Department of the Treasury

Public Key Infrastructure

Treasury Validation Services:

SCVP Request and Response Profile

October 7th, 2016

TABLE OF CHANGES

Version	Change Description	Section
1.0	Production Release	ALL
1.1	Updating GSA Profile URL Rename existing request profile as “Long Term SCVP Request” Addition of draft “Lightweight SCVP Request” Addition of draft “Batch SCVP Request” Replaced CMS reference RFC 3852 with RFC 5652 Removed "6.1 - No support above TLS 1.0 from Signer or Repeater" Removed "6.3 - SHA-1 Signed Protected Responses for Error Conditions"	1 4 6
1.2	Removed All SHA-1 Policy OIDs and References Added the option for wantBacks to be requested in Lightweight Requests Removed "5.3 - Federal PKI Defined SHA-1 Policies" Removed "6.1 - RFC 5055 Non-Conformance" Removed "6.2 - DPV SCVP Request (with WantBacks) Affects Repeater Stability"	ALL 4 5 6
1.3	Altered TLS requirements to set TLS 1.2 as the baseline Altered TLS requirements to include specific cipher suites Added section for “Development” Policies Removed Fiscal Service SSO Policy	4 5

TABLE OF CONTENTS

TABLE OF FIGURES

1. Introduction

This document outlines the Server-Based Certificate Validation Protocol (SCVP) client request and server response profiles for the Treasury Validation Service.

The intent is to assist relying party applications when communicating with the validation service by:

- Defining a governance structure for policy management
- Defining the SCVP request requirements;
- Defining the SCVP response to be expected;
- Define requirements for validation policies; and,
- Track known infrastructure limitations.

This document is based on the GSA FIPS 201 Evaluation Program document titled "Server-Based Certificate Validation Protocol (SCVP) Profile", which is available at the following location:

https://www.idmanagement.gov/IDM/articles/Document/SCVP-Application-Package

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.

The SCVP service provides Delegated Path Validation (DPV), where the client explicitly trusts the SCVP service to validate the certificate. In this case, the client trusts the response and requires no proof back in the form of a wantBack.

The SCVP service also provides Delegated Path Discovery (DPD), where the client uses the SCVP service to perform the work of path discovery, and possibly validation. In this scenario, the client may require some form of proof, such as the certificate path, and revocation data, in order to make a client decision to consider the certificate valid or not. However, the client must be able to process the wantBack(s) received to perform validation of the certificate in question.

Initial business requirements within the Department of the Treasury specify Delegated Path Validation, and are within the current scope of this document. As additional business requirements for SCVP are conveyed by the Department of the Treasury and its reimbursable services customer base, this profile may further articulate request and response profiles for Delegated Path Discovery.

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

2. Treasury Validation Services

This document provides details on the SCVP service, which is offered under the Treasury Validation Services. This section provides scope and background on the intent of the SCVP service.

This service provides certificate validation only. The validation result is not intended to convey authorization or entitlement information.

2.1. Approach to Certificate Validation

Treasury makes use of the Federal PKI as a relying party. Validation Services provides a way for applications to simply validate certificates from the Federal PKI, without having to understand the details of the complex relationships between the Federal PKI and all of its associated affiliates.

The Trust Anchor for all Federal Agency relying parties is the Common Policy Root CA.

```
   -----BEGIN CERTIFICATE-----
   MIIEYDCCA0igAwIBAgICATAwDQYJKoZIhvcNAQELBQAwWTELMAkGA1UEBhMCVVMx
   GDAWBgNVBAoTD1UuUy4gR292ZXJubWVudDENMAsGA1UECxMERlBLSTEhMB8GA1UE
   AxMYRmVkZXJhbCBDb21tb24gUG9saWN5IENBMB4XDTEwMTIwMTE2NDUyN1oXDTMw
   MTIwMTE2NDUyN1owWTELMAkGA1UEBhMCVVMxGDAWBgNVBAoTD1UuUy4gR292ZXJu
   bWVudDENMAsGA1UECxMERlBLSTEhMB8GA1UEAxMYRmVkZXJhbCBDb21tb24gUG9s
   aWN5IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2HX7NRY0WkG/
   Wq9cMAQUHK14RLXqJup1YcfNNnn4fNi9KVFmWSHjeavUeL6wLbCh1bI1FiPQzB6+
   Duir3MPJ1hLXp3JoGDG4FyKyPn66CG3G/dFYLGmgA/Aqo/Y/ISU937cyxY4nsyOl
   4FKzXZbpsLjFxZ+7xaBugkC7xScFNknWJidpDDSPzyd6KgqjQV+NHQOGgxXgVcHF
   mCye7Bpy3EjBPvmE0oSCwRvDdDa3ucc2Mnr4MrbQNq4iGDGMUHMhnv6DOzCIJOPp
   wX7e7ZjHH5IQip9bYi+dpLzVhW86/clTpyBLqtsgqyFOHQ1O5piF5asRR12dP8Qj
   wOMUBm7+nQIDAQABo4IBMDCCASwwDwYDVR0TAQH/BAUwAwEB/zCB6QYIKwYBBQUH
   AQsEgdwwgdkwPwYIKwYBBQUHMAWGM2h0dHA6Ly9odHRwLmZwa2kuZ292L2ZjcGNh
   L2NhQ2VydHNJc3N1ZWRCeWZjcGNhLnA3YzCBlQYIKwYBBQUHMAWGgYhsZGFwOi8v
   bGRhcC5mcGtpLmdvdi9jbj1GZWRlcmFsJTIwQ29tbW9uJTIwUG9saWN5JTIwQ0Es
   b3U9RlBLSSxvPVUuUy4lMjBHb3Zlcm5tZW50LGM9VVM/Y0FDZXJ0aWZpY2F0ZTti
   aW5hcnksY3Jvc3NDZXJ0aWZpY2F0ZVBhaXI7YmluYXJ5MA4GA1UdDwEB/wQEAwIB
   BjAdBgNVHQ4EFgQUrQx6dVzl85jEeZgOrCj9l/TnAvwwDQYJKoZIhvcNAQELBQAD
   ggEBAI9z2uF/gLGH9uwsz9GEYx728Yi3mvIRte9UrYpuGDco71wb5O9Qt2wmGCMi
   TR0mRyDpCZzicGJxqxHPkYnos/UqoEfAFMtOQsHdDA4b8Idb7OV316rgVNdF9IU+
   7LQd3nyKf1tNnJaK0KIyn9psMQz4pO9+c+iR3Ah6cFqgr2KBWfgAdKLI3VTKQVZH
   venAT+0g3eOlCd+uKML80cgX2BLHb94u6b2akfI8WpQukSKAiaGMWMyDeiYZdQKl
   Dn0KJnNR6obLB6jI/WNaNZvSr79PMUjBhHDbNXuaGQ/lj/RqDG8z2esccKIN47lQ
   A2EC/0rskqTcLe4qNJMHtyznGI8=
   -----END CERTIFICATE-----
```

```
Digests of the DER encoded certificate are included below:

MD5:     8C42B6360DD024CE4CB1BA06D26A6BC9
SHA-1:   905F942FD9F28F679B378180FD4F846347F645C1
SHA-256: 894EBC0B23DA2A50C0186B7F8F25EF1F6B2935AF32A94584EF80AAF877A3A06E
```

Table 1 – Federal Common Policy CA Certificate

From the Common Policy Root CA, there multiple intermediate certificates, which lead to hundreds of issuing certification authorities. From these issuing certification authorities, there are millions of end entity certificates.

