

**PIV Authentication System
Approval Procedure**

VERSION 2.0.0

**April Giles
Nabil Ghadiali**



FIPS 201 EVALUATION PROGRAM

April 14, 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	05/15/2009	Initial Version	Public
Approved	2.0.0	04/14/2010	Updated to incorporate key size and algorithm support requirements from SP 800-78-2	Public

Table of Contents

Office of Governmentwide Policy Office of Technology Strategy Identity Management Division Washington, DC 20405	1
1 Introduction.....	1
1.1 Overview.....	1
1.2 Category Description	1
1.3 Purpose.....	1
2 Application Package Contents.....	3
2.1 Compatibility Acknowledgement	3
3 Evaluation Procedure for the PIV Authentication System.....	5
3.1 Requirements	5
3.2 Approval Mechanism Matrix.....	7
3.3 Evaluation Criteria.....	7
3.3.1 Vendor Documentation Review.....	7
3.3.2 Vendor Test Data Report	7
3.3.2.1 PIV-AS.2.....	7
3.3.2.2 PIV-AS.6.....	9
3.3.2.3 PIV-AS.7.....	9
3.3.3 Lab Test Data Report	10
3.3.4 Certification	10
3.3.5 Attestation	11

List of Tables

Table 1 - Applicable Requirements	6
Table 2 - Approval Mechanism Matrix	7

1 Introduction

1.1 Overview

The FIPS 201 Evaluation Program (EP) is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency. The goal of the FIPS 201 Evaluation Program (EP) is to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. In addition to derived test requirements developed to test conformance to the National Institute of Standards and Technology (NIST) Standard, GSA has also established interoperability and performance metrics to further determine product suitability. A set of approval and test procedures have been developed which outline the evaluation criteria, approval mechanisms and test process employed by the Laboratory during their evaluation of a Supplier's product or service against the requirements for that category.

A Supplier submitting a PIV Authentication System (hereafter referred to as the Product) which is a physical access control system that implements the PIV Authentication use case for evaluation must follow the Suppliers Policies and Procedures Handbook. In addition to this handbook, the Supplier also needs to refer to this Approval Procedure which provides the necessary category-specific details in order to have a Supplier's Product evaluated by the EP and placed on the Approved Products List (APL).

1.2 Category Description

The PIV Authentication System product category provides the capability to perform a cryptographic challenge/response with the PIV Authentication Key stored on PIV Card and makes an authorization decision based on the FASC-N stored on the PIV Card. Implementing the PIV Authentication use case is a multi-step process requiring the integration of several components referred to herein as a "System". These components include but may not be limited to: (i) transparent reader (an EP category), (ii) access controllers, and (iii) host system consisting of application software and PIV-specific middleware (an EP category). In addition, depending on the architecture of the PACS, other components may also be utilized to meet the functional requirements of the PACS PIV Authentication use case (as defined in FIPS 201-1).

At a high-level, the PIV Authentication System performs the following: 1) cryptographic challenge/response with the PIV authentication key and corresponding certificate, 2) validation of the PIV Authentication certificate and 3) access control decision. Readers in this product category must use the contact interface.

1.3 Purpose

The purpose of this document is to provide the following information:

- (i) Provide a list of the artifacts and/or documentation that needs to be submitted to the Evaluation Lab as part of the application package submission.
- (ii) Document the list of the requirements that apply to this category

- (iii) Specify the evaluation criteria along with their approval mechanisms that will be used by Evaluation Labs to verify compliance of the Product against the requirements that apply to this category.

2 Application Package Contents

The Application Package Contents include the artifacts, documentation and in some cases the product itself that needs to be submitted to the Evaluation Lab so that evaluation can be performed. The Application Package Contents for this category include the following:

- Completed Application Form, provided on the Evaluation Program website. (This form will be available through the web interface once users have been assigned a login credential.);
- Completed and signed Lab Service Agreement (found in the application submission package ZIP file). The Lab Service Agreement should be completed and scanned into a document to be uploaded to the Evaluation Program website;
- Completed and signed Attestation Form (found in the application submission package ZIP file). The Attestation Form should be completed and scanned into a document to be uploaded to the Evaluation Program website;
- Completed Supplier VDR-VTDR justification worksheet (found in the application submission package ZIP file);
- A Vendor Test Data Report, which provides test results showing that the Product complies with the requirements for this category. In this regard, the Supplier is expected to develop and document the test procedures used to determine how the Product was tested to arrive at the conclusion that it met all necessary requirements. The VTDR must typically contain information as stated in Section 3.2. Wherever possible, information to be supplied as part of this Vendor Test Data Report has been described in Section 3.3;
- Official Certification documentation from the appropriate entity (e.g., NIST) showing conformance of the Product to the tested requirements of FIPS 201. Specific reference to the exact type of certification necessary can be found in the Section 3.3; and
- All necessary Supplier documentation providing proof that the Product complies with the subset of requirements (as outlined in Section 3.1) for this category which has Supplier documentation review as its approval mechanism. Examples of specific documentation would include: user guides, technical specifications, white papers, line cards, etc.

