X660LDAP
Internet-Draft
Intended status: Standards Track
Expires: July 5, 2021

J. Coretta

January 1, 2021

Lightweight Directory Access Protocol (LDAP) Procedures and Schema Definitions for the Storage of X.660 Registration Information

draft-coretta-x660-ldap-02.txt

Abstract

This specification defines models and schema definitions facilitating the storage of [X.660] registration data in a Lightweight Directory Access Protocol Directory Information Tree.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on July 5, 2021.

Copyright Notice

Table of Contents

1. Introduction

This specification describes a means for storing [X.660] registration and contextual within an LDAP [RFC4510] implementation.

1.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Intended Audience

This specification is intended for use by any entity or individual in need of a means for storing and serving [X.660] data, in whole or in part.

1.3. Limitations

Some design decisions set forth in this document tend to favor a more generalized implementation as opposed to a strict adherence to all of the precepts defined in [X.660].

One obvious example of this relates to the lack of enforcement of the use (or non-use) of Unicode values during attribute value assignment. While Unicode values are supported where expected, this specification provides no such enforcement.

1.4. OIDs Used in this Document

This specification provides a registered OID for LDAP schema elements as defined in Section 2.

- 1.3.6.1.4.1.56521 (author root)
- 1.3.6.1.4.1.56521.101 (specification OID)
- 1.3.6.1.4.1.56521.101.1 (schema OID)
- 1.3.6.1.4.1.56521.101.1.1 (attribute types OID)
- 1.3.6.1.4.1.56521.101.1.2 (object classes OID)

1.5. Acronyms Used in this Document

DN Distinguished Name
RDN Relative Distinguished Name
DUA Directory User Agent (an LDAP client)
DIT Directory Information Tree
OID (ASN.1) Object Identifier
LDAP Lightweight Directory Access Protocol
ASN.1 Abstract Syntax Notation v1

2. Schema Definitions

This section discusses the particulars of the LDAP schema definitions made available through this specification.

These schema definitions described in this section are provided using LDAP description formats [RFC4512]. These elements are line-wrapped

and indented for readability.

2.1. Attribute Types

The following subsections detail LDAP attribute types created for use within implementations of this specification.

2.1.1. arc

The arc attribute type allows the storage of an unsigned integer that is meant to represent the primary identifier for an arc registration.

```
( 1.3.6.1.4.1.56521.101.1.1.1
    NAME 'arc'
    DESC 'A single unsigned integer value assigned to an X.660 arc
       to represent its primary integer identifier'
    EQUALITY integerMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )
```

2.1.2. arcOID

The arcOID attribute type allows the storage of an arc's ASN.1 Object Identifier value [X.680] in dot-delimited form.

```
( 1.3.6.1.4.1.56521.101.1.1.2
    NAME 'arcOID'
    DESC 'Dotted ASN.1 Object Identifier for non-root X.660 arcs'
    EQUALITY objectIdentifierMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
```

2.1.3. arcId

The arcId attribute type allows the storage of the primary identifier Unicode value (non-numeric) [X.660] in an arc registration entry.

```
( 1.3.6.1.4.1.56521.101.1.1.3
    NAME 'arcId'
    DESC 'The primary non-numeric Unicode identifier for
       an X.660 arc'
    EQUALITY caseIgnoreMatch
    SINGLE-VALUE
    SUP name )
```

2.1.4. arcSecId

The arcSecId attribute type allows the storage of an arc registration entry's non-Unicode, non-numeric secondary identifier [X.660].

```
( 1.3.6.1.4.1.56521.101.1.1.4
    NAME 'arcSecId'
    DESC 'The non-Unicode secondary identifier for an
       X.660 arc'
    EQUALITY caseIgnoreMatch
    SINGLE-VALUE
    SUP name )
```

2.1.5. arcAddlSecId

The arcAddlSecId attribute type allows the OPTIONAL storage of one or more additional secondary identifiers [X.660] in an arc registration entry.

```
( 1.3.6.1.4.1.56521.101.1.1.5
    NAME 'arcAddlSecId'
    DESC 'The non-Unicode additional secondary identifier for an
       X.660 arc'
    EQUALITY caseIgnoreMatch
    SUP name )
```

2.1.6. arcData

The arcData attribute type allows the OPTIONAL storage of octet-based values intended meant for extended documentation or notes in an arc registration entry.

```
( 1.3.6.1.4.1.56521.101.1.1.6
    NAME 'arcData'
    DESC 'Extended information for an X.660 arc'
    EQUALITY octetStringMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

2.1.7. arcAuthority

The arcAuthority attribute type allows a DN value that references an entry containing arc registration authority information.

