

**Caching Status Proxy
Approval Procedure**

VERSION 1.0.0

April Giles
Nabil Ghadiali



FIPS 201 EVALUATION PROGRAM

May 15, 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	05/15/2009	Initial Version	Public

Table of Contents

1	Introduction	1
1.1	Overview	1
1.2	Category Description	1
1.3	Purpose.....	1
2	Application Package Contents	2
2.1	Compatibility Acknowledgement	2
3	Evaluation Procedure for Cached Status Proxy.....	3
3.1	Requirements	3
3.2	Approval Mechanism Matrix.....	5
3.3	Evaluation Criteria	5
3.3.1	Vendor Documentation Review.....	5
3.3.2	Vendor Test Data Report	5
3.3.2.1	CSP.3	5
3.3.2.2	CSP.5	7
3.3.3	Certification	8
3.3.4	Attestation	9
	Appendix A— Document Release Summary of Changes.....	10

List of Tables

Table 1 - Applicable Requirements	4
Table 2 - Approval Mechanism Matrix	5

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 Caching Status Proxy (hereafter referred to as the Product) 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 caching status proxy is a product (hardware and/or software) that polls the status of all registered PIV Cards periodically, and cache the status responses from their issuer(s). Caching status proxies are useful in scenarios that require extremely quick query-responses for certificate revocation status information or when physical access control systems need to cache certificate revocation information so as to be able to make an access control decision when on-line certificate validation is not possible.

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 Forms (found in the application submission package ZIP file). The Attestation Forms 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 at a 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 4.3; and
- All necessary Supplier documentation providing proof that the Product complies with the subset of requirements (as outlined in Section 4.1) for this category which has Vendor documentation review as its approval mechanism. Examples of specific documentation would include: user guides, technical specifications, white papers, line cards, etc.

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 CSP.3) 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 Cached Status Proxy

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	Req. #	Approval Mechanism
CSP.1	If a caching status proxy is employed, information about the cardholder {for performing all PIV authentication mechanisms}, including the cardholder's certificate, must be added to the database {used}.	SP 800-116, Section 7.4	N/A	Vendor Documentation Review Vendor Test Data Report
CSP.2	Enrollment using a caching status proxy {shall} collect and store information required for all supported FIPS 201 authentication mechanisms needed. {i.e. PIV, BIO, CHUID and CAK},	SP 800-116, Section 7.4	N/A	Vendor Documentation Review
CSP.3	The caching status proxy obtains the PIV Authentication or asymmetric Card Authentication Key certificate from the PIV Card, validates the certificate (including checking the certificate's revocation status), and sends a challenge to the card to verify that the card holds the private key corresponding to the certificate prior to adding it to its database along with other information regarding the individual.	SP 800-116, Section 7.4	N/A	Vendor Documentation Review Vendor Test Data Report Certification ¹
CSP.4	The cached data shall be protected against tampering.	SP 800-116, Section 7.5	N/A	Vendor Documentation Review
CSP.5	The caching status proxy shall	SP 800-116,	N/A	Vendor

¹ This approval mechanism is necessary only if the Product internally performs path discovery and validation.

Identifier #	Requirement Description	Source	Reqt. #	Approval Mechanism
	periodically re-validate all of the certificates in its database. The cache status must be updated at least once every 24 hours.	Section 7.4		Documentation Review Vendor Test Data Report
CSP.6	The caching status proxy shall deactivate the access privileges of any {registered} individual {in the database} whose certificate has expired or has been revoked.	SP 800-116, Section 7.4	N/A	Vendor Documentation Review Vendor Test Data Report
CSP.7	The CHUID may be collected at registration, but it should be treated as if it were a password for purposes of retention, i.e., hashed, the hash stored, and the CHUID deleted.	SP 801-116, Section 7.4	N/A	Vendor Documentation Review
CSP.8	If the Product is capable of registering PIV information directly from a PIV Card, it uses GSA FIPS 201 EP approved PIV Middleware.	Derived	N/A	Certification
CSP.9	The Product must support all of the asymmetric algorithms permitted for the PIV Authentication Key and/or Card Authentication Key, as specified in Table 3-1 of SP 800-78-1, i.e., RSA 1024 (through 31 December 2013), RSA 2048, and ECDSA P-256.	SP 800-116, Section 6.1	N/A	Vendor Documentation Review
CSP.10	The Product uses a cryptographic module validated to FIPS 140-2.	Derived	N/A	Certification
CSP.11	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	N/A	Certification

Table 1 - Applicable Requirements

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
11	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):	CSP.1, CSP.2, CSP.3, CSP.4, CSP.5, CSP.7, CSP.8, CSP.9
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>Collection and Storage of Information (CSP.1, CSP.2)</i> <ul style="list-style-type: none"> Identification of all information that is being stored within the Product’s database including an explanation on why each information type is collected and how it will be used. <i>Validation process prior to Registration (CSP.3)</i> <ul style="list-style-type: none"> Description of the process of challenge/response including how the algorithm to be used is selected by the Product. Algorithms used must be inline with those specified in CSP.9. The Product’s capability to (i) perform standards-complaint path validation internally, and/or (ii) to interface with an approved certificate validator (an EP category) In case of option (i), follow steps from Section 3.3.3. In case of option (ii), review the letter from the Supplier with which the Product is capable of interfacing. <i>Data Protection (CSP.4)</i> <ul style="list-style-type: none"> The options available and the mechanism by which the Product protects all the registered data from authorized access or tampering (i.e. confidentiality and integrity of the data).

