INTERNET-DRAFT
Intended Category: BCP
Expires in six months
Obsoletes: RFC 3383

Kurt D. Zeilenga
OpenLDAP Foundation
27 October 2003

IANA Considerations for LDAP
<draft-ietf-ldapbis-bcp64-01.txt>

Status of Memo

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

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>. The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This document provides procedures for registering extensible elements of Lightweight Directory Access Protocol (LDAP). The document also provides guidelines to Internet Assigned Numbers Authority (IANA)

describing conditions under which new values can be assigned.

1. Introduction

The Lightweight Directory Access Protocol [Roadmap] (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 including:

- LDAP message types;
- LDAP extended operations and controls;
- LDAP result codes;
- LDAP authentication methods;
- LDAP attribute description options; and
- Object Identifier descriptors.

These registries are maintained by the Internet Assigned Numbers Authority (IANA).

In addition, this document provides guidelines to IANA describing the conditions under which new values can be assigned.

This document replaces RFC 3383.

2. Terminology and Conventions

This section details terms and conventions used in this document.

2.1. Policy Terminology

The terms "IESG Approval", "Standards Action", "IETF Consensus", "Specification Required", "First Come First Served", "Expert Review", and "Private Use" are used as defined in BCP 26 [RFC2434].

2.2. Requirement Terminology

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]. In

this case, "the specification" as used by BCP 14 refers to the processing of protocols being submitted to the IETF standards process.

2.3. Common ABNF Productions

A number of syntaxes in this document are described using ABNF [RFC2234]. These syntaxes rely on the following common productions:

```
ALPHA = %x41-5A / %x61-7A    ; A-Z / a-z

LDIGIT = %x31-39             ; 1-9

DIGIT = %x30 / LDIGIT        ; 0-9

HYPHEN = %x2D                ; "-"

DOT = %x2E                   ; "."

number = DIGIT / ( LDIGIT 1*DIGIT )

keychar = ALPHA / DIGIT / HYPHEN

leadkeychar = ALPHA

keystring = leadkeychar *keychar
```

A keyword is a case-insensitive string of UTF-8 [UTF-8] encoded characters from the Universal Character Set (UCS) [ISO10646] restricted to the <keystring> production.

3. IANA Considerations for LDAP

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

IANA may reject obviously bogus registrations described.

3.1. Object Identifiers

Numerous LDAP schema and protocol elements are identified by Object Identifiers (OIDs) [X.680]. Specifications which assign OIDs to elements SHOULD state who delegated the OIDs for its use.

For IETF developed elements, specifications SHOULD use OIDs under

"Internet Directory Numbers" (1.3.6.1.1.x). Numbers under this OID arc will be assigned upon Expert Review with Specification Required. Only one OID per specification will be assigned. The specification MAY then assign any number of OIDs within this arc without further coordination with IANA.

For elements developed by others, any properly delegated OID can be used, including those under "Internet Private Enterprise Numbers" (1.3.6.1.4.1.x) assigned by IANA <http://www.iana.org/cgi-bin/enterprise.pl>.

To avoid interoperability problems between early implementations of a "work in progress" and implementations of the published specification (e.g., the RFC), experimental OIDs SHOULD be used in "works in progress" and early implementations. OIDs under the Internet Experimental OID arc (1.3.6.1.3.x) may be used for this purpose.

Experimental OIDs SHALL NOT be used in published specifications (e.g. RFCs).

Practices for IANA assignment of Internet Enterprise and Experimental OIDs are detailed in STD 16 [RFC1155].

3.2 Protocol Mechanisms

LDAP provides a number of Root DSE attributes for discovery of protocol mechanisms identified by OIDs, including:

- supportedControl [Models],
- supportedExtension [Models], and
- supportedFeatures [Features],

A registry of OIDs used for discover of protocol mechanisms is provided to allow implementors and others to locate the technical specification for these protocol mechanisms. Future specifications of additional Root DSE attributes holding values identifying protocol mechanisms MAY extend this registry for their values.

OIDs associated with discoverable protocol mechanisms SHOULD be registered. These are be considered on a First Come First Served with Specification Required basis.

OIDs associated with Standard Track mechanisms MUST be registered and require Standards Action.

3.3. Object Identifier Descriptors

LDAP allows short descriptive names (or descriptors) to be used instead of a numeric Object Identifier to identify protocol extensions [Protocol], schema elements [Models], LDAP URL [LDAPURL] extensions, and other objects.

Descriptors SHOULD be registered unless in private-use name space (e.g., they begin with "x-"). Descriptors defined in RFCs MUST be registered.

While the protocol allows the same descriptor to refer to different object identifiers in certain cases and the registry supports multiple registrations of the same descriptor (each indicating a different kind of schema element and different object identifier), multiple registrations of the same descriptor are to be avoided. All such registration requests require Expert Review.

Descriptors are restricted to strings of UTF-8 encoded UCS characters restricted by the following ABNF:

```
     name = keystring
```

Descriptors are case-insensitive.

