INTERNET-DRAFT
Intended Category: BCP
Expires: 1 October 2001

Editor: Kurt D. Zeilenga
OpenLDAP Foundation

1 April 2001

IANA Considerations for LDAP

<draft-ietf-ldapbis-iana-00.txt>

Status of Memo

Abstract

This document provides procedures for registering extensible elements of LDAP. The document also provides guidelines to IANA describing conditions under which new values can be assigned.

1. Introduction

The Lightweight Directory Access Protocol [RFC2251] (LDAP) is an extensible protocol. LDAP supports:

- addition of new operations,
- extension of existing operations, and
- extensible schema.

This document details procedures for registering values of used to unambiguously identify extensible elements of the protocol with IANA including:

- LDAP message types,
- LDAP result codes,
- LDAP authentication methods,
- LDAP attribute description options, and
- Object Identifiers descriptive names

This document also provides guidelines to IANA describing the conditions under which new values can be assigned.

2. Terms and Conventions

This section details terms and conventions are used in this document.

2.1. Policy terms

The terms "IESG Approval", "Standards Action", "IETF Consensus", "Specification Required", "First Come First Served", "Expert Review", and "Private Use" are used as defined in [RFC2434].

2.2. Requirement terms

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 [RFC2119].

2.3. Common ABNF productions

A number of syntaxes in this document are described using ABNF [RFC2324]. These syntaxes rely on the following common productions:

```
a = %x41-5A / %61-7A  ; A-Z / a-z

ld = %x31-39          ; 1-9
```

```
d = %x30 / ld          ; 0-9

hyphen = %x2D          ; "-"

period = %x2E          ; "."

keychar = ( a / d / hyphen )
leadkeychar = ( a / d )

keystring = leadkeychar *keychar
```

A keyword is case-insensitive UTF-8 [RFC2279] string restricted to the keystring production.

3. IANA Considerations for LDAP

This section details each of the types of protocol values which can be registered and provides IANA guidelines on how to assign new values.

3.1. Object Identifiers Descriptive Names

LDAP allows short descriptive names to be used instead of an numeric Object Identifier to identify protocol extensions [RFC2251], schema elements [RFC2252], protocol extensions, LDAP URL [RFC2255] extensions, and other objects. These names SHALL be restricted to case-insensitive UTF-8 strings limited by the following ABNF:

```
name = keystring
```

Multiple names MAY be assigned to a given OID. For purposes of registration, an OID SHALL be represented in numeric OID form conforming to the ABNF:

```
numericoid = number *( period number ) ; e.g. 1.1.23.4

number = d / ( ld 1*d )
```

While the protocol places no maximum length restriction upon descriptive names, they SHOULD be short. IANA MAY refuse to register any name over 48 characters in length. IANA MAY reject obviously bogus registrations.

Names beginning with "x-" are for Private Use. IANA SHALL NOT register any name beginning with "x-".

Names beginning with "e-" are reserved for experiments. IANA SHALL

register any name beginning with "e-" on a First Come First Served basis.

Expert Review is REQUIRED before accepting registration of all other names.

IANA SHALL NOT verify the registrant "owns" the OID being named.

The OID namespace is managed by The ISO/IEC Joint Technical Committee 1 - Subcommittee 6.

3.2. AttributeDescription Options

An AttributeDescription [RFC2251, Section 4.1.5] can contain zero or options specifying additional semantics. An option SHALL be restricted to case-insensitive UTF-8 string limited by the following ABNF:

```
option = keystring
```

While the protocol places no maximum length restriction upon option strings, they SHOULD be short. IANA MAY refuse to register any option over 16 characters in length. IANA MAY reject obviously bogus registrations.

Values ending with a hyphen ("-") reserve all option names which start with the name. For example, the registration of the option "optionFamily-" reserves all options which start with "optionFamily-" for some related purpose.

Options beginning with "x-" are for Private Use. IANA SHALL NOT register any option beginning with "x-".

Options beginning with "e-" are reserved for experiments. IANA SHALL register any option beginning with "e-" on a First Come First Served basis.

IANA SHALL register other options by either Standards Action or Expert Review with Specification Required.

