Network Working Group
Request for Comments: 2587
Category: Standards Track

S. Boeyen
Entrust
T. Howes
Netscape
P. Richard
Xcert

June 1999

Internet X.509 Public Key Infrastructure LDAPv2 Schema

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

1. Abstract

The schema defined in this document is a minimal schema to support PKIX in an LDAPv2 environment, as defined in RFC 2559. Only PKIX-specific components are specified here. LDAP servers, acting as PKIX repositories should support the auxiliary object classes defined in this specification and integrate this schema specification with the generic and other application-specific schemas as appropriate, depending on the services to be supplied by that server.

The key words ’MUST’, ’SHALL’, ’REQUIRED’, ’SHOULD’, ’RECOMMENDED’, and ’MAY’ in this document are to be interpreted as described in RFC 2119.

2. Introduction

This specification is part of a multi-part standard for development of a Public Key Infrastructure (PKI) for the Internet. LDAPv2 is one mechanism defined for access to a PKI repository. Other mechanisms, such as http, are also defined. If an LDAP server, accessed by LDAPv2 is used to provide a repository, the minimum requirement is that the repository support the addition of X.509 certificates to directory entries. Certificate Revocation List (CRL)is one mechanism for publishing revocation information in a repository. Other mechanisms, such as http, are also defined.

This specification defines the attributes and object classes to be used by LDAP servers acting as PKIX repositories and to be understood by LDAP clients communicating with such repositories to query, add, modify and delete PKI information. Some object classes and attributes defined in X.509 are duplicated here for completeness. For end entities and Certification Authorities (CA), the earlier X.509 defined object classes mandated inclusion of attributes which are optional for PKIX. Also, because of the mandatory attribute specification, this would have required dynamic modification of the object class attribute should the attributes not always be present in entries. For these reasons, alternative object classes are defined in this document for use by LDAP servers acting as PKIX repositories.

3. PKIX Repository Objects

The primary PKIX objects to be represented in a repository are:

- End Entities
- Certification Authorities (CA)

These objects are defined in RFC 2459.

3.1. End Entities

For purposes of PKIX schema definition, the role of end entities as subjects of certificates is the major aspect relevant to this specification. End entities may be human users, or other types of entities to which certificates may be issued. In some cases, the entry for the end entity may already exist and the PKI-specific information is added to the existing entry. In other cases the entry may not exist prior to the issuance of a certificate, in which case the entity adding the certificate may also need to create the entry. Schema elements used to represent the non PKIX aspects of an entry, such as the structural object class used to represent organizational persons, may vary, depending on the particular environment and set of applications served and are outside the scope of this specification.

The following auxiliary object class MAY be used to represent certificate subjects:

```
pkiUser   OBJECT-CLASS   ::= {
   SUBCLASS OF   { top}
   KIND          auxiliary
   MAY CONTAIN   {userCertificate}
   ID    joint-iso-ccitt(2) ds(5) objectClass(6) pkiUser(21)}

userCertificate    ATTRIBUTE  ::=  {
     WITH SYNTAX   Certificate
     EQUALITY MATCHING RULE   certificateExactMatch
     ID  joint-iso-ccitt(2) ds(5) attributeType(4) userCertificate(36) }
```

An end entity may obtain one or more certificates from one or more Certification Authorities. The userCertificate attribute MUST be used to represent these certificates in the directory entry representing that user.

3.2. Certification Authorities

As with end entities, Certification Authorities are typically represented in directories as auxiliary components of entries representing a more generic object, such as organizations, organizational units etc. The non PKIX-specific schema elements for these entries, such as the structural object class of the object, are outside the scope of this specification.

The following auxiliary object class MAY be used to represent Certification Authorities:

```
pkiCA   OBJECT-CLASS   ::= {
   SUBCLASS OF   { top}
   KIND          auxiliary
   MAY CONTAIN   {cACertificate |
                  certificateRevocationList |
                  authorityRevocationList |
                  crossCertificatePair }
   ID    joint-iso-ccitt(2) ds(5) objectClass(6) pkiCA(22)}

cACertificate    ATTRIBUTE  ::=  {
     WITH SYNTAX   Certificate
     EQUALITY MATCHING RULE   certificateExactMatch
     ID  joint-iso-ccitt(2) ds(5) attributeType(4) cACertificate(37) }

crossCertificatePairATTRIBUTE::={
   WITH SYNTAX   CertificatePair
   EQUALITY MATCHING RULE certificatePairExactMatch
 ID joint-iso-ccitt(2) ds(5) attributeType(4) crossCertificatePair(40)}
```

The cACertificate attribute of a CA’s directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA.

