Network Working Group
INTERNET-DRAFT
Expires in six months from

M. Wahl
Critical Angle Inc.
10 Oct. 1997

A Summary of the X.500(96) User Schema for use with LDAPv3
<draft-ietf-asid-ldapv3schema-x500-03.txt>

1. Status of this Memo

This document is an Internet-Draft. 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."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

2. Abstract

This document provides an overview of the attribute types and object classes defined by the ISO and ITU-T committees in the X.500 documents, in particular those intended for use by directory clients. This is the most widely used schema for LDAP/X.500 directories, and many other schema definitions for white pages objects use it as a basis. This document does not cover attributes used for the administration of X.500 directory servers, nor does it include attributes defined by other ISO/ITU-T documents.

3. General Issues

This document references syntaxes given in section 6 of this document and section 6 of [1]. Matching rules are listed in section 8 of this document and section 8 of [1].

The attribute type and object class definitions are written using the BNF form of AttributeTypeDescription and ObjectClassDescription given in [1]. Lines have been folded for readability.

4. Source

The schema definitions in this document are based on those found in X.500 [2],[3],[4],[5], and updates to these documents, specifically:

Sections	Source
5.1 - 5.2	X.501(93)
5.3 - 5.36	X.520(88)
5.37 - 5.41	X.509(93)
5.42 - 5.52	X.520(93)
5.53 - 5.54	X.509(96)
5.55	X.520(96)
6.1	RFC 1274
6.2	(new syntax)
6.3 - 6.6	RFC 1274
7.1 - 7.2	X.501(93)
7.3 - 7.18	X.521(93)
7.19 - 7.21	X.509(96)
7.22	X.521(96)

Some attribute names are different from those found in X.520(93).

Three new attributes supportedAlgorithms, deltaRevocationList and dmdName, and the objectClass dmd, are defined in the X.500(96) documents.

5. Attribute Types

An LDAP server implementation SHOULD recognize the attribute types described in this section.

5.1. objectClass

The values of the objectClass attribute describe the kind of object which an entry represents. The objectClass attribute is present in every entry, with at least two values. One of the values is either "top" or "alias".

```
( 2.5.4.0 NAME 'objectClass' EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
```

5.2. aliasedObjectName

The aliasedObjectName attribute is used by the directory service if the entry containing this attribute is an alias.

```
( 2.5.4.1 NAME 'aliasedObjectName' EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE )
```


5.3. knowledgeInformation

This attribute is no longer used.

```
( 2.5.4.2 NAME 'knowledgeInformation' EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

5.4. cn

This is the X.500 commonName attribute, which contains a name of an object. If the object corresponds to a person, it is typically the person's full name.

```
( 2.5.4.3 NAME 'cn' SUP name )
```

5.5. sn

This is the X.500 surname attribute, which contains the family name of a person.

```
( 2.5.4.4 NAME 'sn' SUP name )
```

5.6. serialNumber

This attribute contains the serial number of a device.

```
( 2.5.4.5 NAME 'serialNumber' EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{64} )
```

5.7. c

This attribute contains a two-letter ISO 3166 country code (countryName).

(2.5.4.6 NAME 'c' SUP name SINGLE-VALUE)

5.8. l

This attribute contains the name of a locality, such as a city, county or other geographic region (localityName).

(2.5.4.7 NAME 'l' SUP name)

5.9. st

This attribute contains the full name of a state or province (stateOrProvinceName).

(2.5.4.8 NAME 'st' SUP name)

5.10. street

This attribute contains the physical address of the object to which the entry corresponds, such as an address for package delivery (streetAddress).

(2.5.4.9 NAME 'street' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128})

5.11. o

This attribute contains the name of an organization (organizationName).

(2.5.4.10 NAME 'o' SUP name)

5.12. ou

This attribute contains the name of an organizational unit (organizationalUnitName).

(2.5.4.11 NAME 'ou' SUP name)

5.13. title

This attribute contains the title, such as "Vice President", of a

person in their organizational context. The "personalTitle" attribute would be used for a person's title independent of their job function.

(2.5.4.12 NAME 'title' SUP name)

5.14. description

This attribute contains a human-readable description of the object.

(2.5.4.13 NAME 'description' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024})

5.15. searchGuide

This attribute is for use by X.500 clients in constructing search filters. It is obsoleted by enhancedSearchGuide, described below in 5.48.

(2.5.4.14 NAME 'searchGuide'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.25)

5.16. businessCategory

This attribute describes the kind of business performed by an organization.

(2.5.4.15 NAME 'businessCategory' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128})

5.17. postalAddress

(2.5.4.16 NAME 'postalAddress' EQUALITY caseIgnoreListMatch
SUBSTR caseIgnoreListSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.41)

5.18. postalCode

(2.5.4.17 NAME 'postalCode' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{40})

5.19. postOfficeBox

