Internet X.509 Public Key Infrastructure
LDAP Schema for X.509 Attribute Certificates
<draft-ietf-pkix-ldap-ac-schema-00.txt>

Copyright (C) The Internet Society (2003). All Rights Reserved.

STATUS OF THIS MEMO

This document is an Internet-Draft and is in full conformance with all the provisions of Section 10 of RFC2026 [1].

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.

Comments and suggestions on this document are encouraged. Comments on this document should be sent to the PKIX working group discussion list <ietf-pkix@imc.org> or directly to the authors.

ABSTRACT

This document describes an LDAP schema for X.509 attribute certificates (ACs). Each AC is broken down into a set of attribute types. These attributes can then be stored in an AC entry. An object class is defined for this AC entry. Each attribute type uses an existing LDAP syntax, so that no new matching rules need to be defined.

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 [2].

1. Introduction

It currently isn’t possible to search LDAP servers for X.509 [6] attributes (public key certificates, CRLs etc.) as no matching rules have been defined for them. A couple of Internet Drafts [9,10] have been specified, but implementation of them is complex.

This document takes an alternative approach. Rather than search for an X.509 attribute in an entry, it suggests the directory user creates an entry (in the case of public key and attribute certificates) or a subtree (in the case of CRLs) from the X.509 attribute. The attributes of these new entries will be created from fields of the X.509 attribute (e.g. the issuer field), and if these new attributes are defined using existing LDAP syntaxes and matching rules, then it will be possible to use existing LDAP server technology to search for fields in X.509 attributes.
This document is one of a set comprising:
i) the LDAP schema for X.509 public key certificates [7]
ii) the LDAP schema for X.509 attribute certificates (this document)
iii) the LDAP schema for X.509 CRLs [8]

Schema definitions are provided using LDAPv3 description formats from RFC2252 [3]. Definitions provided here are formatted (line wrapped) for readability. The specifications use the augmented Backus-Naur Form (ABNF) as described in RFC2234 [4].

2. DIT Structure and Naming

If the schema presented in this document is used to store information about ACs in an LDAP directory, each AC SHOULD be stored as a direct subordinate of the AC holder’s entry. These entries SHOULD be named using either the x509ACNameForm i.e. by a multi-valued RDN formed by the AC issuer and serial number, or by the x509ACAltNameForm i.e. by a single valued RDN formed by concatenating the AC issuer and serial number, as these are the only ways to enforce unique RDNs under the holder’s entry. Exceptionally, if it can be guaranteed that only ACs from a single issuer will be stored under the holder’s entry, the x509ACserialNumberNameForm MAY be used, i.e. the single valued RDN formed from the AC serial number.

```
(1.2.826.0.1.3344810.1.3.3
 NAME ’x509ACNameForm’
 OC x509AC
 MUST ( x509serialNumber $ x509issuer ) )

(1.2.826.0.1.3344810.1.3.4
 NAME ’x509ACAltNameForm’
 OC x509AC
 MUST ( x509issuerSerial ) )

(1.2.826.0.1.3344810.1.3.5
 NAME ’x509ACserialNumberNameForm’
 OC x509AC
 MUST ( x509serialNumber ) )
```

The following attribute description describes the attribute used to hold the alternative RDN name form.

```
(1.2.826.0.1.3344810.1.1.60
 NAME ’x509issuerSerial’
 DESC ’Used to hold the RDN of a certificate entry, formed by concatenating the AC serial number and issuer fields ’
 EQUALITY distinguishedNameMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
 SINGLE-VALUE )
```

When encoding DNs that contain an x509issuer field, the string representation must be made according to [RFC2253]. These strings contain RFC2253 special characters and must therefore be escaped. For example, the issuer name in a certificate may be:

```
x509issuer: OU=VeriSign Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 1 Public Primary Certification Authority - G2,O=VeriSign Inc.,C=US
```

When used in the x509issuerSerial attribute of a DN, this may appear as:

```
dn: x509issuerSerialNumber=123456\,OU=VeriSign Trust Network \,OU\=(c) 1998 VeriSign Inc. - For authorized use only\,OU=Class 1 Public Primary Certification Authority - G2\,O=VeriSign Inc.\,C=US,cn=Joe Example, ...
```
3. X.509 schema Object Classes

The base object class is defined in [8].

