GSA U.S General Services Administration

SCVP Client (without authentication capability) Test Procedure

VERSION 2.0.0

April Giles
Nabil Ghadiali

FIPS 201 EVALUATION PROGRAM

November 10, 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	04/06/2010	Initial Version	Public
Approved	2.0.0	11/10/2010	Updated the test process	Public

Table of Contents

List of Tables

1 Overview

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In addition to derived test requirements developed to test conformance to the NIST standard, GSA has established interoperability and performance metrics to further determine product suitability. Vendors whose products and services are deemed to be conformant with NIST standards and the GSA interoperability and performance criteria will be eligible to sell their products and services to the Federal Government.

1.1 Identification

This document provides the detailed test procedures that need to be executed by the Lab in order to evaluate a SCVP Client (without authentication capability) (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.

2 Testing Process

As previously mentioned, this document prescribes detailed test steps that need to be executed in order to test the requirements applicable for this category. Please note that conformance to the tests specified in this document will not result in the Product being compliant to the applicable requirements of FIPS 201. The Product must undergo an evaluation using all the evaluation criteria listed for that category prior to being deemed as compliant. Only products and services that have successfully completed the entire Approval Process will be designated as conformant to the Standard. To this effect, this document only provides details for the evaluation using the Lab Test Data Report approval mechanism.

A Lab Engineer follows the steps outlined below in order to test those requirements that have been identified to be electronically tested. The end result is a compilation of the observed behavior of the Product in the Lab Test Data Report.

Section 3 provides the test procedures that need to be executed for evaluating the Product as conformant to the requirements of FIPS 201.

3 Test Procedure for SCVP Client

3.1 Requirements

The following table provides a reference to the requirements that need to be electronically tested within the Lab as outlined in the Approval Procedures document for the Product. The different test cases that are used to check compliance to the requirements are cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
CLI.1	The Product must be compliant with RFC 5055 – Server-based Certificate Validation Protocol. [1]	Derived	CLI-TP.1

Table 1 - Applicable Requirements

3.2 Test Components

Table 2 provides the details of all the components required by the Lab to execute the test procedures for the Product. Based on the different test cases, different components may be required for execution. It is the responsibility of the vendor to provide all the components required to carryout required test procedures for their Product.

#	Component	Component Details	Identifier
1	SCVP Client (without authentication capability) [2]	-	PROD
2	Data Populator Tool	Current Version	DATA-GEN
3	GSA Central Certificate Validator	Online GSA Certificate Validator service (SCVP Responder)	CCV
4	Test Certificates[3]	PIV Authentication Certificates generated using DATA-GEN	CERT

Table 2 - Test Procedure: Components

[1] At a minimum, the Product needs to comply with the most current version of the GSA EP – CCV Request and Response Profiles as it relates to the Client, except for the ability to digitally sign SCVP requests and establish a client authenticated SSL connection.

[2] Prior to commencing testing, ensure that the Product has been setup and configured correctly. This includes but not limited to setting of SCVP configuration options, communication options/parameters, trust anchors etc.

[3] It is assumed that there is a mechanism to pass the certificates to the SCVP client in order to create the SCVP request.

3.3 Test Cases

This section discusses the various test cases performed to check Product compliance to requirements outlined in the Approval Procedure for the Product. Vendors submitting Products may be required to demonstrate in the Lab that the Product meets the requirements listed in Section 3.1.

Vendor shall be given one (1) Lab workday to demonstrate the Product's ability to meet test requirements. Upon completion, the Supplier is required to provide the results of testing for each requirement, which will be incorporated into the Lab Test Data Report.

3.3.1 Test Case PIV-AS-TP.1

3.3.1.1 Purpose

The purpose of this test is to verify that the Product:

- Is compliant with RFC 5055 – Server-based Certificate Validation Protocol.

3.3.1.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CERT (4 Nos.) ▪ DATA-GEN ▪ PROD ▪ CCV
Preparation:	▪ Using DATA-GEN, generate the following types of PIV Authentication certificates: a) CERT-1 (with corresponding private key) that is expired b) CERT-2 (with corresponding private key) that is revoked c) CERT-3 (with corresponding private key) for which a certificate path cannot be built successfully (e.g. certificate policy OID incorrect, or cannot chain to a valid configured trust anchor etc.) d) CERT-4 (with corresponding private key) for which certificate path can be built successfully to a valid configured trust anchor. **Note**: - All other fields in the PIV Authentication certificate should be valid and in accordance to the Standard. ▪ Configure the PROD and the CCV to accept unsigned requests over HTTP

3.3.1.3 Test Process

Test Steps:	After completing each test, the Lab must capture a screenshot of CERT's validation status displayed in PROD. All screen captures must be uploaded into appropriate case number in the Web Enabled Tool (WET). 1. Using CERT-1, attempt to perform the PIV authentication use case with the CCV. 2. Using CERT-2, attempt to perform the PIV authentication use case with the CCV.

	3. Using CERT-3, attempt to perform the PIV authentication use case with the CCV. 4. Using CERT-4, attempt to perform the PIV authentication use case with the CCV. 5. Repeat steps 1 through 4 with the CCV and PROD configured for unsigned requests over HTTPs (server-side) 6. Verify that the tests were completed by reviewing the results on the PROD. Document observed results.
Expected Result(s):	In all scenarios tested: 1. CERT-1 is rejected because of an expired PIV authentication certificate. 2. CERT-2 is rejected because of a revoked certificate, and CERT-3 is rejected because the path validation failed. 3. CERT-4 was accepted since the path validation completed successfully. For rejected certificates - The PROD indicates a failure, returns an error and/or notifies the user of the error reason.