eduPerson 1.0 Specification

Internet2/Educause
eduPerson Working Group
12-Feb-2001

eduPersonAffiliation (defined in eduPerson); *OID*: 1.3.6.1.4.1.5923.1.1.1.1

Application utility class: standard; *# of values*: multi

Definition

Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary)

Permissible values (if controlled)

faculty, student, staff, alum, member, affiliate, employee

Notes

If there is a value in eduPersonPrimaryAffiliation, that value should be stored here as well.

The list of allowed values in the current version 1.0 of the object class is CERTAINLY incomplete. We felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included as part of the post-1.0 versions of eduPerson.

We also deliberately avoided including a value such as "other" or "misc" because it would be semantically equivalent to "none of the above." To indicate "none of the above," for a specific person, leave the attribute empty.

"member" is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). It could be glossed as "member in good standing of the university community."

"affiliate" is intended to apply to people with whom the university has dealings, but to whom no general set of "community membership" privileges are extended.

Semantics

Each institution decides the criteria for membership in each affiliation classification.

A reasonable person should find the listed relationships commonsensical.

Example applications for which this attribute would be useful

directory of directories, white pages,
controlling access to resources

Example (LDIF fragment)

eduPersonAffiliation: faculty

Syntax: CIS; *Indexing*: pres,eq,sub

eduPersonNickname (defined in eduPerson); *OID*: 1.3.6.1.4.1.5923.1.1.1.2

Application utility class: standard; *# of values*: multi

Definition

Person's nickname, or the informal name by which they are accustomed to be hailed

Permissible values (if controlled)

Notes

Most often a single name as opposed to displayName which often consists of a full name. Useful for user-friendly search by name. As distinct from the cn (common name) attribute, the eduPersonNickname attribute is intended primarily to carry the person's preferred nickname(s). E.g., Jack for John, Woody for Durwood, JR for Joseph Robert.

Carrying this in a separate attribute makes it relatively easy to make this a self-maintained attribute (editorial oversight is advisable!). If it were merely one of the multiple values of the cn attribute, this would be harder to do.

Application developers can use this attribute to make directory search functions more "user friendly."

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

eduPersonNickname: Spike

Syntax: CIS; *Indexing*: pres,eq,sub

eduPersonOrgDN (defined in eduPerson); *OID*: 1.3.6.1.4.1.5923.1.1.1.3

Application utility class: core; *# of values*: single

Definition

The distinguished name (DN) of the of the directory entry representing the institution with which the person is associated.

Permissible values (if controlled)

Notes

With a distinguished name, the client can do an efficient lookup in the institution's directory.to find out more about the organization with which the person is associated.

Cn (common name), sn (surname, family name) and this attribute, eduPersonOrgDN, are the three attributes satisfying the "core" application utility class of eduPerson.

Semantics

The directory entry pointed to by this dn should be represented in the X.521(1993) "organization" object class   The attribute set for organization is defined as follows:

o (Organization Name, required}

Optional attributes include:
description
localeAttributeSet
postalAttributeSet
telecommunicationsAttributeSet
businessCategory
seeAlso
searchGuide
userPassword

Note that labeledURI is not included in the above list. We recommend adding the labeledURIObject auxilliary object class to the organization object pointed to by this dn, which endows it with a labeledURI attribute. Some directory servers implement this object class by default. For others, the schema may need to be extended using this definition (using the syntax specified by RFC2252):

```
( 1.3.6.1.4.1.250.3.15 NAME 'labeledURIObject' SUP top AUXILIARY
     MAY labeledURI )
```

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

eduPersonOrgDN: o=Hogwarts, dc=hsww, dc=wiz

Syntax: CIS;   *Indexing*:

eduPersonOrgUnitDN (defined in eduPerson); *OID*: 1.3.6.1.4.1.5923.1.1.1.4

Application utility class: standard; *# of values*: multi

Definition

The distinguished name (DN) of the directory entries representing the person's Organizational Unit(s).

Permissible values (if controlled)

Notes

With a distinguished name, the client can do an efficient lookup in the institution's directory for information about the person's organizational unit(s).

