

**Certificate Validator (without
client authentication)
Approval Procedure**

VERSION 1.0.0

April Giles
Nabil Ghadiali



FIPS 201 EVALUATION PROGRAM

March 26, 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	03/26/2010	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
3	Evaluation Procedure for Certificate Validator	3
3.1	Requirements	3
3.2	Approval Mechanism Matrix.....	4
3.3	Evaluation Criteria.....	4
3.3.1	Vendor Documentation Review.....	4
3.3.2	Vendor Test Data Report	4
3.3.2.1	CV.3, CV.4	4
3.3.3	Certification	4
3.3.4	Attestation.....	6
	Appendix A— Document Release Summary of Changes	7

List of Tables

Table 1 - Applicable Requirements	3
Table 2 - Approval Mechanism Matrix	4

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 Certificate Validator (without client authentication) for evaluation, hereafter referred to as the Product, 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 *Certificate Validator (without client authentication)* is a product that is used to determine if a presented identity credential (PKI certificate) is valid, i.e. was legitimately issued and has not expired or been terminated. The Certificate Validator uses the processes of path validation to verify the binding between the subject identifier and the subject public key in the certificate, based on the public key of a trust anchor through the validation of a chain of certificates that begins with a certificate issued by the trust anchor and ends with the target certificate. This product does not have the capability to authenticate clients that communicate with it.

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 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 and signed Non-Disclosure Agreement (found in the application submission package ZIP file). The Non-Disclosure Agreement should be completed and scanned into a document to be uploaded to the Evaluation Program website;

Note: This NDA can be substituted with a Supplier-provided document; however, this will slow the evaluation process as the NDA submitted will need to be reviewed by the Lab.

- Completed Supplier VDR-VTDR justification worksheet (found in the application submission package ZIP file); 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 Supplier documentation review as its approval mechanism. Examples of specific documentation would include: user guides, technical specifications, white papers, line cards, etc.

3 Evaluation Procedure for Certificate Validator (without client authentication)

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
CV.1	The Product must be compliant with RFC 5055 – Server-based Certificate Validation Protocol. ¹	Derived	-	Vendor Documentation Review Lab Test Data Report
CV.2	The Product has demonstrated Path Discovery and Validation capability using the PKITS and the Path Discovery Test Suite.	Derived	-	Certification
CV.3	The {SCVP Response} must be signed with a public key or hash algorithm that satisfies the requirements for signing new PIV information, as specified in Table 3-3 ² .	Derived from SP 800-78-1, Section 4	-	Vendor Documentation Review Vendor Test Data Report
CV.4	The object identifiers specified in Table 3-4 must be used in CRLs and {SCVP} messages to identify the signature algorithm.	Derived from SP 800-78-1, Section 4	-	Vendor Documentation Review Vendor Test Data Report
CV.5	The cryptographic module used for signing {SCVP responses} shall be validated to FIPS 140-2 with an overall Security Level 2 (or higher).	FIPS 201-1, Section B.4	1.1-221	Certification

Table 1 - Applicable Requirements

¹ At a minimum, the Product needs to comply with the most current version of the GSA EP - CCV RTM as it relates to the Responder, except for the ability to digitally sign SCVP requests and established a client authenticated SSL connection.

² Larger key sizes and hash algorithms are acceptable.

3.2 Approval Mechanism Matrix

The table below provides an indication of the total number of requirements applicable for the Product and provides a breakup of how the evaluation will be conducted based on the different approval mechanisms available to the Lab.

Total Requirements	Approval Mechanisms					
	SV	VTDR	LTDR	VDR	C	A
5	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):	CV.1, CV.3
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 documentation submitted by the Supplier to ascertain the following: <ul style="list-style-type: none"> <i>Compliance to RFC 5055 (CV.1)</i> <ul style="list-style-type: none"> The compliance of the Product to RFC 5055 – “Server-Based Certificate Validation Protocol (SCVP)”. <i>Hash Algorithms and Key Sizes (CV.3)</i> <ul style="list-style-type: none"> Capability of the Product of being configured to use the appropriate hash algorithms and key sizes to sign SCVP Responses in accordance with Table 3-3. Evidence shall be provided using the Security Policy of the cryptographic module used. <i>Signature Algorithm Object Identifiers (CV.4)</i> <ul style="list-style-type: none"> Usage of the appropriate OIDs as specified in Table 3-4 for signature algorithm used to sign the SCVP responses. The Lab will update the status to “VDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Result:	<ol style="list-style-type: none"> The Product is compliant with RFC 5055. The Product is capable of being configured to use the public key size and hash algorithms as specified in Table 3-3 of SP 800-78-1 for generating SCVP response signatures. The Product uses the appropriate signature algorithms to sign the SCVP

	responses.
--	------------

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 CV.3, CV.4

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>Key Size and Hash Algorithm Conformance:</i> The Product has been tested to verify that the SCVP responses sent to relying parties are signed in accordance requirements for key sizes found in SP 800-78-1, Table 3-3 and hash algorithms specified in Table 3-4. <p>As a result of testing, the following must be included as part of the Vendor Test Data forwarded to the Lab:</p> <ol style="list-style-type: none"> Using the GSA-provided SCVP client, send a certificate status request to the Product. After retrieving the status of the certificate in question, capture the outgoing SCVP response back to the relying party. Convert the binary data captured to a textual form, of the ASN.1 format of the RFC 5055 status response sent back to the relying party. Identify, in the ASN.1 dump, the public key value and size as well as the hash algorithm OID that was used to generate the signature. Repeat Steps a-e for all key sizes and hash algorithms supported by the Product. (Note: - Only those key sizes and algorithms that are demonstrated within the VTDR will be listed as supported.)
Expected Result:	The key size and hash algorithms, as identified in the submitted content of the ASN.1 data, has been verified to conform with Table 3-3 and Table 3-4.

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):	CV.2, CV.5
----------------------	------------

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 for the Cryptographic Module in order to determine certification status of the Product with FIPS 140-2 Level 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. 3. The Lab will perform the following activities to determine the Product’s ability to perform Path Discovery and Validation (PD-VAL): <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 4. 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. The Cryptographic Module has been found to be certified by NIST/CSE at FIPS 140-2 Level 2. 2. 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.

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