The forward elements of the crossCertificatePair attribute of a CA’s directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the reverse elements of the crossCertificatePair attribute, of a CA’s directory entry may contain a subset of certificates issued by this CA to other CAs. When both the forward and the reverse elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

When a reverse element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values.

In the case of V3 certificates, none of the above CA certificates shall include a basicConstraints extension with the cA value set to FALSE.

The definition of realm is purely a matter of local policy.

```
certificateRevocationListATTRIBUTE::={
     WITH SYNTAX  CertificateList
     EQUALITY MATCHING RULE certificateListExactMatch
  ID joint-iso-ccitt(2) ds(5) attributeType(4)
     certificateRevocationList(39)}
```

The certificateRevocationList attribute, if present in a particular CA’s entry, contains CRL(s) as defined in RFC 2459.

```
authorityRevocationListATTRIBUTE::={
   WITH SYNTAX   CertificateList
   EQUALITY MATCHING RULE certificateListExactMatch
 ID joint-iso-ccitt(2) ds(5) attributeType(4)
    authorityRevocationList(38)}
```

The authorityRevocationList attribute, if present in a particular CA’s entry, includes revocation information regarding certificates issued to other CAs.

3.2.1. CRL distribution points

CRL distribution points are an optional mechanism, specified in RFC 2459, which MAY be used to distribute revocation information.

A patent statement regarding CRL distribution points can be found at the end of this document.

If a CA elects to use CRL distribution points, the following object class is used to represent these.

```
 cRLDistributionPoint   OBJECT-CLASS::= {
    SUBCLASS OF     { top }
    KIND            structural
    MUST CONTAIN    { commonName }
    MAY CONTAIN     { certificateRevocationList |
                      authorityRevocationList |
                      deltaRevocationList }
    ID joint-iso-ccitt(2) ds(5) objectClass(6) cRLDistributionPoint(19) }
```

The certificateRevocationList and authorityRevocationList attributes are as defined above.

The commonName attribute and deltaRevocationList attributes, defined in X.509, are duplicated below.

```
   commonName   ATTRIBUTE::={
      SUBTYPE OF     name
      WITH SYNTAX   DirectoryString
      ID joint-iso-ccitt(2) ds(5) attributeType(4) commonName(3) }

   deltaRevocationList        ATTRIBUTE ::= {
      WITH SYNTAX             CertificateList
      EQUALITY MATCHING RULE  certificateListExactMatch
      ID joint-iso-ccitt(2) ds(5) attributeType(4)
         deltaRevocationList(53) }
```

3.2.2. Delta CRLs

Delta CRLs are an optional mechanism, specified in RFC 2459, which MAY be used to enhance the distribution of revocation information.

If a CA elects to use delta CRLs, the following object class is used to represent these.

```
      deltaCRL   OBJECT-CLASS::= {
         SUBCLASS OF     { top }
         KIND            auxiliary
         MAY CONTAIN     { deltaRevocationList }
         ID joint-iso-ccitt(2) ds(5) objectClass(6) deltaCRL(23) }
```

4. Security Considerations

Since the elements of information which are key to the PKI service (certificates and CRLs) are both digitally signed pieces of information, no additional integrity service is REQUIRED.

Security considerations with respect to retrieval, addition, deletion, and modification of the information supported by this schema definition are addressed in RFC 2559.

5. References

[1] Yeong, Y., Howes, T. and S. Kille, "Lightweight Directory Access Protocol", RFC 1777, March 1995.

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

6 Intellectual Property Rights

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

7. Authors' Addresses

Sharon Boeyen
Entrust Technologies Limited
750 Heron Road
Ottawa, Ontario
Canada K1V 1A7

EMail: sharon.boeyen@entrust.com

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043
USA

EMail: howes@netscape.com

Patrick Richard
Xcert Software Inc.
Suite 1001, 701 W. Georgia Street
P.O. Box 10145
Pacific Centre
Vancouver, B.C.
Canada V7Y 1C6

EMail: patr@xcert.com

Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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