

FIPS 201 Evaluation Program - Transparent Reader Approval Procedure

Version 8.0.0
October 31, 2007



Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	05/23/06	Document creation	Limited
Draft	0.1.0	05/23/06	Submitted to GSA for approval	GSA
Approved	1.0.0	05/23/06	Approved by GSA	Public
Approved	2.0.0	05/25/06	Approved by GSA	Public
Revision	2.0.1	06/29/06	Updated based on feedback from GSA	Limited
Revision	2.1.0	06/29/06	Submitted to GSA for approval	GSA
Revision	2.1.1	06/30/06	Updated based on feedback from GSA	Limited
Revision	2.2.0	06/30/06	Submitted to GSA for approval	GSA
Approved	3.0.0	06/30/06	Approved by GSA	Public
Revision	3.0.1	09/11/06	Updated based on feedback from GSA	Limited
Revision	3.1.0	09/18/06	Updated based on feedback from Evaluation Lab and submitted to GSA for approval	GSA
Revision	3.2.0	09/19/06	Updated based on feedback from GSA and re-submitted for approval	GSA
Approved	4.0.0	10/18/06	Approved by GSA	Public
Approved	5.0.0	02/09/07	Updated to include process for product updates, resubmissions and evaluation fees	Public
Approved	6.0.0	04/02/07	Updated with details for the evaluation fees.	Public
Approved	7.0.0	04/26/07	Updated with details for the upgrade process.	Public
Approved	8.0.0	10/24/07	Updated to split approval processes from document. Processes can now be found in Suppliers Handbook.	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
3	Evaluation Procedure for a Transparent Reader	3
3.1	Requirements	3
3.2	Approval Mechanism Matrix.....	6
3.3	Evaluation Criteria.....	6
3.3.1	Vendor Documentation Review.....	6
3.3.2	Vendor Test Data Report	6
3.3.2.1	R-TRE.3	6
3.3.2.2	R-TRE.4	7
3.3.2.3	R-TRE.5	7
3.3.2.4	R-TRE.6	8
3.3.2.5	R-TRE.7, R-TRE.8	8
3.3.2.6	R-TRE.9	9
3.3.2.7	R-TRE.10	9
3.3.2.8	R-TRE.11	10
3.3.2.9	R-TRE.12	10
3.3.2.10	R-TRE.13	11
3.3.3	Lab Test Data Report	12
3.3.4	Attestation	12
Attachment A: Card/Reader Interoperability, Electronic Authentication and Security Requirements.....		13

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 Transparent 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 *Transparent Reader* is a smart card reader with the capability to read data from a PIV Card via contact or contactless interface. This reader may function within a physical or logical system. Reader must work in conjunction with other system components in order to assure compliance with the CHUID, Biometric, and Authentication Key use cases described in FIPS 201 or 800-73.

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 4.3; and
- All necessary Supplier documentation providing proof that the Product complies with the subset of requirements (as outlined in Section 4.1) 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 a Transparent 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 #	Interface	Requirement Description	Source	Reqt. #	Approval Mechanism
R-TRE.1	Contact	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-TRE.2	Contact, Contactless	Logical PIV 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-TRE.3	Contact	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-TRE.4	Contact	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-TRE.5	Contact	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-TRE.6	Contact	Data retrieved from the PIV readers shall be the data that was written by the lab on each “Golden” test card.	Derived Test Requirement	N/A	Lab Test Data Report Vendor Test Data Report
R-TRE.7	Contactless	The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in	Card /Card Reader Interoperability Requirements,	3-5	Lab Test Data Report Vendor Test Data Report

