NETWORK WG
Internet Draft
Intended Status: Standards Track
Expires: December 3, 2010

Sean Turner, IECA
Russ Housley, Vigil Security

June 3, 2010

Additional CMS Revocation Information Choices
draft-turner-additional-cms-ri-choices-06.txt

Abstract

The Cryptographic Message Syntax (CMS) allows revocation information to be conveyed as part of the SignedData, EnvelopedData, AuthenticatedData, and AuthEnvelopedData content types. The preferred format for revocation information is the Certificate Revocation List (CRL), but an extension mechanism supports other revocation information formats. This document defines two additional revocation information formats for Online Certificate Status Protocol (OCSP) responses and Server-Based Certificate Validation Protocol (SCVP).

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on December 3, 2010.

1. Introduction

The RevocationInfoChoices type defined in [CMS] provides a set of revocation status information alternatives, which allows revocation information to be conveyed as part of the SignedData, EnvelopedData, AuthenticatedData, and AuthEnvelopedData content types. The intent is to provide information sufficient to determine whether the certificates and attribute certificates carried elsewhere in the CMS-protected content have been revoked. There may be more revocation status information than necessary or there may be less revocation status information than necessary.

X.509 Certificate revocation lists (CRLs) [PROFILE] are the primary source of revocation status information, but any other revocation information format can be supported. This document specifies two other formats: Online Certificate Status Protocol (OCSP) responses [OCSP] and Server-Based Certificate Validation Protocol (SCVP) requests and responses [SCVP].

Section 2 discusses the RevocationInformation structure. Section 3 defines a mechanism to carry OCSP responses. Section 4 defines a mechanism to carry SCVP requests and responses. Appendix A provides the normative ASN.1 syntax for the two mechanisms.

1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

document are to be interpreted as described in [WORDS].

2. Revocation Information

For convenience, the ASN.1 definition of the RevocationInfoChoices type from [CMS] is repeated here:

```
RevocationInfoChoices ::= SET OF RevocationInfoChoice

RevocationInfoChoice ::= CHOICE {
  crl        CertificateList,
  other  [1] IMPLICIT OtherRevocationInfoFormat }

OtherRevocationInfoFormat ::= SEQUENCE {
  otherRevInfoFormat  OBJECT IDENTIFIER,
  otherRevInfo        ANY DEFINED BY otherRevInfoFormat }
```

The other CHOICE MUST be used to convey OCSP responses, SCVP requests, and SCVP responses.

This document defines the id-ri arc under which the revocation information formats are defined. The id-ri object identifier is:

```
id-ri OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
  dod(6) internet(1) security(5) mechanisms(5) pkix(7) ri(16) }
```

NOTE: Numbers 1 and 3 were assigned to CRL and Delta CRL. These two numbers are not used because these formats use the RevocationInfoChoice crl CHOICE when included in CMS [CMS].

3. OCSP Response

To carry an OCSP response, the otherRevInfoFormat is set to id-ri-ocsp-response, which has the following ASN.1 definition:

```
id-ri-ocsp-response OBJECT IDENTIFIER ::= { id-ri 2 }
```

In this case, otherRevInfo MUST carry the OCSP response using the OCSPResponse type defined in [OCSP]. The responseStatus field MUST be successful and the responseBytes field MUST be present.

4. SCVP Request and Response

Unlike OSCP, SCVP permits unprotected and protected responses, where protected responses can be digitally signed or include message authentication codes. While this provides more flexibility, it complicates implementations when an SCVP response can be validated by entities other than the entity that generated the SCVP request. If a lower layer provides authentication and integrity for the client-

server interaction and the response is not protected, then a third party cannot validate the response because there is no way to know that the response was returned over a protected connection. If a message authentication code is used, then the third party will be unable to validate the message authentication code because it does not possess the necessary private key. For these reasons, SCVP responses sent to a third party MUST be signed by the SCVP server so that the third party can validate them.

SCVP response validation requires matching it to the SCVP request. This means that the SCVP request MUST always be included with the response. SCVP permits the client to retain the response, and SCVP permits the request to be returned in the response (in the requestReq field). The request need not be protected for matching to be performed; nonces and certIds can be checked.

To carry the SCVP request and response, the otherRevInfoFormat is set to id-ri-scvp, which has the following ASN.1 definition:

```
id-ri-scvp OBJECT IDENTIFIER ::= { id-ri 4 }
```

In this case, the otherRevInfo MUST carry both the SCVP request and response with the following structure:

```
SCVPReqRes ::= SEQUENCE {
  request  [0] EXPLICIT ContentInfo OPTIONAL,
  response     ContentInfo }
```

The SCVPReqRes has the following fields:

- request contains the SCVP request. It contains the unprotected request, authenticated request, or the signed request. The request MUST be present if the response does not include the

requestRef fullRequest field.

- response contains the SCVP response. It MUST contain the signed response. Additionally, the responseStatus MUST be okay. Unprotected and authenticated responses MUST NOT be included.

5. Security Considerations

The security considerations of [CMS], [CMS-ASN], [OCSP], [SCVP], and [PROFILE-ASN] apply.