```
    ( 2.5.4.18 NAME 'postOfficeBox' EQUALITY caseIgnoreMatch
      SUBSTR caseIgnoreSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{40} )
```

5.20. physicalDeliveryOfficeName

```
    ( 2.5.4.19 NAME 'physicalDeliveryOfficeName' EQUALITY caseIgnoreMatch
      SUBSTR caseIgnoreSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} )
```

5.21. telephoneNumber

```
    ( 2.5.4.20 NAME 'telephoneNumber' EQUALITY telephoneNumberMatch
      SUBSTR telephoneNumberSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

5.22. telexNumber

```
    ( 2.5.4.21 NAME 'telexNumber'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.52 )
```

5.23. teletexTerminalIdentifier

```
    ( 2.5.4.22 NAME 'teletexTerminalIdentifier'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.51 )
```

5.24. facsimileTelephoneNumber

```
    ( 2.5.4.23 NAME 'facsimileTelephoneNumber'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.22 )
```


5.25. x121Address

```
    ( 2.5.4.24 NAME 'x121Address' EQUALITY numericStringMatch
      SUBSTR numericStringSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.36{15} )
```

5.26. internationaliSDNNumber

```
    ( 2.5.4.25 NAME 'internationaliSDNNumber' EQUALITY numericStringMatch
      SUBSTR numericStringSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.36{16} )
```

5.27. registeredAddress

This attribute holds a postal address suitable for reception of telegrams or expedited documents, where it is necessary to have the recipient accept delivery.

```
( 2.5.4.26 NAME 'registeredAddress' SUP postalAddress
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.41 )
```

5.28. destinationIndicator

This attribute is used for the telegram service.

```
( 2.5.4.27 NAME 'destinationIndicator' EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{128} )
```

5.29. preferredDeliveryMethod

```
( 2.5.4.28 NAME 'preferredDeliveryMethod'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.14
  SINGLE-VALUE )
```

5.30. presentationAddress

This attribute contains an OSI presentation address.

```
( 2.5.4.29 NAME 'presentationAddress'
  EQUALITY presentationAddressMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.43
  SINGLE-VALUE )
```

5.31. supportedApplicationContext

This attribute contains the identifiers of OSI application contexts.

```
( 2.5.4.30 NAME 'supportedApplicationContext'
  EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
```

5.32. member

```
( 2.5.4.31 NAME 'member' SUP distinguishedName )
```


5.33. owner

```
( 2.5.4.32 NAME 'owner' SUP distinguishedName )
```

5.34. roleOccupant

```
    ( 2.5.4.33 NAME 'roleOccupant' SUP distinguishedName )
```

5.35. seeAlso

```
    ( 2.5.4.34 NAME 'seeAlso' SUP distinguishedName )
```

5.36. userPassword

```
    ( 2.5.4.35 NAME 'userPassword' EQUALITY octetStringMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{128} )
```

Passwords are stored using an Octet String syntax and are not encrypted. Transfer of cleartext passwords are strongly discouraged where the underlying transport service cannot guarantee confidentiality and may result in disclosure of the password to unauthorized parties.

