

INTERNET-DRAFT  
Intended Category: Standard Track  
Expires in six months

Kurt D. Zeilenga  
OpenLDAP Foundation  
18 July 2005

**The LDAP entryUUID operational attribute**  
**<[draft-zeilenga-ldap-uuid-06.txt](#)>**

Status of this Memo

This document is intended to be, after appropriate review and revision, submitted to the RFC Editor as an Standard Track document. Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF LDAP Extensions 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/1id-abstracts.html>

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

Copyright (C) The Internet Society (2005). All Rights Reserved.

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

Abstract

This document describes the LDAP/X.500 'entryUUID' operational attribute and associated matching rules and syntax. The attribute holds a server-assigned Universally Unique Identifier (UUID) for the object. Directory clients may use this attribute to distinguish objects identified by a distinguished name or to locate an object after renaming.

## **1. Background and Intended Use**

In X.500 Directory Services [[X.501](#)], such as those accessible using the Lightweight Directory Access Protocol (LDAP) [[Roadmap](#)], an object is identified by its distinguished name (DN). However, DNs are not stable identifiers. That is, a new object may be identified by a DN which previously identified another (now renamed or deleted) object.

A Universally Unique Identifier (UUID) is "an identifier unique across both space and time, with respect to the space of all UUIDs" [[UUIDURN](#)]. UUIDs are used in a wide range of systems.

This document describes the 'entryUUID' operational attribute which holds the UUID assigned to the object by the server. Clients may use this attribute to distinguish objects identified by a particular distinguished name or to locate a particular object after renaming.

This document defines the UUID syntax, the 'uuidMatch' and 'uuidOrderingMatch' matching rules, and the 'entryUUID' attribute type.

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

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](#)].

## **2. UUID Schema Elements**

### **2.1 UUID Syntax**

A Universally Unique Identifier (UUID) [[UUIDURN](#)] is a 16-octet (128-bit) value which identifies an object. The ASN.1 [[X.680](#)] type UUID is defined to represent UUIDs as follows:

```
UUID ::= OCTET STRING (SIZE(16))
      -- constrained to an UUID [UUIDURN]
```



In LDAP, UUID values are encoded using the [[ASCII](#)] character string representation described in [[UUIDURN](#)]. For example, "597ae2f6-16a6-1027-98f4-d28b5365dc14".

The following is a LDAP syntax description suitable for publication in subschema subentries.

```
( IANA-ASSIGNED-OID.1 DESC 'UUID' )
```

## [2.2](#) 'uuidMatch' Matching Rule

The 'uuidMatch' matching rule compares an asserted UUID with a stored UUID for equality. Its semantics are same as the 'octetStringMatch' [[X.520](#)][Syntaxes] matching rule. The rule differs from 'octetStringMatch' in that the assertion value is encoded using the UUID string representation instead of the normal OCTET STRING string representation.

The following is a LDAP matching rule description suitable for publication in subschema subentries.

```
( IANA-ASSIGNED-OID.2 NAME 'uuidMatch'  
  SYNTAX IANA-ASSIGNED-OID.1 )
```

## [2.3](#) 'uuidOrderingMatch' Matching Rule

The 'uuidOrderingMatch' matching rule compares an asserted UUID with a stored UUID for ordering. Its semantics are the same as the 'octetStringOrderingMatch' [[X.520](#)][Syntaxes] matching rule. The rule differs from 'octetStringOrderingMatch' in that the assertion value is encoded using the UUID string representation instead of the normal OCTET STRING string representation.

The following is a LDAP matching rule description suitable for publication in subschema subentries.

```
( IANA-ASSIGNED-OID.3 NAME 'uuidOrderingMatch'  
  SYNTAX IANA-ASSIGNED-OID.1 )
```

It is noted that not all UUID variants have a defined ordering and, even where so, servers are not obligated to assign UUIDs in any particular order. This matching rule is provided for completeness.

## [2.4](#). 'entryUUID' attribute



The 'entryUUID' operational attribute provides the Universally Unique Identifier (UUID) assigned to the entry.

The following is a LDAP attribute type description suitable for publication in subschema subentries.

```
( IANA-ASSIGNED-OID.4 NAME 'entryUUID'  
  DESC 'UUID of the entry'  
  EQUALITY uuidMatch  
  ORDERING uuidOrderingMatch  
  SYNTAX IANA-ASSIGNED-OID.1  
  SINGLE-VALUE  
  NO-USER-MODIFICATION  
  USAGE directoryOperation )
```

Servers SHALL generate and assign a new UUID to each entry upon its addition to the directory and provide that UUID as the value of the 'entryUUID' operational attribute. An entry's UUID is immutable.

