INTERNET-DRAFT   Hallvard B. Furuseth
Intended Category: Informational   University of Oslo
Expires: December 2006   L. Howard
                                                          PADL Software
                                                       Alexey Melnikov
                                                         Isode Limited
                                                             June 2006

             Structural object class 'namedObject' for LDAP/X.500
                    <<u>draft-furuseth-ldap-untypedobject-02.txt</u>>

Status of this Memo

   This document is intended to be published as an Informational RFC.
   Distribution of this memo is unlimited. Technical discussions of
   this document are held on the LDAP Extension mailinglist
   <ldapext@ietf.org>. Please send editorial comments directly to the
   author <h.b.furuseth@usit.uio.no>.

   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 <u>Section 6 of BCP 79</u>.

   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
   <u>http://www.ietf.org/1id-abstracts.html</u>

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

Abstract

   This document defines an 'namedObject' structural object class for
   the Lightweight Directory Access Protocol (LDAP) and X.500. This is
   useful for entries with no natural choice of structural object class,

e.g. if an entry must exist even though its contents are
uninteresting.

1. Introduction

An entry in a Lightweight Directory Access Protocol (LDAP) [LDAPV3]
or [X.500] directory must have a structural object class, such as
'person' or 'country'. However, an entry may lack a natural choice
of structural object class. For example, the desired structure of a
directory tree might require an entry to exist for grouping purposes
even though it describes no real-world object. This document defines
an 'namedObject' structural object class for this use.

As 'namedObject' structural object class doesn't have any mandatory
attributes, it can also be used in combination with arbitrary
auxiliary object classes. For example, the posixGroup object class
[LDAP-NIS] is an auxiliary object class that may be used to overlay
POSIX group identification on an existing group of distinguished
names. In this case, it is suggested that the groupOfUniqueNames
object class be used as a structural object class. However, this may
sometimes be inappropriate: that groupOfUniqueNames requires at least
one member may make it impossible to migrate existing group
information. [LDAP-NIS] could define a specific structural object
class for this case (say, structuralPosixGroup), but this would
unnecessarily add to the proliferation of redundant schema.

2. Object class definition

namedObject is defined as follows. The definition uses the BNF form
of ObjectClassDescription from [MODEL], but with lines folded for
readability.

```
( IANA-ASSIGNED-OID NAME 'namedObject'
  DESC 'Entry of no particular type [RFC XXXX]'
  SUP top STRUCTURAL
  MAY ( cn $ o $ ou $ l $ c $ st $ street $
        description $ owner $ seeAlso ) )
```

<<Reuse Luke's OID: 1.3.6.1.4.1.5322.13.1.1?>>

The attribute types are defined in [SCHEMA].

The name of an entry with this object class will normally be a cn,
but attributes o through street are allowed as well in case the entry
name relates to the name of something else. Of these, only the one
used for naming is intended to be used in the entry. Use of the
others may be an indication that the entry should have a more
descriptive object class instead of or in addition to this one.

3. Example

   In a directory with entries named as follows, the entries with RDNs
   cn=people etc. can use namedObject:

                 uid=john,cn=people,dc=example,dc=com
          uid=john,cn=users,cn=system,dc=example,dc=com
       cn=www,cn=filegroups,cn=system,dc=example,dc=com

4. Security Considerations

   Attributes of directory entries are used to provide descriptive
   information about the real-world objects they represent, which can be
   people, organizations or devices. Most countries have privacy laws
   regarding the publication of information about people.

   <<TBD>>

5. IANA Considerations

   It is requested that the Internet Assigned Numbers Authority (IANA)
   register the following upon Expert Review:

      Subject: Request for LDAP OID Registration
      Person & email address to contact for further information:
         Hallvard B Furuseth <h.b.furuseth@usit.uio.no>
      Specification: RFC XXXX
      Author/Change Controller: IESG
      Comments:
         OID of structural object class 'namedObject'.

      Subject: Request for LDAP Descriptor Registration
      Descriptor (short name): namedObject
      Object Identifier: IANA-ASSIGNED-OID
      Person & email address to contact for further information:
         Luke Howard <lukeh@padl.com>
      Usage: Object class
      Specification: RFC XXXX
      Author/Change Controller: IESG
      Comments:
         Structural object class for entries of no particular type.

   [Editor: Here and in Section 2, replace IANA-ASSIGNED-OID with the
   assigned OID and XXXX with the RFC number assigned this document.]

6. References

6.1. Normative References

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

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

6.2. Informative References

    [LDAP-NIS] Howard, L., "An Approach for Using LDAP as a Network
               Information Service", RFC 2307, March 1998.

               [Note to the RFC editor: 2307bis gets approved as RFC
               before this document, relace the reference above:
               L. Howard, M. Ansari, "An Approach for Using LDAP as
               a Network Information Service".
               ]

    [LDAPV3]   Zeilenga, K., "Lightweight Directory Access Protocol
               (LDAP): Technical Specification Road Map", RFC 4510,
               June 2006.

    [STRING-DN] Zeilenga, K., "Lightweight Directory Access Protocol
                (LDAP): String Representation of Distinguished Names",
                RFC 4514, June 2006.

    [X.500]   The Directory, ITU-T Recommendations X.500-X.525, 1993.

7. Author's Address

    Hallvard B. Furuseth
    USIT, University of Oslo
    Pb. 1059 - Blindern
    0316 Oslo
    Norway

    E-mail: h.b.furuseth@usit.uio.no
    Phone: +47-22 85 28 13

    Luke Howard
    PADL Software Pty. Ltd.

   PO Box 59
   Central Park Vic 3145
   Australia

   EMail: lukeh@padl.com

   Alexey Melnikov
   Isode Limited
   5 Castle Business Village
   36 Station Road
   Hampton, Middlesex
   TW12 2BX, United Kingdom

   Email: Alexey.Melnikov@isode.com
   URI: http://www.melnikov.ca/

8. Acknowledgments

   Authors would like to thank Kurt Zeilenga for comments and
   corrections.

Appendix A: Notes on choices made for the object class

   (This section will be deleted in the final RFC.)

   The c through uid attributes (for naming of entries) match the table
   of naming attributes in [STRING-DN] (UTF-8 String Representation of
   Distinguished Names), in case the entry's RDN needs to match the RDN
   of something else.

   The description, owner and seeAlso attributes seem good to offer for
   "nothing in particular"-kind of entries, since such entries might not
   contain anything else which indicates what they are for and who is
   responsible for them.

Appendix B: Issues for consideration

   (This section will be deleted in the final RFC.)

   Is the name of this object class properly reflects its purpose?

   Is the choice of naming attributes good?