

INTERNET-DRAFT
Intended Category: Standard Track
Expires in six months
Obsoletes: RFC [1274](#)
Updates: RFC [2247](#), [RFC 2798](#)

Editor: Kurt D. Zeilenga
OpenLDAP Foundation
6 February 2006

COSINE LDAP/X.500 Schema
<[draft-zeilenga-ldap-cosine-02.txt](#)>

Status of this Memo

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 LdapEXT mailing list <ldapext@ietf.org>. Please send editorial comments directly to the author <Kurt@OpenLDAP.org>.

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Copyright (C) The Internet Society (2006). All Rights Reserved.

Please see the Full Copyright section near the end of this document for more information.

Abstract

INTERNET-DRAFT

COSINE Schema

6 February 2006

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 [RFC 2247](#) and [RFC 2798](#).

Table of Contents

Status of this Memo	1
Abstract	2
Table of Contents	
1. Background and Intended Use	3
1.1. Relationship with Other Documents	
1.2. Terminology and Conventions	
2. COSINE Attribute Types	4
2.1. associatedDomain	
2.2. associatedName	
2.3. buildingName	
2.3. co	
2.5. documentAuthor	
2.6. documentIdentifier	
2.7. documentLocation	
2.8. documentPublisher	
2.9. documentTitle	
2.10. documentVersion	
2.11. drink	
2.12. homePhone	
2.13. homePostalAddress	
2.14. host	
2.16. info	
2.17. mail	
2.18. manager	
2.19. mobile	
2.20. organizationalStatus	
2.21. pager	
2.22. personalTitle	
2.23. roomNumber	
2.24. secretary	
2.26. uniqueIdentifier	
2.27. userClass	
3. COSINE Object Classes	14
3.1. account	

- 3.2. document
- 3.3. documentSeries
- 3.4. domain
- 3.5. domainRelatedObject
- 3.6. friendlyCountry

3.7.	rFC822LocalPart	
3.8.	room	
3.9.	simpleSecurityObject	
4.	Security Considerations	19
5.	IANA Considerations	20
6.	Acknowledgments	21
7.	Editor's Address	
8.	References	
A.	Changes Since RFC 1274	23
	Intellectual Property Rights	24
	Full Copyright	

1. Background and Intended Use

In the late 1980s, X.500 Directory Services were standardised 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 large scale directory pilots, [RFC 1274](#) was published to standardize 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) [[Roadmap](#)] was introduced in the early 1990s [[RFC1487](#)], with Version 3 of LDAP introduced in the late 1990s [[RFC2251](#)] and subsequently revised in the 2005 [[Roadmap](#)].

While much of the material in [RFC 1274](#) has been superceed 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 [[Schema](#)] and [[Syntaxes](#)], obsoletes [RFC 1274](#) in its entirety. [[Schema](#)] replaces sections [9.3.1](#) (Userid) and [9.3.21](#) (Domain Component) of [RFC 1274](#). [[Syntaxes](#)] 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 RFC 2247](#).

Some of schema elements specified here were described in [RFC 2798](#) (inetOrgPerson schema). This document supersedes these descriptions. This document, together with [[Schema](#)], 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 [[Models](#)].

Schema definitions are provided using LDAP description formats [[Models](#)]. 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](#)] which 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 [[Syntaxes](#)].

It is noted that the directory will not ensure that values of this attribute conform to the <domain> production provided above. It is the application responsibility to ensure domains it stores in this

attribute are appropriately represented.

It is also noted 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 [[Syntaxes](#)].

[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 [[Syntaxes](#)].

[2.3.](#) 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) [[Schema](#)] 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 [[Syntaxes](#)].

[2.5.](#) documentAuthor

The 'documentAuthor' attribute specifies the distinguished name 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 [[Syntaxes](#)].

[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 which (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 [[Syntaxes](#)].

[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 [[Syntaxes](#)].

[2.8.](#) documentPublisher

The 'documentPublisher' attribute is the persons and/or organizations that published the document. Documents which 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 [[Syntaxes](#)].

[2.9.](#) documentTitle

The 'documentTitle' attribute specifies the titles of a document. Multiple values are allowed to accomodate 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 [[Syntaxes](#)].

