

**FIPS 201 Evaluation Program -
Central Certificate Validator
SCVP Client Request and Server Response Profiles**

Version 2.0.0
July 22, 2009



Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	11/26/2008	Initial Document	Public
Approved	2.0.0	07/22/2009	Updated to add validationPolicy fields within the request to override the default validation policy	Public

Table of Contents

1. Introduction.....	4
1.1 Background.....	4
1.2 Purpose.....	4
1.3 SCVP Overview.....	4
1.4 Scope.....	5
1.5 Assumptions.....	5
2. SCVP Client Request Profile	7
3. CCV SCVP Response Profile.....	11
4. SCVP Client Requirements.....	16
5. CCV SCVP Responder Requirements	17
Appendix A— Signed Request Details.....	18
Appendix B— Signed Response Details.....	19
Appendix C— CCV Status Codes	20
Appendix D— Abbreviations and Acronyms.....	21

1. Introduction

1.1 Background

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. The goal of HSPD-12 is to increase security and Government efficiency, reduce identity fraud and terrorist exploitations and protect the privacy of the individual.

The Office of Management and Budget (OMB) has designated the General Services Administration (GSA) as the Executive Agent for government-wide acquisitions for the implementation of HSPD-12. Additionally, OMB has directed Federal agencies to purchase only products and services that are compliant with the Federal policy, standards and supporting technical specifications.

The FIPS 201 Evaluation Program is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within GSA. The goal of the FIPS 201 Evaluation Program is to evaluate products and services against the requirements outlined in FIPS 201-1 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.

Once evaluated and approved by the FIPS 201 Evaluation Program, products and services are placed on the FIPS 201 Approved Products List (APL). Agencies can then procure these products and services from Suppliers for their HSPD-12 implementations having full assurance that they meet all the requirements of FIPS 201-1 as well as the GSA interoperability and performance criteria.

1.2 Purpose

In addition to performing routine evaluations of products and services, the GSA EP identified a potential need for and is therefore instantiating a centralized Government-Owned server (referred to as the "Central Certificate Validator") that is capable of performing certificate path discovery and validation (PD-VAL) in compliance with RFC 3280 in support of PKI-based authentication mechanisms described in FIPS 201.

It is envisioned that this Central Certificate Validator, accessible by any organization (at no cost), capable of performing certificate PD-VAL in a bridge-environment is a vital and must-needed element that would enable ubiquitous, interoperable, and standardized implementation of PKI certificate validation.

1.3 SCVP Overview

There are a variety of applications that can make use of public key certificates. In the context of HSPD-12 these include applications both for physical and logical access. However in order to accept and trust a PKI-based transaction, these applications are burdened with the overhead and complexity of constructing and validating the certification paths.

The primary goals of SCVP are to make it easier to deploy Public Key Infrastructure (PKI)-enabled applications by delegating path discovery and/or validation processing to a server, and to allow central administration of validation policies within an organization. Especially, when the client has complete trust in the SCVP Server, SCVP can be used to delegate the work of certification path construction and validation, and SCVP can be used to ensure that policies are consistently enforced throughout an organization.

For complete details on the specifications of SCVP, please refer to RFC 5055.

1.4 Scope

The scope of this document is to define the profiles (and thereby all associated requirements) that need to be supported by SCVP Clients and provide specifics on the configuration of the Central Certification Validator such that certificate path discovery, construction and validation is performed consistently and uniformly by relying parties using this GSA-provided server.

Additionally by providing the profiles for the SCVP request and response, participating organizations can be made aware of the format of the request that is expected by the CCV as well as the response that they would be returned. Physical Access Control Systems (PACS) manufacturers who implement PKI-based authentication mechanisms can build/implement/integrate appropriate software modules that are able to communicate with the CCV based on these profiles without having to implement every single requirement specified within SCVP.

1.5 Assumptions

RFC 5055 provides several optional parameters that can be part of the validation and policy requests and responses. Based on these options provided within the request as well as by configuring the SCVP server differently, certain parameters need to be/are made available as part of the response.

At the highest-level, all SCVP requests and responses conform to RFC 5055. Details of the RFC 5055 have been omitted for the sake of brevity. Wherever specifics are not mentioned for request and response fields mentioned in Section 2 and Section 3 respectively, it is assumed that the CCV follows the requirements as dictated within the Standard.