Semantics

The directory entry pointed to by this dn should be represented in the X.521(1993) "organizational unit" object class. In addition to organizationalUnitName, this object class has the same optional attribute set as the organization object class:

ou (Organization Unit Name, required}

Optional attributes include:
description
localeAttributeSet
postalAttributeSet
telecommunicationsAttributeSet
businessCategory
seeAlso
searchGuide
userPassword

Note that labeledURI is not included in the above list. We recommend adding the labeledURIObject auxilliary object class to the organization object pointed to by this dn, which endows it with a labeledURI attribute. Some directory servers implement this object class by default. For others, the schema may need to be extended using this definition (using the syntax specified by RFC2252):

```
( 1.3.6.1.4.1.250.3.15 NAME 'labeledURIObject' SUP top AUXILIARY
     MAY labeledURI )
```

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

eduPersonOrgUnitDN: ou=Potions, o=Hogwarts, dc=hsww, dc=wiz

Syntax: CIS; *Indexing*: pres,eq, sub

---

eduPersonPrimaryAffiliation (defined in eduPerson);

OID: 1.3.6.1.4.1.5923.1.1.1.5

Application utility class: standard; *# of values*: single

Definition

Specifies the person's PRIMARY relationship to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary)

Permissible values (if controlled)

faculty, student, staff, alum, member, affiliate, employee

Notes

Appropriate if the person carries at least one of the defined eduPersonAffiliations. The choices of values are the same as for that attribute.

Think of this as the affiliation one might put on the name tag if this person were to attend a general institutional social gathering. Note that the single-valued eduPersonPrimaryAffiliation attribute assigns each person in the directory into one and only one category of affiliation. There are application scenarios where this would be useful.

The list of allowed values in the current version 1.0 of the object class is CERTAINLY incomplete. We felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included as part of post-1.0 versions of eduPerson.

We also deliberately avoided including a value such as "other" or "misc" because it is semantically equivalent to "none of the above." To indicate "none of the above," for a specific person, leave the attribute unpopulated.

"member" is intended to include faculty, staff, student, and other persons granted a basic set of privileges that go with membership in the university community (e.g., library privileges). It could be glossed as "member in good standing of the university community."

"affiliate" is intended to apply to people with whom the university has dealings, but to whom no general set of "community membership" privileges are extended.

Semantics

Each institution decides the criteria for membership in each affiliation classification.

A reasonable person should find the listed relationships commonsensical.

Example applications for which this attribute would be useful

directory of directories, controlling access to resources

Example (LDIF fragment)

eduPersonPrimaryAffiliation: student

Syntax: CIS; *Indexing*: pres,eq,sub

---

eduPersonPrincipalName (defined in eduPerson); *OID*: 1.3.6.1.4.1.5923.1.1.1.6

Application utility class: standard; *# of values*: single

Definition

The "NetID" of the person for the purposes of inter-institutional authentication. Should be stored in the form of user@univ.edu, where univ.edu is the name of the local security domain.

Permissible values (if controlled)

Notes

If populated, the user should be able to authenticate with this identifier, using locally operated services. Local authentication systems should be able to adequately affirm (to both local and remote applications) that the authenticated principal is the person to whom this identifier was issued.

The initial intent is to use this attribute within the Shibboleth project, http://middleware.internet2.edu/shibboleth. However, it has quickly become clear that a number of other applications could also make good use of this attribute (e.g. H.323 video, chat software, etc). eduPersonPrincipalName (EPPN) would be used as follows: A resource owner, A, would look at B's directory entry to discover B's EPPN. A would then tell the local authorization system that B's EPPN is allowed to use the resource. When B tries to access the resource, the application (or access control infrastructure) would validate B's identity, check with the local authorization system to ensure that B has been granted the appropriate access privileges, and then either grant or deny access.

EPPN looks like a Kerberos identifier (principal@realm). A site might choose to locally implement EPPN as Kerberos principals. However, this is not a requirement. A site can choose to do authentication in any way that is locally acceptable. Over time, many sites are expected to be using PKI for authentication; however, they may still be specifying identity in EPPN format.

