LDAP Items

d.w.chadwick@salford.ac.uk
Peter.Gietz@daasi.de
Contents

• LDAPv3 Profile
• New strings for RDNs
• LDAP schema for attribute extraction
• LDAPv3 protocol update
• LDAP schema for component matching
• Finding the LDAP server of a subject
• ;binary
LDAPv3 Profile

- `<draft-ietf-pkix-ldap-v3-05.txt>` issued in January 2002
- No comments received except from Microsoft that does not support multi-attributes in RDNs. This feature is currently mandatory in the profile.
**New strings for RDNs**

- Update `<draft-ietf-pkix-dnstrings-01.txt>` sent to the ID editor but 10 minutes late, so bounced. Will be resubmitted next week.

<table>
<thead>
<tr>
<th>String</th>
<th>X.500/LDAP AttributeType</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERIALNUMBER</td>
<td>serialNumber</td>
</tr>
<tr>
<td>ADDR</td>
<td>postalAddress</td>
</tr>
<tr>
<td>PSEUDO</td>
<td>pseudonym</td>
</tr>
<tr>
<td>GN</td>
<td>givenName</td>
</tr>
<tr>
<td>SN</td>
<td>surname</td>
</tr>
<tr>
<td>MAIL</td>
<td>mail/rfc822Mailbox</td>
</tr>
<tr>
<td>PI</td>
<td>permanentIdentifier</td>
</tr>
<tr>
<td>X509SN</td>
<td>x509serialNumber</td>
</tr>
<tr>
<td>ISSUER</td>
<td>x509issuer</td>
</tr>
<tr>
<td>ISSUERSN</td>
<td>x509issuerSerial</td>
</tr>
<tr>
<td>UPDATE</td>
<td>x509crlThisUpdate</td>
</tr>
</tbody>
</table>
LDAP Schema for Attribute Extraction

• Revised IDs issued for certificates, CRLs and attribute certs
• Issue: whether the attribute for the binary cert/CRL should have a different attribute type in the child entry (in PKC it is different, in CRL and AC it is not)
• Issue: How much information to store from a CRLDP – just the URI of the full CRL or all general names plus reasons, issuers and relative name
• Issue: PKC schema has not added AA Controls extension from AC profile – should it?
• Issue: The attribute types defined in AC profile are not defined by LDAP (and cant be supported “as is” due to their complex syntax).
• The Klasen draft needs to become a full PKIX draft (the reason it did not this time was due to cut off dates)
Changes to PKC –03 draft

• Changed Matching Rules from caseIgnoreMatch to caseIgnoreIA5Match
• moved the references to RFC 3280 from the DESC part of the attribute definition to the text
• added some additional text about CIP in Introduction
• reworded text in Section 4.1.7 on Subject public key info algorithm to:
  „OID identifying the algorithm associated with the certified public key“
Changes to PKC –03 draft contd.

• changed x509userCert and x509caCert to be inherited from userCertificate and caCertificate respectively
• added clarification about x509subject and subject alternative names in section Section 4.5
• added attribute type x509issuerSerial to x509PKC object class
• added attribute type x509basicConstraintsCa to x509PKC object class
• renamed attribute type 509cRLDistributionPointURI to x509FullcRLDistributionPointURI
Changes to PKC –03 draft contd.

• devided references in normative and non normative
• deleted attributetype mail from x509PKC objectclass
• created separate Name Forms for 509userCertificate and x509caCertificate object classes
• changed attributetype x509SerialNumber to MULTI-VALUE
• adjusted examples to new schema
• Fixed more typos
Still todo

• Include AAcontrol extension from RFC 3281 into X509-PKC objectclass
• Add new auxiliary object class for qualified certificates (draft-ietf-pkix-sonof3039-00.txt)
  – What is the status of that draft?
• IANA considerations
• Resolve the issues with the AC and CRL draft
LDAPv3 Protocol Update

- Protocol is currently proposed standard but draft standard is in preparation
- ;binary has been removed from latest revision
- Probably will be added as an extension to LDAPv3 (Steven Legg ID)
- But this currently gives PKIX users a problem
- Chairs decided to ballot PKIX members on which LDAP they use and how
LDAPv3 Schema for Component Matching

- Separated into two IDs – PKI schema and PMI schema
- PKI schema has defined a native LDAP encoding for PKI attributes, which is bitwise identical to the ;binary encodings of the current LDAPv3 proposed standard
- Also added back the simple encoding for exact matching (from first ID) that is now implemented in OpenLDAP
- PKI schema is now finished (apart from ;binary issue)
- PMI schema needs a bit more work on it
LDAPv3 Any Other Issues

- There is currently no direct way for the recipient of a user certificate to find out where other certificates for the same user might be found
- The AIA and SIA do not provide this functionality
- ID has been written which defines a new Subject Certificate Access extension, and will be submitted next week
- Alternative would be to add a new value for SIA (or AIA) that points to the location(s) of the subject’s cert