Network Working Group
Request for Comments: 4524
Obsoletes: 1274
Updates: 2247, 2798
Category: Standards Track

K. Zeilenga, Ed.
OpenLDAP Foundation

June 2006

COSINE LDAP/X.500 Schema

Status of This Memo

Copyright Notice

Abstract

This document provides a collection of schema elements for use with the Lightweight Directory Access Protocol (LDAP) from the COSINE and Internet X.500 pilot projects.

This document obsoletes RFC 1274 and updates RFCs 2247 and 2798.

Table of Contents

1. Introduction 3
   1.1. Relationship to Other Documents 3
   1.2. Terminology and Conventions 4
2. COSINE Attribute Types 4
   2.1. associatedDomain 4
   2.2. associatedName 5
   2.3. buildingName 5
   2.4. co 5
   2.5. documentAuthor 6
   2.6. documentIdentifier 6
   2.7. documentLocation 6
   2.8. documentPublisher 7
   2.9. documentTitle 7
   2.10. documentVersion 7
   2.11. drink 8
   2.12. homePhone 8
   2.13. homePostalAddress 8

2.14. host 9
2.15. info 9
2.16. mail 9
2.17. manager 10
2.18. mobile 10
2.19. organizationalStatus 11
2.20. pager 11
2.21. personalTitle 11
2.22. roomNumber 12
2.23. secretary 12
2.24. uniqueIdentifier 12
2.25. userClass 13
3. COSINE Object Classes 13
3.1. account 13
3.2. document 14
3.3. documentSeries 14
3.4. domain 15
3.5. domainRelatedObject 16
3.6. friendlyCountry 16
3.7. rFC822LocalPart 17
3.8. room 18
3.9. simpleSecurityObject 18
4. Security Considerations 18
5. IANA Considerations 19
6. Acknowledgements 20
7. References 20
7.1. Normative References 20
7.2. Informative References 21
Appendix A. Changes since RFC 1274 23
A.1. LDAP Short Names 23
A.2. pilotObject 23
A.3. pilotPerson 23
A.4. dNSDomain 24
A.5. pilotDSA and qualityLabelledData 24
A.6. Attribute Syntaxes 24
Appendix B. Changes since RFC 2247 24

1. Introduction

In the late 1980s, X.500 Directory Services were standardized by the CCITT (Commite' Consultatif International de Telegraphique et Telephonique), now a part of the ITU (International Telephone Union). This lead to Directory Service piloting activities in the early 1990s, including the COSINE (Co-operation and Open Systems Interconnection in Europe) PARADISE Project pilot [COSINEpilot] in Europe. Motivated by needs for large-scale directory pilots, RFC 1274 was published to standardize the directory schema and naming architecture for use in the COSINE and other Internet X.500 pilots [RFC1274].

In the years that followed, X.500 Directory Services have evolved to incorporate new capabilities and even new protocols. In particular, the Lightweight Directory Access Protocol (LDAP) [RFC4510] was introduced in the early 1990s [RFC1487], with Version 3 of LDAP introduced in the late 1990s [RFC2251] and subsequently revised in 2005 [RFC4510].

While much of the material in RFC 1274 has been superceded by subsequently published ITU-T Recommendations and IETF RFCs, many of the schema elements lack standardized schema descriptions for use in modern X.500 and LDAP directory services despite the fact that these schema elements are in wide use today. As the old schema descriptions cannot be used without adaptation, interoperability issues may arise due to lack of standardized modern schema descriptions.

This document addresses these issues by offering standardized schema descriptions, where needed, for widely used COSINE schema elements.

1.1. Relationship to Other Documents

This document, together with [RFC4519] and [RFC4517], obsoletes RFC 1274 in its entirety. [RFC4519] replaces Sections 9.3.1 (Userid) and 9.3.21 (Domain Component) of RFC 1274. [RFC4517] replaces Section 9.4 (Generally useful syntaxes) of RFC 1274.

This document replaces the remainder of RFC 1274. Appendix A discusses changes since RFC 1274, as well as why certain schema elements were not brought forward in this revision of the COSINE schema. All elements not brought are to be regarded as Historic.

