□

Document: Internet2-mace-dir-eduPerson-200312
December, 2003

Internet2 Middleware Architecture Committee
for Education, Directory Working Group
(MACE-Dir)

□

Comments to: nmi-support@nsf-middleware.org

EduPerson Specification (200312)

For the first time with this (200312) version, the eduPerson specification document contains both an auxiliary object class definition for LDAP directories and a new section for eduPerson attributes that are not included in the eduPerson auxiliary object class. In this version, there is but one attribute in the latter category, eduPersonTargetedID. EduPersonTargetedID is intended primarily to support the operation of federated identity management systems such as Shibboleth (http://shibboleth.internet2.edu). The first section below contains the object class definition in the same format as the (200210) version of this specification. It is followed by the new section containing eduPersonTargetedID.

EduPerson Object Class Specification (200312)

Status of this document

The (200312) version of the eduPerson object class specification is described in this document. This version is appropriate for adoption in a production enterprise directory service environment.

Introduction

EduPerson is an auxiliary object class for campus directories designed to facilitate communication among higher education institutions. It consists of a set of data elements or attributes about individuals within higher education, along with recommendations on the syntax and semantics of the data that may be assigned to those attributes. The

eduPerson attributes are found in the next section. All these attribute names are prefaced with eduPerson. The eduPerson auxiliary object class contains all of them as “MAY” attributes:

(1.3.6.1.4.1.5923.1.1.2

NAME 'eduPerson'

AUXILIARY

MAY (eduPersonAffiliation $ eduPersonNickname $

eduPersonOrgDN $ eduPersonOrgUnitDN $

eduPersonPrimaryAffiliation $ eduPersonPrincipalName $

eduPersonEntitlement $ eduPersonPrimaryOrgUnitDN $

eduPersonScopedAffiliation

□

)

It is recommended that person entries have the person, organizationalPerson and inetOrgPerson object classes defined. The former two are defined in X.521 (2001) and inetOrgPerson is defined in RFC 2798 and based in part on RFC2256. EduPerson attributes would be brought in to the person entry as appropriate from the auxiliary eduPerson object class. This represents a change from eduPerson 1.0 where the object class was defined as structural, and inherited from other person classes. Sites that have implemented eduPerson 1.0 should not experience any operational difficulties due to the object class difference between structural and auxiliary. If, however, one were to export an ldif file of person entries from an eduPerson 1.0-based directory, the ldif would have to be tweaked before being imported into a directory implementing the current version, 200312 to add the person, orgPerson and inetOrgPerson object classes to the entry.

Upgrading the schema from the previous version of eduPerson, 200210, to this version, 200312, should not require reworking of existing directory contents.

Attributes from the person, organizationalPerson and inetOrgPerson classes are listed alphabetically in the second section of this document. The purpose of listing them is primarily as a convenience to enterprise directory designers, but in some cases notes were added to clarify aspects of meaning or usage in the education community beyond what can be found in the original standards documents.

If widespread agreement and implementation of this object class in campus directories is achieved, a broad and powerful new class of higher education applications can be deployed. Additional information on eduPerson including LDIF for implementing the object class and attributes, is available at its home on the web: http://www.educause.edu/eduperson.

Attributes in the following section were newly defined for eduPerson. Each entry specifies the version in which the attribute was first defined.

---

1. **eduPersonAffiliation** (defined in eduPerson 1.0); *OID:* 1.3.6.1.4.1.5923.1.1.1.1

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.1

NAME 'eduPersonAffiliation'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseIgnoreMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

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 eduPersonPrimary Affiliation, that value should be stored here as well.

The list of allowed values in the current version 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 later 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: directoryString; *Indexing:* pres,eq

2. eduPersonEntitlement (defined in eduPerson 200210); *OID:* 1.3.6.1.4.1.5923.1.1.1.7

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.7

NAME 'eduPersonEntitlement'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseIgnoreMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

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

Definition

URI (either URN or URL) that indicates a set of rights to specific resources.

Notes

A simple example would be a URL for a contract with a licensed resource provider. When a principal's home institutional directory is allowed to assert such entitlements, the business rules that evaluate a person's attributes to determine eligibility are evaluated there. The target resource provider does not learn characteristics of the person beyond their entitlement. The trust between the two parties must be established out of band. One check would be for the target resource provider to maintain a list of subscribing institutions. Assertions

of entitlement from institutions not on this list would not be honored. See the first example below.

URN values would correspond to a set of rights to resources based on an agreement across the relevant community. MACE (Middleware Architecture Committee for Education) affiliates may opt to register with MACE as a naming authority, enabling them to create their own URN values. See the second example below.

The driving force behind the definition of this attribute has been the MACE Shibboleth project. Shibboleth defines an architecture for inter-institutional sharing of web resources subject to access controls. For further details, see the project's web pages at http://shibboleth.internet2.edu/.

