FIPS 201 Evaluation Program -
CHUID Authentication Reader (Contactless) Approval Procedure

Version 2.0.0
October 31, 2007

Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	07/11/07	Initial Version	Public
Approved	2.0.0	10/24/07	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 a CHUID Authentication Reader (Contactless) (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 *CHUID Authentication Reader (Contactless)* is a smart card reader with the capability to access and determine authenticity of the CHUID (as defined by SP 800-73, Section 1.8.3) stored on PIV Card. Authenticity will be determined by verifying the CHUID signature, followed by building a trusted path between the CHUID signer's certificate and the root Certification Authority (CA) which issued the CHUID signer's certificate, including intermediate certificates. After an authentic CHUID has been determined, reader will provide a user access control decision based person identifier values of the FASC-N and optionally other person identifier data elements of the CHUID. This reader uses the contactless interface.

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 (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);
- 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 Vendor documentation review as its approval mechanism. Examples of specific documentation would include: user guides, technical specifications, white papers, line cards, etc.
- 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 at a typically contain information as stated in Section 3.3.1.

3 Evaluation Procedure for CHUID Authentication Reader (Contactless)

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-CHU-CLA.1	Contactless card readers shall conform to the [ISO 14443] standard for the card-to-reader interface.	FIPS 201-1, Section 4.5.2	1.1-150	Vendor Documentation Review
R-CHU-CLA.2	Logical contactless card readers shall conform to PC/SC specification for the reader-to-host system interface in cases where these readers are connected to general purpose desktop computing systems.	FIPS 201-1, Section 4.5.2	1.1-148	Vendor Documentation Review
R-CHU-CLA.3	The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.	Card /Card Reader Interoperability Requirements, Section 2.2.1.1	3-5	Lab Test Data Report Vendor Test Data Report
R-CHU-CLA.4	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-CHU-CLA.5	Buffers shall not be readable through the contactless interface more than 10 cm from the reader.	Card /Card Reader Interoperability Requirements, Section 4.1.1.1	3-22	Lab Test Data Report Vendor Test Data Report
R-CHU-CLA.6	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-CHU-	The contactless interface of the reader shall support Type B	Card /Card Reader	3-6	Vendor Test

Identifier #	Requirement Description	Source	Reqt. #	Approval Mechanism
CLA.7	initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.	Interoperability Requirements, Section 2.2.1.2		Data Report
R-CHU-CLA.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-CHU-CLA.9	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-CHU-CLA.10	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
R-CHU-CLA.11	The authentication attempt shall 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-CHU-CLA.12	The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered.	FIPS 201-1, Section 6.2.2	1.1-212	Lab Test Data Report Vendor Test Data Report
R-CHU-CLA.13	One or more of the CHUID data elements are used as input to the authorization check	FIPS 201-1, Section 6.2.2	1.1-212	Vendor Test Data Report Lab Test Data Report
R-CHU-CLA.14	For performing cryptographic operations (during verification of CHUID signature), the cryptographic module shall be FIPS 140-2 validated with an overall Security Level 2 (or higher).	FIPS 201-1, Appendix B.4	1.1-221	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
14	N/A	10	6	3	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 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-CHU-CLA.3 and R-CHU-CLA.4

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • 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. At a minimum, the following test scenario must be performed to confirm compliance: a. Populate the CHUID container with valid data on a Type A reference smart card[1] 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. Verify that the data read from the Reader matches the expected

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

	data. f. Repeat steps a-e using a Type B reference smart card
Expected Results:	The CHUID data read off the reference smart cards matches the expected data values.

3.3.1.2 **R-CHU-CLA.5**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • Data buffers are not readable through the contactless interface more than 10 cm from the reader. At a minimum, the following test scenario must be performed to confirm compliance: 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 Results:	The CHUID data read off the reference smart card shall match the expected data value as identified in step f. When performing step g, it is expected that the Reader will not be able to read any data from the card.

3.3.1.3 **R-CHU-CLA.6**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • The contactless interface of the reader supports Type A initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001. At a minimum, the following test scenario must be performed to confirm compliance: a. Create two unique CHUID containers containing different data

	elements b. Populate the two CHUID containers onto two separate Type A reference smart cards c. Present both reference smart cards simultaneously to the Reader and perform a GET_DATA request for the CHUID container d. Output the expected CHUID data container for both cards e. Output the CHUID data container(s) read from the Reader f. 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. Data from both cards must be read successfully.