Likewise, EPPN should NOT be confused with the user's published email address, although the two values may be the same. Some sites have chosen to make the user portion of email addresses and security principals the same character string; other sites have chosen not to do this. Even when they appear to be the same, they are used in different subsystems and for different purposes, and there is no requirement that they have to remain the same.

The uid attribute of the user's object within the local white pages directory may also contain a login id, a security principal; some systems (eg NDS) may put a login id in the cn attribute. These attributes are defined within objectclasses that are universal. Unfortunately, their use is not prescribed in a sufficiently precise and consistent manner for use with cross domain authorization. A variety of systems already make conflicting use of these attributes; consequently, we have defined this new attribute.

An assumption is that EPPNs are managed on an enterprise basis by the univ of univ.edu. A particular EPPN is assigned solely to the associated user; it is not a security principal identifier shared by more than one person. Lastly, each EPPN is unique within the local security domain.

How long, if ever, before a formerly assigned EPPN is reassigned to a differrent individual is an institutional decision. Some institutions will choose never to reassign EPPNs. Others may opt for a relatively short hiatus before reassignment. While this complicates the work of the relying parties, it is unavoidable given institutional autonomy. See MACE best practice documents on identifiers for further discussion of these issues.

This attribute should prove useful in creating some applications that are based on currently deployed technologies and on code that does not currently use LDAP or require a PKI. This attribute should help to create a framework to foster interesting inter-institutional collaborations between sites that use different technologies. In short, this attribute provides a foundation for yet another abstraction layer.

It is expected that this attribute may become deprecated in some future version of eduPerson. This would occur as LDAP enabled infrastructures and applications become more mature. One metric of this maturity will be the convergence on best practices and their widespread adoption.

Semantics

Example applications for which this attribute would be useful

controlling access to resources

Example (LDIF fragment)

eduPersonPrincipalName: hputter@hsww.wiz

Syntax: CES; *Indexing*: pres,eq,sub

---

c (defined in X.521(1993)); *OID*: 2.5.4.6

Application utility class: extended; *# of values*: multi

Definition

country name According to RFC 2256, "This attribute contains a two-letter ISO 3166 country code (countryName).

Permissible values (if controlled)

set of ISO 3166 country codes

Notes

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

c: ca

Syntax: CIS; *Indexing*:

---

cn (defined in person); *OID*: 2.5.4.3

Application utility class: core; *# of values*: multi

Definition

Common name.

According to RFC 2256, "This is the X.500 commonName attribute, which contains a name of an object. If the object corresponds to a person, it is typically the person's full name.

Permissible values (if controlled)

Notes

Required. One of the two required attributes in the person object class from which eduPerson derives (the other is sn). As such it is one of eduPerson's three "core application utility" attributes. The third is eduPersonOrgDN.

With eduPersonOrgDN and cn, the client knows the person's name and the distinguished name of the organization with which he/she is assoicated. The latter could help them find a directory entry for the person's organization.

Semantics

Example applications for which this attribute would be useful

all

Example (LDIF fragment)

cn: Mary Francis Xavier

Syntax: CIS; *Indexing*: pres,eq,sub

---

description (defined in person); *OID*: 2.5.4.13

Application utility class: standard; *# of values*: multi

Definition

Open-ended; whatever the person or the directory manager puts here. According to RFC 2256, "This attribute contains a human-readable description of the object."

Permissible values (if controlled)

Notes

Can be anything. According to RFC 2256, "This attribute contains a human-readable description of the object."

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

description: A jolly good felon

Syntax: CIS; *Indexing*:

---

displayName (defined in inetOrgPerson); *OID*: 2.16.840.1.113730.3.1.241

Application utility class: standard; *# of values*: single

Definition

The name(s) that should appear in white-pages-like applications for this person

From RFC 2798 description: "preferred name of a person to be used when displaying entries."

Permissible values (if controlled)

Notes

Cn (common name) is multi-valued and overloaded to meet the needs of multiple applications. displayName is a better candidate for use in Dod, white pages and configurable email clients.