[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 [[Syntaxes](#)].

[2.11.](#) drink

The 'drink' (favoriteDrink) attribute specifies 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 [[Syntaxes](#)].

[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 [[Syntaxes](#)].

[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 [[Syntaxes](#)].

[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 [[Syntaxes](#)].

[2.16.](#) `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 [[Schema](#)] 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 [[Syntaxes](#)].

[2.17.](#) 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 [[Syntaxes](#)].

It is noted that the directory will not ensure that values of this attribute conform to the <Mailbox> production [[RFC2821](#)]. It is the application responsibility to ensure 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 which 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 which 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 by the

'caseIgnoreIA5Match' rule to be equal).

It is also noted that applications supporting internationalized domain names SHALL use the ToASCII method [[RFC3490](#)] to produce <sub-domain> components of the <Mailbox> production.

[2.18.](#) 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 [[Syntaxes](#)].

[2.19.](#) 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 [[Syntaxes](#)].

[2.20.](#) 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", "staff", etc.. Multiple values are allowed were 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 [[Syntaxes](#)].

[2.21.](#) 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 [[Syntaxes](#)].

[2.22.](#) 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 [\[Syntaxes\]](#).

[2.23.](#) 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 [\[Syntaxes\]](#).

[2.24.](#) secretary

The 'secretary' attribute specifies secretaries and/or administrative assistants, by distinguish name, of a person.

```
( 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 [\[Syntaxes\]](#).

[2.26.](#) 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 [[Syntaxes](#)].

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

[2.27.](#) 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", "faculty", etc.. 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 [[Syntaxes](#)].

[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 [[Models](#)]. The 'description', 'seeAlso', 'l', 'o', 'ou', and 'uid' attribute types are described in [[Schema](#)]. The 'host' attribute type is described in [Section 2](#) of this document.

Example:

```
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 which 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 [[Models](#)]. The 'cn', 'description', 'seeAlso', 'l', 'o', and 'ou' attribute types are described in [[Schema](#)]. The 'documentIdentifier', 'documentTitle', 'documentVersion', 'documentAuthor', 'documentLocation', and

'documentPublisher' attribute types are described in [Section 2](#) of this document.

Example:

```
dn: documentIdentifier=RFCXXXX,cn=RFC,dc=Example,dc=COM
objectClass: document
documentIdentifier: RFC XXXXX
documentTitle: COSINE LDAP/X.500 Schema
documentAuthor: cn=Kurt D. Zeilenga,cn=Persons,dc=Example,dc=COM
documentLocation: http://www.rfc-editor.org/rfc/rfcXXXX.txt
documentPublisher: Internet Engineering Task Force
description: A collection of schema elements for use in LDAP
description: Obsoletes RFC 1274
seeAlso: documentIdentifier=[Roadmap],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 which 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 [[Models](#)]. The 'description', 'l', 'o', 'ou', 'seeAlso', and 'telephoneNumber' attribute types are described in [[Schema](#)].

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 which represent DNS domains for objects which 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', etc.).

The 'dc' attribute should be used for naming entries of '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', 'o', types are described in [\[Schema\]](#). 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 which represent DNS domains which 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 )
```

INTERNET-DRAFT

COSINE Schema

6 February 2006

The 'top' object class is described in [[Models](#)]. 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 [[Schema](#)].

[3.5.](#) 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' [[Schema](#)].

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

The 'country' object class is described in [[Schema](#)]. 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 [[Schema](#)].

[3.6.](#) rFC822LocalPart

The 'rFC822LocalPart' object class is used to define entries which 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 [[Schema](#)].

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 [[Schema](#)].

[3.7.](#) 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 [[Models](#)]. The 'cn', 'description', 'seeAlso' and 'telephoneNumber' attribute types are described in [[Schema](#)]. 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
```

[3.8.](#) simpleSecurityObject

The 'simpleSecurityObject' object class is used to require an entry to have an '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 [[Models](#)]. The 'userPassword' attribute type is described in [[Schema](#)].

```
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 [[Roadmap](#)] is applicable to the use of this schema. Additional considerations are noted above where appropriate.

