

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

Version 1.0.0
July 03, 2007



Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	07/03/07	Initial Version	Public

Table of Contents

1	Overview	1
1.1	Identification	1
2	Testing Process	2
3	Test Procedure for CHUID Authentication Reader (Contactless).....	3
3.1	Requirements	3
3.2	Test Components	4
3.3	Test Cases	4
3.3.1	Test Case R-CHU-CLA-TP.1	5
3.3.2	Test Case R-CHU-CLA-TP.2	6
3.3.3	Test Case R-CHU-CLA-TP.3	7
3.3.4	Test Case R-CHU-CLA-TP.4	8
3.3.5	Test Case R-CHU-CLA-TP.5	9

List of Tables

Table 1 - Applicable Requirements	3
Table 2 - Test Procedure: Components.....	4

1 Overview

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In addition to derived test requirements developed to test conformance to the NIST standard, GSA has established interoperability and performance metrics to further determine product suitability. Vendors whose products and services are deemed to be conformant with NIST standards and the GSA interoperability and performance criteria will be eligible to sell their products and services to the Federal Government.

1.1 Identification

This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the CHUID Authentication Reader (Contactless) (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.

2 Testing Process

As previously mentioned, this document prescribes detailed test steps that need to be executed in order to test the requirements applicable for this category. Please note that conformance to the tests specified in this document will not result in the Product being compliant to the applicable requirements of FIPS 201. The Product must undergo an evaluation using all the evaluation criteria listed for that category prior to being deemed as compliant. Only products and services that have successfully completed the entire Approval Process will be designated as conformant to the Standard. To this effect, this document only provides details for the evaluation using the Lab Test Data Report approval mechanism.

A Lab Engineer follows the steps outlined below in order to test those requirements that have been identified to be electronically tested. The end result is a compilation of the observed behavior of the Product in the Lab Test Data Report.

Section 3 provides the test procedures that need to be executed for evaluating the Product as conformant to the requirements of FIPS 201.

3 Test Procedure for CHUID Authentication Reader (Contactless)

3.1 Requirements

The following table provides a reference to the requirements that need to be electronically tested within the Lab as outlined in the Approval Procedures document for the Product. The different test cases that are used to check compliance to the requirements is also cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
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	R-CHU-CLA-TP.1 R-CHU-CLA-TP.2
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	R-CHU-CLA-TP.1 R-CHU-CLA-TP.2
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 4.2.1.1	R-CHU-CLA-TP.1
R-CHU-CLA.11	The authentication attempt shall compare the CHUID expiration date to the current date and determine card expiry.	FIPS 201, Section 6.2.2	R-CHU-CLA-TP.3
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, Section 6.2.2	R-CHU-CLA-TP.4
R-CHU-CLA.13	One or more of the CHUID data elements are used as input to the authorization check.	FIPS 201, Section 6.2.2	R-CHU-CLA-TP.5

Table 1 - Applicable Requirements

3.2 Test Components

Table 2 provides the details of all the components required by the Lab to execute this test procedure. Based on the different test cases, different components may be required to execute different test cases.

#	Component	Component Details	Identifier
1	The Card Reader Test Fixture	Includes a Workstation with the Card Reader Test Application installed and operational	CRTF
2	CHUID Authentication Reader (contactless) under test	-	PROD
3	A PIV Card that supports the Type A communication signal interface and transmission protocol only	SafesITe FIPS 201 applet on Gemalto GemCombi'Xpresso R4 E72K Card	PCARD-A
4	A PIV Card that supports the Type B communication signal interface and transmission protocol only	StepNexus PIV Application v4.2.1 on Keycorp MULTOS 64K Smart Card	PCARD-B
5	A metric ruler longer than 10 centimeters	-	RULER

Table 2 - Test Procedure: Components

3.3 Test Cases

This section discusses the various test cases that are needed to test the CHUID Authentication Reader (contactless) that use the contactless interface to read the CHUID data. Vendors submitting such Products may be required to demonstrate in the Lab that the product meets the same requirements mentioned in Section 3.1.

Vendors will be provided with an eight foot (8') table and four (4) 120 volt AC outlets. Vendor shall be given one (1) Lab workday to demonstrate products ability to meet the said requirements. Upon completion, Vendor is required to print the results of testing for each requirement, which will be incorporated into the Lab Test Data Report.