5.37. userCertificate

This attribute is to be stored and requested in the binary form, as 'userCertificate;binary'.

```
    ( 2.5.4.36 NAME 'userCertificate'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
```

5.38. cACertificate

This attribute is to be stored and requested in the binary form, as 'cACertificate;binary'.

```
    ( 2.5.4.37 NAME 'cACertificate'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
```

5.39. authorityRevocationList

This attribute is to be stored and requested in the binary form, as 'authorityRevocationList;binary'.

```
    ( 2.5.4.38 NAME 'authorityRevocationList'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.9 )
```

5.40. certificateRevocationList

This attribute is to be stored and requested in the binary form, as 'certificateRevocationList;binary'.

```
    ( 2.5.4.39 NAME 'certificateRevocationList'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.9 )
```

5.41. crossCertificatePair

This attribute is to be stored and requested in the binary form, as 'crossCertificatePair;binary'.

```
( 2.5.4.40 NAME 'crossCertificatePair'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.10 )
```

5.42. name

The name attribute type is the attribute supertype from which string attribute types typically used for naming may be formed. It is unlikely that values of this type itself will occur in an entry. LDAP server implementations which do not support attribute subtyping need not recognize this attribute in requests. Client implementations MUST NOT assume that LDAP servers are capable of performing attribute subtyping.

```
( 2.5.4.41 NAME 'name' EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

5.43. givenName

The givenName attribute is used to hold the part of a person's name which is not their surname nor middle name.

```
( 2.5.4.42 NAME 'givenName' SUP name )
```

5.44. initials

The initials attribute contains the initials of some or all of an individuals names, but not the surname(s).

```
( 2.5.4.43 NAME 'initials' SUP name )
```

5.45. generationQualifier

The generationQualifier attribute contains the part of the name which typically is the suffix, as in "IIIrd".

```
( 2.5.4.44 NAME 'generationQualifier' SUP name )
```

5.46. x500UniqueIdentifier

The x500UniqueIdentifier attribute is used to distinguish between objects when a distinguished name has been reused. This is a different attribute type from both the "uid" and "uniqueIdentifier" types.

```
( 2.5.4.45 NAME 'x500UniqueIdentifier' EQUALITY bitStringMatch
```

```
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.6 )
```


5.47. dnQualifier

The dnQualifier attribute type specifies disambiguating information to add to the relative distinguished name of an entry. It is intended for use when merging data from multiple sources in order to prevent conflicts between entries which would otherwise have the same name. It is recommended that the value of the dnQualifier attribute be the same for all entries from a particular source.

```
 ( 2.5.4.46 NAME 'dnQualifier' EQUALITY caseIgnoreMatch
   ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstringsMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.44 )
```

5.48. enhancedSearchGuide

This attribute is for use by X.500 clients in constructing search filters.

```
 ( 2.5.4.47 NAME 'enhancedSearchGuide'
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.21 )
```

5.49. protocolInformation

This attribute is used in conjunction with the presentationAddress attribute, to provide additional information to the OSI network service.

```
 ( 2.5.4.48 NAME 'protocolInformation'
   EQUALITY protocolInformationMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.42 )
```

5.50. distinguishedName

This attribute type is not used as the name of the object itself, but it is instead a base type from which attributes with DN syntax inherit.

It is unlikely that values of this type itself will occur in an entry. LDAP server implementations which do not support attribute subtyping need not recognize this attribute in requests. Client implementations MUST NOT assume that LDAP servers are capable of performing attribute subtyping.

```
    ( 2.5.4.49 NAME 'distinguishedName' EQUALITY distinguishedNameMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

5.51. uniqueMember

```
    ( 2.5.4.50 NAME 'uniqueMember' EQUALITY uniqueMemberMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.34 )
```


5.52. houseIdentifier

This attribute is used to identify a building within a location.

```
    ( 2.5.4.51 NAME 'houseIdentifier' EQUALITY caseIgnoreMatch
      SUBSTR caseIgnoreSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

5.53. supportedAlgorithms

This attribute is to be stored and requested in the binary form, as 'supportedAlgorithms;binary'.