For requirements that have an approval mechanism as Lab Test Data Report, the Supplier must be able to demonstrate product's capability of meeting these requirements from Section 3.0. The Product may be setup and configured by the Supplier at either the Supplier or Lab location.

2.1 Compatibility Acknowledgement

For a Product to be submitted under this category, it needs to meet all requirements as stated in Section 3.1. However, in the event that the Supplier's Product interfaces with another product/service (specifically to meet PIV-AS.6) to implement the required functionality, the Supplier needs to perform the following activities:

- Submit the Product and include details on the product/service(s) it is capable of interfacing with.

- Obtain a letter from the Supplier of the interfaced product/service(s) stating that the product being submitted is known to work with that product/service. This letter needs to be submitted by the Supplier along with their application package. Please note that this letter doesn't eliminate the requirement for Lab Testing as per the Test Procedure.

3 Evaluation Procedure for the PIV Authentication System

3.1 Requirements

In order to approve the Product as conformant to the requirements of PIV, it at a minimum, must comply with all the requirements listed below. The approval mechanism column describes the technique utilized by the Lab to evaluate compliance to that particular requirement.

Identifier #	Requirement Description	Source	Reqt. #	Approval Mechanism
PIV-AS.1	{Reader used shall be listed on FIPS 201 Evaluation Program Approved Products List under the Transparent Reader ¹ category.}	Derived	10-16	Certification
PIV-AS.2	{The Product shall be capable of performing an asymmetric cryptographic challenge/response with the PIV Card.}	Derived	10-22	Vendor Test Data Report Lab Test Data Report
PIV-AS.3	The PACS must support all of the asymmetric algorithms permitted for the PIV Authentication Key, as specified in Table 3-1 of SP800-78-2 ² .	SP 800-116, Section 6.1 Para 1 pg.19	9-11	Vendor Documentation Review
PIV-AS.4	{The reader shall be able to provide the personal identification number (PIN) to the card to access the PIV Authentication Key stored on the PIV Card.}	Derived	10-18	Vendor Documentation Review Lab Test Data Report
PIV-AS.5	{Reader used shall include integrated PIN input device.}	FIPS 201-1, Section 4.5.3 Para 1 pg.37	1.1-153	Vendor Documentation Review Lab Test Data Report
PIV-AS.6	The response signature is verified and standards-compliant {(IETF X.509 path	FIPS 201-1 Section 6.2.4	1.1-215	Vendor Documentation

¹ Alternately, the Reader used within the System must meet all requirements from Section 3.1 of the most current version of the Transparent Reader Approval Procedure or the Authentication Key Reader Approval Procedure.

² Only FIPS 140-2 approved algorithms within the Cryptographic Module are permitted for use by the System

	validation)} PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity.	Para 1 pg.50		Review Vendor Test Data Report Lab Test Data Report Certification ³
PIV-AS.7	{ 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 Para 4 pg.21	9-16	Vendor Test Data Report Lab Test Data Report Vendor Documentation Review
PIV-AS.8	{ The cryptographic module(s) used shall be validated to FIPS 140-2. }	Derived from Appendix B.4 FIPS 201-1	10-25	Certification
PIV-AS.9	{ If the Product uses middleware to communicate with the PIV Card (e.g. as part of Card Management System functionality), this middleware is approved by the GSA FIPS 201 Evaluation program as approved PIV Middleware. }	Derived	10-26	Certification
PIV-AS.10	{ If the Product interfaces with a Certificate Validator to perform certificate path discovery and validation, it uses a GSA FIPS 201 EP approved SCVP client. }	Derived	10-20	Certification

Table 1 - Applicable Requirements

³ This approval mechanism is necessary only if the Product internally performs path discovery and validation.

3.2 Approval Mechanism Matrix

The table below provides an indication of the total number of requirements applicable for the Product and identifies the approval mechanisms that will be used during the evaluation by the Lab.

Total Requirements	Approval Mechanisms					
	SV	VTDR	LTDR	VDR	C	A
10	N/A	✓	✓	✓	✓	✓
Legend: SV – Site Visit; VTDR – Vendor Test Data Report; LTDR – Lab Test Data Report; VDR – Vendor Doc. Review; C – Certification; A – Attestation						

Table 2 - Approval Mechanism Matrix

3.3 Evaluation Criteria

This section provides details on the process employed by the Lab for evaluating the Product against the requirements enumerated above.

