INTERNET-DRAFT
Intended Category: Standard Track
Expires 25 August 2003
Obsoletes: RFC 2256, RFC 2252

K. Dally, Editor
The MITRE Corp.

25 February 2003

LDAP: User Schema
<draft-ietf-ldapbis-user-schema-04>

[Editor's note:
This Internet-Draft (I-D) is an updated version of text from RFC 2256 and RFC 2252. This action is part of the maintenance activity that is needed in order to progress LDAP (v3) to Draft Standard. The changes are described in Annex A of this document.
End of Editor's note]

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026 [RFC2026].

This document is intended to be, after appropriate review and revision, submitted to the RFC Editor as a Standard Track document. Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF LDAP Revision Working Group (LDAPbis) mailing list <ietf-ldapbis@openldap.org>. Please send editorial comments directly to the author <kdally@mitre.org>.

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.

Abstract

This document provides an overview of attribute types and object classes defined by the ISO/IEC JTC1 and ITU-T committees in the IS0/IEC 9594 and X.500 documents, in particular those intended for use by directory clients. This is the most widely used schema for LDAP/X.500 directories. It is used as a basis for many other white pages objects schema definitions. 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.

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 [RFC2119].

Table of Contents

1. General Issues

This document references Syntaxes given in Section 3 of [Syntaxes] and Matching Rules specified in Section 4 of [Syntaxes].

The definitions of Attribute Types and Object Classes are written using the ABNF form of AttributeTypeDescription and ObjectClassDescription given in [Models]. Lines have been folded for readability.

2. Source

The schema definitions in this document are based on those found in the X.500-series [X.520] and [X.521] and RFC 2247 [RFC2247], specifically:

Sections	Source
3.1 - 3.3	X.520 [X.520]
3.4	RFC 2247 [RFC2247]
3.5 - 3.42	X.520 [X.520]
4.1 - 4.3	X.521 [X.521]
4.4	RFC 2247 [RFC2247]
4.5 - 4.13	X.521 [X.521]

3. Attribute Types

The Attribute Types contained in this section hold user information.

There is no requirement that servers implement the following Attribute Types:

searchGuide
teletexTerminalIdentifier

In fact, their use is greatly discouraged.

An LDAP server implementation SHOULD recognize the rest of the Attribute Types described in this section.

3.1 businessCategory

This Attribute Type 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} )
```

The SYNTAX oid indicates the Directory String syntax.

3.2 c

This is the X.520 [X.520] countryName Attribute Type, which contains a two-letter ISO 3166 [ISO3166]country code.

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

3.3 cn

This is the X.520 [X.520] commonName Attribute Type, 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 )
```

3.4 dc

The dc (short for domainComponent) attribute type is defined as follows:

```
( 0.9.2342.19200300.100.1.25 NAME 'dc'
   EQUALITY caseIgnoreIA5Match
   SUBSTR caseIgnoreIA5SubstringsMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
   SINGLE-VALUE )
```

The value of this attribute is a string holding one component of a DNS domain name. The encoding of IA5String for use in LDAP is simply the characters of the string itself. The equality matching rule is case insensitive, as is today's DNS.

3.5 description

This Attribute Type 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} )
```

The SYNTAX oid indicates the Directory String syntax.

3.6 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} )
```

The SYNTAX oid indicates the Printable String syntax.

3.7 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 )
```

The SYNTAX oid indicates the DN syntax.

3.8 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 )
```

The SYNTAX oid indicates the Printable String syntax.

3.9 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 )
```

The SYNTAX oid indicates the Enhanced Guide syntax.

3.10 facsimileTelephoneNumber

A value of this Attribute Type is a telephone number for a facsimile terminal (and, optionally, its parameters).

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

The SYNTAX oid indicates the Facsimile Telephone Number syntax.

3.11 generationQualifier

The generationQualifier Attribute Type contains the part of a person's name which typically is the suffix, as in "IIIrd".

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

3.12 givenName

The givenName Attribute Type 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 )
```

3.13 houseIdentifier

This Attribute Type 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} )
```

The SYNTAX oid indicates the Directory String syntax.

3.14 initials

The initials Attribute Type contains the initials of some or all of an individuals names, except the surname(s).

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

3.15 internationalISDNNumber

A value of this Attribute Type is an ISDN address, as defined in ITU Recommendation E.164 [E.164].

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

The SYNTAX oid indicates the Numeric String syntax.

3.16 l

This is the X.520 [X.520] localityName Attribute Type, which contains the name of a locality or place, such as a city, county or other geographic region.

```
( 2.5.4.7 NAME 'l'
  SUP name )
```

3.17 member

A value of this Attribute Type is the Distinguished Name of an object that is on a list or in a group.

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

3.18 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} )
```

The SYNTAX oid indicates the Directory String syntax.

