U.S General Services Administration

Biometric 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 Biometric 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 Biometric 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 #
BIO-AS.3	Reader contains an integrated {within the same housing} PIN input device	FIPS 201-1, Section 4.5.3	BIO-AS-TP.2
BIO-AS.4	The reader shall provide the personal identification number (PIN) to the card to access the biometric stored on the PIV Card.	Derived	BIO-AS-TP.2
BIO-AS.5	The authentication attempt shall compare the CHUID expiration date to the current date and determine card expiry.	FIPS 201-1, Section 6.2.2	BIO-AS-TP.1
BIO-AS.6	{The Product performs a 1:1 biometric match using the enrollment template and the live authentication template.}	FIPS 201-1, Section 6.2.3.1	BIO-AS-TP.2
BIO-AS.7	{The Product} extracts the FASC-N in the Signed Attributes field of the biometric signature block and compare to the FASC-N found in the CHUID.	FIPS 201-1, Section 6.2.3.1	BIO-AS-TP.3
BIO-AS.8	A PACS {must} always verify the digital signature on the biometric template data object, and do path validation.	SP 800-116 Section 7.1.6	BIO-AS-TP.4
BIO-AS.11	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	BIO-AS-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 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	Biometric Authentication System[1]	-	PROD
2	A set of PIV Cards (10 Nos.)	Any FIPS 201 EP approved PIV Card.	PCARD

Table 2 - Test Procedure: Components

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[2] 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 BIO-AS-TP.1

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.

3.3.1.1 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).

[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 FASC-N data elements), loading of PKI trust anchors for path validation (if applicable), configuration of algorithms etc.

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

	All other fields in the CHUID should be valid and in accordance to the Standard.

3.3.1.2 Test Process

Test Steps:	1. Using PCARD-1, attempt to perform the Biometric authentication use case. 2. Using PCARD-2, attempt to perform the Biometric 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.

3.3.2 Test Case BIO-AS-TP.2

3.3.2.1 Purpose

The purpose of this test is to verify that the Product:

- Has an integrated PIN input device within the Reader to be used to access the Biometric fingerprints
- Performs a 1:1 biometric match using the enrollment template and the live authentication template.

3.3.2.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD ▪ PROD
Preparation:	▪ Populate PCARD with a valid Biometric Fingerprint Template[3].

3.3.2.3 Test Process

Test Steps:	1. Using PCARD, attempt to perform the biometric authentication use case, by an individual whose fingerprints are not the ones loaded 2. Repeat step 1. with the individual whose fingerprints are the ones loaded on the reference smart card 3. Verify that the tests were completed by reviewing the results on the PROD. Document observed results.

[3] All fields must be per FIPS 201 specifications and the biometric template signed by an issuer whose certificate is trusted by the PROD.

Expected Result(s):	The first attempt was denied access because the 1:1 biometric fingerprint match failed. The Product indicates a failure, returns an error and/or notifies the user of the error reason. The second attempt was allowed access since the 1:1 biometric match and the path validation completed successfully.

3.3.3 Test Case BIO-AS-TP.3

3.3.3.1 Purpose

The purpose of this test is to verify that the Product:

- Extracts the FASC-N in the Signed Attributes field of the biometric signature block and compare to the FASC-N found in the CHUID.

3.3.3.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD ▪ PROD
Preparation:	▪ Populate PCARD with a valid Biometric Fingerprint Template[4] and a valid CHUID where the FASC-N in the Signed Attributes field of the biometric does not match the FASC-N in the CHUID.

3.3.3.3 Test Process

Test Steps:	1. Using PCARD, attempt to perform the biometric authentication use case. 2. Verify that the tests were completed by reviewing the results on the PROD. Document observed results.
Expected Result(s):	The authorization attempt was denied access because the FASC-N match failed. The Product indicates a failure, returns an error and/or notifies the user of the error reason.

3.3.4 Test Case BIO-AS-TP.4

3.3.4.1 Purpose

The purpose of this test is to verify that the Product:

- Is capable of conducting a standards-compliant PKI path validation[5] on the biometric signer's certificate

[4] All other fields must be per FIPS 201 specifications and the biometric template signed by an issuer whose certificate is trusted by the PROD.

3.3.4.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD (4 Nos.) ▪ PROD
Preparation:	▪ Populate PCARD-1 with a biometric template that has been signed with a biometric signer's certificate that has expired. ▪ Populate PCARD-2 with a biometric template that has been signed with a biometric signer's certificate that has been revoked. ▪ Populate PCARD-3 with a biometric template that has been signed with a biometric 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-4[6] a biometric template that has been signed with a biometric signer's certificate for which certificate path can be built successfully to a valid configured trust anchor. All other fields in the Biometric Template should be valid and in accordance to the Standard.

3.3.4.3 Test Process

Test Steps:	1. Using PCARD-1, attempt to perform the biometric authentication use case. 2. Using PCARD-2, attempt to perform the biometric authentication use case. 3. Using PCARD-3, attempt to perform the biometric authentication use case. 4. Using PCARD-4, attempt to perform the biometric authentication use case. 5. 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 expired biometric signer's certificate. PCARD-2 was denied access because of a revoked certificate, and PCARD-3 was denied access because the path validation failed. The Product indicates a failure, returns an error and/or notifies the user of the error reason.

[5] Trust validation implies building a certification path from the Biometric signer's 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).

[6] It is assumed that the FASC-N contained in the biometric template/CHUID has the appropriate values set so as to be granted access and the 1:1 biometric match is completed successfully.

	PCARD-4 was allowed access since the path validation completed successfully.

3.3.5 Test Case PIV-AS-TP.5

3.3.5.1 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.

3.3.5.2 Test Setup

Equipment :	The following components are necessary for executing this test case: ▪ PCARD (2 Nos.) ▪ PROD
Preparation	▪ Populate PCARD-1 with a biometric template and CHUID that contains an invalid 14 digit FASC-N Identifier for which the PROD will not allow access. ▪ Populate PCARD-2 with a biometric template and CHUID that contains a valid 14 digit FASC-N Identifier for which the PROD will allow access[7].

3.3.5.3 Test Process

Test Steps:	1. Using PCARD-1, attempt to perform the biometric authentication use case. 2. Using PCARD-2, attempt to perform the biometric 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 the FASC-N was 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 FASC-N within the biometric template and CHUID.

[7] This assumes that the biometric signer’s certificate is unexpired, not-revoked and can be validated to a Trust Anchor that is trusted by the PROD.