The description of the 'domain' object class provided in this document supercedes that found in RFC 2247. That is, Section 3.4 of this document replaces Section 5.2 of [RFC2247].

Some of the schema elements specified here were described in RFC 2798 (inetOrgPerson schema). This document supersedes these descriptions. This document, together with [RFC4519], replaces Section 9.1.3 of RFC 2798.

1.2. Terminology and Conventions

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 BCP 14 [RFC2119].

DIT stands for Directory Information Tree.
DN stands for Distinguished Name.
DSA stands for Directory System Agent, a server.
DSE stands for DSA-Specific Entry.
DUA stands for Directory User Agent, a client.

These terms are discussed in [RFC4512].

Schema definitions are provided using LDAP description formats [RFC4512]. Definitions provided here are formatted (line wrapped) for readability.

2. COSINE Attribute Types

This section details COSINE attribute types for use in LDAP.

2.1. associatedDomain

The 'associatedDomain' attribute specifies DNS [RFC1034][RFC2181] host names [RFC1123] that are associated with an object. That is, values of this attribute should conform to the following ABNF:

```
 domain = root / label *( DOT label )
 root   = SPACE
 label  = LETDIG [ *61( LETDIG / HYPHEN ) LETDIG ]
 LETDIG = %x30-39 / %x41-5A / %x61-7A ; "0" - "9" / "A"-"Z" / "a"-"z"
 SPACE  = %x20                        ; space (" ")
 HYPHEN = %x2D                        ; hyphen ("-")
 DOT    = %x2E                        ; period (".")
```

For example, the entry in the DIT with a DN <DC=example,DC=com> might have an associated domain of "example.com".

```
   ( 0.9.2342.19200300.100.1.37 NAME 'associatedDomain'
     EQUALITY caseIgnoreIA5Match
     SUBSTR caseIgnoreIA5SubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

The IA5String (1.3.6.1.4.1.1466.115.121.1.26) syntax and the 'caseIgnoreIA5Match' and 'caseIgnoreIA5SubstringsMatch' rules are described in [RFC4517].

Note that the directory will not ensure that values of this attribute conform to the <domain> production provided above. It is the application's responsibility to ensure that domains it stores in this attribute are appropriately represented.

Also note that applications supporting Internationalized Domain Names SHALL use the ToASCII method [RFC3490] to produce <label> components of the <domain> production.

2.2. associatedName

The 'associatedName' attribute specifies names of entries in the organizational DIT associated with a DNS domain [RFC1034][RFC2181].

```
( 0.9.2342.19200300.100.1.38 NAME 'associatedName'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

The DistinguishedName (1.3.6.1.4.1.1466.115.121.1.12) syntax and the 'distinguishedNameMatch' rule are described in [RFC4517].

2.3. buildingName

The 'buildingName' attribute specifies names of the buildings where an organization or organizational unit is based, for example, "The White House".

```
( 0.9.2342.19200300.100.1.48 NAME 'buildingName'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.4. co

The 'co' (Friendly Country Name) attribute specifies names of countries in human-readable format, for example, "Germany" and "Federal Republic of Germany". It is commonly used in conjunction with the 'c' (Country Name) [RFC4519] attribute (whose values are restricted to the two-letter codes defined in [ISO3166]).

```
( 0.9.2342.19200300.100.1.43 NAME 'co'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.5. documentAuthor

The 'documentAuthor' attribute specifies the distinguished names of authors (or editors) of a document. For example,

```
( 0.9.2342.19200300.100.1.14 NAME 'documentAuthor'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

The DistinguishedName (1.3.6.1.4.1.1466.115.121.1.12) syntax and the 'distinguishedNameMatch' rule are described in [RFC4517].

2.6. documentIdentifier

The 'documentIdentifier' attribute specifies unique identifiers for a document. A document may be identified by more than one unique identifier. For example, RFC 3383 and BCP 64 are unique identifiers that (presently) refer to the same document.