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages, email client

Example (LDIF fragment)

displayName: Jack Dougherty

Syntax: CIS; *Indexing*:

---

facsimileTelephoneNumber (defined in orgPerson); *OID*: 2.5.4.23

Application utility class: extended; *# of values*: multi

Definition

A fax number for the directory entry. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567"."

Permissible values (if controlled)

Notes

Semantics

A fax number for the directory entry.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

facsimileTelephoneNumber: +44 71 123 4567

Syntax: TEL; *Indexing*:

---

givenName (defined in inetOrgPerson); *OID*: 2.5.4.42

Application utility class: standard; *# of values*: multi

Definition

From RFC 2256 description:" The givenName attribute is used to hold the part of a person's name which is not their surname nor middle name."

Permissible values (if controlled)

Notes

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

givenName: Stephen

Syntax: CIS; *Indexing*: pres,eq,sub

---

homePhone (defined in inetOrgPerson); *OID*: 0.9.2342.19200300.100.1.20

Application utility class: extended; *# of values*: multi

Definition

From RFC 1274 description: "The [homePhone] attribute type specifies a home telephone number associated with a person. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567".

Permissible values (if controlled)

Notes

In RFC 1274, this was originally called homeTelephoneNumber

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

homePhone: +1 608 555 1212

Syntax: TEL; *Indexing*:

---

homePostalAddress (defined in inetOrgPerson);
OID: 0.9.2342.19200300.100.1.39

Application utility class: extended; *# of values*: multi

Definition

From RFC 1274 description: "The Home postal address attribute type specifies a home postal address for an object. This should be limited to up to 6 lines of 30 characters each."

Permissible values (if controlled)

Notes

Semantics

Home address. OrgPerson has a PostalAddress that complements this attribute

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

homePostalAddress: 1212 Como Ave.$Midton, SD 45621

Syntax: CIS; *Indexing*:

---

initials (defined in inetOrgPerson); *OID*: 2.5.4.43

Application utility class: extended; *# of values*: multi

Definition

From RFC 2256 description: "The initials attribute contains the initials of some or all of an individuals names, but not the surname(s)."

Permissible values (if controlled)

Notes

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

initials: f x

Syntax: CIS; *Indexing*:

---

jpegPhoto (defined in inetOrgPerson); *OID*: 0.9.2342.19200300.100.1.60

Application utility class: extended; *# of values*: multi

Definition

Follow inetOrgPerson definition of RFC 2798: "Used to store one or more images of a person using the JPEG File Interchange Format [JFIF]."

Permissible values (if controlled)

Notes

A smallish photo in jpeg format.

Semantics

A smallish photo in jpeg format.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

Syntax: ; *Indexing*:

---

l (defined in orgPerson); *OID*: 2.5.4.7

Application utility class: extended; *# of values*: multi

Definition

locality name.

According to RFC 2256, "This attribute contains the name of a locality, such as a city, county or other geographic region (localityName".

X.520(2000) reads: "The Locality Name attribute type specifies a locality. When used as a component of a directory name, it identifies a geographical area or locality in which the named object is physically located or with which it is associated in some other important way.

Permissible values (if controlled)

Notes

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

l: Hudson Valley

Syntax: CIS;   *Indexing*: pres,eq,sub

---

labeledURI (defined in inetOrgPerson);   *OID*: 1.3.6.1.4.1.250.1.57

Application utility class: extended;   *# of values*: multi

Definition

Follow inetOrgPerson definition of RFC 2079: "Uniform Resource Identifier with optional label."

Permissible values (if controlled)

Notes

Commonly a URL for a web site associated with this person. Good candidate for a self-maintained attribute. Note, however, that the vocabulary for the label portion of the value is not standardized.

Note from RFC 2079: "The labeledURI attribute type has the caseExactString syntax (since URIs are case-sensitive) and it is multivalued. Values placed in the attribute should consist of a URI (at the present time, a URL) optionally followed by one or more space characters and a label. Since space characters are not allowed to appear un-encoded in URIs, there is no ambiguity about where the label begins. At the present time, the URI portion must comply with the URL specification.