The Central Certificate Validator is a trusted server. As such, the clients are expected to operate in a “delegated path validation (DPV)” mode and have the CCV perform certificate path construction and validation for them. These clients inherently trust the CCV as it would its own path validation software. This results in serving two purposes:

1. These clients (integrated within the PACS and LACS) do not have to incur the overhead of including certification path validation software and running it for each certificate it receives.
2. Certificate validation for PKI-based authentication mechanisms is standardized across the Federal community since there are standard validation policy requirements. More specifically, this policy dictates the particular trust anchor that can be used and the types of

policy checking that are to be performed during certificate path validation. The default Validation Policy includes the following:

- a. Trust Anchor – Common Policy Root CA
- b. Certificate Policy – id-fpki-common-authentication {2 16 840 1 101 3 2 1 3 13}
- c. initial-explicit-policy = true
- d. initial-policy-mapping-inhibit = false

2. SCVP Client Request Profile

The following table provides the SCVP Request profile that needs to be adhered to by clients interacting with the CCV.

Field	Description	RTM Mapping
CVRequest		
cvRequestVersion	Defines the version of the SCVP CVRequest used in a request	VRQ-17; VRQ-19
query		
queriedCerts	The queriedCerts item is a SEQUENCE of one or more certificates, each of which is a subject of the request	VRQ-29; VRQ-32
pkcRef	Only 1 pkcRefs to be present	VRQ-46
cert	Certificate whose certification path and revocation status needs to be obtained	VRQ-46
checks	Describes the checking that the SCVP client wants the SCVP server to perform on the certificate in the queriedCerts item	VRQ-59
	Following identifier supported:	
	id-stc 3 (id-stc-build-status-checked-pkc-path) - build a validated certification path to a trust anchor and perform revocation status checks on the certification path	VRQ-57; VRQ-59
wantBack	Describes any information the SCVP client wants from the SCVP server for the certificate(s) in the queriedCerts item in addition to the results of the checks specified in the checks item	VRQ-61
	Following identifier supported:	
	id-swb-pkc-cert (10): The certificate that was the subject of the request	VRQ-61; VRQ-64

Field		Description	RTM Mapping
		id-swb-pkc-best-cert-path (1): The certification path built for the certificate including the certificate that was validated	
		id-swb-pkc-public-key-info (4): The public key from the certificate that was the subject of the request	
	validationPolicy	defines the validation policy(s) that the client wants the SCVP server to use during certificate validation	VRQ-29
	validationPolRef	Reference to the validation policy that the client and server have agreed represents a particular validation policy	VRQ-73; VRQ-76
		default validation policy corresponds to standard certification path processing with server-chosen default values (e.g., with a server-determined policy set and a trust anchors	VRQ-81; VRQ-83
		Following identifier supported:	
		id-svp (1) : id-svp-defaultValPolicy	VRQ-87
	userPolicySet	The userPolicySet item specifies a list of certificate policy identifiers that the SCVP server MUST use when constructing and validating a certification path Specification of multiple (1 or more) certificate policies is supported	VRQ-108, VRQ-109
	inhibitPolicyMapping	The inhibitPolicyMapping item specifies an input to the certification path validation algorithm, and it controls whether policy mapping is allowed during certification path validation	VRQ-111
	requireExplicitPolicy	The requireExplicitPolicy item specifies an input to the certification path validation algorithm, and it controls whether there must be at least one valid policy in the certificate policies extension	VRQ-113

Field		Description	RTM Mapping
	inhibitAnyPolicy	The inhibitAnyPolicy item specifies an input to the certification path validation algorithm and it controls whether the anyPolicy OID is processed or ignored when evaluating certificate policy	VRQ-115
	trustAnchors	The trustAnchors item specifies the trust anchors at which the certification path must terminate if the path is to be considered valid by the SCVP server for the request Specification of multiple (1 or more) trust anchors is supported. Trust anchors can only be provided directly.	VRQ-121
	pkcRef	1 or more pkcRefs can be present	
	cert	Trust Anchor to be used	
	ResponseFlags	The optional responseFlags item allows the SCVP client to indicate which optional features in the CVResponse it wants the SCVP server to include.	VRQ-133
	fullRequestInResponse	Allows the SCVP client to indicate if it wants the responding SCVP server to include the full request in its response. Following values supported: False	VRQ-136; VRQ-137
	responseValidationPolByRef	The responseValidationPolByRef item controls whether the response includes just a reference to the policy or a reference to the policy plus all the parameters by value of the policy used to process the request. Following values supported: True, False	VRQ-141; VRQ-142

