An LDAPv3 Schema for X.509 Certificates
draft-klasen-ldap-x509certificate-schema-01

IETF 55, PKIX Meeting
November 20, 2002,
Atlanta, GA

Peter Gietz, Norbert Klasen
DAASII International / DFN
peter.gietz@daasi.de
Agenda

- Motivation and General Idea
- Changes in –01 ID
- Proposed changes from list discussions
- Open issues and future work
Motivation

• Address problem of multiple certificates for one entity
  – How can the client find the right certificate?
• Find a simple and easy to implement solution
• Solution should be usable in the frame of a large scale distributed LDAP / Common Indexing Protocol (CIP) based certificate repository
Schema as a simple solution

• Find a set of certificate fields and extensions that one might want to search upon
  – Meta-data approach
• Parse the certificate and store this set as LDAP attributes
• Advantages:
  – no new server features needed
  – easy to implement in clients
  – usable in a CIP environment
DIT Structure in white-pages services

Organization
  o=abc, ...

Person
  cn=Alice, ...
  X509certificate
    X509issuer=CA1DN
    +x509serialNumber=1,...

Person
  cn=Bob, ...
  X509certificate
    X509issuer=CA1DN
    +x509serialNumber=2,...
DIT Structure in certificate repositories

CA

- `cn=xyz ca, ...

x509certificate

- `x509serialNumber=1, ...

x509certificate

- `x509serialNumber=2, ...
CIP Architecture

LDAP Client

Search request

LDAP referral

LDAP Indexserver

virtual db backend

Referral as LDIF file

GET <url> accept text/ldif

TIO Server

LDAP Crawler

LDAP Server

HTTP

LDAP
Related work

• This approach:

• The smarter but more complex solution:
  – Chadwick, D. and S. Mullan, "Returning Matched Values with LDAPv3", Internet Draft (work in progress, expired), June 2002, draft-ietf-ldapext-matchedval-06.txt
Changes in Draft 01

• Fixed bug in definition of objectclass x509certificate
• updated references (RFC 3280, RFC 3377)
• new attributes
  – x509authorityKeyId
  – x509authorityCertIssuer
  – x509authorityCertSerialNumber
  – x509CertificateLocation
  – x509CertificateHolder
• new objectclass
  – x509CertificateHolder
Changes in Draft –01 (cont’d)

attributetype ( 1.3.6.1.4.1.10126.1.5.4.73
NAME 'x509CertificateHolder'
DESC 'Pointer to the directory entry of the end entity to which this certificate was issued'
EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
Changes in Draft –01 (cont’d)

attributetype ( 1.3.6.1.4.1.10126.1.5.4.71
NAME 'x509certificateLocation'
DESC 'Pointer to an x509certificate Entry'
EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

objectclass ( 1.3.6.1.4.1.10126.1.5.4.2.2
NAME 'x509certificateHolder'
AUXILIARY
MAY ( x509certificateLocation ) )
Changes in Draft –01 (cont’d)

• Deleted ";binary" in examples (??)
• Included new section
  – Comparison with component matching approach
• Some minor changes
  – in wording
  – section titles
  – other editorial changes
Proposed new changes for next draft version

• Some valuable input from the list
• Thanks to Russ, Kurt and David
Abstract x509Certificate object class

objectclass ( 1.3.6.1.4.1.10126.x..x..x
 NAME 'x509Certificate' ABSTRACT
 MUST ( x509SerialNumber $ x509SignatureAlgorithm
 $ x509Issuer $ x509ValidityNotBefore $ x509ValidityNotAfter
 $ PublicKeyInfoAlgorithm )
 MAY ( mail $ x509AuthorityKeyIdentifier $ x509AuthorityCertIssuer
 $ x509AuthorityCertSerialNumber $ x509SubjectKeyIdentifier
 $ x509KeyUsage $ x509PolicyInformationIdentifier
 $ x509SubjectAltNameRfc822Name $ x509SubjectAltNameDnsName
 $ x509SubjectAltNameDirectoryName $ x509SubjectAltNameURI
 $ x509SubjectAltNameIpAddress $ x509SubjectAltNameRegisteredID
 $ x509IssuerAltNameRfc822Name $ x509IssuerAltNameDnsName
 $ x509IssuerAltNameDirectoryName $ x509IssuerAltNameURI
 $ x509IssuerAltNameIpAddress $ x509IssuerAltNameRegisteredID
 $ x509ExtKeyUsage $ x509FullCRLDistributionPoint
 $ x509CertHolder ) )
New structural objectclasses

attributetype ( x.x.x.x NAME 'x509userCert'
   EQUALITY certificateExactMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 SINGLE-VALUE )

attributetype ( x.x.x.x NAME 'x509cACert'
   EQUALITY certificateExactMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 SINGLE-VALUE )

objectclass ( x.x.x.x NAME 'x509userCertificate'
   SUP x509certificate
   MUST x509userCert MAY x509subject )

objectclass ( x.x.x.x NAME 'x509cACertificate'
   SUP x509certificate
   MUST x509cACert $ x509subject )
Thus no more additional rules needed

• Following is now defined within the schema:
  – Entries MUST also have one of the two auxiliary object classes:
    • "pkiUser"
    • "pkiCA"
  – This way the entry will contain the binary certificate in one of the two attributes:
    • "userCertificate"
    • "caCertificate"
Open issues

• Support for implementations that can’t do multi-valued RDNs
  – include a third name form with yet another naming attribute x509serialIssuer?
  – x509SerialIssuer=x509SerialNumber\3D12345\2Co\3DsomeCA\2Cc\3Dsomecountry,ou=somedepartment,o=someorg,c=somecountry

• Include some more clarifying language
  – 2: redundancy, consistency, transition
  – 2: CIP
  – 4.1.6: x509subject vs. x509subjectAltNames
  – 4.1.7: x509subjectPublicKeyInfoAlgorithm
  – 4.3.1: x509certLocation (missing)
Open Issues (contd.)

• ";binary"
• Bug in examples
• Include a use case chapter
• Include IANA consideration
• Make this part of PKIX work
• Publish as proposed or experimental RFC
Future work

• Include attributes for Qualified certificates (RFC 3039)
• New draft on CRLs
• New draft on Attribute Certificates