```
    ( 2.5.4.52 NAME 'supportedAlgorithms'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.49 )
```

5.54. deltaRevocationList

This attribute is to be stored and requested in the binary form, as 'deltaRevocationList;binary'.

```
    ( 2.5.4.53 NAME 'deltaRevocationList'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.9 )
```

5.55. dmdName

The value of this attribute specifies a directory management domain (DMD), the administrative authority which operates the directory server.

```
    ( 2.5.4.54 NAME 'dmdName' SUP name )
```

6. Syntaxes

Servers SHOULD recognize the syntaxes defined in this section. Each syntax begins with a sample value of the ldapSyntaxes attribute

which defines the OBJECT IDENTIFIER of the syntax. The descriptions of syntax names are not carried in protocol, and are not guaranteed to be unique.

6.1. Delivery Method

(1.3.6.1.4.1.1466.115.121.1.14 DESC 'Delivery Method')

Values in this syntax are encoded according to the following BNF:

```
delivery-value = pdm / ( pdm whsp "$" whsp delivery-value )

pdm = "any" / "mhs" / "physical" / "telex" / "teletex" /
          "g3fax" / "g4fax" / "ia5" / "videotex" / "telephone"
```

Example:

```
telephone
```


6.2. Enhanced Guide

(1.3.6.1.4.1.1466.115.121.1.21 DESC 'Enhanced Guide')

Values in this syntax are encoded according to the following BNF:

```
EnhancedGuide = woid whsp "#" whsp criteria whsp "#" whsp subset

subset = "baseobject" / "oneLevel" / "wholeSubtree"
```

The criteria production is defined in the Guide syntax below. This syntax has been added subsequent to RFC 1778.

Example:

```
person#(sn)#oneLevel
```

6.3. Guide

(1.3.6.1.4.1.1466.115.121.1.25 DESC 'Guide')

Values in this syntax are encoded according to the following BNF:

```
guide-value = [ object-class "#" ] criteria

object-class = woid

criteria = criteria-item / criteria-set / ( "!" criteria )
```

```
  criteria-set = ( [ "(" ] criteria "&" criteria-set [ ")" ] ) /
                 ( [ "(" ] criteria "|" criteria-set [ ")" ] )

  criteria-item = [ "(" ] attributetype "$" match-type [ ")" ]

  match-type = "EQ" / "SUBSTR" / "GE" / "LE" / "APPROX"
```

This syntax should not be used for defining new attributes.

6.4. Octet String

(1.3.6.1.4.1.1466.115.121.1.40 DESC 'Octet String')

Values in this syntax are encoded as octet strings.

Example:

```
   secret
```


6.5. Teletex Terminal Identifier

(1.3.6.1.4.1.1466.115.121.1.51 DESC 'Teletex Terminal Identifier')

Values in this syntax are encoded according to the following BNF:

```
   teletex-id = ttx-term  0*("$" ttx-param)

   ttx-term   = printablestring

   ttx-param  = ttx-key ":" ttx-value

   ttx-key    = "graphic" / "control" / "misc" / "page" / "private"

   ttx-value  = octetstring
```

In the above, the first printablestring is the encoding of the first portion of the teletex terminal identifier to be encoded, and the subsequent 0 or more octetstrings are subsequent portions of the teletex terminal identifier.

6.6. Telex Number

(1.3.6.1.4.1.1466.115.121.1.52 DESC 'Telex Number')

Values in this syntax are encoded according to the following BNF:

```
telex-number  = actual-number "$" country "$" answerback

actual-number = printablestring

country       = printablestring

answerback    = printablestring
```

In the above, actual-number is the syntactic representation of the number portion of the TELEX number being encoded, country is the TELEX country code, and answerback is the answerback code of a TELEX terminal.

6.7. Supported Algorithm

(1.3.6.1.4.1.1466.115.121.1.49 DESC 'Supported Algorithm')

No printable representation of values of the supportedAlgorithms attribute is defined in this document. Clients which wish to store and retrieve this attribute MUST use "supportedAlgorithms;binary", in which the value is transferred as a binary encoding.

7. Object Classes

LDAP servers MUST recognize the object classes "top" and "subschema". LDAP servers SHOULD recognize all the other object classes listed here as values of the objectClass attribute.

7.1. top