3.1 X509 Attribute Certificate object class

(1.2.826.0.1.3344810.1.0.16
 NAME 'x509AC'
 SUP x509base
 STRUCTURAL
 MUST ( x509version $ 
 x509serialNumber $ 
 x509validityNotBefore $ 
 x509validityNotAfter )
 MAY ( x509acHolderPKCSerialNumber $ 
 x509acHolderPKCissuerDN $ 
 x509acHolderRfc822Name $ 
 x509acHolderDnsName $ 
 x509acHolderDN $ 
 x509acHolderURI $ 
 x509acHolderIpAddress $ 
 x509acHolderRegisteredID $ 
 x509acObjectDigest $ 
 x509acDigestAlgorithm $ 
 x509acDigestedObjectType $ 
 x509acAuditID $ 
 x509acTargetRfc822Name $ 
 x509acTargetDnsName $ 
 x509acTargetDN $ 
 x509acTargetURI $ 
 x509acTargetIpAddress $ 
 x509acTargetRegisteredID $ 
 x509acNoRevocation )
)

4. Common X.509 attribute types
The following attribute types defined in [7] are used to hold the corresponding fields of ACs:

- x509serialNumber Â» used to hold the serial number of the AC
- x509version Â» used to hold the version of the AC
- x509signatureAlgorithm Â» used to hold the OID of the algorithm used to sign the CRL
- x509issuer Â» used to hold the DN of the AC issuer
- x509ValidityNotBefore Â» used to hold the not before validity time of the AC (note that only the Generalized Time format is permitted)
- x509ValidityNotAfter Â» used to hold the not after validity time of the AC (note that only the Generalized Time format is permitted)
- x509authorityCertIssuer Â» used in conjunction with x509authorityCertSerialNumber to identify the public key certificate of the AC issuer
- x509authorityCertSerialNumber Â» used in conjunction with x509authorityCertIssuer to identify the public key certificate of the AC issuer
- x509issuerRfc822Name Â» used to hold the email address of the AC issuer
- x509issuerDnsName Â» used to hold the DNS name of the AC issuer
- x509issuerURI Â» used to hold a URI for the AC issuer
- x509issuerIPAddress Â» used to hold the IP address of the AC issuer
- x509issuerRegisteredID Â» used to hold a registered OID of the AC issuer
- x509authorityKeyIdIdentifier Â» used to hold the identifier of the public key used to sign the AC, taken from the attribute cert issuer object digest field

5. Attribute types for AC specific fields

The following attribute types may be used to store basic fields of an AC. The following basic fields are supported:

- x509acHolderPKCSerialNumber and x509acHolderPKCissuerDN Â» used to identify the holder via their public key certificate
- x509acHolderRfc822Name Â» identifies the holder via their email address
- x509acHolderDnsName Â» identifies the holder via their DNS name
- x509acHolderDN Â» identifies the holder via their DN
- x509acHolderURI Â» identifies the holder via their URI
- x509acHolderIPAddress Â» identifies the holder via their IP address
- x509acHolderRegisteredID Â» identifies the holder via a registered OID
- x509acObjectIdDigest, x509acDigestAlgorithm and x509acDigestedObjectType Â» identifies the holder via a hash of information directly associated with the holder

5.1 AC holder PKC

The x509acHolderPKCSerialNumber and x509acHolderPKCissuerDN attributes are to hold the contents of the holder base certificate ID fields, in order to identify the holder via their public key certificate

5.1.1 AC holder PKC serial number

(1.2.826.0.1.3344810.1.1.61
 NAME 'x509acHolderPKCSerialNumber'
 DESC 'The serial number of the PKC of the AC holder' - see RFC3281 4.2.2'
 EQUALITY integerMatch
 ORDERING integerOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
 SINGLE-VALUE )

5.1.2 AC holder PKC issuer DN

(1.2.826.0.1.3344810.1.1.62
5.2 AC Holder General Names

The following attributes are used to hold the alternative forms of the general name of the holder. Separate attribute types are defined for all choices of the ASN.1 type "GeneralName" except for "otherName", "x400Address" and "ediPartyName".

5.2.1 Holder RFC 822 name

(1.2.826.0.1.3344810.1.1.63
 NAME 'x509acHolderRfc822Name'
 DESC 'Internet electronic mail address of the AC holder
 - see RFC3281 4.2.2'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC 822 [11].

5.2.2 Holder DNS name

(1.2.826.0.1.3344810.1.1.64
 NAME 'x509acHolderDnsName'
 DESC 'Internet domain name of the AC Holder, see
 RFC3281 4.2.2'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded as Internet domain names in accordance with RFC1035 [12].