Identifier #	Interface	Requirement Description	Source	Reqt. #	Approval Mechanism
		ISO/IEC 14443-2:2001.	Section 2.2.1.1		
R-TRE.8	Contactless	The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.	Card /Card Reader Interoperability Requirements, Section 2.2.1.3	3-7	Lab Test Data Report Vendor Test Data Report
R-TRE.9	Contactless	Buffers shall not be readable through the contactless interface more than 10 cm from the reader.	Card /Card Reader Interoperability Requirements, Section 4.2.1.1	3-21	Lab Test Data Report Vendor Test Data Report
R-TRE.10	Contactless	The contactless interface of the reader shall support Type A initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.	Card /Card Reader Interoperability Requirements, Section 2.2.1.2	3-6	Vendor Test Data Report
R-TRE.11	Contactless	The contactless interface of the reader shall support Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.	Card /Card Reader Interoperability Requirements, Section 2.2.1.2	3-6	Vendor Test Data Report
R-TRE.12	Contactless	The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s), fc/64 (~212 kbits/s) and fc/32 (~424 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005.	Card /Card Reader Interoperability Requirements, Section 3.2.2.1	3-17	Vendor Test Data Report
R-TRE.13	Contact, Contactless	For evaluation purposes, the data format for physical readers shall consist of the two parity bits, Agency Code, System Code and Credential Code elements of the FASC-N along with the Expiration Date (YYYYMMDD) from the CHUID as defined by Appendix A of NIST SP 800-73. Each element shall be individually formatted as binary numbers and combined to form a 75 bit string as shown in the figure below. Section 5 of the SIA standard defines a 26 bit format that does not meet the requirements	Transparent Reader Test Procedure	N/A	Lab Test Data Report Vendor Test Data Report

Identifier #	Interface	Requirement Description	Source	Reqt. #	Approval Mechanism																					
		<p>outlined in FIPS or its supporting documents and shall not be used.</p> <table><tr><td></td><td>Position</td><td>Length</td></tr><tr><td>Parity Bit P1</td><td>1</td><td>1</td></tr><tr><td>Agency Code</td><td>2-15</td><td>14</td></tr><tr><td>System Code</td><td>16-29</td><td>14</td></tr><tr><td>Credential Code</td><td>30-49</td><td>20</td></tr><tr><td>Expiration Date</td><td>50-74</td><td>25</td></tr><tr><td>Parity Bit P2</td><td>75</td><td>1</td></tr></table> <p>Note: The first parity bit (P1) is even and shall be calculated over the first 37 bits. The second parity bit (P2) is odd and shall be calculated over the last 36 bits.</p>		Position	Length	Parity Bit P1	1	1	Agency Code	2-15	14	System Code	16-29	14	Credential Code	30-49	20	Expiration Date	50-74	25	Parity Bit P2	75	1			
	Position	Length																								
Parity Bit P1	1	1																								
Agency Code	2-15	14																								
System Code	16-29	14																								
Credential Code	30-49	20																								
Expiration Date	50-74	25																								
Parity Bit P2	75	1																								

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
13	N/A	11	7	1	N/A	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-TRE.1, R-TRE.2, R-TRE.5
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 documentation submitted by the Supplier to determine if Supplier claims that: <ol style="list-style-type: none"> <i>ISO7816 Conformance (R-TRE-C.1)</i> <ul style="list-style-type: none"> The card-to-reader interface is compliant with the specifications of ISO7816. <i>PC/SC Specifications (R-TRE-C.2)</i> <ul style="list-style-type: none"> Logical contact card readers conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface. The Lab will update the status to “VDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	Submitted documentation demonstrates that the requirements are met by the product.

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-TRE.3

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

	<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 card¹ 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 Result:	The CHUID data read off the reference smart cards matches the expected data values.

3.3.2.2 R-TRE.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 card 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 Result:	The CHUID data read off the reference smart cards matches the expected data values.

3.3.2.3 R-TRE.5

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

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

	<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"> Begin the test using an unpopulated reference smart card Create a test harness that will allow monitoring of the Vpp pin of the reader/smart card Begin monitoring of the Vpp pin voltage level Present the reference smart card to the Reader and perform a PUT_DATA on the CHUID container. Monitor the Vpp pin. Repeat step d for all other mandatory containers on the PIV card End monitoring of Vpp pin.
Expected Results:	Results of the Vpp log shall show that no voltage is applied during operation of the PUT_DATA command on any of the mandatory containers.

3.3.2.4 R-TRE.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"> Data received from the reader shall be the data that was written by the lab on each “Golden” test card. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Perform same test scenario for R-TRE-C.4
Expected Result:	See expected test results for R-TRE-C.4

3.3.2.5 R-TRE.7, R-TRE.8

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 contactless interface of the reader supports both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001 The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001. <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 Type A reference smart card² Present Type A reference smart card to Reader and perform a
------------------------------	---

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

	<p>GET_DATA request for the CHUID container</p> <ul style="list-style-type: none"> c. Output the expected CHUID data container d. Output the CHUID 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 Type B reference smart card
Expected Result:	The CHUID data read off the reference smart cards matches the expected data values.

