INTERNET-DRAFT
Intended Category: Standard Track
Expires 04 October 2001
Obsoletes: 2256

K. Dally, Editor
The MITRE Corp.
04 April 2001

A Summary of the X.500(3rd edition) User Schema for use with LDAPv3

<draft-ietf-ldapbis-user-schema-00>

[Editor's note:
This Internet-Draft (I-D) is a modified version of the text of RFC 2256, in order to bring it up to date. This action is part of the maintenance activity that is needed in order to progress LDAPv3 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 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 the 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, 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.

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 [6].

Table of Contents

Status of this Memo 1
Abstract 2
1. General Issues 5
2. Source 5
3. Attribute Types 5
3.1 "MUST" Attribute Types 5
3.1.1 objectClass 5
3.2 "SHOULD" Attribute Types 6
3.2.1 aliasedObjectName 6
3.2.2 cn 6
3.2.3 sn 6
3.2.4 serialNumber 6
3.2.5 c 6
3.2.6 l 6
3.2.7 st 7
3.2.8 street 7
3.2.9 o 7
3.2.10 ou 7
3.2.11 title 7
3.2.12 description 7
3.2.13 businessCategory 8
3.2.14 postalAddress 8
3.2.15 postalCode 8
3.2.16 postOfficeBox 8
3.2.17 physicalDeliveryOfficeName 8
3.2.18 telephoneNumber 9
3.2.19 telexNumber 9
3.2.20 facsimileTelephoneNumber 9
3.2.21 x121Address 9
3.2.22 internationalISDNNumber 9
3.2.23 registeredAddress 9
3.2.24 destinationIndicator 10
3.2.25 preferredDeliveryMethod 10
3.2.26 presentationAddress 10
3.2.27 supportedApplicationContext 10
3.2.28 member 10
3.2.29 owner 10
3.2.30 roleOccupant 11
3.2.31 seeAlso 11
3.2.32 userPassword 11
3.2.33 userCertificate 11
3.2.34 cACertificate 11
3.2.35 authorityRevocationList 12
3.2.36 certificateRevocationList 12
3.2.37 crossCertificatePair 12
3.2.38 name 12

3.2.39 **givenName** 12
3.2.40 **initials** 12
3.2.41 **generationQualifier** 13
3.2.42 **x500UniqueIdentifier** 13
3.2.43 **dnQualifier** 13
3.2.44 **enhancedSearchGuide** 13

3.2.45 protocolInformation 13
3.2.46 distinguishedName 14
3.2.47 uniqueMember 14
3.2.48 houseIdentifier 14
3.2.49 supportedAlgorithms 14
3.2.50 deltaRevocationList 14
3.2.51 dmdName 15
3.3 Superseded and Withdrawn Attribute Types 15
3.3.1 knowledgeInformation 15
3.3.2 searchGuide 15
3.3.3 teletexTerminalIdentifier 15
4. Syntaxes 15
4.1 Delivery Method 15
4.2 Enhanced Guide 16
4.3 Guide 16
4.4 Octet String 16
4.5 Teletex Terminal Identifier 17
4.6 Telex Number 17
4.7 Supported Algorithm 17
5. Object Classes 18
5.1 top 18
5.2 alias 18
5.3 country 18
5.4 locality 18
5.5 organization 18
5.6 organizationalUnit 18
5.7 person 18
5.8 organizationalPerson 19
5.9 organizationalRole 19
5.10 groupOfNames 19
5.11 residentialPerson 19
5.12 applicationProcess 19
5.13 applicationEntity 19
5.14 dSA 19
5.15 device 20
5.16 strongAuthenticationUser 20
5.17 certificationAuthority 20
5.18 groupOfUniqueNames 20
5.19 userSecurityInformation 20
5.20 certificationAuthority-V2 20
5.21 cRLDistributionPoint 20
5.22 dmd 20
6. Matching Rules 21
6.1 octetStringMatch 21
7. Security Considerations 21
8. Acknowledgements 21
9. Bibliography 22
10. Author's Address 22

Annex A Change Log 23

1. General Issues

This document references syntaxes given in section 4 of this document and section 6 of [1]. Matching rules are listed in section 6 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.