```
( 1.3.6.1.4.1.56521.101.1.1.7
    NAME 'arcAuthority'
    DESC 'LDAP Distinguished Name of an entry bearing authoritative
       information for an X.660 arc'
    EQUALITY distinguishedNameMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

2.1.8. arcSponsor

The arcSponsor attribute type allows a DN value that references an entry containing arc registration sponsorship information.

```
( 1.3.6.1.4.1.56521.101.1.1.8
    NAME 'arcSponsor'
    DESC 'LDAP Distinguished Name of an entry bearing sponsorship
       information for an X.660 arc'
    EQUALITY distinguishedNameMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

2.1.9. arcContact

The arcContact attribute type allows a DN value that references an entry containing arc registration contact information.

```
( 1.3.6.1.4.1.56521.101.1.1.9
   NAME 'arcContact'
   DESC 'LDAP Distinguished Name of an entry bearing generalized
      contact information for an X.660 arc'
   EQUALITY distinguishedNameMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

2.1.10. arcTitle

The arcTitle attribute type allows for an official title to be set for an arc registration entry.

```
( 1.3.6.1.4.1.56521.101.1.1.10
   NAME 'arcTitle'
   DESC 'Title assigned to an X.660 arc'
   SUP title )
```

2.1.11. arcDescription

The arcDescription attribute type allows for a short description of an arc registration entry.

```
( 1.3.6.1.4.1.56521.101.1.1.11
   NAME 'arcDescription'
   DESC 'Short description of an X.660 arc'
   SUP description )
```

2.2. Object Classes

The following subsections describes LDAP object classes made available by this specification.

2.2.1. x660RootArcEntry

The x660RootArcEntry class is meant to define a maximum of three (3) root arcs within a directory model.

```
( 1.3.6.1.4.1.56521.101.1.2.1
    NAME 'x660RootArcEntry'
    DESC 'Top-level class for entries meant to represent ITU-T, ISO
       or Joint-ISO-ITU-T root arcs as defined in Section A.2 of
       the X.660 specification'
    SUP top
    STRUCTURAL
    MUST ( arc $ arcId )
    MAY ( arcData $ arcAuthority $ arcSponsor $ arcContact $
          arcSecId $ labeledURI $ arcDescription $ arcTitle $
          arcAddlSecId ) )
```

2.2.2. x660ArcEntry

The x660ArcEntry object class makes a collection of attribute types available for use when crafting non-root arc entries within a DIT.

```
( 1.3.6.1.4.1.56521.101.1.2.2
    NAME 'x660ArcEntry'
    DESC 'A generalized class meant to represent subordinate arcs
       beneath any root, as defined in X.660 Sections A.3-A.5'
    SUP top
    STRUCTURAL
    MUST ( arc )
    MAY ( arcAddlSecId $ arcData $ arcOID $ arcSecId $ arcId $
          arcAuthority $ arcSponsor $ arcContact $ labeledURI $
          arcDescription $ arcTitle ) )
```

3. Directory Models

This specification offers two (2) distinct models by which directory architects and application developers SHOULD be guided during their efforts for implementation.

3.1. Naming Context and Organization Entries

In these examples, a naming context of "dc=example, dc=com" is used as the fictional "suffix". Within this suffix are two (2) entries:

- "ou=X660, dc=example, dc=com" - Storage of all arc registration entries.

- "ou=Registrants, dc=example, dc=com" - Storage of all arc contact, authority and sponsorship entries.

Directory architects MAY choose to use models of their own design, so long as noted requirements in the following sections are satisfied.

3.2. Two-Dimensional Model

This model suggests that arc registration entries reside as siblings within an LDAP DIT in singular, non-hierarchical locations.

3.2.1. Requirements

One requirement of this model is strict use of the arcOID attribute type, covered in Section 2.1.2. This attribute MUST be used on all non-root arc registration entries.

Root arc registration entries SHALL NOT bear an arcOID value, as the syntax for OIDs (see Section 3.3.26 of [RFC4517]) requires at least two (2) nodes in a given value.

Uniqueness of arcOID values within a directory structure MUST always be enforced to ensure unambiguous results. The simplest way to meet this requirement would be to adopt arcOID-based DN structure as shown in the next section.

3.2.2. Distinguished Name Convention

Because all LDAP search requests can be conducted using a "one-level scope" below the circumscribing directory branch, a hierarchical DN structure is unnecessary. While the three-dimensional model (shown in Section 3.3) uses the integer-based arc attribute type (defined in Section 2.1.1) to form the effective LDAP RDN of an entry, it is not practical in this model.