3.19 o

This is the X.520 [X.520] organizationName Attribute Type, which contains the name of an organization.

```
( 2.5.4.10 NAME 'o'
   SUP name )
```

3.20 ou

This is the X.520 [X.520] organizationalUnitName Attribute Type, which contains the name of an organizational unit.

```
 ( 2.5.4.11 NAME 'ou'
   SUP name )
```

3.21 owner

A value of this Attribute Type is the Distinguished Name of an object that has an ownership responsibility for the object that is owned.

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

3.22 physicalDeliveryOfficeName

This attribute contains the name that a Postal Service uses to identify a post office.

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

The SYNTAX oid indicates the Directory String syntax.

3.23 postalAddress

This attribute contains an address used by a Postal Service to perform services for the object.

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

The SYNTAX oid indicates the Postal Address syntax.

3.24 postalCode

This attribute contains a code used by a Postal Service to identify a postal service zone, such as the southern quadrant of a city.

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

The SYNTAX oid indicates the Directory String syntax.

3.25 postOfficeBox

This attribute contains the number that a Postal Service uses when a customer arranges to receive mail at a box on premises of the Postal Service.

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

The SYNTAX oid indicates the Directory String syntax.

3.26 preferredDeliveryMethod

This attribute contains an indication of the preferred method of getting a message to the object.

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

The SYNTAX oid indicates the Delivery Method syntax.

3.27 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 )
```

The SYNTAX oid indicates the Postal Address syntax.

3.28 roleOccupant

A value of this Attribute Type is the Distinguished Name of an object (normally a person) that fulfills the responsibilities of a role object.

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

3.29 searchGuide

This Attribute Type is for use by clients in constructing search filters. It is superseded by enhancedSearchGuide, described above in section 3.9.

```
( 2.5.4.14 NAME 'searchGuide'
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.25 )  ; Guide
```

The SYNTAX oid indicates the Guide syntax.

3.30 seeAlso

A value of this Attribute Type is the Distinguished Name of an object that is related to the subject object.

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

3.31 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} )
```

The SYNTAX oid indicates the Printable String syntax.

3.32 sn

This is the X.520 [X.520] surname Attribute Type, which contains the family name of a person.

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

3.33 st

This is the X.520 [X.520] stateOrProvinceName attribute, which contains the full name of a state or province.

```
( 2.5.4.8 NAME 'st'
   SUP name )
```

3.34 street

This is the X.520 [X.520] streetAddress attribute, which contains the physical address of the object to which the entry corresponds, such as an address for package delivery.

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

The SYNTAX oid indicates the Directory String syntax.

3.35 telephoneNumber

A value of this Attribute Type is a telephone number complying with ITU Recommendation E.123 [E.123].

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

The SYNTAX oid indicates the Telephone Number syntax.

3.36 teletexTerminalIdentifier

The withdrawal of Rec. F.200 has resulted in the withdrawal of this attribute.

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

The SYNTAX oid indicates the Teletex Terminal Identifier syntax.

3.37 telexNumber

A value of this Attribute Type is a telex number, country code, and

answerback code of a telex terminal.

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

The SYNTAX oid indicates the Telex Number syntax.

3.38 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 )
```

3.39 uniqueMember

A value of this Attribute Type is the Distinguished Name of an object that is on a list or in a group, where the Relative Distinguished Name of the object includes a value that distinguishs between objects when a distinguished name has been reused.

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

The SYNTAX oid indicates the Name and Optional UID syntax.

3.40 userPassword

A value of this Attribute Type is a character string that is known only to the user and the system to which the user has access.

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

The SYNTAX oid indicates the Octet String syntax.

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

3.41 x121Address

A value of this Attribute Type is a data network address as defined by ITU Recommendation X.121 [X.121].

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

The SYNTAX oid indicates the Numeric String syntax.

3.42 x500UniqueIdentifier

The x500UniqueIdentifier Attribute Type is used to distinguish between objects when a distinguished name has been reused. In X.520 [X.520], this Attribute Type is called uniqueIdentifier. This is a different Attribute Type from both the "uid" and "uniqueIdentifier" Attribute Types.

```
( 2.5.4.45 NAME 'x500UniqueIdentifier'
   EQUALITY bitStringMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.6 )
```

The SYNTAX oid indicates the Bit String syntax.

4. Object Classes

LDAP servers SHOULD recognize all the Object Classes listed here as values of the objectClass attribute.

4.1 applicationProcess

The applicationProcess Object Class definition is the basis of an entry which represents an application executing in a computer system.

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

4.2 country

The country Object Class definition is the basis of an entry which represents a country.

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

4.3 device

The device Object Class is the basis of an entry which represents an appliance or computer or network element.

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

4.4 domain

The domain Object Class is the basis of an entry which represents a portion of a network, as organized by DNS.