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

```
     numericoid = number *( DOT number ) ; e.g. 1.1.0.23.40
```

While the protocol places no maximum length restriction upon descriptors, they should be short. Descriptors longer than 48 characters may be viewed as too long to register.

A values ending with a hyphen ("-") reserve all descriptors which start with the value. For example, the registration of the option "descrFamily-" reserves all options which start with "descrFamily-" for some related purpose.

Descriptors beginning with "x-" are for Private Use and cannot be registered.

Descriptors beginning with "e-" are reserved for experiments and will be registered on a First Come First Served basis.

All other descriptors require Expert Review to be registered.

The registrant need not "own" the OID being named.

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

3.4. AttributeDescription Options

An AttributeDescription [Models] can contain zero or more options specifying additional semantics. An option SHALL be restricted to a string UTF-8 encoded UCS characters limited by the following ABNF:

```
option = keystring
```

Options are case-insensitive.

While the protocol places no maximum length restriction upon option strings, they should be short. Options longer than 24 characters may be viewed as too long to register.

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 and cannot be registered.

Options beginning with "e-" are reserved for experiments and will be registered on a First Come First Served basis.

All other options require Standards Action or Expert Review with Specification Required to be registered.

3.5. LDAP Message Types

Each protocol message is encapsulated in an LDAPMessage envelope [Protocol]. 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 [Protocol].

New values will be registered upon Standards Action.

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

3.6. LDAP Result Codes

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

New resultCodes integers in the range 0-1023 require Standards Action to be registered. New resultCode integers in the range 1024-4095 require Expert Review with Specification Required. New resultCode integers in the range 4096-16383 will be registered on a First Come First Served basis. Keywords associated with integers in the range 0-4095 SHALL NOT start with "e-" or "x-". Keywords associated with integers in the range 4096-16383 SHALL start with "e-". Values greater than or equal to 16384 and keywords starting with "x-" are for Private Use and cannot be registered.

3.7. LDAP Authentication Method

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

The registrant SHALL classify the authentication method usage using one of the following terms:

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

Methods without publicly available specifications SHALL NOT be classified as COMMON. New registrations of class OBSOLETE cannot be registered.

New authentication method integers in the range 0-1023 require Standards Action to be registered. New authentication method integers in the range 1024-4095 require Expert Review with Specification Required. New authentication method integers in the range 4096-16383 will be registered on a First Come First Served basis. Keywords associated with integers in the range 0-4095 SHALL NOT start with "e-" or "x-". Keywords associated with integers in the range 4096-16383 SHALL start with "e-". Values greater than or equal to 16384 and keywords starting with "x-" are for Private Use and cannot be registered.

Note: LDAP supports Simple Authentication and Security Layers [SASL]

as an authentication choice. SASL is an extensible LDAP authentication method.

3.8. Directory Systems Names

The IANA-maintained "Directory Systems Names" registry [IANADSN] of valid keywords for well known attributes used in the LDAPv2 string representation of a distinguished name [RFC1779], now Historic [RFC3494].

Directory systems names are not known to be used in any other context. LDAPv3 uses Object Identifier Descriptors [Section 3.2] (which have a different syntax than directory system names).

New Directory System Names will no longer be accepted. For historical purposes, the current list of registered names should remain publicly available.

4. Registration Procedure

The procedure given here MUST be used by anyone who wishes to use a new value of a type described in Section 3 of this document.

The first step is for the requester 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. The IESG SHALL be viewed as the owner of all values requiring Standards Action.

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 by 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). The requester is viewed as the owner of values registered under Expert Review.

If the policy is First Come First Served, the requester SHALL submit the completed form directly to the IANA: <iana@iana.org>. The requester is viewed as the owner of values registered under First Come First Served.

Neither the Expert nor IANA will take position on the claims of copyright or trademarks issues regarding completed forms.

Prior to submission of the Internet Draft (I-D) to the RFC Editor but after IESG review and tentative approval, the document editor SHOULD revise the I-D to use registered values.

5. Registration Maintenance

This section discusses maintenance of registrations.

5.1. Lists of Registered Values

IANA makes lists of registered values readily available to the Internet community on their web site: <http://www.iana.org/>.

5.2. Change Control

The registration owner MAY update the registration subject to the same constraints and review as with new registrations. In cases where the owner is not unable or unwilling to make necessary updates, the IESG MAY assert ownership in order to update the registration.

5.3. Comments

For cases where others (anyone other than the owner) have significant objections to the claims in a registration and the owner does not agree to change the registration, comments MAY be attached to a registration upon Expert Review. For registrations owned by the IESG, the objections SHOULD be addressed by initiating a request for Expert Review.

The form to these requests is ad hoc, but MUST include the specific objections to be reviewed and SHOULD contain (directly or by reference) materials supporting the objections.

