GSA U.S General Services Administration

Authentication Key Reader Test Procedure

VERSION 4.0.0

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
Draft	0.0.1	03/20/06	Document creation.	Limited
Draft	0.1.0	03/21/06	Submitted to GSA for approval.	GSA
Draft	0.1.1	04/21/06	Updated based on feedback from GSA.	Limited
Draft	0.2.0	04/21/06	Submitted to GSA for approval.	GSA
Draft	0.2.1	05/19/06	Updated based on feedback from GSA.	Limited
Draft	0.2.2	05/22/06	Updated based on feedback from GSA.	Limited
Approved	1.0.0	05/23/06	Approved by GSA.	Public
Revision	1.0.1	06/29/06	Updated based on feedback from GSA.	Limited
Revision	1.1.0	06/29/06	Submitted to GSA for approval.	GSA
Approved	2.0.0	06/30/06	Approved by GSA.	Public
Approved	3.0.0	07/03/07	Updated to include test scenarios for PKI path validation and revocation checking.	Public
Approved	4.0.0	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 Authentication Key Reader (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 Authentication Key Reader

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-AUK.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-AUK-TP.2
R-AUK.9	{The reader shall be able to read the PIV Authentication buffer on the PIV Card.}	Derived	R-AUK-TP.1
R-AUK.10	{The reader shall be able to generate and send a cryptographic challenge to the PIV Card.}	FIPS 201-1 Section 6.2.4 Para 1 pg.50	R-AUK-TP.1
R-AUK.11	{The reader shall be able to decrypt and match the cryptographic response from the PIV Card.}	FIPS 201 Section 6.2.4 Para 1 pg.50	R-AUK-TP.1
R-AUK.13	{The reader shall be able to determine the validity of the PIV Authentication Certificate.}	Derived	R-AUK-TP.3
R-AUK.14	{The reader shall be able to conduct a standards-compliant PKI path validation on the PIV Authentication Certificate.} The related digital certificate is checked to ensure that it is from a trusted source.	FIPS 201-1 Section 6.2.4 Para 1 pg. 50	R-AUK-TP.4
R-AUK.15	{The revocation status of the certificate is checked to ensure current validity.}	FIPS 201-1 Section 6.2.4 Para 1 pg.50	R-AUK-TP.5
R-AUK.17	The reader shall be able to parse the PIV Authentication Certificate	FIPS 201-1	R-AUK-TP.6

	to extract relevant fields (signer DN, FASC-N) for the purpose of access control.	Section 6.2.4 Para 1 pg.50	

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	Authentication Key Reader under test	-	PROD
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[1]	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 the Product against the requirements mentioned above. 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.

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

3.3.1 Test Case R-AUK-TP.1

3.3.1.1 Purpose

The purpose of this test is to verify that:

i. The Reader supports the T=0 transmission protocol as defined in ISO/IEC 7816-3:1997
ii. The Reader is capable of reading the PIV Authentication buffer on the PIV Card.
iii. The Reader is capable of generating and sending a cryptographic challenge to the PIV Card; and
iv. The Reader is capable of decrypting and matching the cryptographic response from the PIV Card.

3.3.1.2 Test Setup

Equipment :	The following components are necessary for executing this test case: ▪ PCARD-T0 ▪ PROD
Preparation	▪ Populate PCARD-T0 with a PIV Authentication Key and Certificate. ▪ Configure PROD such that the PIV Authentication Certificate is trusted (i.e. a valid certification path can be built from the PIV Authentication Certificate to a trust anchor/Root CA trusted by the PROD.) ▪ Make sure that the PROD has been configured with a current certificate revocation list (CRL) in order to determine the status of the PIV Authentication Certificate. ▪ Configure PROD to allow access[2] if presented with this PIV Authentication Certificate (i.e. access control decision is based on one of the fields in the Certificate e.g. FASC-N or Subject DN)

3.3.1.3 Test Process

Test Steps:	1. Insert PCARD-T0 into PROD. 2. Using PROD, attempt to perform the PIV Asymmetric Cryptography authentication use case. 3. Verify that the test was completed by reviewing the result on the Product. The test should complete successfully and access should be granted. 4. Document observed results.
Expected Result(s):	1. The Reader supports the T=0 transmission protocol as defined in ISO/IEC 7816-3:1997 2. The Reader is capable of reading the PIV Authentication buffer

[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.

	on the PIV Card. 3. The Reader is capable of generating and sending a cryptographic challenge to the PIV Card; and 4. The Reader is capable of decrypting and matching the cryptographic response from the PIV Card.

3.3.2 Test Case R-AUK-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 PIV Authentication Key and Certificate. ▪ Configure PROD such that the PIV Authentication Certificate is trusted (i.e. a valid certification path can be built from the PIV Authentication Certificate to a trust anchor/Root CA trusted by PROD.) ▪ Make sure that the PROD has been configured with a current certificate revocation list (CRL) in order to determine the status of the PIV Authentication Certificate. ▪ Configure PROD to allow access[3] if presented with this PIV Authentication Certificate (i.e. access control decision is based on one of the fields in the Certificate e.g. FASC-N or Subject DN)

3.3.2.3 Test Process

Test Steps:	1. Insert PCARD-T1 into PROD. 2. Using PROD, attempt to perform the PIV Asymmetric Cryptography authentication use case. 3. Verify that the test was completed by reviewing the result on the Product. The test should complete successfully and access should be granted[4]. 4. 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] 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.