3.3.1.4 **R-CHU-CLA.7**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • The contactless interface of the reader supports Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001. At a minimum, the following test scenario must be performed to confirm compliance: a. Create two unique CHUID containers containing different data elements b. Populate the two CHUID containers onto two separate Type B reference smart cards c. Present both reference smart cards simultaneously to the Reader and perform a GET_DATA request for the CHUID container d. Output the expected CHUID data container for both cards e. Output the CHUID data container(s) read from the Reader f. 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. Data from both cards must be read successfully.

3.3.1.5 **R-CHU-CLA.9**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • The contactless interface of the reader supports 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. At a minimum, the following test scenario must be performed to confirm compliance:

	a. Populate the CHUID container with valid data on a Type A reference smart card supporting all bit rates b. Configure reader to only accept bit rate of fc/128 (~106 kbits/s) c. Present Type A reference smart card to Reader and perform a GET_DATA request for the CHUID container d. Output the expected CHUID data container e. Output the CHUID data container read from the Reader f. Verify that the data read from the Reader matches the expected data. g. Repeat steps a-e using each bit rate supported by the Reader
Expected Results:	The actual CHUID data read for each bit rate test should be identical to the expected CHUID data.

3.3.1.6 **R-CHU-CLA.10**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • The reader is able to extract the CHUID from the PIV Card. At a minimum, the following test scenario must be performed to confirm compliance: a. Perform same test scenario for R-CHU-CLA.3 or R-CHU-CLA.4.
Expected Results:	See expected test results for R-CHU-CLA.3/R-CHU-CLA.4.

3.3.1.7 **R-CHU-CLA.11**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • 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. At a minimum, the following test scenario must be performed to confirm compliance: 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 Type A or B reference smart card

	c. Present reference smart card to Reader and perform a GET_DATA request for the CHUID container
Expected Results:	The Reader shall not grant access to the cardholder based on the invalid expiration date. The Reader must return an error indicator or simply deny access.

3.3.1.8 **R-CHU-CLA.12**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered. At a minimum, the following test scenario must be performed to confirm compliance: a. Populate the CHUID container on a Type A or B reference smart card. b. Present reference smart card to Reader and perform a GET_DATA request for the CHUID container c. The Product performs a digital signature verification on the CHUID followed by a path validation on the certificate that signed the CHUID to determine authenticity of the CHUID and thereby the PIV Card d. Present another Type A or B reference smart card wherein the CHUID is signed by a certificate that is not trusted by the Product. e. Path Validation should fail in this case and the authentication attempt should conclude.
Expected Results:	The Product successfully verifies the digital signature on the CHUID and is capable of performing a path validation on the CHUID signer's certificate to determine authenticity of the CHUID.

3.3.1.9 **R-CHU-CLA.13**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • One or more of the CHUID data elements are used as input to the authorization check. At a minimum, the following test scenario must be performed to confirm compliance: 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. b. Provide CHUID container value created in VTDR c. Populate the CHUID container on a Type A or B reference smart card d. Present reference smart card to Reader and perform a GET_DATA request for the CHUID container e. Repeat steps a-c for each additional CHUID data element that the Reader verifies (as documented by the Supplier)
Expected Results:	For test scenario executed, the Reader shall not grant access to the cardholder based on the invalid CHUID data element. The Reader must return an error indicator or simply deny 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 once the VTDR review has been completed.

3.3.2 Vendor Documentation Review

Reference(s):	R-CHU-CLA.1, R-CHU-CLA.2, R-CHU-CLA.8
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 documentation submitted by the Supplier to ascertain the following: *a. ISO14443 Conformance (R-CHU-CL.1)* • The card-to-reader interface is compliant with the specifications of ISO14443. The tester shall verify that the documentation provided by the Supplier clearly shows that the reader conforms to all parts of ISO14443. *b. PC/SC Specifications (R-CHU-CL.2)* • For logical readers, the tester shall verify that the documentation 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. *c. Buffer Size (R-CHU-CL.8)* • The reader buffer size shall be no less than 256 bytes. 3. The Lab will update the status to "VDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Result:	1. The Product conforms to the specifications of ISO 14443. 2. The Product conforms to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface. 3. The reader buffer size is at least 256 bytes

3.3.3 Lab Test Data Report

Reference(s):	R-CHU-CLA.3 to R-CHU-CLA.5, R-CHU-CLA.11, R-CHU-CLA.12, R-CHU-CLA.13

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 "*CHUID Authentication Reader (Contactless) Test Procedure*". 3. 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 Certification

Reference(s):	R-CHU-CLA.14
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: ▪ 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. ▪ 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 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 is 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.