6. Security Considerations

The security considerations detailed in BCP 26 [RFC2434] are generally applicable to this document. Additional security considerations specific to each name space are discussed in Section 3 where appropriate.

Security considerations for LDAP are discussed in documents comprising the technical specification [Roadmap].

7. Acknowledgment

This document is a product of the IETF LDAP Revision (LDAPBIS) Working Group (WG). This document is a revision of RFC 3383, also a product of the LDAPBIS WG.

This document includes text borrowed from "Guidelines for Writing an IANA Considerations Section in RFCs" [RFC2434] by Thomas Narten and Harald Alvestrand.

8. Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation

Email: Kurt@OpenLDAP.org

9. Normative References

[RFC1155] Rose, M. and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", STD 16 (also RFC 1155), May 1990.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9 (also RFC 2026), October 1996.

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

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26 (also RFC 2434), October 1998.

[Roadmap] Zeilenga, K. (editor), "LDAP: Technical Specification

Road Map", draft-ietf-ldapbis-roadmap-xx.txt, a work in progress.

[Protocol] Sermersheim, J. (editor), "LDAP: The Protocol", draft-ietf-ldapbis-protocol-xx.txt, a work in progress.

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

[LDAPURL] Smith, M. (editor), "LDAP: Uniform Resource Locator", draft-ietf-ldapbis-url-xx.txt, a work in progress.

[UTF-8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", draft-yergeau-rfc2279bis-xx.txt, a work in progress.

[ISO10646] International Organization for Standardization, "Universal Multiple-Octet Coded Character Set (UCS) - Architecture and Basic Multilingual Plane", ISO/IEC 10646-1 : 1993.

[X.680] International Telecommunication Union - Telecommunication Standardization Sector, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", X.680(1997) (also ISO/IEC 8824-1:1998).

10. Informative References

[RFC1779] Kille, S., "A String Representation of Distinguished Names", RFC 1779, March 1995.

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

[SASL] Melnikov, A. (Editor), "Simple Authentication and Security Layer (SASL)", draft-ietf-sasl-rfc2222bis-xx.txt, a work in progress.

Appendix A. Registration Templates

This appendix provides registration templates for registering new LDAP values.

A.1. LDAP Object Identifier Registration Template

Subject: Request for LDAP OID Registration

Person & email address to contact for further information:

Specification: (I-D)

Author/Change Controller:

Comments:

(Any comments that the requester deems relevant to the request)

A.2. LDAP Protocol Mechanism Registration Template

Subject: Request for LDAP Protocol Mechanism Registration

Object Identifier:

Description:

Person & email address to contact for further information:

Usage: (One of Control or Extension or Feature)

Specification: (I-D)

Author/Change Controller:

Comments:

(Any comments that the requester deems relevant to the request)

A.3. LDAP Descriptor Registration Template

Subject: Request for LDAP Descriptor Registration

Descriptor (short name):

Object Identifier:

Person & email address to contact for further information:

Usage: (One of attribute type, URL extension,
object class, or other)

Specification: (RFC, I-D, URI)

Author/Change Controller:

Comments:

(Any comments that the requester deems relevant to the request)

A.4. LDAP Attribute Description Option Registration Template

Subject: Request for LDAP Attribute Description Option Registration

Option Name:

Family of Options: (YES or NO)

Person & email address to contact for further information:

Specification: (RFC, I-D, URI)

Author/Change Controller:

Comments:

(Any comments that the requester deems relevant to the request)

A.5. LDAP Message Type Registration Template

Subject: Request for LDAP Message Type Registration

LDAP Message Name:

Person & email address to contact for further information:

Specification: (Approved I-D)

Comments:

(Any comments that the requester deems relevant to the request)

A.6. LDAP Result Code Registration Template

Subject: Request for LDAP Result Code Registration

Result Code Name:

Person & email address to contact for further information:

Specification: (RFC, I-D, URI)

Author/Change Controller:

Comments:

(Any comments that the requester deems relevant to the request)

A.7. LDAP Authentication Method Registration Template

Subject: Request for LDAP Authentication Method Registration

Authentication Method Name:

Person & email address to contact for further information:

Specification: (RFC, I-D, URI)

Intended Usage: (One of COMMON, LIMITED-USE, OBSOLETE)

Author/Change Controller:

Comments:

(Any comments that the requester deems relevant to the request)

Appendix B. Changes since RFC 3383

This informative appendix provides a summary of changes made since RFC 3383.

- Object Identifier Descriptors practices were updated to require all descriptors defined in RFCs to be registered and recommending all other descriptors (excepting those in private-use name space) be registered. Additionally, all requests for multiple registrations of the same descriptor are now subject to Expert Review.

- Protocol Mechanisms practices were updated to include values of the 'supportedFeatures' attribute type.

- References to RFCs comprising the LDAP technical specifications have been updated to latest revisions.

- The "Assigned Values" appendix providing initial registry values was removed.

- Numerous editorial changes were made.

Full Copyright