3.3. LDAP Message Types

Each protocol message is encapsulated in an LDAPMessage envelope [RFC2251, Section 4.1.1]. The protocolOp CHOICE indicates the type of message encapsulated. Each message type consists of a keyword and a non-negative choice number is combined with the class (APPLICATION)

and data type (CONSTRUCTED or PRIMITIVE) to construct the BER tag in the message's encoding. The choice numbers for existing protocol messages are implicit in the protocol's ASN.1 defined in [RFC2251].

New values SHALL only be registered by Standards Track action.

Note: LDAP provides extensible messages which reduces, but does not eliminate, the need to add new message types.

3.4. LDAP Result Codes

LDAP result messages carry an resultCode enumerated value to indicate the outcome of the operation [RFC2251, Section 4.1.10]. Each result code consists of a keyword and a non-negative integer.

IANA SHALL register resultCode integers from 0-255 upon Standards Action, 256-1023 with Expert Review, and 1024-8191 on a First Come First Served basis. Keywords associated with integers in the range 1024-8191 SHALL start with "e-". IANA MAY reject obviously bogus registrations.

Values greater than or equal to 8192 are for Private Use.

3.5. LDAP Authentication Method

The LDAP Bind operation supports multiple authentication methods [RFC2251, Section 4.2]. Each authentication choice consists of a keyword and a non-negative integer.

Authentication methods usage SHALL be classified using one of the following terms:

COMMON - method is appropriate for common use on the Internet,
LIMITED USE - method is appropriate for limited uses.
OBSOLETE - method has been deprecated or other found to be inappropriate for any use.

IANA SHALL NOT register new OBSOLETE mechanisms. Methods without publicly available specifications SHALL NOT be classified as COMMON.

IANA SHALL register authentication method integers from 0-255 upon Standards Action, 256-1023 with Expert Review with Specification Required, and 1024-8191 on a First Come First Served basis. Keywords associated with integers in the range 1024-8191 SHALL start with "e-". IANA MAY reject obviously bogus registrations.

Values greater than or equal to 8192 are for Private Use.

Note: LDAP supports SASL [RFC2222] as an Authentication CHOICE. SASL is an extensible LDAP authentication method.

Developers of new authentication methods are SHOULD seek appropriate review.

3.6. Other values?

Other LDAP name spaces?

4. Registration Procedure

The procedure given here MUST be used by anyone who to use a new value of a type described in Section 3 of this document which is not currently registered with IANA.

The first step is for the request to fill out the appropriate form. Templates are provided in Appendix A.

If the policy is Standards Action, the completed form SHOULD be provided to the IESG with the request for Standards Action. Upon approval of the Standards Action, the IESG SHALL forward the request (possibly revised) to IANA.

If the policy is Expert Review, the requester SHALL post the completed form to the <directory@apps.ietf.org> mailing list for public review. The review period is two (2) weeks. If a revised form is later submitted, the review period is restarted. Anyone may subscribe to this list my sending a request to <directory-request@apps.ietf.org>. During the review, objections may be raised by anyone (including the Expert) on the list. After completion of the review, the Expert, based upon public comments, SHALL either approve the request and forward it to the IESG OR deny the request. In either case, the Expert SHALL promptly notify the requester of the action . Actions of the Expert may be appealed [RFC2026]. The Expert is appointed by Applications Area Director(s).

If the policy is First Come First Served, the requester SHALL submit the completed form directly to the IESG <iesg@iesg.org>.

5. Registration Maintenance

This section needs to be flushed out.

6. Security Considerations

The security considerations detailed in [RFC2434] are generally applicable to this document. Security considerations to each namespace are discussed in Section 3.

7. Acknowledgment

This document is a product of the IETF LDAP Revision (LDAPbis) WG.

8. Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation

Email: Kurt@OpenLDAP.org

9. References

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

[RFC2234] D. Crocker, P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[RFC2279] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

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

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

[RFC2255] T. Howes, M. Smith, "The LDAP URL Format", RFC 2255, December, 1997.

[RFC2256] Wahl, M., "A Summary of the X.500(96) User Schema for use with LDAPv3", RFC 2256, December 1997.

[RFC2434] T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2119, October 1998.

Appendix A. Registration Templates

This appendix provides registration templates for registering new LDAP values. <<add templates>>

Appendix B. Assigned Values

The following values are currently assigned.