Multiple labeledURI values will generally indicate different resources that are all related to the X.500 object, but may indicate different locations for the same resource.

The label is used to describe the resource to which the URI points, and is intended as a friendly name fit for human consumption. This document does not propose any specific syntax for the label part. In some cases it may be helpful to include in the label some indication of the kind and/or size of the resource referenced by the URI.

Note that the label may include any characters allowed by the caseExactString syntax, but that the use of non-IA5 (non-ASCII) characters is discouraged as not all directory clients may handle them in the same manner. If non-IA5 characters are included, they should be represented using the X.500 conventions, not the HTML conventions (e.g., the character that is an "a" with a ring above it should be encoded using the T.61 sequence 0xCA followed by an "a" character; do not use the HTML escape sequence "&aring").

Examples of labeledURI Attribute Values

An example of a labeledURI attribute value that does not include a label:

ftp://ds.internic.net/rfc/rfc822.txt

An example of a labeledURI attribute value that contains a tilde character in the URL (special characters in a URL must be encoded as specified by the URL document [1]). The label is "LDAP Home Page":

http://www.umich.edu/%7Ersug/ldap/ LDAP Home Page

Another example. This one includes a hint in the label to help the user realize that the URL points to a photo image.

http://champagne.inria.fr/Unites/rennes.gif Rennes [photo]"

Semantics

Most commonly a URL for a web site associated with this person

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

labeledURI: http://www.hsww.wiz/%7Eputter Harry's home page

Syntax: CIS; *Indexing*:

---

mail (defined in inetOrgPerson); *OID*: 0.9.2342.19200300.100.1.3

Application utility class: standard; *# of values*: multi

Definition

Follow inetOrgPerson definition of RFC 1274: "The [mail] attribute type specifies an electronic mailbox attribute following the syntax specified in RFC 822. Note that this attribute should not be used for greybook or other non-Internet order mailboxes."

Permissible values (if controlled)

Notes

Preferred address for the "to:" field of email to be sent to this person. nowadays usually of the form localid@univ.edu. Likely only one value.

Some mail cllents will not display entries unless the mail attribute is populated. See the LDAP Recipe for further guidance on email addresses, routing, etc. http://www.georgetown.edu/giia/internet2/ldap-recipe/

Note: RFC 1274 uses the longer name 'rfc822Mailbox' and syntax OID of 0.9.2342.19200300.100.3.5. All recent LDAP documents and most deployed LDAP implementations refer to this attribute as 'mail' and define the IA5 String (ASCII string) syntax using using the OID 1.3.6.1.4.1.1466.115.121.1.26, as is done here.

Semantics

Preferred address for the "to:" field of email to be sent to this person

Example applications for which this attribute would be useful

directory of directories, white pages, email client

Example (LDIF fragment)

mail: dumbledore@hsww.wiz

Syntax: CIS; *Indexing*: pres,eq,sub

---

mobile (defined in inetOrgPerson); *OID*: 0.9.2342.19200300.100.1.41

Application utility class: extended; *# of values*: multi

Definition

Follow inetOrgPerson definition of RFC 1274: "The [mobile] attribute type specifies a mobile telephone number associated with a person. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567"."

Permissible values (if controlled)

Notes

cellular or mobile phone number

RFC 1274 uses the longer name 'mobileTelephoneNumber'.

Semantics

cellular or mobile phone number

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

mobile: +47 22 44 66 88

Syntax: TEL; *Indexing*:

---

o (defined in X.521(1993)); *OID*: 2.5.4.10

Application utility class: standard; *# of values*: multi

Definition

Standard name of the top-level organization (institution) with which this person is associated.

Permissible values (if controlled)

Notes

Likely only one value.

Meant to carry the TOP-LEVEL organization name. Do not use this attribute to carry school college names.

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

o: St. Cloud State

Syntax: ; *Indexing*:

---

ou (defined in X.521(1993)); *OID*: 2.5.4.11

Application utility class: standard; *# of values*: multi

Definition

Organizational unit(s). According to X.520(2000), "The Organizational Unit Name attribute type specifies an organizational unit. When used as a component of a directory name it identifies an organizational unit with which the named object is affiliated.