3.3.1 Vendor Documentation Review

Reference(s):	PIV-AS.3 to PIV-AS.7
Evaluation Procedure:	<ol style="list-style-type: none"> The Lab will update the status in the Web-Enabled Tool to “VDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide. The Lab will review the Supplier’s documentation to determine the following: <ul style="list-style-type: none"> <i>Algorithm Support (PIV-AS.3)</i> <ul style="list-style-type: none"> The algorithms supported by the Product used within the PIV Authentication use case including how the algorithm to be used is selected by the Product. Only acceptable algorithms from Table 3-1 of SP 800-78-2 to be used. Evidence shall be demonstrated using the Security Policy of the cryptographic module being used. <i>PIN Provisioning (PIV-AS.4, PIV-AS.5)</i> <ul style="list-style-type: none"> The capability of the Reader(s) to be able to provide the PIN to the PIV Card to access the PIV Authentication Key. Integration of the PIN input device within the Reader. <i>Validation of PIV Authentication Certificate (PIV-AS.6)</i> <ul style="list-style-type: none"> The Product’s capability to (i) perform standards-compliant path validation internally, (ii) to interface with an approved credential validator (an EP category), (iii) to interface with an approved cached status proxy (an EP category) In case of option (i), follow steps from Section 3.3.4. In case of options (ii) and (iii), review the letter from the Suppliers with which the product is capable of interfacing. a. Basis for Access Control Decision (PIV-AS.7)

	<ul style="list-style-type: none"> The Product's ability in terms of the FASC-N fields it supports for making access control decisions. <ol style="list-style-type: none"> The Lab will update the status to "VDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	<ol style="list-style-type: none"> The reader is able to provide the PIN to the PIV Card to access the PIV Key. Reader includes integrated PIN input device. The Product is capable of validating the PIV Authentication certificate using one or more of the options as identified. The Product is capable of making access control decision based on at least prescribed 14 digits within the FASC-N (Agency Code, System Code, and Credential Number.)

3.3.2 Vendor Test Data Report

The Lab will update the status in the Web-Enabled Tool to "VTDR Begun" as instructed in the Web-enabled Tool Laboratory User Guide.

3.3.2.1 PIV-AS.2

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <i>Asymmetric Cryptographic Challenge/Response:</i> The Product is capable of executing asymmetric cryptographic challenge/response. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> A report generated as a result of testing which shows that a cryptographic challenge has been generated and sent to the card. The report should also show the plaintext output of the challenge that was sent to the PIV Card. A report generated as a result of testing which shows an encrypted response returned from the PIV Card. At the minimum, the report should display: <ul style="list-style-type: none"> The encrypted response returned from the Card The result of the decryption operation The algorithm⁴ used to decrypt the data is inline with those specified in SP 800-78-2. The public key that was used to decrypt the response The original challenge that matches the decrypted response
Expected Result:	<ol style="list-style-type: none"> The Product is capable of generating a cryptographic challenge and transmitting it to the PIV Card.

⁴ VTDRs demonstrating support for RSA and ECDSA need to be provided if the Product supports both of these algorithms.

	2. The decrypted response from the card should match the value reported in the plaintext output of the challenge that was sent to the PIV Card
--	--

3.3.2.2 PIV-AS.6

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • <i>PKI Path Validation:</i> The capability of the Product to validate the PIV Authentication Certificate. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Populate test PIV Cards (T=0 or T=1) with following types of PIV Authentication Certificates: <ol style="list-style-type: none"> An expired certificate A revoked certificate A valid certificate whose 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.) A valid certificate whose certificate path can be built successfully. Attempt to present the above-configured PIV Cards to the Product and note the results.
Expected Result:	The Product successfully validates the PIV Authentication certificate. All cases except the last result in access being denied.

3.3.2.3 PIV-AS.7

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • 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. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> Populate test PIV Cards (T=0 or T=1) with following types of FASC-N configurations within the PIV Authentication Certificate: <ol style="list-style-type: none"> A valid FASC-N with the Agency Code, System Code, or Credential Number incorrect such that access will be denied) A valid FASC-N with the Agency Code, System Code, and Credential Number correct, however if the Product is capable of using additional fields from the FASC-N, then one of those fields is incorrect. This test card is optional
------------------------------	--

	<p>based on the capability of the Product.</p> <ul style="list-style-type: none"> iii. A valid FASC-N with the Agency Code, System Code, and Credential Number correct iv. A valid FASC-N with the Agency Code, System Code, and Credential Number correct and other fields within the FASC-N used for access control also set correctly. This test card is also optional based on the capability of the Product. <ul style="list-style-type: none"> b. Configure the Product appropriately to ensure access is granted for correctly presented FASC-N values. c. Attempt to present the above-configured PIV Cards to the Product and note the results.
Expected Results:	For test scenario executed, the Product shall not grant access to the cardholder based on the incorrect FASC-N elements. The Product returns an error indicator or simply denies access.