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

	3:1997.

3.3.3 Test Case R-AUK-TP.3

3.3.3.1 Purpose

The purpose of this test is to verify that the reader is able to determine the expiration date of the PIV Authentication Certificate.

3.3.3.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD-T0 ▪ PCARD-T1 ▪ PROD
Preparation:	▪ Populate PCARD-T0 with a PIV Authentication Certificate that is corrupted (i.e. it format is not per specifications e.g. invalid date). ▪ Populate PCARD-T1 with a PIV Authentication Certificate that has expired (i.e. it has an expiry date in the past).

3.3.3.3 Test Process

Test Steps:	1. Insert PCARD-T0 into PROD. 2. Using PROD, attempt to perform the PIV Asymmetric Cryptography authentication use case. 3. Insert PCARD-T1 into PROD. 4. Using PROD, attempt to perform the PIV Asymmetric Cryptography authentication use case. 5. Verify that the tests were completed by reviewing the results on the PROD for each case. 6. Document observed results.
Expected Result(s):	1. The test completes successfully showing that the Product is able to determine the expiration date of the PIV Authentication Certificate.

3.3.4 Test Case R-AUK-TP.4

3.3.4.1 Purpose

The purpose of this test is to verify that the reader is able to conduct a standards-compliant PKI path validation on the PIV Authentication Certificate. The related digital certificate is checked to ensure that it is from a trusted source[5].

[5] Trust implies building a certification path from the PIV Authentication Certificate to a known Trust Anchor and determining its revocation status. This can be obtained in several ways including (i) performing

3.3.4.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD-T0 ▪ PROD
Preparation:	▪ Populate PCARD-T0 with a PIV Authentication Key and Certificate. ▪ Configure PROD such that the PIV Authentication Certificate is not trusted (i.e. a valid certification path cannot be built from the PIV Authentication Certificate to a trust anchor/Root CA trusted by PROD.)

3.3.4.3 Test Process

Test Steps:	1. Insert PCARD-T0 into PROD. 2. Using PROD, attempt to perform the PIV Asymmetric Cryptography authentication use case. 3. Verify that the tests were completed by reviewing the results on the PROD. 4. Document observed results.
Expected Result(s):	1. The test completes successfully showing that the Product is able to conduct a standards-compliant PKI path validation on the PIV Authentication Certificate. The related digital certificate is checked to ensure that it is from a trusted source. 2. PCARD-T0 was denied access[6] because the path validation failed. The Product indicates a failure, returns an error and/or notifies the user of the error reason.

3.3.5 Test Case R-AUK-TP.5

3.3.5.1 Purpose

The purpose of this test is to verify that the reader is able to check the revocation status of the certificate to ensure current validity.

3.3.5.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD-T0 ▪ PROD
Preparation:	▪ Populate PCARD-T0 with a PIV Authentication Key and Certificate. ▪ Configure PROD such that the PIV Authentication Certificate is trusted (i.e. a valid certification path can be built from the PIV Authentication Certificate to a trust anchor/Root CA trusted by

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

	PROD.) ▪ Make sure that the PROD has been configured with a current certificate revocation list (CRL) in order to determine the status of the PIV Authentication Certificate. Note: - The PIV Authentication Certificate (i.e. its serial number) must appear on the CRL for successful completion of this test case.

3.3.5.3 Test Process

Test Steps:	1. Insert PCARD-T0 into PROD. 2. Using the PROD, attempt to perform the PIV Asymmetric Cryptography authentication use case. 3. Verify that the test was completed by reviewing the result on the PROD. The test should complete successfully and access should not be granted since the PIV Authentication Certificate was revoked. The Product should return an error or simply deny access[7].
Expected Result(s):	1. The test completes successfully showing that the Product is able to check the revocation status for the PIV Authentication Certificate prior to allowing access.

3.3.6 Test Case R-AUK-TP.6[8]

3.3.6.1 Purpose

The purpose of this test is to verify that the reader is able to parse the PIV Authentication Certificate to extract relevant fields (signer DN, FASC-N) for the purpose of access control.

3.3.6.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ PCARD-T0 ▪ PROD
Preparation:	▪ Populate PCARD-T0 with a PIV Authentication Key and Certificate. ▪ Configure PROD such that the PIV Authentication Certificate is trusted (i.e. a valid certification path can be built from the PIV Authentication Certificate to a trust anchor/Root CA trusted by PROD.) ▪ Make sure that the PROD has been configured with a current certificate revocation list (CRL) in order to determine the status of the PIV Authentication Certificate.

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

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

	▪ Configure PROD such that it doesn't allow access if presented with this PIV Authentication Certificate (i.e. access control decision is based on one of the fields in the Certificate e.g. FASC-N or Subject DN whose value isn't that present in the Certificate)

3.3.6.3 Test Process

Test Steps:	1. Insert PCARD-T0 into PROD. 2. Using the PROD, attempt to perform the PIV Asymmetric Cryptography use case. 3. Verify that the test was completed by reviewing the result on the Product. The test should complete successfully and access should not be granted since the values of the fields in the PIV Authentication Certificate (e.g. FASC-N or Subject DN) were not permitted for access. The Product should return an error or simply deny access. 4. Repeat the test based on the various fields supported by the PROD in determining access control. Document the results for each case.
Expected Result(s):	1. The test completes successfully showing that the Product is able to parse the PIV Authentication Certificate to extract relevant fields (signer DN, FASC-N) for the purpose of access control.