3.3.1 Test Case R-CHU-CLA-TP.1

3.3.1.1 Purpose

The purpose of this test is to verify that:

1. The contactless interface of the reader supports both the Type A communication signal interface as defined in ISO/IEC 14443-2:2001.
2. The contactless interface of the reader supports both the Type A transmission protocol as defined in ISO/IEC 14443-2:2001.

3.3.1.2 Test Setup

Equipment:	The following components are necessary for executing this test case: <ul style="list-style-type: none"> ▪ CRTF ▪ PCARD-A ▪ PROD ▪ RULER
Preparation:	<ul style="list-style-type: none"> ▪ Populate PCARD-A with a valid CHUID object. ▪ Configure PROD to allow access if presented with this CHUID (Note: The Product is to be configured such that the certificate that signed the CHUID is trusted by the PROD and that access is granted based on certain fields within this CHUID.) All fields in the CHUID should be in accordance to the Standard.

3.3.1.3 Test Process

Test Steps:	<ol style="list-style-type: none"> 1. Execute the Test Application on the CRTF. 2. Make sure that the details of the PCARD-A are entered into the Test Application by in the File → Edit Reference Contactless Card Implementation Info. 3. Select the tab for the “CHUID Authentication Reader (Contactless)”. This selects the test for the CHUID Authentication Reader (Contactless) in the Test Application. 4. Fill in all the information as required in the screen for the testing the PROD. 5. Select the Test Case radio button corresponding to R-CHU-CLA-TP.1 6. Bring the PCARD-A within 10 centimeters of the PROD. (Make sure the distance is measured with RULER) 7. Using PROD, attempt to perform the CHUID authentication use case. 8. Verify that the test was completed by reviewing the result on the screen. The test should complete successfully and access should be granted. 9. Take PCARD-A outside of the 10 centimeter range from the PROD 10. Once again attempt to perform the CHUID authentication use
--------------------	--

	<p>case.</p> <ol style="list-style-type: none"> 11. The PROD should not be able to read PCARD-A. 12. Enter any observations in the edit box for the R-CHU-CLA-TP.1 test case.
Expected Result(s):	<ol style="list-style-type: none"> 1. The test completes successfully for PCARD-A showing that the Product supports Type A communication signal interface and transmission protocol as defined in ISO/IEC 14443-2:2001 and ISO/IEC 14443-4:2001 respectively. 2. The PIV Card buffers are not readable through the contactless interface more than 10 cm from the reader.

3.3.2 Test Case R-CHU-CLA-TP.2

3.3.2.1 Purpose

The purpose of this test is to verify that:

1. The contactless interface of the reader supports both the Type B communication signal interface as defined in ISO/IEC 14443-2:2001.
2. The contactless interface of the reader supports both the Type B transmission protocol as defined in ISO/IEC 14443-2:2001.

3.3.2.2 Test Setup

Equipment:	<p>The following components are necessary for executing this test case:</p> <ul style="list-style-type: none"> ▪ CRTF ▪ PCARD-B ▪ PROD ▪ RULER
Preparation:	<ul style="list-style-type: none"> ▪ Populate PCARD-B with a valid CHUID object. ▪ Configure PROD to allow access if presented with this CHUID (Note: The Product is to be configured such that the certificate that signed the CHUID is trusted by the PROD and that access is granted based on certain fields within this CHUID.) All fields in the CHUID should be in accordance to the Standard.

3.3.2.3 Test Process

Test Steps:	<ol style="list-style-type: none"> 1. Select the Test Case radio button corresponding to R-CHU-CLA-TP.2 2. Make sure that the details of the PCARD-B are entered into the Test Application by in the File → Edit Reference Contactless Card Implementation Info 3. Bring the PCARD-B within 10 centimeters of the PROD. 4. Using PROD, attempt to perform the CHUID authentication use
--------------------	--

	<p>case.</p> <ol style="list-style-type: none"> 5. Verify that the test was completed by reviewing the result on the screen. The test should complete successfully and access should be granted. 6. Enter any observations in the edit box for the R-CHU-CLA-TP.2 test case.
Expected Result(s):	<ol style="list-style-type: none"> 1. The test completes successfully for PCARD-B showing that the Product supports Type B communication signal interface and transmission protocol as defined in ISO/IEC 14443-2:2001 and ISO/IEC 14443-4:2001 respectively.

3.3.3 Test Case R-CHU-CLA-TP.3

3.3.3.1 Purpose

The purpose of this test is to verify that the authentication attempt compares the CHUID expiration date to the current date and determines card expiry.