Field		Description	RTM Mapping
protectResponse		The protectResponse item indicates whether the SCVP client requires the SCVP server to protect the response.	VRQ-144; VRQ-145
		Following Values Supported:	
		True	
cachedResponse		The cachedResponse item indicates whether the SCVP client will accept a cached response from the SCVP server.	VRQ-148; VRQ-149
		Following values supported:	
		False	
requestNonce		The optional requestNonce item contains a request identifier generated by the SCVP client. If the client includes a requestNonce value in the request, it is expressing a preference that the SCVP server SHOULD return a non-cached response	VRQ-21

Table 1 - SCVP Client Request Profile

3. CCV SCVP Response Profile

The following table provides the SCVP Response profile that will be generated by the CCV.

Field		Description	RTM Mapping
CVResponse			
	cvResponseVersion	Defines the version of the SCVP CVResponse used in the request. Must match request version.	VRS-29
	serverConfigurationID	Represents the version of the SCVP server configuration when it processed the request	VRS-29
	producedAt	Tells the date and time at which the SCVP server generated the response	VRS-29
	responseStatus	Gives status information to client about its request	VRS-29
	statusCode	In accordance with RFC 5055 ¹	VRS-48; VRS-49
	respValidationPolicy ²	Contains either a reference to the full validation policy (if default policy used) or the full policy by value (if policy parameters overridden and provided in the client request) used by the server to validate the request	VRS-50
	ValidationPolRef	Reference to the validation policy that the client and server have agreed represents a particular validation policy	VRQ-73; VRQ-76
	ValPolId	default validation policy corresponds to standard certification path processing with server-chosen default values (e.g., with a server-determined policy set and a trust anchors)	VRQ-81; VRQ-83
Following identifier supported:			

¹ Status codes supported by the CCV are provided in Appendix C.

² Individual fields within the respValidationPolicy structure not included here. Refer to individual fields within the SCVP Request.

Field		Description	RTM Mapping
		id-svp (1) : id-svp-defaultValPolicy	VRQ-87
	userPolicySet	The userPolicySet item specifies a list of certificate policy identifiers that the SCVP server used when constructing and validating a certification path (from the request)	VRQ-108, VRQ-109
	inhibitPolicyMapping	The inhibitPolicyMapping item specifies an input to the certification path validation algorithm, and it controls whether policy mapping is allowed during certification path validation (from the request)	VRQ-111
	requireExplicitPolicy	The requireExplicitPolicy item specifies an input to the certification path validation algorithm, and it controls whether there must be at least one valid policy in the certificate policies extension (from the request)	VRQ-113
	inhibitAnyPolicy	The inhibitAnyPolicy item specifies an input to the certification path validation algorithm and it controls whether the anyPolicy OID is processed or ignored when evaluating certificate policy (from the request)	VRQ-115
	trustAnchors	The trustAnchors item specifies the trust anchors at which the certification path must terminate if the path is to be considered valid by the SCVP server for the request (from the request)	VRQ-121
	pkcRef	1 or more pkcRefs can be present	
	cert	Trust Anchor certificate	
	requestRef	Allows the SCVP client to identify the request that corresponds to this response from the server	VRS-37; VRS-38
	requestHash	Hash of CVRequest	VRS-62
	algorithm		VRS-59
	value		VRS-59

Field	Description	RTM Mapping
replyObjects	Returns requested objects to the SCVP client, telling the client about the certificate from the request.	VRS-30; VRS-70
CertReply	replyobjects items returned	VRS-31
cert	contains the certificate about which the client is requesting information	VRS-71
pkc		VRS-71
cert		VRS-71
replyStatus	Gives status information to the client about the request for the specific certificate.	VRS-71
	Choice of Following values:	
	0 Success: all checks were performed successfully	
	1 Failure: the public key certificate was malformed	
	2 Failure: the attribute certificate was malformed	
	3 Failure: historical data for the requested validation time is not available	
	4 Failure: the server could not locate the reference certificate or the referenced certificate did not match the hash value provided	
	5 Failure: no certification path could be constructed	
	6 Failure: the constructed certification path is not valid with respect to the validation policy	
8 Failure: all checks were performed successfully; however, one or more of the wantBacks could not be satisfied	VRS-78; VRS-79	
replyValTime	Tells the time at which the information in the CertReply was correct	VRS-71
replyChecks	Contains the responses to the checks item requested from the client	VRS-71
ReplyCheck		VRS-83