5.2.3 Holder directory name

(1.2.826.0.1.3344810.1.1.65
 NAME 'x509acHolderDN'
 DESC 'Distinguished name of the AC Holder, see
 RFC3281 4.2.2'
 EQUALITY distinguishedNameMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

Values of this attribute type must be encoded according to the syntax given in RFC2253 [13].

5.2.4 Holder Uniform Resource Identifier

(1.2.826.0.1.3344810.1.1.66
 NAME 'x509acHolderURI'
 DESC 'Uniform Resource Identifier of the AC Holder
 - see RFC3281 4.2.2'
 EQUALITY caseExactMatch
 SUBSTR caseExactSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC2396 [14].

5.2.5 Holder IP address
(1.2.826.0.1.3344810.1.1.67
 NAME 'x509acHolderIpAddress'
 DESC 'Internet Protocol address of the AC Holder, see RFC3281 4.2.2'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute type must be stored in the syntax given in Appendix B of RFC2373 [16].

5.2.6 Holder registered ID

(1.2.826.0.1.3344810.1.1.68
 NAME 'x509acHolderRegisteredID'
 DESC 'Any registered OID of the AC holder, see RFC3281 4.2.2'
 EQUALITY objectIdentifierMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )

registeredID is an identifier of any registered object assigned in accordance with ITU-T Rec. X.660. [17]

5.3 AC object digest

x509acObjectDigest, x509acDigestAlgorithm and x509acDigestedObjectType are used to hold the contents of the holder object digest info fields. They are used to identify the holder via a hash of information directly associated with the holder.

5.3.1 Object digest

( 1.2.826.0.1.3344810.1.1.69
 NAME 'x509acObjectDigest'
 DESC 'Holds the hash value of the object identified by x509acDigestedObjectType û see RFC 3281, section 7.3'
 EQUALITY bitstringMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.6
 SINGLE-VALUE )

5.3.2 Object digest algorithm

( 1.2.826.0.1.3344810.1.1.70
 NAME 'x509acDigestAlgorithm'
 DESC 'OID of the hashing algorithm used to create the Object digest, see RFC3281, section 7.3'
 EQUALITY objectIdentifierMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
 SINGLE-VALUE )

5.3.3 Object Type

(1.2.826.0.1.3344810.1.1.71
 NAME 'x509acDigestedObjectType'
 DESC 'Type of object being digested û see RFC3281, section 7.3'
 EQUALITY integerMatch
 ORDERING integerOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
 SINGLE-VALUE )

6. Attributes for selected AC extensions

In line with the AC profile RFC 3281 [5], the following AC extensions are supported:
- Audit Identity (defined here)
AC targets (defined here)
- Authority Key Identifier (defined in [7])
- Authority Information Access (defined in [7])
- CRL distribution points (defined here)
- No revocation (defined here)

(Note. The CRL distribution point attributes defined in [7] were inadequate for our needs)

6.1 Audit identity

This attribute may be used to store the sequence number of the CRL.

(1.2.826.0.1.3344810.1.1.72
  NAME 'x509acAuditID'
  DESC 'Identity of holder used in audit trails - see RFC3281 4.3.1'
  EQUALITY octetStringMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
  SINGLE-VALUE )

6.2 AC targets

ACs can be targeted at specific objects, or groups of objects. Objects and groups of objects are identified by their general names. Separate sets of attributes are specified for individual targets and groups of targets. Attribute types are defined for all choices of the ASN.1 type "GeneralName" except for "otherName", "x400Address" and "ediPartyName".

6.2.1 Target RFC 822 name

(1.2.826.0.1.3344810.1.1.73
  NAME 'x509acTargetRfc822Name'
  DESC 'Internet electronic mail address of the AC’s Target - see RFC3281 4.3.2'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC 822 [11].

6.2.2 Target DNS name

(1.2.826.0.1.3344810.1.1.74
  NAME 'x509acTargetDnsName'
  DESC 'Internet domain name of the AC’s Target, see RFC3281 4.3.2'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded as Internet domain names in accordance with RFC1035 [12].

6.2.3 Target directory name

(1.2.826.0.1.3344810.1.1.75
  NAME 'x509acTargetDN'
  DESC 'Distinguished name of the AC’s Target, see RFC3281 4.3.2'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

Values of this attribute type must be encoded according to the syntax given in RFC2253 [13].
6.2.4 Target Uniform Resource Identifier

(1.2.826.0.1.3344810.1.1.33)  
NAME ‘x509acTargetURI’  
DESC ‘Uniform Resource Identifier of the AC’s Target'  
- see RFC3281 4.3.2’  
EQUALITY caseExactMatch  
SUBSTR caseExactSubstringsMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC2396 [14].