Directories administrators should ensure that access to sensitive information is restricted to authorized entities, but ensure 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 reasonable strong authentication and data security services [[AuthMeth](#)].

5. IANA Considerations

Zeilenga

[draft-zeilenga-ldap-cosine-02](#)

[Page 19]

INTERNET-DRAFT

COSINE Schema

6 February 2006

It is requested that the Internet Assigned Numbers Authority (IANA) update upon Standard Action the LDAP descriptors registry [[BCP64bis](#)] as indicated 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 XXXX
Author/Change Controller: IESG
Comments:

The following descriptors should be updated to refer to RFC XXXX.

NAME	Type	OID
-----	----	-----
account	0	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 and Type O is ObjectClass, and * indicates the registration is historic in nature.

[6. Acknowledgments](#)

This document is based upon [RFC 1274](#) by Paul Barker and Steve Kille, as well as [RFC 2247](#) by Steve Kill, Mark Wahl, Al Grimstad, Rick Huber, and Sri Satuluri.

[7. Editor's Address](#)

Kurt D. Zeilenga
OpenLDAP Foundation

Email: Kurt@OpenLDAP.org

[8. References](#)

[[Note to the RFC Editor: please replace the citation tags used in referencing Internet-Drafts with tags of the form RFCnnnn where possible.]]

[8.1. Normative References](#)

- [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13 (also [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](#) (also [RFC 2119](#)), March 1997.

- [RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", [RFC 2181](#), July 1997.
- [RFC2247] Kille, S., M. Wahl, A. Grimstad, R. Huber and S. Sataluri, "Using Domains in LDAP/X.500 Distinguished

Names", January 1998.

- [RFC2821] Klensin, J. (editor), "Simple Mail Transfer Protocol", [RFC 2822](#), April 2001.
- [RFC3490] Faltstrom, P., P. Hoffman, and A. Costello, "Internationalizing Domain Names in Applications (INDA)", [RFC 3490](#), March 2003.
- [Roadmap] Zeilenga, K. (editor), "LDAP: Technical Specification Road Map", [draft-ietf-ldapbis-roadmap-xx.txt](#), a work in progress.
- [Models] Zeilenga, K. (editor), "LDAP: Directory Information Models", [draft-ietf-ldapbis-models-xx.txt](#), a work in progress.
- [Syntaxes] Legg, S. (editor), "LDAP: Syntaxes and Matching Rules", [draft-ietf-ldapbis-syntaxes-xx.txt](#), a work in progress.
- [Schema] Dally, K. (editor), "LDAP: User Schema", [draft-ietf-ldapbis-user-schema-xx.txt](#), a work in progress.
- [AuthMeth] Harrison, R. (editor), "LDAP: Authentication Methods and Connection Level Security Mechanisms", [draft-ietf-ldapbis-authmeth-xx.txt](#), a work in progress.

[8.2](#). Informative References

[COSINEpilot]

- [NamingPlan] Zeilenga, K., "The Internet Naming Plan for LDAP/X.500 Directories", [draft-zeilenga-ldap-namingplan-xx.txt](#), a work in progress.
- [IS03166] 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", November 1991.

- [RFC2798] Smith, M., "The LDAP inetOrgPerson Object Class", [RFC 2798](#), April 2000.
- [BCP64bis] Zeilenga, K., "IANA Considerations for LDAP", [draft-ietf-ldapbis-bcp64-xx.txt](#), a work in progress.

[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 [Historic]) 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 [[Schema](#)].

[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 [[Models](#)]. For instance, the function of the 'lastModifiedBy' and 'lastModifiedTime' attribute types is now served by the 'creatorsName', 'createTimestamp', 'modifiersName', and 'modifyTimestamp' operational attributes [[Models](#)].

[A.3](#). pilotPerson

The 'pilotPerson' object class was not brought forward as its function

INTERNET-DRAFT

COSINE Schema

6 February 2006

is largely replaced by the 'organizationalPerson' [[Models](#)] object class and its subclasses, such as 'inetOrgPerson' [[RFC2798](#)].

Most of the related attribute types (e.g., 'mail', 'manager', etc.) 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.

Intellectual Property Rights

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights

might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

