

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

Version 1.0.0  
July 03, 2007



## Document History

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

## Table of Contents

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

## 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 (Contact) (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 (Contact)

#### 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-CA.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	R-CHU-CA-TP.1
R-CHU-CA.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	R-CHU-CA-TP.2
R-CHU-CA.10	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-CA-TP.3
R-CHU-CA.11	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-CA-TP.4
R-CHU-C.12	One or more of the CHUID data elements are used as input to the authorization check.	FIPS 201, Section 6.2.2	R-CHU-CA-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
---	-----------	-------------------	------------

#	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 (contact) under test	-	PROD
3	A PIV Card that supports the Class A operating Class only	SafesITe FIPS 201 applet on Gemalto GemCombi'Xpresso R4 E72K Card	PCARD-CLA
4	A PIV Card that supports the T=0 transmission protocol only	SafesITe FIPS 201 applet on Gemalto GemCombi'Xpresso R4 E72K Card	PCARD-T0
5	A PIV Card that supports the T=1 transmission protocol only	PIV EP v.108 Java Card Applet on Oberthur ID-One Cosmo 64 v5 Smart Card	PCARD-T1

Table 2 - Test Procedure: Components

### 3.3 Test Cases

This section discusses the various test cases that are needed to test CHUID Authentication Readers (contact) that use the contact 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-CA-TP.1

##### 3.3.1.1 Purpose

The purpose of this test is to verify that:

- i. The Reader supports the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.
- ii. The Reader supports T=0 transmission protocol as defined in ISO/IEC 7816-3:1997.

3.3.1.2 Test Setup

<b>Equipment :</b>	<p>The following components are necessary for executing this test case:</p> <ul style="list-style-type: none"> <li>▪ CRTF</li> <li>▪ PCARD-CLA</li> <li>▪ PROD</li> </ul>
<b>Preparation</b>	<ul style="list-style-type: none"> <li>▪ Populate PCARD-CLA<sup>1</sup> with a valid CHUID object.</li> <li>▪ 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.</li> </ul>

3.3.1.3 Test Process

<b>Test Steps:</b>	<ol style="list-style-type: none"> <li>1. Execute the Test Application on the CRTF.</li> <li>2. Make sure that the details of PCARD-CLA are entered into the Test Application using the File → Edit Reference Contact Card Implementation Info</li> <li>3. Select the tab for the “CHUID Authentication Reader (Contact)”. This selects the test for the CHUID Authentication Reader (Contact) in the Test Application</li> <li>4. Fill in all the information as required in the screen for the testing PROD.</li> <li>5. Insert PCARD-CLA into PROD.</li> <li>6. Select the Test Case radio button corresponding to R-CHU-CA-TP.1.</li> <li>7. Using PROD, attempt to perform the CHUID authentication use case.</li> <li>8. Verify that the test was completed by reviewing the result on the screen. The test should complete successfully and access should be granted.</li> <li>9. Enter any observations in the edit box for the R-CHU-C-TP.1 test case.</li> </ol>
<b>Expected Result(s):</b>	<ol style="list-style-type: none"> <li>1. The test completes successfully showing that the Product supports Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.</li> <li>2. The test verifies that the Product is able to support the T=0 transmission protocol as defined in ISO/IEC 7816-3:1997.</li> </ol>

<sup>1</sup> PCARD-CLA is the same as PCARD-T0.

### 3.3.2 Test Case R-CHU-CA-TP.2

#### 3.3.2.1 Purpose

The purpose of this test is to verify that the contact interface of the reader supports the T=1 transmission protocol as defined in ISO/IEC 7816-3:1997..

#### 3.3.2.2 Test Setup

<b>Equipment :</b>	The following components are necessary for executing this test case: <ul style="list-style-type: none"> <li>▪ CRTF</li> <li>▪ PCARD-T1</li> <li>▪ PROD</li> </ul>
<b>Preparation</b>	<ul style="list-style-type: none"> <li>▪ Populate PCARD-T1 with a valid CHUID object.</li> <li>▪ 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.</li> </ul>