3.3.3.2 Test Setup

Equipment:	<p>The following components are necessary for executing this test case:</p> <ul style="list-style-type: none"> ▪ CRTF ▪ PCARD-A ▪ PROD ▪ RULER
Preparation:	<ul style="list-style-type: none"> ▪ Populate PCARD-A with a CHUID object that has expired (i.e. it has an expiry date in the past). All other fields in the CHUID should be valid and in accordance to the Standard.

3.3.3.3 Test Process

Test Steps:	<ol style="list-style-type: none"> 1. Select the Test Case radio button corresponding to R-CHU-CLA-TP.3 2. Bring the PCARD-A within 10 cm of the PROD. 3. Using PROD, attempt to perform the CHUID authentication use case. 4. The Product should indicate a failure, return an error and/or notify the user of an expired CHUID. 5. Enter any observations in the edit box for the R-CHU-CLA-TP.3 test case.
Expected Result(s):	<ol style="list-style-type: none"> 1. The PCARD-A was denied access because of an expired CHUID thereby proving that the Product is able to determine the expiration of the CHUID.

--	--

3.3.4 Test Case R-CHU-CLA-TP.4

3.3.4.1 Purpose

The purpose of this test is to verify that during the authentication attempt the digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered.

3.3.4.2 Test Setup

Equipment:	The following components are necessary for executing this test case: <ul style="list-style-type: none"> ▪ CRTF ▪ PCARD-A (2 Nos) ▪ PROD ▪ RULER
Preparation:	<ul style="list-style-type: none"> ▪ Generate test data that resembles CHUID objects. ▪ The 1st PCARD-A shall be configured to have a CHUID which has been altered (i.e. signature verification fails). ▪ The 2nd PCARD-A has the CHUID signed by a certificate that is not trusted by the Product. All fields in the CHUID should be in accordance to the Standard.

3.3.4.3 Test Process

Test Steps:	<ol style="list-style-type: none"> 1. Select the Test Case radio button corresponding to R-CHU-CLA-TP.4. 2. Bring the 1st PCARD-A within 10 cm of the PROD. 3. Using the PROD, attempt to perform the CHUID authentication use case. 4. Verify that the test was completed by reviewing the result on the Product. The Product should indicate a failure, return an error and/or notify the user of an altered CHUID. 5. Next, bring the 2nd PCARD-A within 10 cm of the PROD. 6. Using the PROD, attempt to perform the CHUID authentication use case. 7. Verify that the test was completed by reviewing the result on the Product. The Product should indicate a failure, return an error and/or notify the user of an untrusted CHUID. 8. Enter any observations in the edit box for the R-CHU-CLA-TP.4 test case.
Expected Result(s):	<ol style="list-style-type: none"> 1. Both of the PCARD-As were denied access because of an altered CHUID and non-trusted certificate used to sign the CHUID thereby showing that the Product is capable to ensure the CHUID

	was signed by a trusted source and is unaltered.
--	--

3.3.5 Test Case R-CHU-CLA-TP.5

3.3.5.1 Purpose

The purpose of this test is to verify that one or more of the CHUID data elements are used as input to the authorization check.

3.3.5.2 Test Setup

Equipment:	<p>The following components are necessary for executing this test case:</p> <ul style="list-style-type: none"> ▪ CRTF ▪ PCARD-A ▪ PROD ▪ RULER
Preparation:	<ul style="list-style-type: none"> ▪ Populate PCARD-A with a CHUID object. The PCARD-A shall be configured to have an incorrect data element on which the Product bases its access control decision on e.g. Access is granted for a particular agency code only, and the CHUID loaded on the PCARD-T1 has another agency code. (Note: The Product may have to be configured such that access is granted based on certain fields within the CHUID.) All fields in the CHUID should be in accordance to the Standard.

3.3.5.3 Test Process

Test Steps:	<ol style="list-style-type: none"> 1. Select the Test Case radio button corresponding to R-CHU-CLA-TP.5. 2. Bring the PCARD-A within 10 cm of the PROD. 3. Using the PROD, attempt to perform the CHUID authentication use case. 4. Verify that the test was completed by reviewing the result on the Product. The Product should deny access by indicating a failure or simply returning an error. 5. Enter any observations in the edit box for the R-CHU-CLA-TP.5 test case.
Expected Result(s):	<ol style="list-style-type: none"> 1. The Product is able to use one or more of the CHUID data elements as input for the authorization check.