```
( 0.9.2342.19200300.100.1.11 NAME 'documentIdentifier'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.7. documentLocation

The 'documentLocation' attribute specifies locations of the document original.

```
( 0.9.2342.19200300.100.1.15 NAME 'documentLocation'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.8. documentPublisher

The 'documentPublisher' attribute is the persons and/or organizations that published the document. Documents that are jointly published have one value for each publisher.

```
( 0.9.2342.19200300.100.1.56 NAME 'documentPublisher'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.9. documentTitle

The 'documentTitle' attribute specifies the titles of a document. Multiple values are allowed to accommodate both long and short titles, or other situations where a document has multiple titles, for example, "The Lightweight Directory Access Protocol Technical Specification" and "The LDAP Technical Specification".

```
( 0.9.2342.19200300.100.1.12 NAME 'documentTitle'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.10. documentVersion

The 'documentVersion' attribute specifies the version information of a document.

```
( 0.9.2342.19200300.100.1.13 NAME 'documentVersion'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.11. drink

The 'drink' (favoriteDrink) attribute specifies the favorite drinks of an object (or person), for instance, "cola" and "beer".

```
( 0.9.2342.19200300.100.1.5 NAME 'drink'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.12. homePhone

The 'homePhone' (Home Telephone Number) attribute specifies home telephone numbers (e.g., "+1 775 555 1234") associated with a person.

```
( 0.9.2342.19200300.100.1.20 NAME 'homePhone'
  EQUALITY telephoneNumberMatch
  SUBSTR telephoneNumberSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.50 )
```

The telephoneNumber (1.3.6.1.4.1.1466.115.121.1.50) syntax and the 'telephoneNumberMatch' and 'telephoneNumberSubstringsMatch' rules are described in [RFC4517].

2.13. homePostalAddress

The 'homePostalAddress' attribute specifies home postal addresses for an object. Each value should be limited to up to 6 directory strings of 30 characters each. (Note: It is not intended that the directory service enforce these limits.)

```
( 0.9.2342.19200300.100.1.39 NAME 'homePostalAddress'
  EQUALITY caseIgnoreListMatch
  SUBSTR caseIgnoreListSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.41 )
```

The PostalAddress (1.3.6.1.4.1.1466.115.121.1.41) syntax and the 'caseIgnoreListMatch' and 'caseIgnoreListSubstringsMatch' rules are described in [RFC4517].

2.14. host

The 'host' attribute specifies host computers, generally by their primary fully qualified domain name (e.g., my-host.example.com).

```
( 0.9.2342.19200300.100.1.9 NAME 'host'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.15. info

The 'info' attribute specifies any general information pertinent to an object. This information is not necessarily descriptive of the object.

Applications should not attach specific semantics to values of this attribute. The 'description' attribute [RFC4519] is available for specifying descriptive information pertinent to an object.

```
( 0.9.2342.19200300.100.1.4 NAME 'info'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{2048} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.16. mail

The 'mail' (rfc822mailbox) attribute type holds Internet mail addresses in Mailbox [RFC2821] form (e.g., user@example.com).

```
( 0.9.2342.19200300.100.1.3 NAME 'mail'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} )
```

The IA5String (1.3.6.1.4.1.1466.115.121.1.26) syntax and the 'caseIgnoreIA5Match' and 'caseIgnoreIA5SubstringsMatch' rules are described in [RFC4517].

Note that the directory will not ensure that values of this attribute conform to the <Mailbox> production [RFC2821]. It is the application's responsibility to ensure that domains it stores in this attribute are appropriately represented.

Additionally, the directory will compare values per the matching rules named in the above attribute type description. As these rules differ from rules that normally apply to <Mailbox> comparisons, operational issues may arise. For example, the assertion (mail=joe@example.com) will match "JOE@example.com" even though the <local-parts> differ. Also, where a user has two <Mailbox>es whose addresses differ only by case of the <local-part>, both cannot be listed as values of the user's mail attribute (as they are considered equal by the 'caseIgnoreIA5Match' rule).

Also note that applications supporting internationalized domain names SHALL use the ToASCII method [RFC3490] to produce <sub-domain> components of the <Mailbox> production.

2.17. manager

The 'manager' attribute specifies managers, by distinguished name, of the person (or entity).