The designated organizational unit is understood to be part of an organization designated by an OrganizationName [o] attribute. It follows that if an Organizational Unit Name attribute is used in a directory name, it must be associated with an OrganizationName [o] attribute.

An attribute value for Organizational Unit Name is a string chosen by the organization of which it is a part."

Permissible values (if controlled)

Notes

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

ou: Faculty Senate

Syntax: CIS; *Indexing*: pres,eq,sub

---

pager (defined in inetOrgPerson); *OID*: 0.9.2342.19200300.100.1.42

Application utility class: extended; *# of values*: multi

Definition

Follow inetOrgPerson definition of RFC 1274: "The [pager] attribute type specifies a pager telephone number for an object. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567"."

Permissible values (if controlled)

Notes

RFC 1274 uses the longer name 'pagerTelephoneNumber'.

Semantics

pager number

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

pager: +1 202 555 4321

Syntax: TEL; *Indexing*:

---

postalAddress (defined in orgPerson); *OID*: 2.5.4.16

Application utility class: extended; *# of values*: multi

Definition

Campus or office address. inetOrgPerson has a homePostalAddress that complements this attribute. X.520(2000) reads: "The Postal Address attribute type specifies the address information required for the physical postal delivery to an object."

Permissible values (if controlled)

Notes

Campus or office address. inetOrgPerson has a homePostalAddress that complements this attribute

Semantics

Campus or office address. X.520(2000) reads: "The Postal Address attribute type specifies the address information required for the physical postal delivery to an object."

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

postalAddress: P.O. Box 333$Whoville, WH 99999

Syntax: CIS;   *Indexing*:

---

postalCode (defined in orgPerson);   *OID*: 2.5.4.17

Application utility class: extended;   *# of values*: multi

Definition

Follow X.500(2000): "The postal code attribute type specifies the postal code of the named object. If this attribute value is present, it will be part of the object's postal address." Zip code in USA, postal code for other countries.

Permissible values (if controlled)

Notes

ZIP code in USA, postal code for other countries.

Semantics

Zip code in USA, postal code for other countries.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

postalCode: 54321

Syntax: CIS;   *Indexing*:

---

postOfficeBox (defined in orgPerson);   *OID*: 2.5.4.18

Application utility class: extended;   *# of values*: multi

Definition

Follow X.500(2000): "The Post Office Box attribute type specifies the Postal Office Box by which the object will receive physical postal delivery. If present, the attribute value is part of the object's postal address."

Permissible values (if controlled)

Notes

Follow X.500(2000): "The Post Office Box attribute type specifies the Postal Office Box by which the object will receive physical postal delivery. If present, the attribute value is part of the object's postal address."

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

postOfficeBox: 109260

Syntax: CIS; *Indexing*:

---

preferredLanguage (defined in inetOrgPerson); *OID*: 2.16.840.1.113730.3.1.39

Application utility class: extended; *# of values*: single

Definition

Follow inetOrgPerson definition of RFC 2798: "preferred written or spoken language for a person'"

Permissible values (if controlled)

Notes

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

preferredLanguage: Esperanto

Syntax: CIS; *Indexing*:

---

seeAlso (defined in person); *OID*: 2.5.4.34

Application utility class: standard; *# of values*: multi

Definition

Follow person object class definition: Identifies (by DN) another directory server entry that may contain information related to this entry.

According to X.520(2000), "The See Also attribute type specifies names of other Directory objects which may be other aspects (in some sense) of the same real world object."

Permissible values (if controlled)

Notes

Semantics

The distinguished name of another directory entry

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

seeAlso: cn=Department Chair, ou=physics, o=University of Technology, dc=utech, dc=ac, dc=uk

Syntax: ; *Indexing*:

---

sn (defined in person); *OID*: 2.5.4.4

Application utility class: core; *# of values*: multi

Definition

Surname or family name. According to RFC 2256, "This is the X.500 surname attribute, which contains the family name of a person."