B.1. Object Identifiers Descriptive Names

NAME	Type	OID [REF]
alias	O	2.5.6.1 [RFC2256]
aliasedObjectName	T	2.5.4.1 [RFC2256]
altServer	T	1.3.6.1.4.1.1466.101.120.6 [RFC2252]
applicationEntity	O	2.5.6.12 [RFC2256]
applicationProcess	O	2.5.6.11 [RFC2256]
associatedDomain	T	0.9.2342.19200300.100.1.37 [RFC2164]
attributeTypes	T	2.5.21.5 [RFC2252]
authorityRevocationList	T	2.5.4.38 [RFC2256]
businessCategory	T	2.5.4.15 [RFC2256]
c	T	2.5.4.6 [RFC2256]
cACertificate	T	2.5.4.37 [RFC2256]
certificateRevocationList	T	2.5.4.39 [RFC2256]
certificationAuthority	O	2.5.6.16 [RFC2256]
certificationAuthority-V2	O	2.5.6.16.2 [RFC2256]
cn	T	2.5.4.3 [RFC2256]
commonName	T	2.5.4.3 [RFC2256]
country	O	2.5.6.2 [RFC2256]
countryName	T	2.5.4.6 [RFC2256]
createTimestamp	T	2.5.18.1 [RFC2252]
creatorsName	T	2.5.18.3 [RFC2252]
cRLDistributionPoint	O	2.5.6.19 [RFC2256]
crossCertificatePair	T	2.5.4.40 [RFC2256]
dc	T	0.9.2342.19200300.100.1.25 [RFC2247]
dcObject	O	1.3.6.1.4.1.1466.344 [RFC2247]
deltaCRL	O	2.5.6.23 [RFC2587]
deltaRevocationList	T	2.5.4.53 [RFC2256]
description	T	2.5.4.13 [RFC2256]

destinationIndicator	T	2.5.4.27 [RFC2256]
device	O	2.5.6.14 [RFC2256]
distinguishedName	T	2.5.4.49 [RFC2256]
dITContentRules	T	2.5.21.2 [RFC2252]
dITStructureRules	T	2.5.21.1 [RFC2252]
dmd	O	2.5.6.20 [RFC2256]
dmdName	T	2.5.4.54 [RFC2256]
dnQualifier	T	2.5.4.46 [RFC2256]
domainComponent	T	0.9.2342.19200300.100.1.25 [RFC2247]
dSA	O	2.5.6.13 [RFC2256]
dynamicObject	O	1.3.6.1.4.1.1466.101.119.2 [RFC2589]
dynamicSubtrees	T	1.3.6.1.4.1.1466.101.119.4 [RFC2589]
enhancedSearchGuide	T	2.5.4.47 [RFC2256]
entryTtl	T	1.3.6.1.4.1.1466.101.119.3 [RFC2589]
extensibleObject	O	1.3.6.1.4.1.1466.101.120.111 [RFC2252]
facsimileTelephoneNumber	T	2.5.4.23 [RFC2256]
fax	T	2.5.4.23 [RFC2256]
generationQualifier	T	2.5.4.44 [RFC2256]
givenName	T	2.5.4.42 [RFC2256]
groupOfNames	O	2.5.6.9 [RFC2256]
groupOfUniqueNames	O	2.5.6.17 [RFC2256]
houseIdentifier	T	2.5.4.51 [RFC2256]
initials	T	2.5.4.43 [RFC2256]
internationaliSDNNumber	T	2.5.4.25 [RFC2256]
knowledgeInformation	T	2.5.4.2 [RFC2256]
l	T	2.5.4.7 [RFC2256]
labeledURI	T	1.3.6.1.4.1.250.1.57 [RFC2079]
labeledURIObject	O	1.3.6.1.4.1.250.3.15 [RFC2079]
LDAPsubEntry	O	2.16.840.1.113719.2.142.6.1.1 [SUBENTRY]
ldapSyntaxes	T	1.3.6.1.4.1.1466.101.120.16 [RFC2251]
locality	O	2.5.6.3 [RFC2256]
localityName	T	2.5.4.7 [RFC2256]
mail	T	0.9.2342.19200300.100.1.3 [RFC2798]
matchingRules	T	2.5.21.4 [RFC2252]
matchingRuleUse	T	2.5.21.8 [RFC2252]
member	T	2.5.4.31 [RFC2256]
modifiersName	T	2.5.18.4 [RFC2252]
modifyTimestamp	T	2.5.18.2 [RFC2252]
name	T	2.5.4.41 [RFC2256]
nameForms	T	2.5.21.7 [RFC2252]
namingContexts	T	1.3.6.1.4.1.1466.101.120.5 [RFC2252]
o	T	2.5.4.10 [RFC2256]
objectClass	T	2.5.4.0 [RFC2256]
objectClasses	T	2.5.21.6 [RFC2252]
organization	O	2.5.6.4 [RFC2256]
organizationalPerson	O	2.5.6.7 [RFC2256]
organizationalRole	O	2.5.6.8 [RFC2256]
organizationalUnit	O	2.5.6.5 [RFC2256]