UUID are to be generated in accordance with Section 4 of [[UUIDURN](#)]. In particular, servers MUST ensure that each generated UUID is unique in space and time.

### **[3. Security Considerations](#)**

An entry's relative distinguish name (RDN) is composed from attribute values of the entry, values which are commonly descriptive of the object the entry represents. While deployers are encouraged to use naming attributes whose values are widely disclosable [[LDAPDN](#)], entries are often named using information which cannot be disclosed to all parties. As UUIDs do not contain any descriptive information of the object they identify, UUIDs may be used to identify a particular entry without disclosure of its contents.

General UUID security considerations [[UUIDURN](#)] apply.

General LDAP security considerations [[RFC3377](#)] apply.

### **[4. IANA Considerations](#)**

It is requested that IANA register upon Standards Action the LDAP values specified in this document.

#### **[4.1. Object Identifier Registration](#)**



Subject: Request for LDAP OID Registration  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@OpenLDAP.org>  
Specification: RFC XXXX  
Author/Change Controller: IESG  
Comments:  
    Identifies the UUID schema elements

#### **4.2. UUID Syntax Registration**

Subject: Request for LDAP Syntax Registration  
Object Identifier: IANA-ASSIGNED-OID.1  
Description: UUID  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@OpenLDAP.org>  
Specification: RFC XXXX  
Author/Change Controller: IESG  
Comments:  
    Identifies the UUID syntax

#### **4.3. 'uuidMatch' Descriptor Registration**

Subject: Request for LDAP Descriptor Registration  
Descriptor (short name): uuidMatch  
Object Identifier: IANA-ASSIGNED-OID.2  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@OpenLDAP.org>  
Usage: Matching Rule  
Specification: RFC XXXX  
Author/Change Controller: IESG

#### **4.3. 'uuidOrderingMatch' Descriptor Registration**

Subject: Request for LDAP Descriptor Registration  
Descriptor (short name): uuidOrderingMatch  
Object Identifier: IANA-ASSIGNED-OID.3  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@OpenLDAP.org>  
Usage: Matching Rule  
Specification: RFC XXXX  
Author/Change Controller: IESG

#### **5.4. 'entryUUID' Descriptor Registration**





It is requested that IANA register upon Standards Action the LDAP 'entryUUID' descriptor.

Subject: Request for LDAP Descriptor Registration  
Descriptor (short name): entryUUID  
Object Identifier: IANA-ASSIGNED-OID.4  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@OpenLDAP.org>  
Usage: Attribute Type  
Specification: RFC XXXX  
Author/Change Controller: IESG

## **6. Acknowledgments**

This document is based upon discussions in the LDAP Update and Duplication Protocols (LDUP) WG. Members of the LDAP Directorate provided review.

## **7. Author'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**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#) (also [RFC 2119](#)), March 1997.
- [Roadmap] Zeilenga, K. (editor), "LDAP: Technical Specification Road Map", [draft-ietf-ldapbis-roadmap-xx.txt](#), a work in progress.
- [UUIDURN] Leach, P, M. Mealling, R. Salz, "A UUID URN Namespace", 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.
- [ASCII] Coded Character Set--7-bit American Standard Code for Information Interchange, ANSI X3.4-1986.
- [X.501] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory -- Models," X.501(1993) (also ISO/IEC 9594-2:1994).
- [X.520] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory: Selected Attribute Types", X.520(1993) (also ISO/IEC 9594-6:1994).
- [X.680] International Telecommunication Union - Telecommunication Standardization Sector, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", X.680(2002) (also ISO/IEC 8824-1:2002).

## **8.2. Informative References**

- [LDAPDN] Zeilenga, K. (editor), "LDAP: String Representation of Distinguished Names", [draft-ietf-ldapbis-dn-xx.txt](#), a work in progress.
- [BCP64bis] Zeilenga, K., "IANA Considerations for LDAP", [draft-ietf-ldapbis-bcp64-xx.txt](#), a work in progress.

## **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](mailto:ietf-ipr@ietf.org).

#### Full Copyright

Copyright (C) The Internet Society (2005).

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.