The most sensible convention for DN involves use of the arcOID attribute as shown:

```
dn: arcOID=1.3,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660ArcEntry
arc: 3
arcId: Identified-Organization
arcOID: 1.3
```

Subsequent entries, regardless of hierarchical superiority, manifest as sibling entries. For example, the addition of deeper arcs would be procedurally identical:

```
dn: arcOID=1.3.6.1,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660ArcEntry
arc: 1
arcId: internet
arcOID: 1.3.6.1
```

3.3. Three-Dimensional Model

This model is hierarchical by nature, providing a means for storing arc registration entries in "nested" fashion, thereby reflecting the

hierarchy of the [X.660] specification itself.

3.3.1. Requirements

In this model, interim arc registrations MUST exist even if they are otherwise unnecessary.

For example, in order to add the well-known arc "internet" (OID: 1.3.6.1, [RFC1155]), directory administrators MUST ensure these registrations exist beforehand:

```
dn: arc=1,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660RootArcEntry
arc: 1
arcId: ISO

dn: arc=3,arc=1,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660ArcEntry
arc: 3
arcId: Identified-Organization

dn: arc=6,arc=3,arc=1,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660ArcEntry
arc: 6
arcId: dod
```

Only once this requirement is satisfied would the administrators be able to create the desired registration, such as a registration entry for the "internet" OID, as shown in [RFC1155]:

```
dn: arc=1,arc=6,arc=3,arc=1,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660ArcEntry
arc: 1
arcId: internet
```

3.3.2. Distinguished Name Convention

Under a strict interpretation of this model, its implementation will provide a means for bidirectional resolution of registered arc OIDs. LDAP DNs can be deduced from OIDs, and vice versa.

This is achieved by using the arc attribute type (as discussed in Section 2.1.1) as components in the effective LDAP DN, but in reverse order to reflect the directory hierarchy.

For example: the "internet" arc (OID: 1.3.6.1) would exist as an entry with a DN as depicted below:

```
dn: arc=1, arc=6, arc=3, arc=1, ou=X660, dc=example, dc=com
        |      |      |      |
        ----------------------
               1.3.6.1
```

3.3.3. Root Arc Entries

A maximum of three (3) root arcs SHOULD exist within the directory landscape. If one or more are created, they MUST be identifiable as follows:

- ITU-T (0)

- ISO (1)

- Joint-ISO-ITU-T (2)

As sibling entries, these root arcs MUST use the x660RootArcEntry class, as shown in Section 2.2.1:

```
dn: arc=0,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660RootArcEntry
arc: 0
arcId: ITU-T

dn: arc=1,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660RootArcEntry
arc: 1
arcId: ISO

dn: arc=2,ou=X660,dc=example,dc=com
objectClass: top
objectClass: x660RootArcEntry
arc: 2
arcId: Joint-ISO-ITU-T
```

Depending on the breadth and scope of an implementation, creation and use of root arc registration entries is RECOMMENDED, but not required in all situations.

3.4. Arc Authority, Sponsorship and Contact Info

Directory architects MAY choose to store authoritative, sponsorship or generalized contact information in one of two main ways:

- Use of an AUXILIARY object class [RFC4512] to facilitate the addition of any desired supplemental attribute types directly

to a given instance of x660RootArcEntry or x660ArcEntry, or ...

- Use of independent arc registration contact entries, which are referenced via LDAP DN through one or more of: arcAuthority, arcContact and/or arcSponsor attribute types assigned directly to a given instance of x660RootArcEntry or x660ArcEntry

For compatibility reasons, it is RECOMMENDED that only [RFC4519] attribute types be used to detail contact, authority or sponsorship information.

4. References

4.1. Normative References

[RFC1155] Rose, M., "Structure and Identification of Management Information for TCP/IP-based Internets", RFC 1155, May 1990.

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

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4512] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[RFC4517] Legg, Ed., S., "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RFC 4517, June 2006.

[RFC4519] Sciberras, Ed., A., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", RFC 8174, May 2017.

[X.660] International Telecommunication Union - Telecommunication Standardization Sector, "General procedures and top arcs of the international object identifier tree", X.660, July 2011.

[X.680] International Telecommunication Union - Telecommunication Standardization Sector, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", X.680, July 2002.

5. IANA Considerations

There are no requests to IANA in this document.

6. Security Considerations

This document focuses on providing flexible directory models and LDAP schema elements in order to serve arc registration data, and to allow an LDAP-based means for OID resolution, either within an organization or within the context of personal use. If some or all of the data in the directory is sensitive in nature, directory architects MUST take appropriate steps to secure this information. This concept is out of scope for this document.

Beyond this, there are no specific concerns in the area of security.

Author's Address

Jesse Coretta
Palm Springs, CA 92262

Email: jesse.coretta@icloud.com