2. Source

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

Sections	Source
3.1 - 3.2	X.501 [2]
3.3 - 3.36	X.520 [4]
3.37 - 3.41	X.509 [3]
3.42 - 3.52	X.520 [4]
3.53 - 3.54	X.509 [3]
3.55	X.520 [4]
4.1 - 4.6	X.520 [4]
4.7	X.509 [4]
5.1 - 5.2	X.501 [2]
5.3 - 5.18	X.521 [5]
5.19 - 5.21	X.509 [3]
5.22	X.521 [5]
6.1	X.520 [4]

Three new attributes: supportedAlgorithms, deltaRevocationList and dmdName, and the objectClass dmd, which were not specified in X.500 edition 2 (1993), are defined in the X.500 edition 3 (1997)[2, 3, 4, 5] documents.

3. Attribute Types

Two kinds of attribute types are contained in this section: ones for holding user information and others which have been superseded or withdrawn.

3.1 "MUST" Attribute Types

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

3.1.1 objectClass

The values of the objectClass attribute describe the kind of object which an entry represents. The objectClass attribute is present in every entry.

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

3.2 "SHOULD" Attribute Types

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

3.2.1 aliasedObjectName

The aliasedObjectName attribute is used by the directory service if the entry containing this attribute is an alias. In X.500, this attribute is called aliasedEntryName.

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

3.2.2 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 )
```

3.2.3 sn

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

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

3.2.4 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} )
```

3.2.5 c

This is the X.500 countryName attribute, which contains a two-letter ISO 3166 country code.

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

3.2.6 l

This is the X.500 localityName attribute, which contains the name of a locality, such as a city, county or other geographic region.

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

3.2.7 st

This is the X.500 stateOrProvinceName attribute, which contains the full name of a state or province.

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

3.2.8 street

This is the X.500 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} )
```

3.2.9 o

This is the X.500 organizationName attribute, which contains the name of an organization.

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

3.2.10 ou

This is the X.500 organizationalUnitName attribute, which contains the name of an organizational unit.

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

3.2.11 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 )
```

3.2.12 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} )
```

3.2.13 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} )
```

3.2.14 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 )
```

3.2.15 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} )
```

3.2.16 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} )
```

3.2.17 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} )
```

3.2.18 telephoneNumber

A value of this attribute is a telephone number complying with CCITT Rec. 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} )
```

3.2.19 telexNumber

A value of this attribute 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 )
```

3.2.20 facsimileTelephoneNumber

A value of this attribute 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 )
```

3.2.21 x121Address

A value of this attribute is a data network address as defined by CCITT Recommendation 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} )
```

3.2.22 internationalISDNNumber

A value of this attribute is an ISDN address, as defined in CCITT Recommendation 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} )
```

3.2.23 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 )
```

3.2.24 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} )
```

3.2.25 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 )
```

3.2.26 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 )
```

3.2.27 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 )
```

3.2.28 member

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

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

3.2.29 owner

A value of this attribute 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)

3.2.30 roleOccupant

A value of this attribute 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 )
```

3.2.31 seeAlso

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

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

3.2.32 userPassword

A value of this attribute 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} )
```

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.

3.2.33 userCertificate

A value of this attribute is a set of information that is used to protect business systems, including the directory system and its contents, from a number of threats. The protection is realized by verifying the object is authorized to use the business system for certain purposes. 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 )
```

3.2.34 cACertificate

A value of this attribute is a set of information that is used to establish a traceable chain of authority for issuing user certificates. 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 )
```

3.2.35 authorityRevocationList

A value of this attribute is a list of CA certificates that are no longer valid. 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 )
```

3.2.36 certificateRevocationList

A value of this attribute is a list of user certificates that are no longer valid. 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 )
```

3.2.37 crossCertificatePair

A value of this attribute is a set of two certificates that are used to enable the certificates issued in two security domains to be usable in both domains. 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 )
```

3.2.38 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} )
```

3.2.39 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 )
```

3.2.40 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 )
```

3.2.41 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 )
```

3.2.42 x500UniqueIdentifier

The x500UniqueIdentifier attribute is used to distinguish between objects when a distinguished name has been reused. In X.500, this attribute is called uniqueIdentifier. This is a different attribute type from both the "uid" and "uniqueIdentifier" (defined in ??) types.

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

3.2.43 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 )
```

3.2.44 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 )
```

3.2.45 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 )
```

3.2.46 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 )
```

3.2.47 uniqueMember

A value of this attribute 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 )
```

3.2.48 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} )
```

3.2.49 supportedAlgorithms

This attribute contains the identifiers of cryptographic algorithms that the object implements. 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 )
```

3.2.50 deltaRevocationList

This attribute contains a list of revoked user certificates that is an addition to a previous certificate revocation list. 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 )
```

3.2.51 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)

3.3 Superseded and Withdrawn Attribute Types

There is no requirement that servers implement the attribute types in this section. In fact, their use is greatly discouraged.

3.3.1 knowledgeInformation

This attribute is superseded by some system schema attributes.

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

3.3.2 searchGuide

This attribute is for use by clients in constructing search filters. It is superseded by enhancedSearchGuide, described above in 3.2.43.

(2.5.4.14 NAME 'searchGuide'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.25)

3.3.3 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)

4. 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.

4.1 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
```

4.2 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
```

4.3 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.

4.4 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

4.5 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.

4.6 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.

4.7 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.

5. Object Classes

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

5.1 top

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

5.2 alias

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

5.3 country

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

5.4 locality

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

5.5 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 ) )
```

5.6 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 ) )
```

5.7 person

```
( 2.5.6.6 NAME 'person' SUP top STRUCTURAL MUST ( sn $ cn )
```

```
    MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

5.8 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 ) )
```

5.9 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 ) )
```

5.10 groupOfNames

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

5.11 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 ) )
```

5.12 applicationProcess

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

5.13 applicationEntity

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

5.14 dSA

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

5.15 device

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

5.16 strongAuthenticationUser

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

5.17 certificationAuthority

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

5.18 groupOfUniqueNames

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

5.19 userSecurityInformation

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

5.20 certificationAuthority-V2

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

5.21 cRLDistributionPoint

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

5.22 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 ) )
```

6. Matching Rules

Servers MAY implement additional matching rules.

6.1 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.

The Octet String Match rule compares for equality an asserted octet string with an attribute value of type OCTET STRING.

The strings match if they are the same length and corresponding octets are identical.

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

7. 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.

8. 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 LDAPBIS Working Group.

This document is based upon input of the IETF LDAPBIS working group. The authors wish to thank ___ for their significant contribution to this update.

9. Bibliography

[1] replacement (draft-hinckley-ldapbis-rfc2252-nn) for Wahl, M., Coulbeck, A., Howes, T., and S. Kille, "Lightweight X.500 Directory Access Protocol(v3): Attribute Syntax Definitions", RFC 2252, December 1997

[2] The Directory: Models, ITU-T Recommendation X.501, 1997

[3] The Directory: Authentication Framework, ITU-T Recommendation X.509, 1997

[4] The Directory: Selected Attribute Types, ITU-T Recommendation X.520, 1997

[5] The Directory: Selected Object Classes. ITU-T Recommendation X.521, 1997

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

10. Author's Address

Kathy Dally
The MITRE Corp.
1820 Dolley Madison Blvd., ms-W650
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. The changes made in this latest version are items 12 - 15.

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.

12. Delete the conformance requirement for subschema object classes in favor of a statement in [1].

13. Add a Table of Contents

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

15. Add explanations to many attributes.