organizationalUnitName	T	2.5.4.11 [RFC2256]
organizationName	T	2.5.4.10 [RFC2256]
ou	T	2.5.4.11 [RFC2256]
owner	T	2.5.4.32 [RFC2256]
person	O	2.5.6.6 [RFC2256]
physicalDeliveryOfficeName	T	2.5.4.19 [RFC2256]
postalAddress	T	2.5.4.16 [RFC2256]
postalCode	T	2.5.4.17 [RFC2256]
postOfficeBox	T	2.5.4.18 [RFC2256]
preferredDeliveryMethod	T	2.5.4.28 [RFC2256]
presentationAddress	T	2.5.4.29 [RFC2256]
protocolInformation	T	2.5.4.48 [RFC2256]
registeredAddress	T	2.5.4.26 [RFC2256]
residentialPerson	O	2.5.6.10 [RFC2256]
rfc822Mailbox	T	0.9.2342.19200300.100.1.3 [RFC1274]
roleOccupant	T	2.5.4.33 [RFC2256]
searchGuide	T	2.5.4.14 [RFC2256]
seeAlso	T	2.5.4.34 [RFC2256]
serialNumber	T	2.5.4.5 [RFC2256]
simpleSecurityObject	O	0.9.2342.19200300.100.4.19 [RFC1274]
sn	T	2.5.4.4 [RFC2256]
st	T	2.5.4.8 [RFC2256]
stateOrProvinceName	T	2.5.4.8 [RFC2256]
street	T	2.5.4.9 [RFC2256]
streetAddress	T	2.5.4.9 [RFC2256]
strongAuthenticationUser	O	2.5.6.15 [RFC2256]
subschema	O	2.5.20.1 [RFC2252]
subschemaSubentry	T	2.5.18.10 [RFC2252]
supportedAlgorithms	T	2.5.4.52 [RFC2256]
supportedApplicationContext	T	2.5.4.30 [RFC2256]
supportedControl	T	1.3.6.1.4.1.1466.101.120.13 [RFC2252]
supportedExtension	T	1.3.6.1.4.1.1466.101.120.7 [RFC2252]
supportedLDAPVersion	T	1.3.6.1.4.1.1466.101.120.15 [RFC2252]
supportedSASLMechanisms	T	1.3.6.1.4.1.1466.101.120.14 [RFC2252]
surname	T	2.5.4.4 [RFC2256]
telephoneNumber	T	2.5.4.20 [RFC2256]
teletexTerminalIdentifier	T	2.5.4.22 [RFC2256]
telexNumber	T	2.5.4.21 [RFC2256]
title	T	2.5.4.12 [RFC2256]
top	O	2.5.6.0 [RFC2256]
uid	T	0.9.2342.19200300.100.1.1 [RFC2253]
uniqueMember	T	2.5.4.50 [RFC2256]
userCertificate	T	2.5.4.36 [RFC2256]
userid	T	0.9.2342.19200300.100.1.1 [RFC1274]
userPassword	T	2.5.4.35 [RFC2256]
userSecurityInformation	O	2.5.6.18 [RFC2256]
x121Address	T	2.5.4.24 [RFC2256]
x500UniqueIdentifier	T	2.5.4.45 [RFC2256]

B.2. Attribute Description Options

Option	Owner	Reference
binary	IESG	[RFC2251]
lang-*	IESG	[RFC2596]