```
( 0.9.2342.19200300.100.4.13 NAME 'domain'
   SUP top
   STRUCTURAL
   MUST dc
   MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
       x121Address $ registeredAddress $ destinationIndicator $
       preferredDeliveryMethod $ telexNumber $
       teletexTerminalIdentifier $ telephoneNumber $
       internationaliSDNNumber $  facsimileTelephoneNumber $ street $
       postOfficeBox $ postalCode $ postalAddress $
       physicalDeliveryOfficeName $ st $ l $ description $ o $
       associatedName ) )
```

An example entry would be:

```
dn: dc=tcp,dc=critical-angle,dc=com
objectClass: top
objectClass: domain
dc: tcp
description: a placeholder entry used with SRV records
```

4.5 groupOfNames

The groupOfNames Object Class is the basis of an entry which represents a set of named objects including information related to the purpose or maintenance of the set.

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

4.6 groupOfUniqueNames

The groupOfUniqueNames Object Class is the same as the groupOfNames object class except that the object names are not repeated or reassigned within a set scope.

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

4.7 locality

The locality Object Class is the basis of an entry which represents a place in the physical world.

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

```
            description ) )
```

4.8 organization

The organization Object Class is the basis of an entry which represents a structured group of people.

```
( 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 ) )
```

4.9 organizationalPerson

The organizationalPerson Object Class is the basis of an entry which represents a person in relation to an organization.

```
( 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 ) )
```

4.10 organizationalRole

The organizationalRole Object Class is the basis of an entry which represents a job or function or position in an organization.

```
( 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 ) )
```

4.11 organizationalUnit

The organizationalUnit Object Class is the basis of an entry which represents a piece of an organization.

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

4.12 person

The person Object Class is the basis of an entry which represents a human being.

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

4.13 residentialPerson

The residentialPerson Object Class is the basis of an entry which includes a person's residence in the representation of the person.

```
( 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 ) )
```

5. 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 is strongly discouraged where the underlying transport service cannot guarantee confidentiality and may result in disclosure of the password to unauthorized parties.

It is required that strong authentication be performed in order to modify directory entries using LDAP.

Several X.500 Attribute Types and Object Classes, such as, the userCertificate Attribute Type or the certificationAuthority Object Class, are used to include key-based security information in directory entries. The Attribute Types are:

```
authorityRevocationList
cACertificate
certificateRevocationList
crossCertificatePair
deltaRevocationList
supportedAlgorithms
userCertificate
```

The Object Classes are:

```
certificationAuthority
certificationAuthority-V2
cRLDistributionPoint
strongAuthenticationUser
userSecurityInformation
```

These Attribute Types and Object Classes are specified for LDAP by the PKIX Working Group, and so, are not included in this document.

It is recommended that the BNF notation in RFC 1778 [RFC1778] not be used for User Certificate, Authority Revocation List, and Certificate Pair.

6. Acknowledgements

The definitions, on which this document is based, have been developed by committees for telecommunications and international standards. No new attribute definitions have been added.

This document is an update of RFC 2256 by Mark Wahl. RFC 2256 was a product of the IETF ASID Working Group.

This document is based upon input of the IETF LDAPBIS working group. The author wishes to thank S. Legg and K. Zeilenga for their significant contribution to this update.

7. References

7.1 Normative

[E.123] Notation for national and international telephone numbers, ITU-T Recommendation E.123, 1988

[E.164] The international public telecommunication numbering plan, ITU-T Recommendation E.164, 1997

[ISO3166] ISO 3166, "Codes for the representation of names of countries".

[Models] K. Zeilenga, "LDAP: The Models", draft-ietf-ldapbis-models-xx.txt (a work in progress).

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", RFC 2026, October 1996

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997

[Syntaxes] S. Legg (editor), "LDAP: Syntaxes", draft-ietf-ldapbis-syntaxes-xx, a work in progress

[X.121] International numbering plan for public data networks, ITU-T Recommendation X.121, 1996

[X.509] The Directory: Authentication Framework, ITU-T Recommendation X.509, 1993

[X.520] The Directory: Selected Attribute Types, ITU-T Recommendation X.520, 1993

[X.521] The Directory: Selected Object Classes. ITU-T Recommendation X.521, 1993

7.2 Informative

[RFC1778] Howes, T., Kille, S., Yeong, W., Robbins, C., "The String Representation of Standard Attribute Syntaxes", RFC 1778,

March 1995.

[RFC2247] Kille, S., Wahl, M., Grimstad, A., Huber, R., and Sataluri, S., "Using Domains in LDAP/X.500 Distinguished Names", RFC 2247, January 1998

[RFC2252] Wahl, M., Coulbeck, A., Howes, T., and S. Kille, "Lightweight X.500 Directory Access Protocol(v3): Attribute Syntax Definitions", RFC 2252, December 1997

8. Author's Address

Kathy Dally
The MITRE Corp.
1575 Colshire Dr., H300
McLean VA 22102
USA

Phone: +1 703 883 6058
Email: kdally@mitre.org

Annex A Change Log

This annex lists the changes that have been made from RFC 2256 to this I-D.

Changes to RFC 2256 resulting in draft-ietf-ldapbis-user-schema-00.txt:

1. Revision of the Status of this Memo.

2. Dependencies on RFC 1274 have been eliminated.

3. The references to X.500(96) have been expressed in terms of the "edition", rather than the standard date. Note that the version of X.500 which is the basis for this document, is the third edition, which was finalized in 1996, but approved in 1997.

4. The "teletexTerminalNumber" attribute and syntax are marked as obsolete.

5. Removed "The syntax definitions are based on the ISODE "QUIPU" implementation of X.500." from section 6.

6. Added text to 6.1, the octetString syntax, in accordance with X.520.

7. Some of the attribute types MUST be recognized by servers. Also, several attributes are obsolete. Therefore, the various kinds of attribute types have been placed in separate sections:

   - necessary for the directory to operate (section 3.1)

   - for holding user information (section 3.2)

   - superseded or withdrawn (section 3.3).

8. Since "top" may be implicitly specified and "alias" is not abstract, the last sentence in the description of the "objectClass" attribute type, section 3.1.1, has been deleted. The clause that preceded the deleted sentence has been removed, also.

9. Add a description to the definition of the "telephoneNumber" attribute type, section 3.2.17.

10. Add text to mark the "teletexTerminalIdentifier" attribute

type as obsolete.

11. Add a security consideration requiring strong authentication in order to modify directory entries.

Changes to draft-ietf-ldapbis-user-schema-00.txt, resulting in draft-ietf-ldapbis-user-schema-01.txt:

12. Delete the conformance requirement for subschema object classes in favor of a statement in [SYNTAX].

13. Add a Table of Contents

14. Replace the term "obsolete" with "superseded or withdrawn"

15. Added explanations to many attributes.

16. In the title, correct the X.500 reference to have the second edition as the basis.

17. Throughout this I-D, cleaned up whitespace in the BNF definitions.

18. Removed Section 4, Syntaxes, and Section 6, Matching Rules, (moved to draft-ietf-ldapbis-syntaxes-01.txt).

19. Reorganized Section 3, Attributes, to eliminate grouping attributes according to conformance requirements. Reordered Section 3, Attributes, and Section 4, Object Classes, alphabetically.

20. Added an explanation for each object class.

Changes to draft-ietf-ldapbis-user-schema-01.txt, resulting in draft-ietf-ldapbis-user-schema-02.txt:

21. Removed the certificate-related Attribute Types:
    authorityRevocationList,
    cACertificate,
    certificateRevocationList,
    crossCertificatePair,
    deltaRevocationList,
    supportedAlgorithms, and
    userCertificate.

    Removed the certificate-related Object Classes:
    certificationAuthority,
    certificationAuthority-V2,
    cRLDistributionPoint,
    strongAuthenticationUser, and
    userSecurityInformation

Noted in the Security Considerations (Section 7) that they are covered in PKIX WG documents.

22. Removed the dmdName Attribute Type and dmd Object Class because they are not in the version of X.500 which is referenced.

23. Removed embedded comments from the ABNF productions throughout the document.

24. Cleaned up the references; adopted word instead of number tags; split Section 7 into normative and informative subsections.

Changes to draft-ietf-ldapbis-user-schema-02.txt, resulting in draft-ietf-ldapbis-user-schema-03.txt:

25. Deleted the 'aliasedObjectName' and 'objectClass' attribute type definitions. They are included in [Models].

26. Deleted the 'alias' and 'top' object class definitions. They are included in [Models].

27. Replaced the document title.

28. Changed reference citations to be consistent with the rest of the LDAPbis documents.

Changes to draft-ietf-ldapbis-user-schema-03.txt, resulting in draft-ietf-ldapbis-user-schema-04.txt:

29. Added references for RFC 2026 and RFC 2247.

30. Corrected the copyright year.

31. Added the 'dc' attribute and the 'domain' object class from RFC 2247.

32. Deleted the 'knowledgeInformation', 'presentationAddress', 'protocolInformation', and 'supportedApplicationContext' attributes.

33. Deleted the 'applicationEntity' and 'dSA' object classes.