The Lab will update the status in the Web-Enabled Tool to “VTDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.

3.3.3 Lab Test Data Report

Reference(s):	PIV-AS.2, PIV-AS.4 to PIV-AS.7
Test Procedure:	<ol style="list-style-type: none"> 1. The Lab will update the status in the Web-Enabled Tool to “LTDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide. 2. The Lab will execute test procedures for this category in accordance with the “<i>PIV Authentication System Test Procedure</i>.” 3. The Lab will update the status to “LTDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	The Product successfully passes all the test cases documented within the test procedure.

3.3.4 Certification

Reference(s):	PIV-AS.1, PIV-AS.6, PIV-AS.8 to PIV-AS.10
Evaluation Procedure:	<ol style="list-style-type: none"> 1. The Lab will update the status in the Web-Enabled Tool to “C Begun” as instructed in the Web-enabled Tool Laboratory User Guide. 2. The Lab will perform the following activities in order to determine status of the PIV Middleware used by the Product (if applicable): <ul style="list-style-type: none"> ▪ Review the FIPS 201 EP APL to determine inclusion of the PIV Middleware used by the Product. The list is available on the website located at: http://fips201ep.cio.gov/apl.php 3. The Lab will perform the following activities to determine the Product’s ability to perform Path Discovery and Validation (PD-VAL). This is required if the Product performs PD-VAL functions internally. <ul style="list-style-type: none"> ▪ Review the list of products approved by the Federal PKI Policy Authority for use by Federal agencies in implementing PD-VAL in a Bridge-enabled environment. The list is available on the website

	<p>located at: http://www.cio.gov/fpkia/validation_solutions.htm</p> <ol style="list-style-type: none"> 4. The Lab will perform the following activities in order to determine status of the Reader with the FIPS 201 Approved Products List: <ul style="list-style-type: none"> ▪ Review the FIPS 201 APL to determine inclusion of the Reader. The list is available on the website located at: http://fips201ep.cio.gov/apl.php 5. The Lab will perform the following activities for the Cryptographic Module in order to determine certification status of the Product with FIPS 140-2 requirements: <ul style="list-style-type: none"> ▪ Examine the certification statement to see if it provided by the NIST/CSE and that it is still current i.e. valid; ▪ Verify the authenticity of this certification provided by the NIST/CSE; and ▪ Review the FIPS 140-2 Cryptographic Modules Validation List to determine inclusion of the Product and the level at which it has been certified. The list is available on the website located at: http://csrc.nist.gov/cryptval/140-1/1401val.htm. 1. The Lab will perform the following activities in order to determine status of the SCVP client used by the Product (if applicable): <ul style="list-style-type: none"> ▪ Review the FIPS 201 EP APL to determine inclusion of the SCVP Client used by the Product. The list is available on the website located at: http://fips201ep.cio.gov/apl.php 6. The Lab will update the status to “C Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	<ol style="list-style-type: none"> 1. PIV Middleware used is listed on the FIPS 201 APL 2. Path Discovery and Validation is performed by an approved module. 3. Transparent Reader(s) used is listed on FIPS 201 APL 4. The Cryptographic Module has been found to be certified by NIST/CSE at FIPS 140-2. 5. The Product uses approved SCVP Client to interface with a certificate validator to obtain certificate status information.

3.3.5 Attestation

Reference(s):	N/A
Evaluation Procedure:	<ol style="list-style-type: none"> 1. The Lab will update the status in the Web-Enabled Tool to “A Begun” as instructed in the Web-enabled Tool Laboratory User Guide. 2. Review the Attestation Form provided by the Supplier, confirming that the Product to the best of their knowledge, conforms to all the necessary requirements of the category under which the Product applies. Verify that person signing this Attestation Form has the authority to do so (a minimum “C” level [e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner]). 3. The Lab will update the status in the Web-Enabled Tool to “A Complete” as instructed in the Web-enabled Tool Laboratory User Guide.

Expected Results:	1. The Attestation Form has been signed by an authorized individual (e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner).
--------------------------	--

Appendix A—Document Release Summary of Changes

Identifier #	Reference	Description of Change
PIV-AS.3	Section 3.1, Pg. 5	Updated for key size and algorithm support based on SP 800-78-2
PIV-AS.9	Section 3.1, Pg.6	Updated Text.