GSA U.S General Services Administration

CHUID Authentication System Test Procedure

VERSION 1.0.0

April Giles
Nabil Ghadiali

FIPS 201 EVALUATION PROGRAM

May 19, 2009

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	05/19/2009	Initial Version	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 procedures that need to be executed by the Lab in order to evaluate a CHUID Authentication System (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 System

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 are cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
CHU-AS.2	The authentication attempt shall compare the CHUID expiration date to the current date and determine card expiry.	FIPS 201-1, Section 6.2.2	CHU-AS-TP.1
CHU-AS.3	To achieve single-factor authentication with CHUID, the relying parties must validate the signature on the CHUID.	SP 800-116, Section 7.1.3	CHU-AS-TP.2
CHU-AS.4	All access control decisions are made by comparing the 14 decimal digit FASC-N Identifier, and optionally the values of additional FASC-N fields, against the ACL entries.	SP 800-116, Section 6.2	CHU-AS-TP.3

Table 1 - Applicable Requirements

3.2 Test Components

Table 2 provides the details of all the components required by the Lab to execute the test procedures for the Product. Based on the different test cases, different components may be required for execution. It is the responsibility of the vendor to provide all the components required to carryout required test procedures for their Product.

#	Component	Component Details	Identifier
1	CHUID Authentication System[1]	-	PROD
2	A set of PIV Cards[2] (6 Nos.)	Any FIPS 201 EP approved PIV Card.	PCARD

Table 2 - Test Procedure: Components

[1] Prior to commencing testing, ensure that the Product has been setup and configured correctly. This includes setting of time parameters, configuration of appropriate access control permissions (based on CHUID data elements), loading of PKI trust anchors for path validation (if applicable) etc.

[2] Depending on whether the Product uses the contact or contactless interface, the Card should support T=0 or T=1 or of either Type A or Type B.

3.3 Test Cases

This section discusses the various test cases performed to check Product compliance to requirements outlined in the Approval Procedure for the Product. Vendors submitting Products may be required to demonstrate in the Lab[3] that the Product meets the requirements listed in Section 3.1.

Vendor shall be given one (1) Lab workday to demonstrate the Product's ability to meet test requirements. Upon completion, the Supplier is required to provide the results of testing for each requirement, which will be incorporated into the Lab Test Data Report.

3.3.1 Test Case CHU-AS-TP.1

3.3.1.1 Purpose

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

3.3.1.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD (2 Nos.) ▪ PROD
Preparation:	▪ Populate PCARD-1 with a CHUID object that is corrupted (i.e. it format is not per specifications). ▪ Populate PCARD-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.

3.3.1.3 Test Process

Test Steps:	1. Using PCARD-1, attempt to perform the CHUID authentication use case. 2. Using PCARD-2, 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):	The PCARD-1 was denied access because of an invalid CHUID and PCARD-2 was denied access because of an expired CHUID. The Product indicates a failure, returns an error and/or notifies the user of the error reason.

[3] Suppliers can co-ordinate with the Lab to perform Product testing at the Supplier's facility.

3.3.2 Test Case CHU-AS-TP.2

3.3.2.1 Purpose

The purpose of this test is to verify that the Product is able to conduct a standards-compliant PKI path validation on the CHUID signing certificate.

3.3.2.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD (2 Nos.) ▪ PROD
Preparation:	▪ Populate PCARD-1 with a valid CHUID object which has been altered (i.e. signature verification fails). ▪ Populate PCARD-2 with a valid CHUID object which is signed by a certificate that is not trusted[4] by the PROD.

3.3.2.3 Test Process

Test Steps:	1. Using PCARD-1, attempt to perform the CHUID authentication use case. 2. Using PCARD-2, 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):	The PCARD-1 was denied access because of an invalid/altered CHUID and PCARD-2 was denied access because of untrusted CHUID. The Product indicates a failure, returns an error and/or notifies the user of the error reason.

3.3.3 Test Case CHU-AS-TP.3

3.3.3.1 Purpose

The purpose of this test is to verify that the Product is able to make an access control decision by comparing the 14 decimal digit FASC-N Identifier against the Product ACL entries.

3.3.3.2 Test Setup

Equipment :	The following components are necessary for executing this test case: ▪ PCARD (2 Nos.) ▪ PROD

[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).

Preparation	▪ Populate PCARD-1 with a CHUID object that contains an invalid 14 digit FASC-N Identifier for which the PROD will not allow access. ▪ Populate PCARD-2 with a CHUID object that contains a valid 14 digit FASC-N Identifier for which the PROD will allow access[5].

3.3.3.3 Test Process

Test Steps:	1. Using PCARD-1, attempt to perform the CHUID authentication use case. 2. Using PCARD-2, 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):	The PCARD-1 was denied access because of a CHUID not authorized for access. The Product indicates a failure, returns an error and/or notifies the user of the error reason. PCARD-2 was granted access because of valid and authorized CHUID.

[5] This assumes that the CHUID is unexpired, unaltered and signed with a certificate that is trusted by the PROD.