6.2.5 Target IP address

(1.2.826.0.1.3344810.1.1.34)  
NAME ‘x509acTargetIpAddress’  
DESC ‘Internet Protocol address of the AC’s Target, see RFC3281 4.3.2’  
EQUALITY caseIgnoreMatch  
SUBSTR caseIgnoreSubstringsMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute type must be stored in the syntax given in Appendix B of RFC2373 [16].

6.2.6 Target registered ID

(1.2.826.0.1.3344810.1.1.35)  
NAME ‘x509acTargetRegisteredID’  
DESC ‘Any registered OID of the AC’s Target, see RFC3281 4.3.2’  
EQUALITY objectIdentifierMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )

registeredID is an identifier of any registered object assigned in accordance with ITU-T Rec. X.660. [17]

6.2.7 Target group RFC 822 name

(1.2.826.0.1.3344810.1.1.36)  
NAME ‘x509acTargetGroupRfc822Name’  
DESC ‘Internet electronic mail address of the AC’s Target group’  
- see RFC3281 4.3.2’  
EQUALITY caseIgnoreMatch  
SUBSTR caseIgnoreSubstringsMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC 822 [11].

6.2.8 Target group DNS name

(1.2.826.0.1.3344810.1.1.37)  
NAME ‘x509acTargetGroupDnsName’  
DESC ‘Internet domain name of the AC’s Target group, see RFC3281 4.3.2’  
EQUALITY caseIgnoreMatch  
SUBSTR caseIgnoreSubstringsMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded as Internet domain names in accordance with RFC1035 [12].

6.2.9 Target group directory name
(1.2.826.0.1.3344810.1.1.81
 NAME 'x509acTargetGroupDN'
 DESC 'Distinguished name of the AC’s Target group, see RFC3281 4.3.2'
 EQUALITY distinguishedNameMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

Values of this attribute type must be encoded according to the syntax given in RFC2253 [13].

6.2.10 Target group Uniform Resource Identifier

(1.2.826.0.1.3344810.1.1.82
 NAME 'x509acTargetGroupURI'
 DESC 'Uniform Resource Identifier of the AC’s Target group - see RFC3281 4.3.2'
 EQUALITY caseExactMatch
 SUBSTR caseExactSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC2396 [14].

6.2.11 Target group IP address

(1.2.826.0.1.3344810.1.1.83
 NAME 'x509acTargetGroupIpAddress'
 DESC 'Internet Protocol address of the AC’s Target group, see RFC3281 4.3.2'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute type must be stored in the syntax given in Appendix B of RFC2373 [16].

6.2.12 Target group registered ID

(1.2.826.0.1.3344810.1.1.84
 NAME 'x509acTargetGroupRegisteredID'
 DESC 'Any registered OID of the AC’s Target group, see RFC3281 4.3.2'
 EQUALITY objectIdentifierMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )

registeredID is an identifier of any registered object assigned in accordance with ITU-T Rec. X.660. [17]

6.3 No revocation

(1.2.826.0.1.3344810.1.1.85
 NAME 'x509acNoRevocation'
 DESC 'If true, the AC will never be revoked, see RFC3281 section 4.3.6'
 EQUALITY booleanMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 )

6.4 CRL Distribution Points

The CRL distribution point extension indicates the locations where CRLs will be published for this AC. It comprises the general name of the DP, plus optionally the general name of the CRL issuer (if different from the AC issuer) plus the reason codes that will be published at this DP. Separate attribute types are defined for all choices of the ASN.1 type "GeneralName" except for "otherName", "x400Address" and "ediPartyName". Note that because there can be multiple
distribution points, the multi-valued attributes defined here will not be able to link each DP with its corresponding reasons and issuer.

6.4.1 Distribution point RFC 822 name
(1.2.826.0.1.3344810.1.1.86
NAME 'x509DPRfc822Name'
DESC 'Internet electronic mail address of the distribution point, see RFC3280 section 4.2.1.14'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC 822 [11].

6.4.2 Distribution point DNS name
(1.2.826.0.1.3344810.1.1.87
NAME 'x509DPDnsName'
DESC 'Internet domain name of the distribution point, see RFC3280 section 4.2.1.14'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded as Internet domain names in accordance with RFC1035 [12].