#### 3.3.2.3 Test Process

<b>Test Steps:</b>	<ol style="list-style-type: none"> <li>1. Select the Test Case radio button corresponding to R-CHU-CA-TP.2</li> <li>2. Make sure that the details of PCARD-T0 are entered into the Test Application under File → Edit Reference Contact Card Implementation Info.</li> <li>3. Insert PCARD-T1 into PROD.</li> <li>4. Using the PROD, attempt to perform the CHUID authentication use case.</li> <li>5. Verify that the test was completed by reviewing the result on the Product. The test completes successfully and access is granted.</li> <li>6. Enter any observations in the edit box for the R-CHU-CA-TP.2 test case.</li> </ol>
<b>Expected Result(s):</b>	<ol style="list-style-type: none"> <li>1. The test completes successfully showing that the Product supports the T=1 transmission protocol as defined in ISO/IEC 7816-3:1997.</li> </ol>

### 3.3.3 Test Case R-CHU-CA-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

<b>Equipment:</b>	The following components are necessary for executing this test case: <ul style="list-style-type: none"> <li>▪ CRTF</li> <li>▪ PCARD-T1</li> <li>▪ PROD</li> </ul>
<b>Preparation:</b>	<ul style="list-style-type: none"> <li>▪ Populate PCARD-T1 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.</li> </ul>

3.3.3.3 Test Process

<b>Test Steps:</b>	<ol style="list-style-type: none"> <li>1. Select the Test Case radio button corresponding to R-CHU-CA-TP.3</li> <li>2. Insert PCARD-T1 into PROD.</li> <li>3. Using the PROD, attempt to perform the CHUID authentication use case.</li> <li>4. Verify that the test was completed by reviewing the result on the PROD. The reader should indicate a failure, return an error and/or notify the user of an expired CHUID.</li> <li>5. Enter any observations in the edit box for the R-CHU-CA-TP.3 test case.</li> </ol>
<b>Expected Result(s):</b>	<ol style="list-style-type: none"> <li>1. The PCARD-T1 was denied access because of an expired CHUID thereby proving that the Product is able to determine the expiration of the CHUID.</li> </ol>

3.3.4 Test Case R-CHU-CA-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

<b>Equipment:</b>	The following components are necessary for executing this test case: <ul style="list-style-type: none"> <li>▪ CRTF</li> <li>▪ PCARD-T1 (2 Nos)</li> <li>▪ PROD</li> </ul>
<b>Preparation:</b>	<ul style="list-style-type: none"> <li>▪ Generate test data that resembles CHUID objects.</li> <li>▪ The 1<sup>st</sup> PCARD-T1 shall be configured to have a CHUID which has been altered (i.e. signature verification fails).</li> <li>▪ The 2<sup>nd</sup> PCARD-T1 has the CHUID signed by a certificate that is</li> </ul>

	not trusted by the Product. All fields in the CHUID should be in accordance to the Standard.
--	--

3.3.4.3 Test Process

<b>Test Steps:</b>	<ol style="list-style-type: none"> <li>1. Select the Test Case radio button corresponding to R-CHU-CA-TP.4.</li> <li>2. Insert the 1<sup>st</sup> PCARD-T1 into PROD.</li> <li>3. Using the PROD, attempt to perform the CHUID authentication use case.</li> <li>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.</li> <li>5. Next, insert the 2<sup>nd</sup> PCARD-T1 into PROD.</li> <li>6. Using the PROD, attempt to perform the CHUID authentication use case.</li> <li>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</li> <li>8. Enter any observations in the edit box for the R-CHU-CA-TP.4 test case.</li> </ol>
<b>Expected Result(s):</b>	<ol style="list-style-type: none"> <li>1. Both of the PCARD-T1s 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</li> </ol>

3.3.5 Test Case R-CHU-CA-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

<b>Equipment:</b>	<p>The following components are necessary for executing this test case:</p> <ul style="list-style-type: none"> <li>▪ CRTF</li> <li>▪ PCARD-T1</li> <li>▪ PROD</li> </ul>
<b>Preparation:</b>	<ul style="list-style-type: none"> <li>▪ Populate PCARD-T1 with a CHUID object. The PCARD-T1 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</li> </ul>

	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

<b>Test Steps:</b>	<ol style="list-style-type: none"> <li>1. Select the Test Case radio button corresponding to R-CHU-CA-TP.5.</li> <li>2. Insert PCARD-T1 into PROD.</li> <li>3. Using the PROD, attempt to perform the CHUID authentication use case.</li> <li>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</li> <li>5. Enter any observations in the edit box for the R-CHU-CA-TP.5 test case.</li> </ol>
<b>Expected Result(s):</b>	<ol style="list-style-type: none"> <li>1. The Product is able to use one or more of the CHUID data elements as input for the authorization check.</li> </ol>