FIPS 201 Evaluation Program -
OCSP Responder Approval Procedure

Version 7.0.0
October 31, 2007

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	04/04/06	Document creation.	Limited
Draft	0.1.0	04/04/06	Submitted to GSA for approval.	GSA
Approved	1.0.0	04/12/06	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
Revision	1.1.1	06/30/06	Updated based on feedback from GSA.	Limited
Revision	1.2.0	06/30/06	Submitted to GSA for approval	GSA
Approved	2.0.0	06/30/06	Approved by GSA.	Public
Revision	2.0.1	08/21/06	Updated based on feedback from GSA	Limited
Revision	2.1.0	08/21/06	Submitted to GSA for approval	GSA
Approved	3.0.0	09/12/06	Approved by GSA	Public
Approved	4.0.0	02/09/07	Updated to include process for product updates, resubmissions and evaluation fees	Public
Approved	5.0.0	04/02/07	Updated with details for the evaluation fees.	Public
Approved	6.0.0	04/26/07	Updated with details for the upgrade process.	Public
Revision	6.1.0	10/22/07	Updated based on requirements from SP 800-78-1. Updated to split approval processes from document. Processes can now be found in Suppliers Handbook.	GSA
Approved	7.0.0	10/31/07	Approved by GSA	Public

Table of Contents

List of Tables

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 desiring to submit a Online Certificate Status Protocol (OCSP) Responder (hereafter referred to as the Product) for evaluation must follow the Suppliers Policies and Procedures Handbook. In addition to this handbook, Supplier also need 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 *Online Certificate Status Protocol (OCSP) Responder* is a product that is used to provide OCSP responses in accordance with RFC 2560 for queries by relying parties (by means of an OCSP request) regarding the revocation status of certificates issued by a Certification Authority.

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 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 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 Online Certificate Status Protocol (OCSP) Responder

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
OCSP.1	OCSP [RFC2560] status responders shall be implemented as a supplementary certificate status mechanism.	FIPS 201-1, Section 5.4.5.2	1.1-203	Vendor Documentation Review Vendor Test Data Report
OCSP.2	The OCSP status responses are digitally signed to support authentication and integrity using a public key and hash algorithm at least as large as that used to sign the certificate.	SP 800-78-1, Section 4	5.1-24	Vendor Documentation Review Vendor Test Data Report
OCSP.3	The OCSP message can also be signed with a larger public key or hash algorithm that satisfies the requirements for signing new PIV information, as specified in Table 3-3.	SP 800-78-1, Section 4	5.1-25	Vendor Documentation Review Vendor Test Data Report
OCSP.4	The object identifiers specified in Table 3-4 must be used in CRLs and OCSP messages to identify the signature algorithm.	SP 800-78-1, Section 4	5.1-26	Vendor Documentation Review Vendor Test Data Report
OCSP.5	The cryptographic module used for signing [OCSP 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

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	4	N/A	4	1	1
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):	OCSP.1, OCSP.2, OCSP.3, OCSP.4
Evaluation Procedure:	1. The Lab will update the status in the Web-Enabled Tool to "VDR Begun" as instructed in the Web-enabled Tool Laboratory User Guide. 2. The Lab will review the documentation submitted by the Supplier to ascertain the following: ▪ *Compliance to RFC 2560 (OCSP.1)* • The compliance of the Product to RFC 2560 – "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol". ▪ *Hash Algorithms and Key Sizes (OCSP.2, OCSP.3)* • Capability of the Product of being configured to use the appropriate hash algorithms and key sizes to sign OCSP Responses in accordance with Table 3-3. ▪ *Signature Algorithm Object Identifiers (OCSP.4)* • Usage of the appropriate OIDs as specified in Table 3-4 for signature algorithm used to sign the OCSP responses. 3. The Lab will update the status to "VDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Result:	1. The Product is compliant with RFC 2560. 2. 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 OCSP response signatures. 3. The Product uses the appropriate signature algorithms to sign the OCSP 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 OCSP.1, OCSP.2

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *RFC 2560 Conformance*: The Product has been tested to verify that the OCSP messages sent to relying parties are in accordance with the protocol specified in RFC 2560. As a result of testing, the following must be included as part of the Vendor Test Data forwarded to the Lab: a. Using an OCSP client, send a certificate status request to the OCSP responder Product. b. After retrieving the status of the certificate in question, capture the outgoing OCSP response back to the relying party. Identify the CA certificate used verify certificates issued by that CA and identify the signature on the OCSP response sent back to the relying party. c. Convert the binary data captured to a textual form, of the ASN.1 format of the RFC 2560 status response sent back to the relying party. d. If variable length key sizes are supported to sign the OCSP response, based on the key size of the certificate in question, repeat steps a-c for each key size supported by the Product.
Expected Result:	The content of the ASN.1 data has been verified to conform with the ASN.1 module found in Appendix A of RFC 2560. The key size supported by the product is at least as large as the CA key used to sign certificates.

3.3.2.2 OCSP.3, OCSP.4

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *Key Size and Hash Algorithm Conformance*: The Product has been tested to verify that the OCSP messages 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. As a result of testing, the following must be included as part of the Vendor Test Data forwarded to the Lab: a. Using an OCSP client, send a certificate status request to the OCSP responder Product. b. After retrieving the status of the certificate in question, capture

	the outgoing OCSP response back to the relying party. c. Convert the binary data captured to a textual form, of the ASN.1 format of the RFC 2560 status response sent back to the relying party. d. Identify, in the ASN.1 dump, both the public key value and size as well as the hash algorithm OID that was used to generate the signature. e. Repeat Steps a-e for all key sizes and hash algorithms supported by the Product.
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):	OCSP.5
Evaluation Procedure:	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: ▪ 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 update the status to "C Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results	1. The Cryptographic Module has been found to be certified by NIST/CSE at FIPS 140-2 Level 2.

3.3.4 Attestation

Reference(s):	N/A

Evaluation Procedure:	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).