The Server Based Certificate Validation Protocol (SCVP) is used within Treasury Validation Service for secure messaging to request and receive validation of all of these certificates, through a centralized system that performs certificate path discovery and validation.

The Federal PKI Policy Authority defines various credential types by way of certificate policy identifiers. Treasury Validation Services offers a validation policy for each credential type (see Federal PKI Defined Policies), as well as groupings of credential types for specific use cases, such as authentication (see OMB M-04-04 Defined Policies).

All of the intermediates, as well as certificate revocation data in the form of Certificate Revocation Lists (CRLs), are cached and periodically updated on the Validation Services signer. This allows for the validation of certificates in the most expeditious manner for relying parties, supported by multiple certificate validation policies according to each credential type within the Federal PKI.

The following table contains a complete list of all certificate policy identifiers that are asserted from the Common Policy Root CA.

2.16.840.1.101.3.2.1.3.1	(id-fpki-certpcy-rudimentaryAssurance)
2.16.840.1.101.3.2.1.3.2	(id-fpki-certpcy-basicAssurance)
2.16.840.1.101.3.2.1.3.6	(id-fpki-common-policy)
2.16.840.1.101.3.2.1.3.7	(id-fpki-common-hardware)
2.16.840.1.101.3.2.1.3.8	(id-fpki-common-devices)
2.16.840.1.101.3.2.1.3.13	(id-fpki-common-authentication)
2.16.840.1.101.3.2.1.3.14	(id-fpki-certpcy-medium-CBP)
2.16.840.1.101.3.2.1.3.15	(id-fpki-certpcy-mediumHW-CBP)
2.16.840.1.101.3.2.1.3.16	(id-fpki-common-high)
2.16.840.1.101.3.2.1.3.17	(id-fpki-common-cardAuth)
2.16.840.1.101.3.2.1.3.18	(id-fpki-certpcy-pivi-hardware)
2.16.840.1.101.3.2.1.3.19	(id-fpki-certpcy-pivi-cardAuth)
2.16.840.1.101.3.2.1.3.20	(id-fpki-certpcy-pivi-contentSigning)
2.16.840.1.101.3.2.1.3.36	(id-fpki-common-devicesHardware)
2.16.840.1.101.3.2.1.3.39	(id-fpki-common-piv-contentSigning)
2.16.840.1.101.3.2.1.3.40	(id-fpki-common-derived-pivAuth)
2.16.840.1.101.3.2.1.3.41	(id-fpki-common-derived-pivAuth-hardware)

Table 2 – Federal Common Policy CA Asserted Certificate Policy Identifiers

Any of the certificate policy identifiers above can be combined to construct a new SCVP policy. By default, there are individual SCVP policies for each certificate policy identifier, where the certificate policy identifier is also used as the validation policy reference (see Federal PKI Defined Policies).

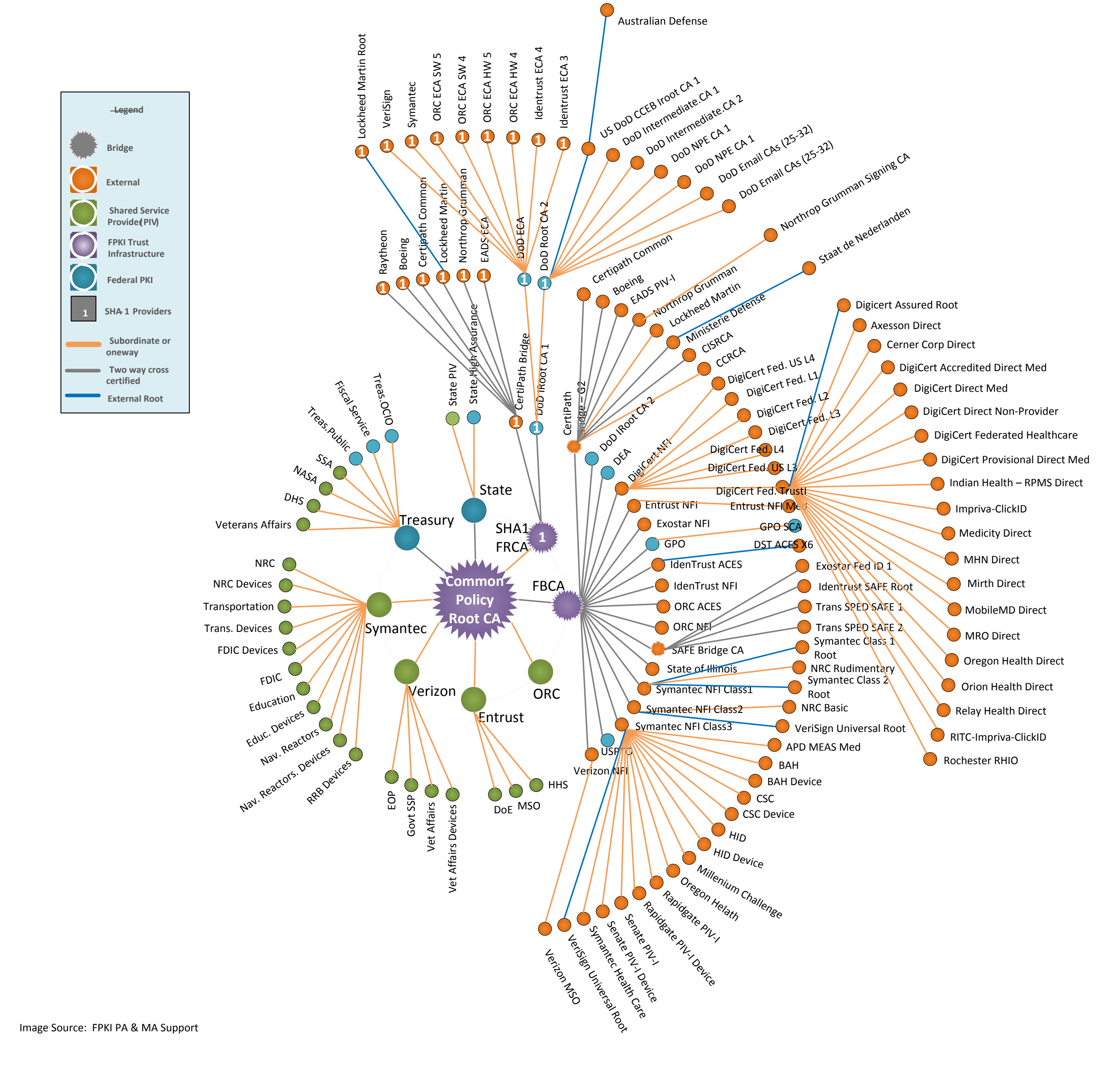

Image Source: FPKI PA & MA Support

Table 3 – Federal Public Key Infrastructure

This graphic depicts the Federal Public Key Infrastructure with all cross-certified affiliates as of July 2015. This service demystifies the cross certification relationships and policy mappings, while relying on the Common Policy Root CA as the trust anchor.