6.4.3 Distribution point directory name
(1.2.826.0.1.3344810.1.1.88
NAME 'x509DPDN'
DESC 'Distinguished name of the distribution point, see RFC3280 section 4.2.1.14'
EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

Values of this attribute type must be encoded according to the syntax given in RFC2253 [13].

6.4.4 Distribution point Uniform Resource Identifier
(1.2.826.0.1.3344810.1.1.89
NAME 'x509DPURI'
DESC 'Uniform Resource Identifier of the distribution point, see RFC3280 section 4.2.1.14'
EQUALITY caseExactMatch
SUBSTR caseExactSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC2396 [14].

6.4.5 Distribution point IP address
(1.2.826.0.1.3344810.1.1.90
NAME 'x509DPIpAddress'
DESC 'Internet Protocol address of the distribution point, see RFC3280 section 4.2.1.14'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute type must be stored in the syntax given in Appendix B of RFC2373 [16].
6.4.6 Distribution point registered ID

(1.2.826.0.1.3344810.1.1.91
  NAME 'x509DPRegisteredID'
  DESC 'Any registered OID of the distribution point, see RFC3280 section 4.2.1.14'
  EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )

registeredID is an identifier of any registered object assigned in accordance with ITU-T Rec. X.660. [17]

6.4.7 Distribution point name relative to CRL issuer

(1.2.826.0.1.3344810.1.1.92
  NAME 'x509DPrelativeToIssuer'
  DESC 'RDN of the distribution point, relative to the issuer, see RFC3280 section 4.2.1.14'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

Values of this attribute type must be encoded according to the syntax given in RFC2253 [13].

6.4.8 Distribution point CRL issuer RFC 822 name

(1.2.826.0.1.3344810.1.1.93
  NAME 'x509DPissuerRfc822Name'
  DESC 'Internet electronic mail address of the distribution point CRL issuer, see RFC3280 section 4.2.1.14'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded according to the syntax given in RFC 822 [11].

6.4.9 Distribution point CRL issuer DNS name

(1.2.826.0.1.3344810.1.1.94
  NAME 'x509DPissuerDnsName'
  DESC 'Internet domain name of the distribution point CRL issuer, see RFC3280 section 4.2.1.14'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute must be encoded as Internet domain names in accordance with RFC1035 [12].

6.4.10 Distribution point CRL issuer directory name

(1.2.826.0.1.3344810.1.1.95
  NAME 'x509DPissuerDN'
  DESC 'Distinguished name of the distribution point CRL issuer, see RFC3280 section 4.2.1.14'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

Values of this attribute type must be encoded according to the syntax given in RFC2253 [13].

6.4.11 Distribution point CRL issuer Uniform Resource Identifier
6.4.12 Distribution point CRL issuer IP address

(1.2.826.0.1.3344810.1.1.97
 NAME 'x509DPissuerIpAddress'
 DESC 'Internet Protocol address of the distribution point CRL issuer, see RFC3280 section 4.2.1.14'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

Values of this attribute type must be stored in the syntax given in Appendix B of RFC2373 [16].

6.4.13 Distribution point CRL issuer registered ID

(1.2.826.0.1.3344810.1.1.98
 NAME 'x509DPissuerRegisteredID'
 DESC 'Any registered OID of the distribution point CRL issuer, see RFC3280 section 4.2.1.14'
 EQUALITY objectIdentifierMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )

registeredID is an identifier of any registered object assigned in accordance with ITU-T Rec. X.660. [17]

6.4.14 Distribution point reason codes

This attribute is used to indicate the reason codes associated with the various DPs.

(1.2.826.0.1.3344810.1.1.99
 NAME 'x509DPReasonCodes'
 DESC 'The reason codes used by a DP, see RFC3280 section 4.2.1.14'
 EQUALITY bitstringMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.6 )

Security Considerations

This [Internet Draft/Standard] describes the subschema for the storage and matching of PKI attributes derived from CRLs. It does not address the protocol for the storage and retrieval of this information.

LDAP servers SHOULD use authentication and access control mechanisms to protect the information during its storage and retrieval.

References

Normative


Informative


Intellectual Property Notice

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. [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.

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights which may cover technology that may be required to practice
this standard.
Please address the information to the IETF Executive
Director.

11. Copyright

Copyright (C) The Internet Society (2001). 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.

12. Authors’ Addresses

David Chadwick, Mikhail Sahalayev
IS Institute
University of Salford
Salford
England
M5 4WT

Email: d.w.chadwick@salford.ac.uk
M.Sahalayev@pgr.salford.ac.uk