```
( 2.5.6.0 NAME 'top' ABSTRACT MUST objectClass )
```

7.2. alias

```
( 2.5.6.1 NAME 'alias' SUP top STRUCTURAL MUST aliasedObjectName )
```

7.3. country

```
( 2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c
  MAY ( searchGuide $ description ) )
```

7.4. locality

```
    ( 2.5.6.3 NAME 'locality' SUP top STRUCTURAL
      MAY ( street $ seeAlso $ searchGuide $ st $ l $ description ) )
```

7.5. organization

```
    ( 2.5.6.4 NAME 'organization' SUP top STRUCTURAL MUST o
      MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
      x121Address $ registeredAddress $ destinationIndicator $
      preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
      telephoneNumber $ internationaliSDNNumber $
      facsimileTelephoneNumber $
      street $ postOfficeBox $ postalCode $ postalAddress $
      physicalDeliveryOfficeName $ st $ l $ description ) )
```

7.6. organizationalUnit

```
    ( 2.5.6.5 NAME 'organizationalUnit' SUP top STRUCTURAL MUST ou
      MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
      x121Address $ registeredAddress $ destinationIndicator $
      preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
      telephoneNumber $ internationaliSDNNumber $
      facsimileTelephoneNumber $
      street $ postOfficeBox $ postalCode $ postalAddress $
      physicalDeliveryOfficeName $ st $ l $ description ) )
```

7.7. person

```
    ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL MUST ( sn $ cn )
      MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

7.8. organizationalPerson

```
    ( 2.5.6.7 NAME 'organizationalPerson' SUP person STRUCTURAL
      MAY ( title $ x121Address $ registeredAddress $
      destinationIndicator $
      preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
      telephoneNumber $ internationaliSDNNumber $
      facsimileTelephoneNumber $
      street $ postOfficeBox $ postalCode $ postalAddress $
      physicalDeliveryOfficeName $ ou $ st $ l ) )
```


7.9. organizationalRole

```
    ( 2.5.6.8 NAME 'organizationalRole' SUP top STRUCTURAL MUST cn
      MAY ( x121Address $ registeredAddress $ destinationIndicator $
      preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
      telephoneNumber $ internationaliSDNNumber $
      facsimileTelephoneNumber $
```

```
      seeAlso $ roleOccupant $ preferredDeliveryMethod $ street $
      postOfficeBox $ postalCode $ postalAddress $
      physicalDeliveryOfficeName $ ou $ st $ l $ description ) )
```

7.10. groupOfNames

```
    ( 2.5.6.9 NAME 'groupOfNames' SUP top STRUCTURAL MUST ( member $ cn )
      MAY ( businessCategory $ seeAlso $ owner $ ou $ o $ description ) )
```

7.11. residentialPerson

```
    ( 2.5.6.10 NAME 'residentialPerson' SUP person STRUCTURAL MUST l
      MAY ( businessCategory $ x121Address $ registeredAddress $
      destinationIndicator $ preferredDeliveryMethod $ telexNumber $
      teletexTerminalIdentifier $ telephoneNumber $
      internationaliSDNNumber $
      facsimileTelephoneNumber $ preferredDeliveryMethod $ street $
      postOfficeBox $ postalCode $ postalAddress $
      physicalDeliveryOfficeName $ st $ l ) )
```

7.12. applicationProcess

```
    ( 2.5.6.11 NAME 'applicationProcess' SUP top STRUCTURAL MUST cn
      MAY ( seeAlso $ ou $ l $ description ) )
```

7.13. applicationEntity

```
    ( 2.5.6.12 NAME 'applicationEntity' SUP top STRUCTURAL
      MUST ( presentationAddress $ cn )
      MAY ( supportedApplicationContext $ seeAlso $ ou $ o $ l $
      description ) )
```