3.3.2.6 R-TRE.9

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • Data buffers are not readable through the contactless interface more than 10 cm from the reader. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ul style="list-style-type: none"> a. Populate the CHUID container with valid data on a Type A reference smart card b. Present Type A reference smart card to Reader and perform a GET_DATA request for the CHUID container c. Output the expected CHUID data container d. Output the CHUID data container read from the Reader e. Present the contactless smart card less than 10 cm from the reader and attempt to perform steps b-d f. Verify that the data read from the Reader matches the expected data. g. Present the contactless smart card at precisely 11cm from the reader and attempt to perform steps b-d. h. Repeat steps a-g using a Type B reference smart card
Expected Result:	<p>The CHUID data read off the reference smart card shall match the expected data value as identified in step f.</p> <p>When performing step g, it is expected that the Reader will not be able to read any data from the card.</p>

3.3.2.7 R-TRE.10

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 contactless interface of the reader supports Type A initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p>
------------------------------	--

	<ol style="list-style-type: none"> Create two unique CHUID containers containing different data elements Populate the two CHUID containers onto two separate Type A reference smart cards Present both reference smart cards simultaneously to the Reader and perform a GET_DATA request for the CHUID container Output the expected CHUID data container for both cards Output the CHUID data container(s) read from the Reader Verify that the data read from the Reader matches the expected data.
Expected Result:	The CHUID data read off the reference smart cards matches the expected data values. Data from both cards must be read successfully.

3.3.2.8 R-TRE.11

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 contactless interface of the reader supports Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Create two unique CHUID containers containing different data elements Populate the two CHUID containers onto two separate Type B reference smart cards Present both reference smart cards simultaneously to the Reader and perform a GET_DATA request for the CHUID container Output the expected CHUID data container for both cards Output the CHUID data container(s) read from the Reader Verify that the data read from the Reader matches the expected data.
Expected Result:	The CHUID data read off the reference smart cards matches the expected data values. Data from both cards must be read successfully.

3.3.2.9 R-TRE.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 contactless interface of the reader supports bit rates of $f_c/128$ (~106 kbits/s), $f_c/64$ (~212 kbits/s) and $f_c/32$ (~424 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005. <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 Type A
------------------------------	---

	<p>reference smart card supporting all bit rates</p> <ol style="list-style-type: none"> Configure reader to only accept bit rate of $f_c/128$ (~106 kbits/s) Present Type A 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 each bit rate supported by the Reader
Expected Result:	The actual CHUID data read for each bit rate test should be identical to the expected CHUID data.

3.3.2.10 R-TRE.13

Evaluation Procedure:

The CHUID is read from the card and put into a structure that conforms to the following table:

	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14
Credential Code	30-49	20
Expiration Date	50-74	25
Parity Bit P2	75	1

- Parity bit P1 is even parity calculated over the first 37 bits of data.
- Parity bit P2 is odd parity calculated over the remaining 36 bits of data.

At a minimum, the following test scenario must be performed to confirm compliance:

For Contactless Readers

- a. Populate the CHUID container with valid data on a Type A reference smart card
- b. Present Type A reference smart card to Reader and perform a GET_DATA request for the CHUID container
- c. Output the expected 75-bit output structure in binary form
- d. Output the data structure read from the Reader
- e. Verify that the data read from the Reader matches the expected data.
- f. Repeat steps a-e using a Type B reference smart card

For Contact Readers

- g. Populate the CHUID container with valid data on a T=0 reference smart card

	<ol style="list-style-type: none"> h. Present T=0 reference smart card to Reader and perform a GET_DATA request for the CHUID container i. Output the expected 75-bit output structure in binary form j. Output the data structure read from the Reader k. Verify that the data read from the Reader matches the expected data. l. Repeat steps g-k using a T=1 reference smart card
Expected Result:	The 75-bit output structure returned by the Reader matches the expected data values (both contact and/or contactless interface[s]).

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-TRE.3, R-TRE.4, R-TRE.6, R-TRE.7 to R-TRE.9, R-TRE.13
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. 1. The Lab will execute test procedures for this category in accordance with the “<i>Transparent Reader Test Procedure</i>”. 2. The Lab will update the status to “LTDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Result:	The Product successfully passes all the test cases documented within the test procedure.

3.3.4 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).

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

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