To locally store unprotected or authenticated SCVP responses, a client can encapsulate the unprotected or authenticated SCVP response in a SignedData. It is a matter of local policy whether these SCVP

responses that are encapsulated and signed by the client are considered valid by another entity.

6. IANA Considerations

This document makes use of object identifiers. These object identifiers are defined in an arc delegated by IANA to the PKIX Working Group. No further action by IANA is necessary for this document or any anticipated updates.

7. References

7.1. Normative References

[CMS] Housley, R., "Cryptographic Message Syntax", RFC 5652, September 2009.

[CMS-ASN] Hoffman, P., and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", RFC 5911, June 2010.

[OCSP] Meyers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[PROFILE-ASN] Hoffman, P., and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC

5912, June 2010.

[SCVP] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, December 2007.

[WORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[X.680] ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002. Information Technology - Abstract Syntax Notation One.

[X.681] ITU-T Recommendation X.681 (2002) | ISO/IEC 8824-2:2002. Information Technology - Abstract Syntax Notation One: Information Object Specification.

[X.682] ITU-T Recommendation X.682 (2002) | ISO/IEC 8824-3:2002. Information Technology - Abstract Syntax Notation One: Constraint Specification.

[X.683] ITU-T Recommendation X.683 (2002) | ISO/IEC 8824-4:2002. Information Technology - Abstract Syntax Notation One: Parameterization of ASN.1 Specifications, 2002.

7.2. Informative References

[PROFILE] Cooper, D. et. al., "Internet X.509 Public Key Infrastructure Certificate and Certification Revocation List (CRL) Profile", RFC 5280, May 2008.

Appendix A. ASN.1 Modules

Appendix A.1 provides the normative ASN.1 definitions for the structures described in this specification using ASN.1 as defined in [X.680] for compilers that support the 1988 ASN.1.

Appendix A.2 provides informative ASN.1 definitions for the structures described in this specification using ASN.1 as defined in

[X.680], [X.681], [X.682], and [X.683] for compilers that support the 2002 ASN.1. This appendix contains the same information as Appendix A.1 in a more recent (and precise) ASN.1 notation, however Appendix A.1 takes precedence in case of conflict.

A.1. 1988 ASN.1 Module

```
CMS-Other-RIs-2009-88
  { iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0) id-mod-cms-otherRIs-2009-88(63)
  }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL
```



```
IMPORTS

-- FROM CMS [CMS]

ContentInfo
  FROM CryptographicMessageSyntax2004
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
    smime(16) modules(0) cms-2004(24) }

;

id-ri OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
  dod(6) internet(1) security(5) mechanisms(5) pkix(7) ri(16) }

-- RevocationInfoChoice for OCSP response
-- OID included in otherRevInfoFormat
-- signed OCSP response included in otherRevInfo
```

```
   id-ri-ocsp-response OBJECT IDENTIFIER ::= { id-ri 2 }

   -- RevocationInfoChoice for SCVP response
   -- OID included in otherRevInfoFormat
   -- SCVPReqRes included in otherRevInfo

   id-ri-scvp OBJECT IDENTIFIER ::= { id-ri 4 }

   SCVPReqRes ::= SEQUENCE {
     request  [0] EXPLICIT ContentInfo OPTIONAL,
     response     ContentInfo }

   END
```

A.2. 2002 ASN.1 Module

```
   CMS-Other-RIs-2009-02
     { iso(1) identified-organization(3) dod(6) internet(1) security(5)
       mechanisms(5) pkix(7) id-mod(0) id-mod-cms-otherRIs-2009-93(64)
     }

   DEFINITIONS IMPLICIT TAGS ::=

   BEGIN

   -- EXPORT ALL
```



```
   IMPORTS

   -- FROM [PROFILE-ASN]

   OCSPResponse
     FROM OCSP-2009
     { iso(1) identified-organization(3) dod(6) internet(1) security(5)
       mechanisms(5) pkix(7) id-mod(0) id-mod-ocsp-02(48) }

   -- FROM [CMS-ASN]

   ContentInfo, OTHER-REVOK-INFO
     FROM CryptographicMessageSyntax-2009
```

```
      { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
        smime(16) modules(0) id-mod-cms-2004-02(41) }

  ;

  -- Defines OCSP and SCVP formats for RevocationInfoChoice

  SupportedOtherRevokInfo OTHER-REVOK-INFO ::= {
    ri-ocsp-response |
    ri-scvp,
    ... }

  ri-ocsp-response OTHER-REVOK-INFO ::= {
    OCSPResponse IDENTIFIED BY id-ri-ocsp-response }

  id-ri OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
    dod(6) internet(1) security(5) mechanisms(5) pkix(7) ri(16) }

  id-ri-ocsp-response OBJECT IDENTIFIER ::= { id-ri 2 }

  ri-scvp OTHER-REVOK-INFO ::= {
    SCVPReqRes IDENTIFIED BY id-ri-scvp }

  id-ri-scvp OBJECT IDENTIFIER ::= { id-ri 4 }

  SCVPReqRes ::= SEQUENCE {
    request  [0] EXPLICIT ContentInfo OPTIONAL,
    response     ContentInfo }

  END
```


Authors' Addresses

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com