Field		Description	RTM Mapping
	check	Supported Identifier:	
		id-stc 3 for build a validated certification path to a trust anchor and perform revocation status checks on the certification path	VRS-83
	status	Supported Identifiers for id-stc 3:	
		0=Valid ; 1=Not Valid 2= Revocation off-line; 3=Revocation unavailable; 4=No known source for revocation information	VRS-83
	replyWantBacks	contains the responses to the wantBack item in the client request	
	ReplyWantBack		VRS-90
	wb	OID identifier from the wantback item in the request	VRS-87
		Supported Identifiers:	
		id-swb-pkc-cert (10): The certificate that was the subject of the request	VRS-87
		id-swb-pkc-best-cert-path (1): The certification path built for the certificate including the certificate that was validated	
id-swb-pkc-public-key-info (4): The public key from the certificate that was the subject of the request			
	value	requested value is within OCTET String (CertBundle for id-swb 1, SubjectPublicKeyInfo type for id-swb 4)	VRS-87
	validationErrors	Specifies reason validation failed. Only present for error responses	VRS-4; VRS-98; VRS-99
		Possible Basic Validation Algorithm Error OID's:	
		id-bvae-expired { id-bvae 1 }	VRS-8
		id-bvae-not-yet-valid { id-bvae 2 }	
		id-bvae-wrongTrustAnchor { id-bvae 3 }	
		id-bvae-noValidCertPath { id-bvae 4 }	
id-bvae-revoked { id-bvae 5 }			

Field		Description	RTM Mapping
		id-bvae-invalidKeyPurpose { id-bvae 9 }	
		id-bvae-invalidKeyUsage { id-bvae 10 }	
		id-bvae-invalidCertPolicy { id-bvae 11 }	
	nextUpdate	Tells the time at which the server expects a refresh of information regarding the validity of the certificate to become available.	VRS-102
	respNonce	Contains an identifier that binds response to request. If the client includes requestNonce then respNonce will be same value.	VRS-33; VRS-108

Table 2 - CCV SCVP Response Profile

4. SCVP Client Requirements

In order for a complete SCVP client implementation that is compliant with the GSA Evaluation Program's CCV, the following additional requirements need to be met in addition to the client profiles specified in Section 2.0.

Requirement No.	Requirement Description	Details/ Notes /	RTM Mapping
1	An SCVP client MUST be capable of creating protected requests ³ .	-	VRQ-3
2	SCVP clients MUST be able to communicate with the CCV via HTTPS using mutual authentication	Client-side certificate and private key to be used for client authentication will be provided by the GSA Evaluation Program.	TRANS-3
3	Clients MUST use the POST method to submit their requests.	-	TRANS-1
4	The Content-Type header MUST have the value "application/scvp-cv-request".	-	TRANS-5

³ Appendix A describes the details for the Signed SCVP Request as per RFC 3852 - Cryptographic Message Syntax (CMS).

5. CCV SCVP Responder Requirements

In order for an SCVP client implementation to be capable of interfacing the GSA FIPS 201 Evaluation Program's CCV, the client needs to be cognizant about the CCV. The following section provides details on such requirements and configurations in addition to the CCV Response Profile that the client needs to be aware of.

Requirement No.	Requirement Description	Details/ Notes /	RTM Mapping
1	The CCV will require all requests to be protected and will always respond using protected responses ⁴ .	-	VRQ-3
2	The CCV will only communicate with clients via HTTPS using mutual authentication.	The CCV will authenticate the client prior to establishing the SSL connection and providing an SCVP response.	TRANS-3
3	The CCV will use the 200 response code for successful responses.	-	TRANS-2
4	The CCV will not assume client support for any type of HTTP authentication such as cookies, Basic authentication, or Digest authentication.	-	TRANS-4
5	The Content-Type header will have the value "application/scvp-cv-response"	-	TRANS-6

⁴ Appendix B describes the details for the Signed SCVP Response as per RFC 3852 - Cryptographic Message Syntax (CMS).