B.3. LDAPMessage types

Name	Code	Owner	Reference
bindRequest	0	IESG	[RFC2251]
bindResponse	1	IESG	[RFC2251]
unbindRequest	2	IESG	[RFC2251]
searchRequest	3	IESG	[RFC2251]
searchResEntry	4	IESG	[RFC2251]
searchResDone	5	IESG	[RFC2251]
modifyRequest	6	IESG	[RFC2251]
modifyResponse	7	IESG	[RFC2251]
addRequest	8	IESG	[RFC2251]
addResponse	9	IESG	[RFC2251]
delRequest	10	IESG	[RFC2251]
delResponse	11	IESG	[RFC2251]
modDNRequest	12	IESG	[RFC2251]
modDNResponse	13	IESG	[RFC2251]
compareRequest	14	IESG	[RFC2251]
compareResponse	15	IESG	[RFC2251]
abandonRequest	16	IESG	[RFC2251]
reserved	17-18	IESG	
searchResRef	19	IESG	[RFC2251]
reserved	20-22	IESG	
extendedReq	23	IESG	[RFC2251]
extendedResp	24	IESG	[RFC2251]

B.4. resultCode values

Name	Code	Owner	Reference
success	0	IESG	[RFC2251]
operationsError	1	IESG	[RFC2251]
protocolError	2	IESG	[RFC2251]
timeLimitExceeded	3	IESG	[RFC2251]
sizeLimitExceeded	4	IESG	[RFC2251]
compareFalse	5	IESG	[RFC2251]
compareTrue	6	IESG	[RFC2251]
authMethodNotSupported	7	IESG	[RFC2251]

strongAuthRequired	8	IESG	[RFC2251]
reserved (partialResults)	9	IESG	[RFC2251]
referral	10	IESG	[RFC2251]
adminLimitExceeded	11	IESG	[RFC2251]
unavailableCriticalExtension	12	IESG	[RFC2251]
confidentialityRequired	13	IESG	[RFC2251]
saslBindInProgress	14	IESG	[RFC2251]
noSuchAttribute	16	IESG	[RFC2251]
undefinedAttributeType	17	IESG	[RFC2251]
inappropriateMatching	18	IESG	[RFC2251]
constraintViolation	19	IESG	[RFC2251]
attributeOrValueExists	20	IESG	[RFC2251]
invalidAttributeSyntax	21	IESG	[RFC2251]
noSuchObject	32	IESG	[RFC2251]
aliasProblem	33	IESG	[RFC2251]
invalidDNSyntax	34	IESG	[RFC2251]
reserved (isLeaf)	35	IESG	[RFC2251]
aliasDereferencingProblem	36	IESG	[RFC2251]
reserved	37-47	IESG	
inappropriateAuthentication	48	IESG	[RFC2251]
invalidCredentials	49	IESG	[RFC2251]
insufficientAccessRights	50	IESG	[RFC2251]
busy	51	IESG	[RFC2251]
unavailable	52	IESG	[RFC2251]
unwillingToPerform	53	IESG	[RFC2251]
loopDetect	54	IESG	[RFC2251]
reserved	55-63	IESG	
namingViolation	64	IESG	[RFC2251]
objectClassViolation	65	IESG	[RFC2251]
notAllowedOnNonLeaf	66	IESG	[RFC2251]
notAllowedOnRDN	67	IESG	[RFC2251]
entryAlreadyExists	68	IESG	[RFC2251]
objectClassModsProhibited	69	IESG	[RFC2251]
reserved (resultsTooLarge)	70	IESG	[RFC2251]
reserved	71-79	IESG	
other	80	IESG	[RFC2251]
reserved (APIs)	81	IESG	[RFC2251]
reserved (APIs)	82	IESG	[RFC2251]
reserved (APIs)	83	IESG	[RFC2251]
reserved (APIs)	84	IESG	[RFC2251]
reserved (APIs)	85	IESG	[RFC2251]
reserved (APIs)	86	IESG	[RFC2251]
reserved (APIs)	87	IESG	[RFC2251]
reserved (APIs)	88	IESG	[RFC2251]
reserved (APIs)	89	IESG	[RFC2251]
reserved (APIs)	90	IESG	[RFC2251]

B.5. Bind Authentication Method

Method	Value	Owner	Usage	Reference
simple	0	IESG	LIMITED USE	[RFC2251,RFC2829]
krbv42LDAP	1	IESG	OBSOLETE*	[RFC1777]
krbv42DSA	2	IESG	OBSOLETE*	[RFC1777]
sasl	3	IESG	COMMON	[RFC2251,RFC2829]

* These LDAPv2-only mechanisms were deprecated in favor LDAPv3 SASL authentication method, specifically when used with the KERBEROS_IV mechanism or the GSSAPI mechanism.