Internet Draft
draft-ietf-pkix-ocsp-valid-00.txt
August, 2000
Expires in six months

Michael Myers, VeriSign
Carlisle Adams, Entrust
Stephen Farrell, Baltimore

Delegated Path Validation
draft-ietf-pkix-ocsp-valid-00.txt

Status of this memo

1.0 Abstract

OCSP [RFC2560] establishes the Internet standard for online certificate status. The baseline response type defined in [RFC2560] supports acquisition of the revocation state of a certificate. This specification builds on the OCSP framework's extensibility by defining an Internet-standard extension to OCSP that can be used to fully delegate all path validation processing to an OCSP server.

2.0 Delegated Path Validation

In order to determine if a certificate is valid an application must have knowledge of the certificate itself, a set of trusted public keys from which relevant certificate chains may be constructed and the validation status of every certificate used to construct the trust chain.

These data may originate from multiple sources. An industry consortium root may issue CA certificates to members of the consortium while members themselves use those CA certificates to either establish subordinate CAs or directly issue end-entity certificates. Equally, a certificate or certificate path established within one trust domain may be "cross certified" into another trust domain.

Locating the certificate validation process within a trusted server reduces the technical footprint of certificate using applications and may ease integration of certificate path processing with other authorization data. The Delegated Path Validation (DPV) extension to OCSP addresses this need.

A DPV request differs from the basic request defined in [RFC2560] by the inclusion of id-pkix-ocsp-valid-req request OID and request options (if any) as illustrated below (prior knowledge of [RFC2560] is assumed):

OCSP REQUEST

In the requestExtensions field of TBSRequest, one extension MUST have an OID of id-pkix-ocsp-valid-req and a value of DPVOptions (see below for syntax).

The initialPolicySet option enables a requestor to establish one or more initial policy identifiers as defined in [RFC2459].

The trustPoints option enables specification of one or more certificates relevant to the relying party's trust model. If included, a successful validation request will pass through at least one of these trust points, else an "unknown" response will be generated.

A DPV response differs from the basic response defined in [RFC2560] in the substitution of id-pkix-ocsp-valid-rsp for id-pkix-ocsp-basic in the ResponseType field of the ResponseBytes syntax. This is illustrated as follows (again, prior knowledge of [RFC2560] is assumed):

OCSP RESPONSE

In the responseBytes field of OCSPResponse, responseType MUST have a value of id-pkix-ocsp-valid-rsp and response MUST have a value of DPVOCSPResponse, where

```
   DPVOCSPResponse ::= BasicOCSPResponse
```

4.0 Delegated Path Validation Requirements

Relying party software desiring to delegate path validation to an OCSP server SHALL include a value of id-pkix-ocsp-valid-req as a requestExtension in the OCSPRequest syntax defined by [RFC2560].

```
id-pkix-ocsp-valid-req   OBJECT IDENTIFIER ::= { id-pkix-ocsp X }
```

One or more policy OIDs MAY be included to enable policy-based control on the OCSP server's path construction and path validation processes. Definition of any such policies and their corresponding OIDs is beyond the scope of this specification. One or more certificates MAY be included to express trust points relevant to the relying party's trust model.

```
DPVOptions  :: = SEQUENCE{
    initialPolicySet [0] EXPLICIT PolicyList OPTIONAL,
    trustPoints       SEQUENCE OF ReqCert OPTIONAL }
```

If neither initialPolicySet nor trustPoints are included in the request, the DPVOptions structure SHALL omit both optional fields.

OCSP servers operated to perform delegated path validation SHALL include a value of id-pkix-ocsp-valid-rsp in the responseType field of the ResponseBytes syntax upon receipt of a request containing a value of id-pkix-ocsp-valid-req as defined above.

```
id-pkix-ocsp-valid-rsp   OBJECT IDENTIFIER ::= { id-pkix-ocsp X }
```

Servers that produce id-pkix-ocsp-valid-rsp responses SHALL execute path validation logic that produces outputs compliant with [RFC2459].

OCSP servers claiming compliance to this specification SHALL support the DPVOptions request syntax as follows.

If a request contains a non-NULL value for initialPolicySet, all OIDs included in that set SHALL be used as initial policy identifier values in the validation logic according to [RFC2459].

If a request contains a non-NULL value for trustPoints, the receiving server MUST attempt to produce a response that incorporates at least one of these certificates. If the receiving server cannot form such a path, the server SHALL return a status value of "unknown" in the response.

5.0 Security Considerations

TBD

6.0 Collected Syntax

```
PathValidation DEFINITIONS EXPLICIT TAGS ::=  {iso(1) identified-organization(3)
dod(6) internet(1) security(5) mechanisms(5) pkix(7) X }

BEGIN

IMPORTS

      -- PKIX
          Extensions
             FROM PKIX1Explicit88 {iso(1) identified-organization(3)
                  dod(6) internet(1) security(5) mechanisms(5) pkix(7)
                  id-mod(0) id-pkix1-explicit-88(1)}
      -- OCSP
             id-pkix-ocsp
             FROM OCSP {iso(1) identified-organization(3)
                  dod(6) internet(1) security(5) mechanisms(5) pkix(7) X }

      -- Directory Authentication Framework (X.509)
             Certificate
             FROM AuthenticationFramework { joint-iso-itu-t ds(5)
                      module(1) authenticationFramework(7) 3 };

-- Delegated Path Validation request
id-pkix-ocsp-valid-req    OBJECT IDENTIFIER ::= { id-pkix-ocsp X }

DPVOptions  :: = SEQUENCE{
    initialPolicySet [0] EXPLICIT PolicyList OPTIONAL,
    trustPoints       SEQUENCE OF Certificate OPTIONAL }
```

```
PolicyList  ::=  SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER

-- Delegated Path Validation response
id-pkix-ocsp-valid-rsp    OBJECT IDENTIFIER ::= { id-pkix-ocsp X }

END
```

5. References

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol", RFC 2560

[RFC2459] Housley, R., Ford, W., Polk, T, & Solo, D., "Internet Public Key Infrastructure - X.509 Certificate and CRL profile", RFC2459.

6. Author's Address

Michael Myers
VeriSign, Inc.
mmyers@verisign.com

Stephen Farrell
Baltimore Technologies
stephen.farrell@baltimore.ie

Carlisle Adams
Entrust Technologies
cadams@entrust.com