To determine if a certificate is valid, and that it was claimed to be issued according to a given FPKI mapped policy, a relying party sends a SCVP request (see SCVP Client Request) to the service with only the certificate in question, with a reference to the respective validation policy (see SCVP Policies). The service will analyze the certificate for validity against the respective validation policy, and provide an answer in the SCVP response (see SCVP Server Response).

3. Roles and Responsibilities

This section will be expanded to cover the operational management of the service, as well as a process for SCVP policy management.

At this time, all requests for policies, as well as any additional information regarding the SCVP service should be sent to:

pki_ops@fiscal.treasury.gov

4. SCVP Client Request(s) and Response

This profile defines three types of SCVP requests, where all requests reference a `ValidationPolicy` that is defined within this profile (see SCVP Policies).

“Lightweight” SCVP Client Request

A “Lightweight” SCVP client request will produce an SCVP response that may be cached. These requests should yield a response that MAY be cached by the server, where the response MAY be served from cache for no more than 18 hours.

This request type is intended to be used to rapidly validate a certificate for authentication use cases, and the relying party does not have long term records retention requirements for the validation information (SCVP Response).

“Long Term Record” SCVP Client Request

A “Long Term Record” SCVP client request will produce an SCVP response that includes the full client request, as well as the server’s copy of the referenced validation policy, at the time of validation. This allows the resulting response to be archived by the relying party (if needed) for records retention purposes.

This request type is intended to be used to validate a certificate for digital signature use cases, where the relying party may have long term records retention requirements for the validation information (SCVP Response). This may be further enhanced by requesting the following wantBacks:

id-swb-pkc-best-cert-path: The certification path built for the certificate including the certificate that was validated.
id-swb-pkc-revocation-info: Proof of revocation status for each certificate in the certification path.

“Batch” SCVP Client Request

A “Batch” SCVP client request includes multiple certificates (up to 256) in a single request, which are validated against a single validation policy. Each certificate within the request SHOULD be issued by the same CA for optimal performance, however, the response processing time will take longer that the individual certificate validation requests defined above.

This request type is intended to be used to validate certificates in batch, where a system possesses the certificates to be validated, and the desire is to periodically validate the certificates.

4.1. “Lightweight” SCVP Client Request

The following information is to be used when configuring the SCVP client. A request based on these settings will produce an SCVP response that may be cached.

1. `CVRequest` MUST contain `cvRequestVersion`.
    1. The value of `cvRequestVersion` MUST be set to 1.

2. `queriedCerts` MUST contain exactly one `CertReferences` item.
    1. `CertReferences` MUST contain exactly one `pkcRefs` item.
        1. `pkcRefs` MUST contain exactly one `PKCReference` item.
            1. `PKCReference` MUST include the certificate in the `cert` item.

3. `checks` MUST contain exactly one `CertChecks` item.
    1. `CertChecks` MUST include the OID 1.3.6.1.5.5.7.17.3 (id-stc-build-status-checked-pkc-path)

4. `wantBack` MAY include one or more `WantBack` OIDs.

5. `validationAlg` SHOULD contain exactly one `ValidationAlg`.
    1. `ValidationAlg` MUST include `valAlgId`.
        1. The value of `valAlgId` MUST be set to the `id-svp-basicValAlg` OID.

6. `responseFlags` SHOULD include the following `ResponseFlags`:
    1. `fullRequestInResponse`
        1. The flag value MUST be set to FALSE.

    2. `responseValidationPolByRef`
        1. The flag value MUST be set to TRUE.

    3. `protectResponse`
        1. The flag MUST be set to TRUE.

    4. `cachedResponse`
        1. The flag MUST be set to TRUE.

7. `revInfos` MUST be omitted.

8. `producedAt` MUST be omitted.

9. `requestNonce` MUST be omitted.

10. `ValidationPolicy` MUST include exactly one `ValidationPolRef`.
    1. The `valPolId` MUST specify one of the policy OIDs defined in this profile, and `valPolParams` MUST be null.

11. `requestorText` MUST be omitted.

4.2. “Long Term Record” SCVP Client Request

The following information is to be used when configuring the SCVP client. A request based on these settings will produce an SCVP response that includes the full client request, as well as the server’s copy of the referenced validation policy, at the time of validation. This allows the resulting response to be archived by the relying party (if needed) for records retention purposes.

1. `CVRequest` MUST contain `cvRequestVersion`.
    1. The value of `cvRequestVersion` MUST be set to 1.

2. `queriedCerts` MAY contain exactly one `CertReferences` item.
    1. `CertReferences` MUST contain exactly one `pkcRefs` item.
        1. `pkcRefs` MUST contain exactly one `PKCReference` item.
            1. `PKCReference` MUST include the certificate in the `cert` item.

3. `checks` MUST contain exactly one `CertChecks` item.
    1. `CertChecks` MUST include the OID 1.3.6.1.5.5.7.17.3 (id-stc-build-status-checked-pkc-path)

4. `wantBack` MAY include one or more `WantBack` OIDs.

5. `validationAlg` SHOULD contain exactly one `ValidationAlg`.
    1. `ValidationAlg` MUST include `valAlgId`.
        1. The value of `valAlgId` MUST be set to the `id-svp-basicValAlg` OID.

6. `responseFlags` SHOULD include the following `ResponseFlags`:
    1. `fullRequestInResponse`
        1. The flag value MUST be set to TRUE.

    2. `responseValidationPolByRef`
        1. The flag value MUST be set to FALSE.

    3. `protectResponse`
        1. The flag MUST be set to TRUE.

    4. `cachedResponse`
        1. The flag value MUST be set to FALSE.

7. `revInfos` MUST be omitted.

8. `producedAt` MUST be omitted.

9. `requestNonce` SHOULD be included.
    1. The requestNonce value SHOULD be at least 16 bytes in length, and MUST NOT exceed 64 bytes.

10. `ValidationPolicy` MUST include exactly one `ValidationPolRef`.
    1. The `valPolId` MUST specify one of the policy OIDs defined in this profile, and `valPolParams` MUST be null.

11. `requestorText` MUST be included.
    1. The `requestorText` item MUST conform to the formatting requirements in this profile. (see requestorText Format Requirements)

4.3. “Batch” SCVP Client Request

The following information is to be used when configuring the SCVP client. A request based on these settings will produce an SCVP response that may be cached.

1. `CVRequest` MUST contain `cvRequestVersion`.
    1. The value of `cvRequestVersion` MUST be set to 1.

2. `queriedCerts` MUST contain exactly one `CertReferences` item.
    1. `CertReferences` MUST contain exactly one `pkcRefs` item.
        1. `pkcRefs` MAY contain one or more `PKCReference` item(s), not to exceed 256.
            1. `PKCReference` MUST include the certificate in the `cert` item.

3. `checks` MUST contain exactly one `CertChecks` item.
    1. `CertChecks` MUST include the OID 1.3.6.1.5.5.7.17.3 (id-stc-build-status-checked-pkc-path)

4. `wantBack` MUST NOT include `WantBack` OIDs.

5. `validationAlg` SHOULD contain exactly one `ValidationAlg`.
    1. `ValidationAlg` MUST include `valAlgId`.
        1. The value of `valAlgId` MUST be set to the `id-svp-basicValAlg` OID.

6. `responseFlags` SHOULD include the following `ResponseFlags`:
    1. `fullRequestInResponse`
        1. The flag value MUST be set to FALSE.

    2. `responseValidationPolByRef`
        1. The flag value MUST be set to TRUE.

    3. `protectResponse`
        1. The flag MUST be set to TRUE.

    4. `cachedResponse`
        1. The flag MUST be set to TRUE.

7. `revInfos` MUST be omitted.

8. `producedAt` MUST be omitted.

9. `requestNonce` MUST be omitted.

10. `ValidationPolicy` MUST include exactly one `ValidationPolRef`.
    1. The `valPolId` MUST specify one of the policy OIDs defined in this profile, and `valPolParams` MUST be null.

11. `requestorText` MUST be omitted.

4.4. SCVP Server Response

The following is a general representation of the response; however, it may vary due to the request options generated by the client.

4.4.1. Response MIME Body Part Details

Since this profile places more attention to Delegated Path Validation, a typical response that is successfully processed by the server will be returned to the client within a Cryptographic Message Syntax (CMS) [RFC 5652] message as a SignedData type.

The CVResponse data will be enclosed in the ContentInfo field:

```
       ContentInfo {
               contentType        id-ct-scvp-certValResponse,
                                           -- (1.2.840.113549.1.9.16.1.11)
               content            CVResponse
       }
```

While validation of the signature is out of scope of this profile, the SCVP signing certificate(s) are signed by the Treasury OCIO CA, which SHOULD be validated using the following validation requirements:

trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.36 (id-fpki-common-devicesHardware)
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

After validating the CMS SignedData object, the CVResponse object should be parsed and validated against the original request.

4.4.2. Response CVResponse Details

The information below is not intended to be a complete representation of every CVResponse returned by the service, however, certain fields are documented to assist a relying party with understanding the contents. For a complete overview of all items that MAY be in the CVResponse, refer to [RFC 5055].

```
       CVResponse ::= SEQUENCE {
         cvResponseVersion         INTEGER,
                                     -- (1)
         serverConfigurationID     INTEGER,
         producedAt                GeneralizedTime,
         responseStatus            ResponseStatus
                                     -- (One of the following ENUMERATED CVStatusCode values)
```

0	The request was fully processed.
1	The request included some unrecognized non-critical extensions; however, processing was able to continue ignoring them.
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.
31	The server could not generate a protected response as requested by the client.
32	The server does not have a certificate matching the requested responder name.
40	The request was previously relayed by the same server.
50	The request contained an unrecognized validation policy reference.
51	The request contained an unrecognized validation algorithm OID.
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.
54	The server does not support the requested value for inhibit policy mapping.
55	The server does not support the requested value for require explicit policy.
56	The server does not support the requested value for inhibit anyPolicy.
57	The server only validates requests using current time.
63	The query item in the request contains a critical extension whose OID is not recognized.
64	The request contains a critical request extension whose OID is not recognized.

Table 4 – CVStatusCode Values & Meanings

```
        respValidationPolicy  [0] RespValidationPolicy OPTIONAL,
```

When responseValidationPolByRef is set to FALSE in the request, all items in the validationPolicy item will be populated. When responseValidationPolByRef is set to TRUE, OPTIONAL items in the validationPolicy will be populated for items for which the value in the request differs from the value from the referenced validation policy. Otherwise, refer to the section of this document titled "SCVP Policies" for the currently configured validation policies.

```
        requestRef            [1] RequestReference OPTIONAL,
```

The requestRef will include the digest of the original CVRequest, or, it will contain the clients full CVRequest, which is dependent on the fullRequestInResponse value in the client's request.

```
        requestorRef          [2] GeneralNames OPTIONAL,
```

requestorRef will only appear if included by the client in the request.

```
        requestorName         [3] GeneralNames OPTIONAL,
```

requestorName will only appear if included by the client in the request.

```
        replyObjects          [4] ReplyObjects OPTIONAL,
```

replyObjects will be a SEQUENCE of CertReply objects, which correspond to the queriedCerts of the request, and the details of this object are documented in the following section.

```
        respNonce             [5] OCTET STRING OPTIONAL,
```

respNonce will contain the value of the requestNonce, if included in the request.

```
        serverContextInfo     [6] OCTET STRING OPTIONAL,
```

At this time, serverContextInfo is not addressed by this profile, and is not part of a typical response.

```
        cvResponseExtensions  [7] Extensions OPTIONAL,
```

At this time, cvResponseExtensions is not addressed by this profile, and is not part of a typical response.

```
        requestorText         [8] UTF8String (SIZE (1..256)) OPTIONAL }
```

requestorText will contain the value of the requestorText, if included in the request.

4.4.3. Response CertReply detail

As mentioned in the prior section, replyObjects will be a SEQUENCE of CertReply objects, which correspond to the queriedCerts of the request. At this time, this profile only addresses X509v3 Certificates, and not Attribute Certificates.

```
      CertReply ::= SEQUENCE {
        cert                       CertReference,
                                     -- (A single CertReference, which corresponds to a single CertReference
                                         in the queriedCerts of the original request)
        replyStatus                ReplyStatus DEFAULT success,
                                     -- (One of the following ENUMERATED ReplyStatus 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.
7	Failure: the constructed certification path is not valid with respect to the validation policy, but a query at a later time may be successful.
8	Failure: all checks were performed successfully; however, one or more of the wantBacks could not be satisfied.

Table 5 – ReplyStatus Values & Meanings

```
        replyValTime               GeneralizedTime,
```

The replyValTime item tells the time at which the information in the CertReply was correct. (time of validation)

```
        replyChecks                ReplyChecks,
```

The replyChecks item contains the responses to the checks item in the query.

```
        replyWantBacks             ReplyWantBacks,
```

The replyWantBacks item contains the WantBack items specified in the query. This will only be populated if requested by the client, and the ReplyStatus code is not 1, 2, 3, or 4.

```
        validationErrors      [0] SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL,
                                     -- (One of the following object identifiers)
```

The validationErrors item will only be present if the certificate failed to validate successfully. (if `replyStatus is not 0`)

1.3.6.1.5.5.7.19.3.1	id-bvae-expired
1.3.6.1.5.5.7.19.3.2	id-bvae-not-yet-valid
1.3.6.1.5.5.7.19.3.3	id-bvae-wrongTrustAnchor
1.3.6.1.5.5.7.19.3.4	id-bvae-noValidCertPath
1.3.6.1.5.5.7.19.3.5	id-bvae-revoked
1.3.6.1.5.5.7.19.3.9	id-bvae-invalidKeyPurpose
1.3.6.1.5.5.7.19.3.10	id-bvae-invalidKeyUsage
1.3.6.1.5.5.7.19.3.11	id-bvae-invalidCertPolicy
1.3.6.1.4.1.2930.6.1.1.1	vlct-scvp-weakCertKey - The key size of the certificate does not meet the requirement of the SCVP policy.
1.3.6.1.4.1.2930.6.1.1.2	vlct-scvp-weakCertHash - The hashing algorithm of the certificate does not meet the requirement of the SCVP policy.

Table 6 – validationErrors Object Identifiers & Meanings

The nextUpdate item tells the time at which the server expects a refresh of information regarding the validity of the certificate to become available.

```
        nextUpdate            [1] GeneralizedTime OPTIONAL,
```

The certReplyExtensions item contains the responses to the queryExtensions item in the request.

```
        certReplyExtensions   [2] Extensions OPTIONAL }
```

4.4.4. Relying Party Archival of SCVP Responses

As stated in the section "SCVP Client Request", the settings will produce an SCVP response that includes the full client request, as well as the server's copy of the referenced validation policy, at the time of validation. This allows the resulting response to be archived by the relying party (if needed) for records retention purposes.

If the relying party wishes to archive the SCVP response for records retention purposes, then the entire mime body part encapsulating the response SHOULD be archived along with all certificates; between the SCVP Signing Certificate to the Common Policy Root CA; in order to support validation of the SCVP response's signature at any time within the transactions records retention period.

4.5. SCVP Security and Transport

1. HTTPS is STRONGLY RECOMMENDED.
   1.1. If used, TLS 1.2 or higher MUST be used.

The following cipher suites SHOULD be limited to the following:

Hexcode	Cipher Suite Name (OpenSSL)	Cipher Suite Name (RFC)
xc030	ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc028	ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc014	ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
xc02f	ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc027	ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc013	ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Table 7 – Recommended Client Cipher Suites

While validation of the server certificate(s) used for TLS is out of scope of this profile, the server certificate(s) are signed by the Treasury OCIO CA, which SHOULD be validated using the following validation requirements:

trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.36 (id-fpki-common-devicesHardware)
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

4.6. requestorText Format Requirements

String characters in the requestorText field describe the physical location or logical resource where a SCVP request for revocation information was originated. The SCVP signer processes this information and passes it to corresponding SCVP response.

For requests originated from physical locations, the requestorText field must contain character string as depicted in the following table.

Field Identifie	# of Characters	Character Position	Value	Notes
1 (Location)	3	1 to 3	PHY	Field which specifies whether the request for revocation information is originated from a physical location or a logical resource.
n/a	1	4	; (semicolon)	Field Separator
2 (Facility Security Level)	2	5 to 6	LO, MD, HI, VH	Facility Security Level for Federal Facilities (An Interagency Security Committee Standard). LO – Low, MD – Medium, HI – High, VH – Very High
n/a	1	7	; (semicolon)	Field Separator
3 (Agency Code)	4	8 to 11	Agency Code. E.g. 891H, 4500	The four letter Agency code from NIST SP 800-87 rev. 1.
4 (Physical Location Information)	10	13 to 22	Street #. E.g. 4701A	Street number of Agency location.
	50	24 to 73	Street Name. E.g. Constitution Avenue Northwest	Street name of Agency location.
	20	75 to 94	City. E.g. New York	City of Agency Location
	2	96 to 97	State. E.g. DC, VA, MD, NC…	Two letter state abbreviation.
	10	99 to 108	Zip Code. E.g. 12345-01234 or 12345-0000	Numeric zip code.
	25	110 to134	Country. E.g. United States of America	Country where Agency is located.
	20	136 to 155	Access Point ID.	The GSA FIPS 201 EP will assign a unique Access Point ID as part of CCV registration process. Schema for this is to be determined.
				Note: Each of the 7 items in field 4 must be separated by a comma. For items that don’t exist, enter "-".
5	101	156 – 256	For future use	

Table 8 – requestorText Format for Physical Asset Identification

For requests originated from logical resources, character string in the requestorText field must contain values specified the following table.

Field Identifier	# of Characters	Character Position	Value	Notes
1 (Location)	3	1 to 3	LOG	Field which specifies whether the request for revocation information is originated from a physical location or a logical resource
n/a	1	4	; (semicolon)	Field Separator
2 (Security Categorization)	2	5 to 6	LO, MD, HI	FIPS 199 System Security Categorization. LO – Low, MD – Medium, HI – High.
n/a	1	7	; (semicolon)	
3 (System Characterization)	3	8 to 10	GSS, MAJ	Whether the logical resource requesting revocation information is part of a General Support System (GSS) or a Major Application (MAJ).
n/a	4	11	; (semicolon)	
4 (Application Type)		12 to 14	NET, VPN, EML, WEB, OTH	Type of the application requesting revocation information. NET – Network, VPN – Virtual Private Network, EML – Email, WEB – Web browser, OTH – Other.
n/a	5	15	; (semicolon)	
5 (Access Point ID) Name of the logical resource, along with any other details are specified in this field.	3	16 to 18	Process Type	Logical resource's (i.e. requestor's) process types. DTP – Desktop, LTP – Laptop, SVR – Server, RTR – Router, SWT – Switch, APP – Application.
	50	20 to 69	URI or Domain Name	Uniform Resource Identifier of the application or domain name of the system device requesting revocation information
	16	71 to 86	IP Address	IP Address of the system device or application requesting revocation information. **Note:** Each of the 3 items in field 5 must be separated by a comma. For items that don't exist, enter "-".
6	170	87 - 256	For future use	

Table 9 – requestorText Format for Logical Asset Identification

5. SCVP Policies

All SCVP policies are identified with an Object Identifier (OID), which are used within the request by setting the `valPolId` field within the `validationPolRef`, encapsulated in the `ValidationPolicy` of the `CVRequest`.

The following tables articulate the currently configured policies. Unless otherwise specified, client override of each SCVP policy is not permitted.

5.1. Default Policy

Per RFC 5055, the default policy OID is:

```
1.3.6.1.5.5.7.19.1 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)
id-svp(19) id-svp-defaultValPolicy(1)}
```

While this policy may be overridden, clients can validate certificates against this policy without overriding the values to determine if the certificate in question is part of the Federal PKI.

1.3.6.1.5.5.7.19.1 (Default)	
The client MAY override the following policy values	
trustAnchors	Federal Common Policy CA
userPolicySet	2.5.29.32.0
inhibitPolicyMapping	FALSE
requireExplicitPolicy	FALSE
inhibitAnyPolicy	TRUE

5.2. Federal PKI Defined Policies

Each policy is intended to validate intermediate and end entity certificates, to determine if a credential is valid under a particular Federal PKI Policy OID.

2.16.840.1.101.3.2.1.3.1 (id-fpki-certpcy-rudimentaryAssurance)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.1
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.2 (id-fpki-certpcy-basicAssurance)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.2
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.6 (id-fpki-common-policy)[1]	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.6
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)[2]	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.7
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.8 (id-fpki-common-devices)[3]	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.8
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.13
inhibitPolicyMapping	TRUE[4]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.14 (id-fpki-certpcy-medium-CBP)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.14
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.15 (id-fpki-certpcy-mediumHW-CBP)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.15
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[1] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumAssurance

[2] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumHardware

[3] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumDevice

[4] id-fpki-common-authentication may only be asserted by Federal Issuers, and are not mapped

2.16.840.1.101.3.2.1.3.16 (id-fpki-common-high)[5]	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.16
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.17
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.18 (id-fpki-certpcy-pivi-hardware)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.18
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.19 (id-fpki-certpcy-pivi-cardAuth)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.19
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.20 (id-fpki-certpcy-pivi-contentSigning)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.20
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.36 (id-fpki-common-devicesHardware)[6]	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.36
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[5] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-highAssurance

[6] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumDeviceHardware

2.16.840.1.101.3.2.1.3.39 (id-fpki-common-piv-contentSigning)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.39
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.40 (id-fpki-common-derived-pivAuth)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.40
inhibitPolicyMapping	TRUE[7]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.3.41 (id-fpki-common-derived-pivAuth-hardware)	
trustAnchors	Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.41
inhibitPolicyMapping	TRUE[8]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[7] id-fpki-common-derived-pivAuth may only be asserted by Federal Issuers, and are not mapped.

[8] id-fpki-common-derived-pivAuth-hardware may only be asserted by Federal Issuers, and are not mapped.

5.3. Treasury Defined Policies

All Treasury defined SCVP policies shall use the following OID arc:

```
2.16.840.1.101.10.2.18.2.1 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) us-government-
org(10) treasury(2) bfs(18) pki(2) scvp-pol(1)}
```

The first four policies are categorized in Levels of Assurance in alignment with [OMB M-04-04]. This allows for the validation of certificates used for authentication by human subscribers.

The following table shows which policy is aligned with a given LOA, defined within [OMB M-04-04]. The resulting SCVP policies allow a certificate that is of a higher LOA to be validated using a lower LOA SCVP policy. I.e., a certificate that is valid under LOA4 will also be valid for LOA1, LOA2, and LOA3.

Meets Level 4	
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication
2.16.840.1.101.3.2.1.3.15	id-fpki-certpcy-mediumHW-CBP
2.16.840.1.101.3.2.1.3.16	id-fpki-common-high
2.16.840.1.101.3.2.1.3.18	id-fpki-certpcy-pivi-hardware
2.16.840.1.101.3.2.1.3.41	id-fpki-common-derived-pivAuth-hardware
Meets Level 3	
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy
2.16.840.1.101.3.2.1.3.14	id-fpki-certpcy-medium-CBP
2.16.840.1.101.3.2.1.3.40	id-fpki-common-derived-pivAuth
Meets Level 2	
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth
2.16.840.1.101.3.2.1.3.19	id-fpki-certpcy-pivi-cardAuth
Meets Level 1	
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance

Table 10 – Certificate Policies and the E-authentication Assurance Levels

While all of the policies above are intended to only be asserted in human subscriber certificates, it is the responsibility of the relying party to determine if the certificate was issued to a human or a device prior to validating each certificate against a corresponding validation policy.

5.3.1. LOA 4

This policy includes id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-certpcy-mediumHW-CBP, id-fpki-common-high, id-fpki-certpcy-pivi-hardware, and id-fpki-common-derived-pivAuth-hardware.

2.16.840.1.101.10.2.18.2.1.4 (LOA4)	
trustAnchors	Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.41

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

5.3.2. LOA 3

This policy includes id-fpki-certpcy-basicAssurance, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-certpcy-medium-CBP, id-fpki-certpcy-mediumHW-CBP, id-fpki-common-high, id-fpki-certpcy-pivi-hardware, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware.

2.16.840.1.101.10.2.18.2.1.3 (LOA3)	
trustAnchors	Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.2;
	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.14;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.40;
	2.16.840.1.101.3.2.1.3.41

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

5.3.3. LOA 2

This policy includes id-fpki-certpcy-basicAssurance, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-certpcy-medium-CBP, id-fpki-certpcy-mediumHW-CBP, id-fpki-common-high, id-fpki-common-cardAuth, id-fpki-certpcy-pivi-hardware, id-fpki-certpcy-pivi-cardAuth, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware.

2.16.840.1.101.10.2.18.2.1.2 (LOA2)	
trustAnchors	Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.2;
	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.14;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.17;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.19;
	2.16.840.1.101.3.2.1.3.40;
	2.16.840.1.101.3.2.1.3.41

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

5.3.4. LOA 1

This policy includes id-fpki-certpcy-rudimentaryAssurance, id-fpki-certpcy-basicAssurance, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-certpcy-medium-CBP, id-fpki-certpcy-mediumHW-CBP, id-fpki-common-high, id-fpki-common-cardAuth, id-fpki-certpcy-pivi-hardware, id-fpki-certpcy-pivi-cardAuth, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware.

2.16.840.1.101.10.2.18.2.1.1 (LOA1)	
trustAnchors	Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.1;
	2.16.840.1.101.3.2.1.3.2;
	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.14;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.17;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.19;
	2.16.840.1.101.3.2.1.3.40;
	2.16.840.1.101.3.2.1.3.41

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

5.3.5. Fiscal Service Payment Management policy

This policy is intended to validate certificates for two different types of credentials, all of which are traditionally LOA4. The first credential type is HSPD-12, or, certificates from PIV, PIV-I, and DOD CAC. The second credential type is the Fiscal Service Medium Hardware credential, where the credential is on a SafeNet/Gemalto iKey, and maps to id-fpki-common-hardware from the Fiscal Service CA to the Common Policy Root CA.

2.16.840.1.101.10.2.18.2.1.11 [PIV, PIV-I, Common Hardware]	
trustAnchors	Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.18

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

5.4. “Development” Policies

All development SCVP policies shall use the following OID arc:

```
2.16.840.1.101.10.2.18.2.0 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) us-government-
org(10) treasury(2) bfs(18) pki(2) dev-scvp-pol(0)}
```

All development SCVP policies that can be used to validate development and production certificates shall use the following OID arc:

```
2.16.840.1.101.10.2.18.2.2 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) us-government-
org(10) treasury(2) bfs(18) pki(2) combined-scvp-pol(2)}
```

All development policies emulating “Federal PKI Defined Policies” shall use the CITE / CSOR-TEST OID arc:

```
2.16.840.1.101.3.2.1.48 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2)
csor-certpolicy(1) csor-test-policies(48)}
```

More information on the CITE OIDs assigned from the CSOR TEST OID arc can be obtained via the following document:

https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNpPAAW&field=File__Body__s

Otherwise, all of the production SCVP policies above shall be available via the development validation services systems.

The Trust Anchor for CITE is the “Test Common Policy Root CA”.