Permissible values (if controlled)

Notes

Required. One of the two required attributes in the person object class from which eduPerson derives (the other is cn). As such it is one of eduPerson's three "core application utility" attributes. The third is eduPersonOrgDN.

If the person has a multi-part surname (whether hyphenated or not), store each component as a separate value in this multi-valued attribute. That yields the best results for the broadest range of clients doing name searches.

Semantics

Example applications for which this attribute would be useful

all

Example (LDIF fragment)

sn: Carson

Syntax: CIS; *Indexing*: pres,eq,sub

---

st (defined in orgPerson); *OID*: 2.5.4.8

Application utility class: extended; *# of values*: multi

Definition

Abbreviation for state name
Format: Standard U.S. postal service two-letter code.

According to RFC 2256, "This attribute contains the full name of a state or province (stateOrProvinceName)."

Permissible values (if controlled)

U.S. Postal Service set of two-letter state name abbreviations

Notes

State or province name. While RFC 2256 specifies use of the "full name," it is customary to use the U.S. Postal Service set of two-letter state name abbreviations for states in the U.S.

Semantics

Standard two-letter abbreviations for U.S. state names

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

st: IL

Syntax: CIS;   *Indexing*:

---

street (defined in orgPerson);   *OID*: 2.5.4.9

Application utility class: extended;   *# of values*: multi

Definition

According to RFC 2256, "This attribute contains the physical address of the object to which the entry corresponds, such as an address for package delivery (streetAddress)."

Permissible values (if controlled)

Notes

Semantics

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF fragment)

street: 303 Mulberry St.

Syntax: CIS;   *Indexing*:

---

telephoneNumber (defined in person);   *OID*: 2.5.4.20

Application utility class: standard;   *# of values*: multi

Definition

Office/campus phone number. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567"."

Permissible values (if controlled)

Notes

Semantics

Example applications for which this attribute would be useful

directory of directories,   white pages

Example (LDIF fragment)

telephoneNumber: +1 212 555 1234

Syntax: TEL; *Indexing*:

---

uid (defined in inetOrgPerson); *OID*: 0.9.2342.19200300.100.1.1

Application utility class: standard; *# of values*: multi

Definition

Follow inetOrgPerson definition of RFC 1274: "The [uid] attribute type specifies a computer system login name."

Permissible values (if controlled)

Notes

Likely only one value. See the extensive discussion in the "LDAP Recipe" http://www.georgetown.edu/giia/internet2/ldap-recipe/

A number of off-the-shelf directory-enabled applications make use of this inetOrgPerson attribute, not always consistently.

RFC 1274 uses the longer name 'userid'.

Semantics

Example applications for which this attribute would be useful

controlling access to resources

Example (LDIF fragment)

uid: gmettes

Syntax: ; *Indexing*:

---

userCertificate (defined in inetOrgPerson); *OID*: 2.5.4.36

Application utility class: extended; *# of values*: multi

Definition

A user's X.509 certificate

Permissible values (if controlled)

Notes

RFC 2256 states that this attribute is to be stored and requested in the binary form, as 'userCertificate;binary'.

Semantics

Following userSMIMECertificate in RFC 2798, "A PKCS#7 [RFC2315] SignedData"

Example applications for which this attribute would be useful

email clients, controlling access to resources

Example (LDIF fragment)

Syntax: ; *Indexing*:

---

userSMIMECertificate (defined in inetOrgPerson);
OID: 2.16.840.1.113730.3.1.40

Application utility class: extended; *# of values*: multi

Definition

An X.509 certificate specifically for use in S/MIME applications (see RFCs 2632, 2633 and 2634)..

Permissible values (if controlled)

Notes

An X.509 certificate specifically for use in S/MIME applications. According to RFC 2798, "If available, this attribute is preferred over the userCertificate attribute for S/MIME applications."

RFC 2256 states that this attribute is to be stored and requested in the binary form, as 'userCertificate;binary'.

Semantics

Following userSMIMECertificate in RFC 2798, "A PKCS#7 [RFC2315] SignedData"

Example applications for which this attribute would be useful

email clients

Example (LDIF fragment)

Syntax: ; *Indexing*: