FIPS 201 Evaluation Program - Cryptographic Module Approval Procedure

Version 7.0.0
October 31, 2007

GSA

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	03/20/06	Document creation	Limited
Draft	0.1.0	03/20/06	Submitted to GSA for approval	GSA
Draft	0.1.1	04/05/06	Updated based on feedback from the EPTWG	Limited
Draft	0.2.0	04/05/06	Submitted to GSA for approval	GSA
Approved	1.0.0	04/07/06	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	Limited
Approved	3.0.0	09/08/06	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
Approved	7.0.0	10/31/07	Updated to split approval processes from document. Processes can now be found in Suppliers Handbook.	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 Cryptographic Module (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 *Cryptographic Module* is hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms and provides capabilities to generate, store and protect cryptographic keying material securely. Cryptographic modules are made use of in a number of places within the PIV system architecture including but not limited to the PIV Card, Certification Authorities providing the PKI credentials, OCSP Responders and Card Management Systems.

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.

- 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 Section 4.3.

3   Evaluation Procedure for Cryptographic Module

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
CM.1	All the cryptographic modules in the PIV system shall be validated to FIPS 140-2 with an overall Security Level 2 (or higher).	FIPS 201, Appendix B – 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**	**LDTR**	**VDR**	**C**	**A**
1	N/A	N/A	N/A	N/A	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 Certification

Reference(s):	CM.1

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.

3.3.2 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).