	<ul style="list-style-type: none"> ▪ <i>Periodic Re-Validation (CSP.5)</i> <ul style="list-style-type: none"> • The Product's capabilities in how it performs re-validation of the information to ensure that each record is still valid, including time frequency² at which such re-validation occurs. • <i>Currency of Access Privileges (CSP.6)</i> <ul style="list-style-type: none"> • Description of how the Product identifies records with certificates that have expired or been revoked, including situations where revocation status was not able to be determined. • Description on how the updated information is shared with the PACS • <i>Interface for Registration of PIV Data (CSP.8)</i> <ul style="list-style-type: none"> • Description of the mechanisms by which the Product is able to read/extract data to be registered. • <i>Asymmetric Algorithms supported (CSP.9)</i> <ul style="list-style-type: none"> • Enumeration of all the algorithms supported for the PIV Authentication Key and/or the Card Authentication Key that are used to perform cryptographic challenge response prior to registration. Evidence of algorithm support needs to be provided via the Security Policy for the cryptographic module being used.
Expected Results:	The Product capability is inline with the requirements identified.

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 CSP.3

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • The registration process of adding information into the Product once it has been validated. • Ability to perform cryptographic challenge responses <p>At a minimum, the following test scenarios must be performed to confirm compliance:</p> <p><u>TEST 1</u></p> <ol style="list-style-type: none"> a. Populate test PIV Cards (T=0 or T=1) with following types of certificates (PIV and/or CAK): <ol style="list-style-type: none"> i. An expired certificate
------------------------------	--

² Maximum time configurable must not exceed 24 hrs.

	<ul style="list-style-type: none"> ii. A revoked certificate iii. 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.) iv. A valid certificate whose certificate path can be built successfully. <p>b. Present the test PIV Cards with the various configurations to the Product and perform registration of the user information.</p> <p><u>TEST 2</u></p> <ul style="list-style-type: none"> a. 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. b. 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 algorithm used to decrypt the data is inline with those specified in SP 800-78-1. • The public key that was used to decrypt the response • The original challenge that matches the decrypted response
Expected Results:	<p>The Product shall not register the cardholder for cases where the information could not be successfully validated. The Product returns a clear error message informing the user of the error condition.</p> <p>The Product is capable of performing cryptographic challenge responses and uses specified algorithms to do so.</p>

3.3.2.2 CSP.5

Evaluation Procedure:	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> • The capability of the Product to re-validate the certificates registered. <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ul style="list-style-type: none"> a. Register four (4) valid records of PIV data within the Product. Note - All records must be valid at the time of registration. b. Configure these records as follows <ul style="list-style-type: none"> i. Record 1 - Has a certificate (PIV or CAK) that is expired
------------------------------	--

	<ul style="list-style-type: none"> ii. Record 2 - Has a certificate that has been revoked iii. Record 3 - Has a certificate for which one of the CRLs in its certification path cannot be accessed (e.g., server not available online) iv. Record 4 - A valid record <p>c. Attempt to validate the above identified records again as per configuration set within the Product for automatic re-validation.</p>
Expected Results:	The Product successfully re-validates the PIV certificate(s) and is capable of providing a distinction between valid and invalid records, or records for which the status was unknown.

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 Certification

Reference(s):	CSP.3, CSP.8, CSP.10 and CSP.11
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 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 4. 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 located at: http://www.cio.gov/fpkia/validation_solutions.htm 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

	<p>been certified. The list is available on the website located at: http://csrc.nist.gov/cryptval/140-1/1401val.htm</p> <p>6. The Lab will update the status to “C Complete” as instructed in the Web-enabled Tool Laboratory User Guide.</p>
Expected Results	<ol style="list-style-type: none"> 1. The Product uses approved PIV Middleware to interact with PIV Cards for registration of their information. 2. The Product uses approved SCVP Client to interface with a certificate validator to obtain certificate status information. 3. The Product is on the Qualified Validation List (QVL) and is approved by the Federal PKI Policy Authority for use by Federal agencies in implementing PD-VAL in a Bridge-enabled environment. 4. The Cryptographic Module has been found to be certified by NIST/CSE at FIPS 140-2.

3.3.4 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:	<ol style="list-style-type: none"> 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
N/A	N/A	N/A