```
   -----BEGIN CERTIFICATE-----
   MIID9jCCAt6gAwIBAgIUZbKm4RGAmMMdO0I5fiLHPUWC4/4wDQYJKoZIhvcNAQEL
   BQAwYjELMAkGA1UEBhMCVVMxGDAWBgNVBAoTD1UuUy4gR292ZXJubWVudDERMA8G
   A1UECxMIVGVzdEZQS0kxJjAkBgNVBAMTHVRlc3QgRmVkZXJhbCBDb21tb24gUG9s
   aWN5IENBMB4XDTE0MTAwNjE0MzYxMloXDTM0MTAwNjE0MzYxMlowYjELMAkGA1UE
   BhMCVVMxGDAWBgNVBAoTD1UuUy4gR292ZXJubWVudDERMA8GA1UECxMIVGVzdEZQ
   S0kxJjAkBgNVBAMTHVRlc3QgRmVkZXJhbCBDb21tb24gUG9saWN5IENBMIIBIjAN
   BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw5jDCmZVQecMslcu4aD3VHShAePE
   54cFLyiIqmRfdren207P3p1mNX9BZMJ+OdwNUdN4bHuXIpXr6PP5sVhRMCDtft0u
   9WqpV7G5HsMUw4V/2Ejfmjk1EIbisyb4etMiEqS36DoOanWWVrnKBwdFxPof6+Mz
   333Q5HANtx3eysBd6Sl0dnGGVy6JXl2mzpp43ShUVR8KTx/ZiMxG7gmFc1HGuaMk
   cyYjHk42ZTjQJOVil88B8njGyZ/WbULjXofcLgWO0FGZHvHg7M+B5hgN2qjRSuiU
   B1Iqykxto3BLOU7WuG8ed4DZzPFaaOf6Dds/tpajx3SfZWqTforSG6cCMQIDAQAB
   o4GjMIGgMA8GA1UdEwEB/wQFMAMBAf8wXgYIKwYBBQUHAQsEUjBQME4GCCsGAQUF
   BzAFhkJodHRwOi8vaHR0cC5jaXRlLmZwa2ktbGFiLmdvdi9jb21tb24vY2FDZXJ0
   c0lzc3VlZEJ5dGVzdENvbW1vbi5wN2MwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQW
   BBTqBnGM05KgDc/nHfSJeXkp548PjTANBgkqhkiG9w0BAQsFAAOCAQEAjtoCkDgI
   q1SR753iOOjdisOiCwcgYF//9/9w5gvJIvVJwioRYtxpasgEDQ+7v7hSVi7QJGBP
   eZiadaimrbjM8Bz2yoORl6xXsbVgOlKDDUxzW3In2jz8QtzdRYmAaS5N8aBpsukw
   PGXsB9s1uNEdxlyVhsVHCAoeXHYNZ3HunaVxjjPp6P95DL5EKuSn4EL2asPtQOOZ
   4hbbLs2qUNWuhwsGs/n+lSvRtzgPqDNyomWth1p+fgwqCss8l+CfzO65bia9qws/
   RhBqntL3OlyIXebK5SNV7Js4VBytdKHuOKvYABrnepzXNtJKPoQkyu1rZCooG2ZO
   jXy1Lk7xEtwbBg==
   -----END CERTIFICATE-----
```

```
Digests of the DER encoded certificate are included below:

MD5:     A9B48F3FFDD86EF030731ED4DE428D2F
SHA-1:   2A1B6D506E9EA898FB75CE8A0675E1626FD3A0C7
SHA-256: 302A03E7DBE8554D49DC1525BA0A74C63750B25011834825CFAF95FF5B002356
```

Table 11 – Test Federal Common Policy CA Certificate

5.4.1. Default Policy

Per RFC 5055, the default policy OID is:

