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 "*Authentication Key Reader Test Procedure*." 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.

3.3.4 Certification

Reference(s):	R-AUK.17
Evaluation Procedure:	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 for the Cryptographic Module in order to determine certification status of the Product with FIPS 140-2 Level 2 requirements: ▪ Examine the certification statement to see if it 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; and ▪ 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: http://csrc.nist.gov/cryptval/140-1/1401val.htm. 3. The Lab will update the status to "C Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	1. The Cryptographic Module has been found to be certified by NIST/CSE at FIPS 140-2 Level 2 or higher.

3.3.5 Attestation

Reference(s):	N/A
Evaluation Procedure:	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:	1. The Attestation Form has been signed by an authorized individual (e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner).

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

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