Appendix A—Signed Request Details

The Signed SCVP Request shall be implemented as a SignedData Type, as specified in RFC 3852 – Cryptographic Message Syntax, and shall include the following information:

- The message shall include a version field specifying version v3
- The digestAlgorithms field shall be as specified in SP800-78-1, Table 3-3.
- The encapContentInfo shall:
 - Specify an eContentType of id-ct-scvp-certValRequest (1.2.840.113549.1.9.16.1.10)
 - The eContent field contains a Distinguished Encoding Rules (DER)-encoded CVRequest
- The certificates field shall include only a single X.509 certificate which can be used to verify the signature in the SignerInfo field (i.e. the certificate used to sign the SCVP Request)⁵.
- The crls field shall be omitted
- signerInfos shall be present and include only a single SignerInfo
- The SignerInfo shall:
 - Use the issuerAndSerialNumber choice for SignerIdentifier
 - Specify a digestAlgorithm in accordance with SP800-78-1, Table 3-3
- Include, at a minimum, the following signed attributes:
 - A MessageDigest attribute containing the hash computed over the CVRequest
 - A ContentType attribute containing the value matching the encapContentInfo eContentType value
- Include the digital signature

⁵ This certificate and its corresponding private key will be provided by the GSA Evaluation Program

Appendix B—Signed Response Details

The Signed SCVP Response shall be implemented as a SignedData Type, as specified in RFC 3852 – Cryptographic Message Syntax, and shall include the following information:

- The message shall include a version field specifying version v3
- The digestAlgorithms field shall be as specified in SP800-78-1, Table 3-3.
- The encapContentInfo shall:
 - Specify an eContentType of id-ct-scvp-certValResponse (1.2.840.113549.1.9.16.1.11)
 - The eContent field contains a Distinguished Encoding Rules (DER)-encoded CVResponse
- The certificates field shall include only a single X.509 certificate which can be used to verify the signature in the SignerInfo field (i.e. the certificate used to sign the SCVP Response)⁶.
- The crls field shall be omitted
- signerInfos shall be present and include only a single SignerInfo
- The SignerInfo shall:
 - Use the issuerAndSerialNumber choice for SignerIdentifier
 - Specify a digestAlgorithm in accordance with SP800-78-1, Table 3-3
- Include, at a minimum, the following signed attributes:
 - A MessageDigest attribute containing the hash computed over the CVResponse
 - A ContentType attribute containing the value matching the encapContentInfo eContentType value
- Include the digital signature

⁶ The SCVP Client must be capable of trusting SCVP Response signing certificates

Appendix C—CCV Status Codes

The following status codes (CVStatusCode) values will be supported and have the following meaning:

- 0 - The request was fully processed.
- 10 - Too busy; try again later.
- 11 - The server was able to decode the request, but there was some other problem with the request.
- 12 - An internal server error occurred.
- 20 - The structure of the request was wrong.
- 21 - The version of request is not supported by this server.
- 22 - The request included unrecognized items, and the server was not able to continue processing.
- 23 - The server could not validate the key used to protect the request.
- 24 - The signature or message authentication code did not match the body of the request.
- 25 - The encoding was not understood.
- 26 - The request was not authorized.
- 27 - The request included unsupported checks items, and the server was not able to continue processing.
- 28 - The request included unsupported wantBack items, and the server was not able to continue processing.
- 29 - The server does not support the signature or message authentication code algorithm used by the client to protect the request.
- 30 - The server could not validate the client's signature or message authentication code on the request.
- 50 - The request contained an unrecognized validation policy reference.
- 52 - The server does not support returning the full request in the response
- 53 - The server does not support returning the full validation policy by value in the response

Appendix D—Abbreviations and Acronyms

DPV	Delegated Path Validation
EP	Evaluation Program
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
NIST	National Institute of Standards and Technology
OGP	Office of Government-wide Policy
OMB	Office of Management and Budget
PD VAL	Path Discovery and Validation
PIV	Personal Identity Verification
SCVP	Server-based Certificate Validation Protocol