```
1.3.6.1.5.5.7.19.1 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)
id-svp(19) id-svp-defaultValPolicy(1)}
```

While this policy may be overridden, clients can validate certificates against this policy without overriding the values to determine if the certificate in question is part of the Federal PKI or CITE.

1.3.6.1.5.5.7.19.1 **(Default)**	
The client MAY override the following policy values	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.5.29.32.0
inhibitPolicyMapping	FALSE
requireExplicitPolicy	FALSE
inhibitAnyPolicy	TRUE

5.4.2. Federal PKI Defined Policies

Each policy is intended to validate intermediate and end entity certificates, to determine if a credential is valid under a particular Federal PKI Policy OID.

2.16.840.1.101.3.2.1.48.1 **(CITE id-fpki-certpcy-rudimentaryAssurance)**	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.1
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.1 **(Prod & CITE id-fpki-certpcy-rudimentaryAssurance)**	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.1 2.16.840.1.101.3.2.1.48.1
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.2 **(CITE id-fpki-certpcy-basicAssurance)**	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.2
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.2 **(Prod & CITE id-fpki-certpcy-basicAssurance)**	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.2 2.16.840.1.101.3.2.1.48.2
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.8 **(CITE id-fpki-common-policy)**[9]	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.8
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.6 **(Prod & CITE id-fpki-common-policy)**[10]	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.6 2.16.840.1.101.3.2.1.48.8
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.9 **(CITE id-fpki-common-hardware)**[11]	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.9
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.7 **(Prod & CITE id-fpki-common-hardware)**[12]	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.7 2.16.840.1.101.3.2.1.48.9
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[9] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumAssurance

[10] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumAssurance

[11] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumHardware

[12] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumHardware

2.16.840.1.101.3.2.1.48.10 (CITE id-fpki-common-devices)[13]	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.10
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.8 (Prod & CITE id-fpki-common-devices)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.8 2.16.840.1.101.3.2.1.48.10
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.11 (CITE id-fpki-common-authentication)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.11
inhibitPolicyMapping	TRUE[14]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.13 (Prod & CITE id-fpki-common-authentication)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.13 2.16.840.1.101.3.2.1.48.11
inhibitPolicyMapping	TRUE[15]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.5 (CITE id-fpki-certpcy-medium-CBP)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.5
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[13] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumDevice

[14] id-fpki-common-authentication may only be asserted by Federal Issuers, and are not mapped

[15] id-fpki-common-authentication may only be asserted by Federal Issuers, and are not mapped

2.16.840.1.101.10.2.18.2.2.14 (Prod & CITE id-fpki-certpcy-medium-CBP)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.14 2.16.840.1.101.3.2.1.48.5
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.6 (CITE id-fpki-certpcy-mediumHW-CBP)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.6
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.15 (Prod & CITE id-fpki-certpcy-mediumHW-CBP)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.15 2.16.840.1.101.3.2.1.48.6
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.12 (CITE id-fpki-common-high)[16]	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.12
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.16 (Prod & CITE id-fpki-common-high) [17]	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.16 2.16.840.1.101.3.2.1.48.12
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[16] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-highAssurance

[17] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-highAssurance

2.16.840.1.101.3.2.1.48.13 (CITE id-fpki-common-cardAuth)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.13
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.17 (Prod & CITE id-fpki-common-cardAuth)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.17 2.16.840.1.101.3.2.1.48.13
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.78 (CITE id-fpki-certpcy-pivi-hardware)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.78
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.18 (Prod & CITE id-fpki-certpcy-pivi-hardware)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.18 2.16.840.1.101.3.2.1.48.78
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.79 (CITE id-fpki-certpcy-pivi-cardAuth)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.79
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.19 (Prod & CITE id-fpki-certpcy-pivi-cardAuth)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.19 2.16.840.1.101.3.2.1.48.79
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.80 (CITE id-fpki-certpcy-pivi-contentSigning)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.80
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.20 (Prod & CITE id-fpki-certpcy-pivi-contentSigning)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.20 2.16.840.1.101.3.2.1.48.80
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.98 (CITE id-fpki-common-devicesHardware)[18]	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.98
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.36 (Prod & CITE id-fpki-common-devicesHardware)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.36 2.16.840.1.101.3.2.1.48.98
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[18] Also used to validate certificates mapped to FBCA policy id-fpki-certpcy-mediumDeviceHardware

2.16.840.1.101.3.2.1.48.86 (CITE id-fpki-common-piv-contentSigning)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.86
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.39 (Prod & CITE id-fpki-common-piv-contentSigning)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.39 2.16.840.1.101.3.2.1.48.86
inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.109 (CITE id-fpki-common-derived-pivAuth)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.109
inhibitPolicyMapping	TRUE[19]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.40 (Prod & CITE id-fpki-common-derived-pivAuth)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.40 2.16.840.1.101.3.2.1.48.109
inhibitPolicyMapping	TRUE[20]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.3.2.1.48.110 (CITE id-fpki-common-derived-pivAuth-hardware)	
trustAnchors	Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.48.110
inhibitPolicyMapping	TRUE[21]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[19] id-fpki-common-derived-pivAuth may only be asserted by Federal Issuers, and are not mapped.
[20] id-fpki-common-derived-pivAuth-hardware may only be asserted by Federal Issuers, and are not mapped.
[21] id-fpki-common-derived-pivAuth-hardware may only be asserted by Federal Issuers, and are not mapped.

2.16.840.1.101.10.2.18.2.2.41 (Prod & CITE id-fpki-common-derived-pivAuth-hardware)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA
userPolicySet	2.16.840.1.101.3.2.1.3.41 2.16.840.1.101.3.2.1.48.110
inhibitPolicyMapping	TRUE[22]
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

[22] id-fpki-common-derived-pivAuth-hardware may only be asserted by Federal Issuers, and are not mapped.

5.4.3. Treasury Defined Policies

5.4.3.1. LOA 4

2.16.840.1.101.10.2.18.2.0.4 (CITE LOA4)	
trustAnchors	Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.110

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.1004 (Prod & CITE LOA4)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.41;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.110

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

5.4.3.2. LOA 3

2.16.840.1.101.10.2.18.2.0.3 (CITE LOA3)	
trustAnchors	Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.48.2;
	2.16.840.1.101.3.2.1.48.8;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.5;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.109;
	2.16.840.1.101.3.2.1.48.110

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.1003 (Prod & CITE LOA3)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.2;
	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.14;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.40;
	2.16.840.1.101.3.2.1.3.41;
	2.16.840.1.101.3.2.1.48.2;
	2.16.840.1.101.3.2.1.48.8;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.5;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.109;
	2.16.840.1.101.3.2.1.48.110

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

6.1.1.1. LOA 2

2.16.840.1.101.10.2.18.2.0.2 (CITE LOA2)	
trustAnchors	Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.48.2;
	2.16.840.1.101.3.2.1.48.8;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.5;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.13;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.79;
	2.16.840.1.101.3.2.1.48.109;
	2.16.840.1.101.3.2.1.48.110

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.1002 (Prod & CITE LOA2)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.2;
	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.14;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.17;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.19;
	2.16.840.1.101.3.2.1.3.40;
	2.16.840.1.101.3.2.1.3.41;
	2.16.840.1.101.3.2.1.48.2;
	2.16.840.1.101.3.2.1.48.8;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.5;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.13;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.79;
	2.16.840.1.101.3.2.1.48.109;
	2.16.840.1.101.3.2.1.48.110

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

6.1.1.2. LOA 1

2.16.840.1.101.10.2.18.2.0.1 (CITE LOA1)	
trustAnchors	Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.48.1;
	2.16.840.1.101.3.2.1.48.2;
	2.16.840.1.101.3.2.1.48.8;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.5;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.13;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.79;
	2.16.840.1.101.3.2.1.48.109;
	2.16.840.1.101.3.2.1.48.110;

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.1001 (Prod & CITE LOA1)	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.1;
	2.16.840.1.101.3.2.1.3.2;
	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.14;
	2.16.840.1.101.3.2.1.3.15;
	2.16.840.1.101.3.2.1.3.16;
	2.16.840.1.101.3.2.1.3.17;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.3.19;
	2.16.840.1.101.3.2.1.3.40;
	2.16.840.1.101.3.2.1.3.41;
	2.16.840.1.101.3.2.1.48.1;
	2.16.840.1.101.3.2.1.48.2;
	2.16.840.1.101.3.2.1.48.8;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.5;
	2.16.840.1.101.3.2.1.48.6;
	2.16.840.1.101.3.2.1.48.12;
	2.16.840.1.101.3.2.1.48.13;
	2.16.840.1.101.3.2.1.48.78;
	2.16.840.1.101.3.2.1.48.79;
	2.16.840.1.101.3.2.1.48.109;
	2.16.840.1.101.3.2.1.48.110;

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

6.1.1.3. Fiscal Service Payment Management Policy

2.16.840.1.101.10.2.18.2.0.11 **(CITE Fiscal Service Payment Management)**	
trustAnchors	Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.78

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

2.16.840.1.101.10.2.18.2.2.1011 **(Prod & CITE Fiscal Service Payment Management)**	
trustAnchors	Federal Common Policy CA Test Federal Common Policy CA

userPolicySet	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.13;
	2.16.840.1.101.3.2.1.3.18;
	2.16.840.1.101.3.2.1.48.9;
	2.16.840.1.101.3.2.1.48.11;
	2.16.840.1.101.3.2.1.48.78

inhibitPolicyMapping	FALSE
requireExplicitPolicy	TRUE
inhibitAnyPolicy	TRUE

7. Outstanding Service Issues

The following information presents the known issues with the products being used to implement the SCVP service, where each issue may affect client interoperability.

8. References

[COMMON] "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework", Common Policy, <http://idmanagement.gov/sites/default/files/documents/FCPCA%20CP%20v1%2024.pdf>.

[NIST SP 800-78] “Cryptographic Algorithms and Key Sizes for Personal Identity Verification”, NIST Special Publication 800-78-3,<http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf>.

[OMB M-04-04] "E-Authentication Guidance for Federal Agencies", OMB M-04-04, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>.

[RFC 5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <http://www.rfc-editor.org/info/rfc5652>.

[RFC 5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, DOI 10.17487/RFC5055, December 2007, <http://www.rfc-editor.org/info/rfc5055>.

[RFC 5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.