An LDAPv3 Schema for X.509 Certificates

IETF 53, PKIX Meeting
March 20, 2002

Peter Gietz / Norbert Klasen
DAASI International
peter.gietz@daasi.de
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
x509certificate object class

( 1.3.6.1.4.1.10126.1.5.4.2.1
NAME 'x509certificate'
STRUCTURAL
MUST ( x509serialNumber $ x509signatureAlgorithm $ x509issuer $ x509validityNotBefore $ x509validityNotAfter $ x509subject $ x509subjectPublicKeyInfoAlgorithm )
MAY ( mail $ x509subjectKeyIdentifier $ x509keyUsage $ x509policyInformationIdentifier $ x509subjectAltNameRfc822Name $ x509subjectAltNameDnsName $ x509subjectAltNameDirectoryName $ x509subjectAltNameURI $ x509subjectAltNameIpAddress $ x509subjectAltNameRegisteredID $ x509isssuerAltNameRfc822Name $ x509isssuerAltNameDnsName $ x509isssuerAltNameDirectoryName $ x509isssuerAltNameURI $ x509isssuerAltNameIpAddress $ x509isssuerAltNameRegisteredID $ x509extKeyUsage $ x509cRLDistributionPoint ) )
Additional rule

- 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"
DIT Structure in white-pages services

- **Organization**
  
  - **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

LDAP Indexserver

virtual db backend

Search request

LDAP referral

Referral as LDIF file

GET <url> accept text/ldif

LDAP Crawler

LDAP Server

HTTP

LDAP
Related work

• This approach:

• The smarter but more complex solutions:
  – Chadwick, D. and S. Mullan, "Returning Matched Values with LDAPv3", Internet Draft (work in progress, expired), December 2000, draft-ietf-ldapext-matchedval-05.txt
Where do we want to go from here?

• Make this part of PKIX work
  – Get comments from this group and integrate them
  – Integrate references to other PKIX WG
• Discuss component matching approach
• Include a use case chapter
• Include IANA consideration
• Fix bugs and language
• Publish as proposed or experimental RFC
• Do similar work for revocation information