```
( 0.9.2342.19200300.100.1.10 NAME 'manager'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

The DistinguishedName (1.3.6.1.4.1.1466.115.121.1.12) syntax and the 'distinguishedNameMatch' rule are described in [RFC4517].

2.18. mobile

The 'mobile' (mobileTelephoneNumber) attribute specifies mobile telephone numbers (e.g., "+1 775 555 6789") associated with a person (or entity).

```
( 0.9.2342.19200300.100.1.41 NAME 'mobile'
  EQUALITY telephoneNumberMatch
  SUBSTR telephoneNumberSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.50 )
```

The telephoneNumber (1.3.6.1.4.1.1466.115.121.1.50) syntax and the 'telephoneNumberMatch' and 'telephoneNumberSubstringsMatch' rules are described in [RFC4517].

2.19. organizationalStatus

The 'organizationalStatus' attribute specifies categories by which a person is often referred to in an organization. Examples of usage in academia might include "undergraduate student", "researcher", "professor", and "staff". Multiple values are allowed where the person is in multiple categories.

Directory administrators and application designers SHOULD consider carefully the distinctions between this and the 'title' and 'userClass' attributes.

```
( 0.9.2342.19200300.100.1.45 NAME 'organizationalStatus'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.20. pager

The 'pager' (pagerTelephoneNumber) attribute specifies pager telephone numbers (e.g., "+1 775 555 5555") for an object.

```
( 0.9.2342.19200300.100.1.42 NAME 'pager'
  EQUALITY telephoneNumberMatch
  SUBSTR telephoneNumberSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.50 )
```

The telephoneNumber (1.3.6.1.4.1.1466.115.121.1.50) syntax and the 'telephoneNumberMatch' and 'telephoneNumberSubstringsMatch' rules are described in [RFC4517].

2.21. personalTitle

The 'personalTitle' attribute specifies personal titles for a person. Examples of personal titles are "Frau", "Dr.", "Herr", and "Professor".

```
( 0.9.2342.19200300.100.1.40 NAME 'personalTitle'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.22. roomNumber

The 'roomNumber' attribute specifies the room number of an object. During periods of renumbering, or in other circumstances where a room has multiple valid room numbers associated with it, multiple values may be provided. Note that the 'cn' (commonName) attribute type SHOULD be used for naming room objects.

```
( 0.9.2342.19200300.100.1.6 NAME 'roomNumber'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

2.23. secretary

The 'secretary' attribute specifies secretaries and/or administrative assistants, by distinguished name.

```
( 0.9.2342.19200300.100.1.21 NAME 'secretary'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

The DistinguishedName (1.3.6.1.4.1.1466.115.121.1.12) syntax and the 'distinguishedNameMatch' rule are described in [RFC4517].

2.24. uniqueIdentifier

The 'uniqueIdentifier' attribute specifies a unique identifier for an object represented in the Directory. The domain within which the identifier is unique and the exact semantics of the identifier are for local definition. For a person, this might be an institution-wide payroll number. For an organizational unit, it might be a department code.

```
( 0.9.2342.19200300.100.1.44 NAME 'uniqueIdentifier'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

Note: X.520 also describes an attribute called 'uniqueIdentifier' (2.5.4.45), which is called 'x500UniqueIdentifier' in LDAP [RFC4519]. The attribute detailed here ought not be confused with 'x500UniqueIdentifier'.

2.25. userClass

The 'userClass' attribute specifies categories of computer or application user. The semantics placed on this attribute are for local interpretation. Examples of current usage of this attribute in academia are "student", "staff", and "faculty". Note that the 'organizationalStatus' attribute type is now often preferred, as it makes no distinction between persons as opposed to users.

```
( 0.9.2342.19200300.100.1.8 NAME 'userClass'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

The DirectoryString (1.3.6.1.4.1.1466.115.121.1.15) syntax and the 'caseIgnoreMatch' and 'caseIgnoreSubstringsMatch' rules are described in [RFC4517].

3. COSINE Object Classes

This section details COSINE object classes for use in LDAP.

3.1. account

The 'account' object class is used to define entries representing computer accounts. The 'uid' attribute SHOULD be used for naming entries of this object class.

```
( 0.9.2342.19200300.100.4.5 NAME 'account'
  SUP top STRUCTURAL
  MUST uid
  MAY ( description $ seeAlso $ l $ o $ ou $ host ) )
```

The 'top' object class is described in [RFC4512]. The 'description', 'seeAlso', 'l', 'o', 'ou', and 'uid' attribute types are described in [RFC4519]. The 'host' attribute type is described in Section 2 of this document.

3.3. documentSeriesExample:

```
dn: uid=kdz,cn=Accounts,dc=Example,dc=COM
objectClass: account
uid: kdz
seeAlso: cn=Kurt D. Zeilenga,cn=Persons,dc=Example,dc=COM
```

3.2. document

The 'document' object class is used to define entries that represent documents.

```
( 0.9.2342.19200300.100.4.6 NAME 'document'
  SUP top STRUCTURAL
  MUST documentIdentifier
  MAY ( cn $ description $ seeAlso $ l $ o $ ou $
    documentTitle $ documentVersion $ documentAuthor $
    documentLocation $ documentPublisher ) )
```

The 'top' object class is described in [RFC4512]. The 'cn', 'description', 'seeAlso', 'l', 'o', and 'ou' attribute types are described in [RFC4519]. The 'documentIdentifier', 'documentTitle', 'documentVersion', 'documentAuthor', 'documentLocation', and 'documentPublisher' attribute types are described in Section 2 of this document.

Example:

```
dn: documentIdentifier=RFC 4524,cn=RFC,dc=Example,dc=COM
objectClass: document
documentIdentifier: RFC 4524
documentTitle: COSINE LDAP/X.500 Schema
documentAuthor: cn=Kurt D. Zeilenga,cn=Persons,dc=Example,dc=COM
documentLocation: http://www.rfc-editor.org/rfc/rfc4524.txt
documentPublisher: Internet Engineering Task Force
description: A collection of schema elements for use in LDAP
description: Obsoletes RFC 1274
seeAlso: documentIdentifier=RFC 4510,cn=RFC,dc=Example,dc=COM
seeAlso: documentIdentifier=RFC 1274,cn=RFC,dc=Example,dc=COM
```

3.3. documentSeries

The 'documentSeries' object class is used to define an entry that represents a series of documents (e.g., The Request For Comments memos).

```
( 0.9.2342.19200300.100.4.9 NAME 'documentSeries'
  SUP top STRUCTURAL
  MUST cn
  MAY ( description $ l $ o $ ou $ seeAlso $
    telephonenumber ) )
```

The 'top' object class is described in [RFC4512]. The 'description', 'l', 'o', 'ou', 'seeAlso', and 'telephoneNumber' attribute types are described in [RFC4519].

Example:

```
dn: cn=RFC,dc=Example,dc=COM
objectClass: documentSeries
cn: Request for Comments
cn: RFC
description: a series of memos about the Internet
```

3.4. domain

The 'domain' object class is used to define entries that represent DNS domains for objects that are not organizations, organizational units, or other kinds of objects more appropriately defined using an object class specific to the kind of object being defined (e.g., 'organization', 'organizationUnit').

The 'dc' attribute should be used for naming entries of the 'domain' object class.

```
( 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 ) )
```

The 'top' object class and the 'dc', 'userPassword', 'searchGuide', 'seeAlso', 'businessCategory', 'x121Address', 'registeredAddress', 'destinationIndicator', 'preferredDeliveryMethod', 'telexNumber', 'teletexTerminalIdentifier', 'telephoneNumber', 'internationaliSDNNumber', 'facsimileTelephoneNumber', 'street', 'postOfficeBox', 'postalCode', 'postalAddress', 'physicalDeliveryOfficeName', 'st', 'l', 'description', and 'o' types

are described in [RFC4519]. The 'associatedName' attribute type is described in Section 2 of this document.

Example:

```
dn: dc=com
objectClass: domain
dc: com
description: the .COM TLD
```

3.5. domainRelatedObject

The 'domainRelatedObject' object class is used to define entries that represent DNS domains that are "equivalent" to an X.500 domain, e.g., an organization or organizational unit.

```
( 0.9.2342.19200300.100.4.17 NAME 'domainRelatedObject'
  SUP top AUXILIARY
  MUST associatedDomain )
```

The 'top' object class is described in [RFC4512]. The 'associatedDomain' attribute type is described in Section 2 of this document.

Example:

```
dn: dc=example,dc=com
objectClass: organization
objectClass: dcObject
objectClass: domainRelatedObject
dc: example
associatedDomain: example.com
o: Example Organization
```

The 'organization' and 'dcObject' object classes and the 'dc' and 'o' attribute types are described in [RFC4519].

3.6. friendlyCountry

The 'friendlyCountry' object class is used to define entries representing countries in the DIT. The object class is used to allow friendlier naming of countries than that allowed by the object class 'country' [RFC4519].

```
( 0.9.2342.19200300.100.4.18 NAME 'friendlyCountry'
  SUP country STRUCTURAL
  MUST co )
```

The 'country' object class is described in [RFC4519]. The 'co' attribute type is described in Section 2 of this document.

Example:

```
dn: c=DE
objectClass: country
objectClass: friendlyCountry
c: DE
co: Deutschland
co: Germany
co: Federal Republic of Germany
co: FRG
```

The 'c' attribute type is described in [RFC4519].

3.7. rFC822LocalPart

The 'rFC822LocalPart' object class is used to define entries that represent the local part of Internet mail addresses [RFC2822]. This treats the local part of the address as a 'domain' object.

```
( 0.9.2342.19200300.100.4.14 NAME 'rFC822localPart'
  SUP domain STRUCTURAL
  MAY ( cn $ description $ destinationIndicator $
    facsimileTelephoneNumber $ internationaliSDNNumber $
    physicalDeliveryOfficeName $ postalAddress $ postalCode $
    postOfficeBox $ preferredDeliveryMethod $ registeredAddress $
    seeAlso $ sn $ street $ telephoneNumber $
    teletexTerminalIdentifier $ telexNumber $ x121Address ) )
```

The 'domain' object class is described in Section 3.4 of this document. The 'cn', 'description', 'destinationIndicator', 'facsimileTelephoneNumber', 'internationaliSDNNumber, 'physicalDeliveryOfficeName', 'postalAddress', 'postalCode', 'postOfficeBox', 'preferredDeliveryMethod', 'registeredAddress', 'seeAlso', 'sn, 'street', 'telephoneNumber', 'teletexTerminalIdentifier', 'telexNumber', and 'x121Address' attribute types are described in [RFC4519].

Example:

```
dn: dc=kdz,dc=example,dc=com
objectClass: domain
objectClass: rFC822LocalPart
dc: kdz
associatedName: cn=Kurt D. Zeilenga,cn=Persons,dc=Example,dc=COM
```

The 'dc' attribute type is described in [RFC4519].

3.8. room

The 'room' object class is used to define entries representing rooms. The 'cn' (commonName) attribute SHOULD be used for naming entries of this object class.

```
( 0.9.2342.19200300.100.4.7 NAME 'room'
  SUP top STRUCTURAL
  MUST cn
  MAY ( roomNumber $ description $ seeAlso $ telephoneNumber ) )
```

The 'top' object class is described in [RFC4512]. The 'cn', 'description', 'seeAlso', and 'telephoneNumber' attribute types are described in [RFC4519]. The 'roomNumber' attribute type is described in Section 2 of this document.

```
dn: cn=conference room,dc=example,dc=com
objectClass: room
cn: conference room
telephoneNumber: +1 755 555 1111
```

3.9. simpleSecurityObject

The 'simpleSecurityObject' object class is used to require an entry to have a 'userPassword' attribute when the entry's structural object class does not require (or allow) the 'userPassword attribute'.

```
( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject'
  SUP top AUXILIARY
  MUST userPassword )
```

The 'top' object class is described in [RFC4512]. The 'userPassword' attribute type is described in [RFC4519].

```
dn: dc=kdz,dc=Example,dc=COM
objectClass: account
objectClass: simpleSecurityObject
uid: kdz
userPassword: My Password
seeAlso: cn=Kurt D. Zeilenga,cn=Persons,dc=Example,dc=COM
```

4. Security Considerations

General LDAP security considerations [RFC4510] are applicable to the use of this schema. Additional considerations are noted above where appropriate.

Directories administrators should ensure that access to sensitive information be restricted to authorized entities and that appropriate data security services, including data integrity and data confidentiality, are used to protect against eavesdropping.

Simple authentication (e.g., plain text passwords) mechanisms should only be used when adequate data security services are in place. LDAP offers reasonably strong authentication and data security services [RFC4513].

5. IANA Considerations

The Internet Assigned Numbers Authority (IANA) has updated the LDAP descriptors registry [RFC4520] as indicated in the following template:

Subject: Request for LDAP Descriptor Registration Update
Descriptor (short name): see comment
Object Identifier: see comments
Person & email address to contact for further information:
Kurt Zeilenga <kurt@OpenLDAP.org>
Usage: see comments
Specification: RFC 4524
Author/Change Controller: IESG
Comments:

The following descriptors have been updated to refer to RFC 4524.

NAME	Type	OID
account	O	0.9.2342.19200300.100.4.5
associatedDomain	A	0.9.2342.19200300.100.1.37
associatedName	A	0.9.2342.19200300.100.1.38
buildingName	A	0.9.2342.19200300.100.1.48
co	A	0.9.2342.19200300.100.1.43
document	O	0.9.2342.19200300.100.4.6
documentAuthor	A	0.9.2342.19200300.100.1.14
documentIdentifier	A	0.9.2342.19200300.100.1.11
documentLocation	A	0.9.2342.19200300.100.1.15
documentPublisher	A	0.9.2342.19200300.100.1.56
documentSeries	O	0.9.2342.19200300.100.4.8
documentTitle	A	0.9.2342.19200300.100.1.12
documentVersion	A	0.9.2342.19200300.100.1.13
domain	O	0.9.2342.19200300.100.4.13
domainRelatedObject	O	0.9.2342.19200300.100.4.17
drink	A	0.9.2342.19200300.100.1.5
favouriteDrink	A*	0.9.2342.19200300.100.1.5
friendlyCountry	O	0.9.2342.19200300.100.4.18

friendlyCountryName	A*	0.9.2342.19200300.100.1.43
homePhone	A	0.9.2342.19200300.100.1.20
homePostalAddress	A	0.9.2342.19200300.100.1.39
homeTelephone	A*	0.9.2342.19200300.100.1.20
host	A	0.9.2342.19200300.100.1.9
info	A	0.9.2342.19200300.100.1.4
mail	A	0.9.2342.19200300.100.1.3
manager	A	0.9.2342.19200300.100.1.10
mobile	A	0.9.2342.19200300.100.1.41
mobileTelephoneNumber	A*	0.9.2342.19200300.100.1.41
organizationalStatus	A	0.9.2342.19200300.100.1.45
pager	A	0.9.2342.19200300.100.1.42
pagerTelephoneNumber	A*	0.9.2342.19200300.100.1.42
personalTitle	A	0.9.2342.19200300.100.1.40
rFC822LocalPart	O	0.9.2342.19200300.100.4.14
rfc822Mailbox	A*	0.9.2342.19200300.100.1.3
room	O	0.9.2342.19200300.100.4.7
roomNumber	A	0.9.2342.19200300.100.1.6
secretary	A	0.9.2342.19200300.100.1.21
simpleSecurityObject	O	0.9.2342.19200300.100.4.19
singleLevelQuality	A	0.9.2342.19200300.100.1.50
uniqueIdentifier	A	0.9.2342.19200300.100.1.44
userClass	A	0.9.2342.19200300.100.1.8

where Type A is Attribute, Type O is ObjectClass, and * indicates that the registration is historic in nature.

6. Acknowledgements

This document is based on RFC 1274, by Paul Barker and Steve Kille, as well as on RFC 2247, by Steve Kill, Mark Wahl, Al Grimstad, Rick Huber, and Sri Satulari.

7. References

7.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1123] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

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

[RFC2821] Klensin, J., Ed., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[RFC3490] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4512] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[RFC4513] Harrison, R., "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms", RFC 4513, June 2006.

[RFC4517] Legg, S., Ed., "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RC 4517, June 2006.

[RFC4519] Sciberras, A., Ed., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

[X.501] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory -- Models," X.501(1993) (also ISO/IEC 9594-2:1994).

7.2. Informative References

[COSINEpilot] Goodman, D., "PARADISE" section of the March 1991 INTERNET MONTHLY REPORTS (p. 28-29), http://www.iana.org/periodic-reports/imr-mar91.txt

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

[RFC1274] Barker, P. and S. Kille, "The COSINE and Internet X.500 Schema", RFC 1274, November 1991.

[RFC1279] Hardcastle-Kille, S., "X.500 and Domains", RFC 1279, November 1991.

[RFC1487] Yeong, W., Howes, T., and S. Kille, "X.500 Lightweight Directory Access Protocol", RFC 1487, July 1993.

[RFC2251] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[RFC2798] Smith, M., "Definition of the inetOrgPerson LDAP Object Class", RFC 2798, April 2000.

[RFC3494] Zeilenga, K., "Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status", RFC 3494, March 2003.

[RFC4520] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 4520.

Appendix A. Changes since RFC 1274

This document represents a substantial rewrite of RFC 1274. The following sections summarize the substantive changes.

A.1. LDAP Short Names

A number of COSINE attribute types have short names in LDAP.

X.500 Name	LDAP Short Name
domainComponent	dc
favoriteDrink	drink
friendCountryName	co
homeTelephoneNumber	homePhone
mobileTelephoneNumber	mobile
pagerTelephoneNumber	pager
rfc822Mailbox	mail
userid	uid

While the LDAP short names are generally used in LDAP, some implementations may (for legacy reasons [RFC3494]) recognize the attribute type by its X.500 name. Hence, the X.500 names have been reserved solely for this purpose.

Note: 'uid' and 'dc' are described in [RFC4519].

A.2. pilotObject

The 'pilotObject' object class was not brought forward as its function is largely replaced by operational attributes introduced in X.500(93) [X.501] and version 3 of LDAP [RFC4512]. For instance, the function of the 'lastModifiedBy' and 'lastModifiedTime' attribute types is now served by the 'creatorsName', 'createTimestamp', 'modifiersName', and 'modifyTimestamp' operational attributes [RFC4512].

A.3. pilotPerson

The 'pilotPerson' object class was not brought forward as its function is largely replaced by the 'organizationalPerson' [RFC4512] object class and its subclasses, such as 'inetOrgPerson' [RFC2798].

Most of the related attribute types (e.g., 'mail', 'manager') were brought forward as they are used in other object classes.

A.4. dNSDomain

The 'dNSDomain' object class and related attribute types were not brought forward as its use is primarily experimental [RFC1279].

A.5. pilotDSA and qualityLabelledData

The 'pilotDSA' and 'qualityLabelledData' object classes, as well as related attribute types, were not brought forward as its use is primarily experimental [QoS].

A.6. Attribute Syntaxes

RFC 1274 defined and used caseIgnoreIA5StringSyntax attribute syntax. This has been replaced with the IA5String syntax and appropriate matching rules in 'mail' and 'associatedDomain'.

RFC 1274 restricted 'mail' to have non-zero length values. This restriction is not reflected in the IA5String syntax used in the definitions provided in this specification. However, as values are to conform to the <Mailbox> production, the 'mail' should not contain zero-length values. Unfortunately, the directory service will not enforce this restriction.

Appendix B. Changes since RFC 2247

The 'domainNameForm' name form was not brought forward as specification of name forms used in LDAP is left to a future specification.

Editor's Address

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).