GSA U.S General Services Administration

CHUID Authentication Reader (Contact) Test Procedure

VERSION 2.0.0

April Giles
Nabil Ghadiali

FIPS 201 EVALUATION PROGRAM

June 28, 2010

Office of Governmentwide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	07/03/07	Initial Version	Public
Approved	2.0.0	06/28/10	Updated Test Components and Test Steps. Updated test cases to remove the ISO 7816 operating class A.	Public

Table of Contents

List of Tables

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.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 2.2.2.2 Para 1 pg.3	R-CHU-CA-TP.1 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 201-1, Section 6.2.2 Para 1 pg.48	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 201-1, Section 6.2.2 Para 1 pg.48	R-CHU-CA-TP.4
R-CHU-C.12	One or more of the CHUID data elements (e.g., FASC-N, Agency Code, Data Universal Numbering System [DUNS]) are used as input to the authorization check to determine whether the cardholder should be granted access.	FIPS 201-1, Section 6.2.2 Para 1 pg.48	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
1	CHUID Authentication Reader (contact) under	-	PROD

#	Component	Component Details	Identifier
	test		
2	A PIV Card that supports the T=0 transmission protocol only	SafesITe FIPS 201 applet on Gemalto GemCombi'Xpresso R4 E72K Card[1]	PCARD-T0
3	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
4	Data Populator Tool	For randomly generating and loading PIV Card containers	DPT

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 T=0 transmission protocol as defined in ISO/IEC 7816-3:1997.

3.3.1.2 Test Setup

Equipment :	The following components are necessary for executing this test case: ▪ PCARD-T0 ▪ PROD

[1] An appropriate PIV Card from the Approved Products List (APL) can be used as a substitute.

Preparation	▪ Populate PCARD-T0 with a valid CHUID object. ▪ Configure PROD to allow access if presented with this CHUID[2] (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:	1. Insert PCARD-T0 into PROD. 2. Using PROD, attempt to perform the CHUID authentication use case. 3. Verify that the tests were completed by reviewing the results on the PROD. The test should complete successfully and access should be granted[2]. 4. Document observed results.
Expected Result(s):	1. The test verifies that the Product is able to support the T=0 transmission protocol as defined in ISO/IEC 7816-3:1997.

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

Equipment :	The following components are necessary for executing this test case: ▪ PCARD-T1 ▪ PROD
Preparation	▪ Populate PCARD-T1 with a valid CHUID object. ▪ Configure PROD to allow access if presented with this CHUID[2] (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.

[2] This step is only applicable if the PROD has the ability to maintain an Access Control List (ACL) internally. If the PROD sends information (e.g. FASC-N) to PACS, then the Suppliers must be able to identify the information sent during the test to the Lab Engineer.

[2] If the PROD is capable of making access control decisions internally.

3.3.2.3 Test Process

Test Steps:	1. Insert PCARD-T1 into PROD. 2. Using the PROD, attempt to perform the CHUID authentication use case. 3. Verify that the test was completed by reviewing the result on the Product. The test completes successfully and access is granted.[3] 4. Verify that the tests were completed by reviewing the results on the PROD. Document observed results.
Expected Result(s):	1. The test completes successfully showing that the Product supports the T=1 transmission protocol as defined in ISO/IEC 7816-3:1997.

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

Equipment:	The following components are necessary for executing this test case: ▪ PCARD-T0 or PCARD-T1 (2 Nos.) ▪ PROD
Preparation:	▪ Populate PCARD-T0-1 with a CHUID object that has a corrupted date ▪ Populate PCARD-T0-2 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:	1. Using PCARD-T0, attempt to perform the CHUID authentication use case. 2. Using PCARD-T1, attempt to perform the CHUID authentication use case. 3. Verify that the tests were completed by reviewing the results on the PROD. Document observed results.
Expected Result(s):	1. The PCARD-T0 was denied access because of an invalid CHUID and PCARD-T1 was denied access because of an expired CHUID. 2. The Product indicates a failure, returns an error and/or notifies the

[3] If the PROD is capable of making access control decisions internally.

	user of the error reason.

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

Equipment:	The following components are necessary for executing this test case: ▪ PCARD-T0 or PCARD-T1 (5 Nos) ▪ PROD
Preparation:	▪ Populate PCARD-T0-1 with a CHUID that has been signed with a CHUID signer's certificate that has expired. ▪ Populate PCARD-T0-2 with a CHUID that has been signed with a CHUID signer's certificate that has been revoked. ▪ Populate PCARD-T0-3 with a CHUID that has been signed with a CHUID signer's certificate for which a certificate path cannot be built successfully (e.g. intermediate certificate revoked, certificate policy OID incorrect, or cannot chain to a valid configured trust anchor etc.). ▪ Populate PCARD-T0-4 with a CHUID whose signature has been altered. ▪ Populate PCARD-T0-5 a CHUID that has been signed with a CHUID signer's certificate for which certificate path can be built successfully to a valid configured trust[4] anchor. ▪ All other fields in the CHUID should be valid and in accordance to the Standard.

3.3.4.3 Test Process

Test Steps:	1. Using PCARD-T0-1, attempt to perform the CHUID authentication use case. 2. Using PCARD-T0-2, attempt to perform the CHUID authentication use case. 3. Using PCARD-T0-3, attempt to perform the CHUID authentication use case. 4. Using PCARD-T0-4, attempt to perform the CHUID

[4] Trust implies building a certification path from the CHUID Signing Certificate to a known Trust Anchor and determining its revocation status. This can be obtained in several ways including (i) performing standards-complaint path validation internally by the PROD, (ii) interfacing with an approved certificate validator (an EP category), and (iii) interfacing with an approved cached status proxy (an EP category).

	authentication use case. 5. Using PCARD-T0-5, attempt to perform the CHUID authentication use case. 6. Verify that the tests were completed by reviewing the results on the PROD. Document observed results.
Expected Result(s):	The PCARD-T0-1 was denied access[5] because of an expired CHUID signer's certificate. PCARD-T0-2 was denied access because of a revoked certificate. PCARD-T0-3 was denied access because the path validation failed. PCARD-T0-4 was denied access due to an invalid signature. The Product indicates a failure, returns an error and/or notifies the user of the error reason. PCARD-T0-5 was allowed access since the path validation completed successfully.

3.3.5 Test Case R-CHU-CA-TP.5[6]

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:	The following components are necessary for executing this test case: ▪ PCARD-T1 ▪ PROD
Preparation:	▪ 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. If access is granted for a particular agency code only, then the CHUID loaded on the PCARD-T1 must have another agency code. (Note: The Product may have to be configured such that access is granted based on certain fields within the CHUID**Error! Bookmark not defined.**.) All fields in the CHUID should be in accordance to the Standard.

3.3.5.3 Test Process

Test Steps:	1. Insert PCARD-T1 into PROD. 2. Using the PROD, attempt to perform the CHUID authentication use case. 3. Repeat the test based on the various fields supported by the

[5] If the PROD is capable of making access control decisions internally.

[6] This test needs to only be performed if the Reader is capable of making access control decisions internally.

	PROD in determining access control. 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 in cases where access was not granted.
Expected Result(s):	1. The Product is able to use one or more of the CHUID data elements as input for the authorization check.