7.14. dSA

```
    ( 2.5.6.13 NAME 'dSA' SUP applicationEntity STRUCTURAL
      MAY knowledgeInformation )
```

7.15. device

```
    ( 2.5.6.14 NAME 'device' SUP top STRUCTURAL MUST cn
      MAY ( serialNumber $ seeAlso $ owner $ ou $ o $ l $ description ) )
```

7.16. strongAuthenticationUser

```
    ( 2.5.6.15 NAME 'strongAuthenticationUser' SUP top AUXILIARY
      MUST userCertificate )
```

7.17. certificationAuthority

```
( 2.5.6.16 NAME 'certificationAuthority' SUP top AUXILIARY
  MUST ( authorityRevocationList $ certificateRevocationList $
  cACertificate ) MAY crossCertificatePair )
```

7.18. groupOfUniqueNames

```
( 2.5.6.17 NAME 'groupOfUniqueNames' SUP top STRUCTURAL
  MUST ( uniqueMember $ cn )
  MAY ( businessCategory $ seeAlso $ owner $ ou $ o $ description ) )
```

7.19. userSecurityInformation

```
( 2.5.6.18 NAME 'userSecurityInformation' SUP top AUXILIARY
  MAY ( supportedAlgorithms ) )
```

7.20. certificationAuthority-V2

```
( 2.5.6.16.2 NAME 'certificationAuthority-V2' SUP
  certificationAuthority
  AUXILIARY MAY ( deltaRevocationList ) )
```

7.21. cRLDistributionPoint

```
( 2.5.6.19 NAME 'cRLDistributionPoint' SUP top STRUCTURAL
  MUST ( cn ) MAY ( certificateRevocationList $
  authorityRevocationList $
  deltaRevocationList ) )
```

7.22. dmd

```
( 2.5.6.20 NAME 'dmd' SUP top STRUCTURAL MUST ( dmdName )
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
  x121Address $ registeredAddress $ destinationIndicator $
  preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
  telephoneNumber $ internationaliSDNNumber $
  facsimileTelephoneNumber $
  street $ postOfficeBox $ postalCode $ postalAddress $
  physicalDeliveryOfficeName $ st $ l $ description ) )
```

8. Matching Rules

Servers MAY implement additional matching rules.

8.1. octetStringMatch

Servers which implement the extensibleMatch filter SHOULD allow the matching rule listed in this section to be used in the extensibleMatch. In general these servers SHOULD allow matching rules to be used with all attribute types known to the server, when

the assertion syntax of the matching rule is the same as the value syntax of the attribute.


```
( 2.5.13.17 NAME 'octetStringMatch'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

9. Security Considerations

Attributes of directory entries are used to provide descriptive information about the real-world objects they represent, which can be people, organizations or devices. Most countries have privacy laws regarding the publication of information about people.

Transfer of cleartext passwords are strongly discouraged where the underlying transport service cannot guarantee confidentiality and may result in disclosure of the password to unauthorized parties.

10. Acknowledgements

The definitions on which this document have been developed by committees for telecommunications and international standards. No new attribute definitions have been added. The syntax definitions are based on the ISODE "QUIPU" implementation of X.500.

11. Bibliography

[1] M. Wahl, A. Coulbeck, T. Howes, S. Kille, "Lightweight X.500 Directory Access Protocol Attribute Syntax Definitions", INTERNET-DRAFT <draft-ietf-asid-ldapv3-attributes-08.txt>, October 1997.

[2] The Directory: Models. ITU-T Recommendation X.501, 1996.

[3] The Directory: Authentication Framework. ITU-T Recommendation X.509, 1996.

[4] The Directory: Selected Attribute Types. ITU-T Recommendation X.520, 1996.

[5] The Directory: Selected Object Classes. ITU-T Recommendation X.521, 1996.

12. Author's Address

Mark Wahl
Critical Angle Inc.
4815 West Braker Lane #502-385
Austin, TX 78759
USA

Phone: +1 512 372 3160
EMail: M.Wahl@critical-angle.com