Network Working Group
Request for Comments: 4325
Updates: 3280
Category: Standards Track

S. Santesson
Microsoft
R. Housley
Vigil Security

December 2005

Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension

Status of This Memo

Copyright Notice

Abstract

This document updates RFC 3280 by defining the Authority Information Access Certificate Revocation List (CRL) extension. RFC 3280 defines the Authority Information Access certificate extension using the same syntax. The CRL extension provides a means of discovering and retrieving CRL issuer certificates.

Table of Contents

1. Introduction

RFC 3280 [PKIX1] specifies the validation of certification paths. One aspect involves the determination that a certificate has not been revoked, and one revocation checking mechanism is the Certificate Revocation List (CRL). CRL validation is also specified in RFC 3280, which involves the constructions of a valid certification path for the CRL issuer. Building a CRL issuer certification path from the signer of the CRL to a trust anchor is straightforward when the certificate of the CRL issuer is present in the certification path associated with the target certificate, but it can be complex in other situations.

There are several legitimate scenarios where the certificate of the CRL issuer is not present, or easily discovered, from the target certification path. This can be the case when indirect CRLs are used, when the Certification Authority (CA) that issued the target certificate changes its certificate signing key, or when the CA employs separate keys for certificate signing and CRL signing.

Methods of finding the certificate of the CRL issuer are currently available, such as through an accessible directory location or through use of the Subject Information Access extension in intermediary CA certificates.

Directory lookup requires existence and access to a directory that has been populated with all of the necessary certificates. The Subject Information Access extension, which supports building the CRL issuer certification path top-down (in the direction from the trust anchor to the CRL issuer), requires that some certificates in the CRL issuer certification path includes an appropriate Subject Information Access extension.

RFC 3280 [PKIX1] provides for bottom-up discovery of certification paths through the Authority Information Access extension, where the id-ad-caIssuers access method may specify one or more accessLocation fields that reference CA certificates associated with the certificate containing this extension.

This document enables the use of the Authority Information Access extension in CRLs, enabling a CRL checking application to use the access method (id-ad-caIssuers) to locate certificates that may be useful in the construction of a valid CRL issuer certification path to an appropriate trust anchor.

1.1. 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 RFC 2119 [RFC2119].

2. Authority Information Access CRL Extension

This section defines the use of the Authority Information Access extension in a CRL. The syntax and semantics defined in RFC 3280 [PKIX1] for the certificate extensions are also used for the CRL extension.

This CRL extension MUST NOT be marked critical.

This extension MUST be identified by the extension object identifier (OID) defined in RFC 3280 (1.3.6.1.5.5.7.1.1), and the AuthorityInfoAccessSyntax MUST be used to form the extension value. For convenience, the ASN.1 [X.680] definition of the Authority Information Access extension is repeated below.

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER  ::=  { id-pe 1 }

AuthorityInfoAccessSyntax  ::=  SEQUENCE SIZE (1..MAX) OF
                          AccessDescription

AccessDescription  ::=  SEQUENCE {
   accessMethod          OBJECT IDENTIFIER,
   accessLocation        GeneralName  }

id-ad OBJECT IDENTIFIER  ::=  { id-pkix 48 }

id-ad-caIssuers OBJECT IDENTIFIER  ::=  { id-ad 2 }
```

When present in a CRL, this extension MUST include at least one AccessDescription specifying id-ad-caIssuers as the accessMethod. Access method types other than id-ad-caIssuers MUST NOT be included. At least one instance of AccessDescription SHOULD specify an accessLocation that is an HTTP [HTTP/1.1] or Lightweight Directory Access Protocol [LDAP] Uniform Resource Identifier [URI].

Where the information is available via HTTP or FTP, accessLocation MUST be a uniformResourceIdentifier and the URI MUST point to a certificate containing file. The certificate file MUST contain either a single Distinguished Encoding Rules (DER) [X.690] encoded certificate (indicated by the .cer file extension) or a collection of certificates (indicated by the .p7c file extension):

.cer A single DER encoded certificate as specified in RFC 2585 [PKIX-CERT].

.p7c A "certs-only" CMS message as specified in RFC 2797 [CMC].

Conforming applications that support HTTP or FTP for accessing certificates MUST be able to accept .cer files and SHOULD be able to accept .p7c files.

HTTP server implementations accessed via the URI SHOULD use the appropriate MIME content-type for the certificate containing file. Specifically, the HTTP server SHOULD use the content-type application/pkix-cert [PKIX-CERT] for a single DER encoded certificate and application/pkcs7-mime [CMC] for CMS certs-only (PKCS#7). Consuming clients may use the MIME type and file extension as a hint to the file content, but should not depend solely on the presence of the correct MIME type or file extension in the server response.

When the accessLocation is a directoryName, the information is to be obtained by the application from whatever directory server is locally configured. When one CA public key is used to validate signatures on certificates and CRLs, the desired CA certificate is stored in the crossCertificatePair and/or cACertificate attributes as specified in [RFC2587]. When different public keys are used to validate signatures on certificates and CRLs, the desired certificate is stored in the userCertificate attribute as specified in [RFC2587]. Thus, implementations that support the directoryName form of accessLocation MUST be prepared to find the needed certificate in any of these three attributes. The protocol that an application uses to access the directory (e.g., DAP or LDAP) is a local matter.

Where the information is available via LDAP, the accessLocation SHOULD be a uniformResourceIdentifier. The URI MUST specify a distingishedName and attribute(s) and MAY specify a host name (e.g., ldap://ldap.example.com/cn=example%20CA,dc=example,dc=com?cACertificate;binary,crossCertificatePair;binary). Omitting the host name (e.g., ldap:///cn=example%20CA,dc=example,dc=com?cACertificate;binary) has the effect of specifying the use of whatever LDAP server is locally configured. The URI MUST list appropriate attribute descriptions for one or more attributes holding certificates or cross-certificate pairs.

3. Security Considerations

Implementers should take into account the possible existence of multiple unrelated CAs and CRL issuers with the same name.

Implementers should be aware of risks involved if the Authority Information Access extensions of corrupted CRLs contain links to malicious code. Implementers should always take the steps of validating the retrieved data to ensure that the data is properly formed.

4. References

4.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2587] Boeyen, S., Howes, T., and P. Richard, "Internet X.509 Public Key Infrastructure: LDAPv2 Schema", RFC 2587, June 1999.

[PKIX1] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[HTTP/1.1] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[URI] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[LDAP] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[PKIX-CERT] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

[CMC] Myers, M., Liu, X., Schaad, J., and J. Weinstein, "Certificate Management Messages over CMS", RFC 2797, April 2000.

4.2. Informative References

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

[X.690] ITU-T Recommendation X.690 Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1997.

Authors' Addresses

Stefan Santesson
Microsoft
Tuborg Boulevard 12
2900 Hellerup
Denmark

EMail: stefans@microsoft.com

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

EMail: housley@vigilsec.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.