Examples:

eduPersonEntitlement: http://xstor.com/contracts/HEd123

eduPersonEntitlement: urn:mace:washington.edu:confocalMicroscope

Example applications for which this attribute would be useful

controlling access to resources

Example (LDIF Fragment)

eduPersonEntitlement: urn:mace:washington.edu:confocalMicroscope

Syntax: directoryString;

3. eduPersonNickname (defined in eduPerson 1.0); *OID:* 1.3.6.1.4.1.5923.1.1.1.2

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.2

NAME 'eduPersonNickname'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseIgnoreMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

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

Definition

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

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 If it were merely one of the multiple values of the cn attribute, this would be harder to do. A review step by a responsible adult is advisable to help avoid institutionally embarrasing values being assigned to this attribute by would-be malefactors!

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

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

eduPersonNickname: Spike

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

4. eduPersonOrgDN (defined in eduPerson 1.0); *OID:* 1.3.6.1.4.1.5923.1.1.1.3

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.3

NAME 'eduPersonOrgDN'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY distinguishedNameMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.12' SINGLE-VALUE)

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.

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(2001) "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 auxiliary 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: distinguishedName; *Indexing:* None recommended

5. eduPersonOrgUnitDN (defined in eduPerson 1.0); *OID:* 1.3.6.1.4.1.5923.1.1.1.4

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.4

NAME 'eduPersonOrgUnitDN'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY distinguishedNameMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.12')

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

Definition

The distinguished name(s) (DN) of the directory entries representing the person's Organizational Unit(s). May be multivalued, as for example, in the case of a faculty member with appointments in multiple departments or a person who is a student in one department and an employee in another.

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(2001) "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) Note that O is NOT 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 auxiliary 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: distinguishedName; *Indexing:* eq

6. eduPersonPrimaryAffiliation (defined in eduPerson 1.0);

OID: 1.3.6.1.4.1.5923.1.1.1.5

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.5

NAME 'eduPersonPrimaryAffiliation'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseIgnoreMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE)

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 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 future 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: directoryString; *Indexing:* pres,eq,sub

7. eduPersonPrimaryOrgUnitDN (defined in eduPerson 200210); *OID:* 1.3.6.1.4.1.5923.1.1.1.8

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.8

NAME 'eduPersonPrimaryOrgUnitDN'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY distinguishedNameMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.12' SINGLE-VALUE)

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

Definition

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

Notes

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

Semantics

Each institution populating this attribute decides the criteria for determining which organization unit entry is the primary one for a given individual.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

eduPersonPrimaryOrgUnitDN: ou=Music Department, o=Notre Dame, dc=nd, dc=edu

Syntax: distinguishedName; *Indexing:* eq

8. eduPersonPrincipalName (defined in eduPerson 1.0); *OID:* 1.3.6.1.4.1.5923.1.1.1.6

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.6

NAME 'eduPersonPrincipalName'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseIgnoreMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE)

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.

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://shibboleth.internet2.edu/. 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.

Example applications for which this attribute would be useful

controlling access to resources

Example (LDIF Fragment)

eduPersonPrincipalName: hputter@hsww.wiz

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

9. **eduPersonScopedAffiliation** (defined in eduPerson (200312)); *OID:* 1.3.6.1.4.1.5923.1.1.1.9

RFC 2252 definition

(1.3.6.1.4.1.5923.1.1.1.9

NAME 'eduPersonScopedAffiliation'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseIgnoreMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

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

Definition

Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc. The values consist of a left and right component separated by an "@" sign. The left component is one of the values from the eduPersonAffiliation controlled vocabulary. The right component identifies the security domain in the form of a dotted string value on the model of DNS domain names. This right-hand side syntax of eduPersonScopedAffiliation intentionally matches that used for the right-hand side values for eduPersonPrincipalName since both identify a security domain.

Permissible values (if controlled)

See controlled vocabulary for eduPersonAffiliation. Only these values are allowed to the left of the "@" sign. The values to the right of the "@" sign should be a dotted string.

Notes

Consumers of eduPersonScopedAffiliation will have to decide whether or not they trust values of this attribute. In the general case, the directory carrying the eduPersonScopedAffiliation is not the ultimate authoritative speaker for the truth of the assertion. Trust must be established out of band with respect to exchanges of this attribute value.

Semantics

An eduPersonScopedAffiliation value of "x@y" is to be interpreted as an assertion that the person in whose entry this value occurs holds an affiliation of type "x" within the security domain "y."

Example applications for which this attribute would be useful

directory of directories, white pages,

controlling access to resources

Example (LDIF Fragment)

eduPersonAffiliation: faculty@cs.berkeley.edu

Syntax: directoryString; *Indexing:* pres,eq

The attributes in the following section are from other standard object classes or attribute definitions. It is not a complete list of such attributes, but in any case where the eduPerson working group considered that some comment was needed to clarify the meaning or utility of an attribute, it can be found here. For details on the syntax and other aspects of these attributes, see the appropriate standards documents.

---

10. audio (defined in inetOrgPerson); *OID:* 0.9.2342.19200300.100.1.55

Application utility class: no recommendation;

Definition

RFC 1274 notes that the proprietary format they recommend is "interim" only.

Notes

Avoid. Not clearly defined, no defacto standard.

---

11. cn (commonName, 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."

Notes

Required. One of the two required attributes in the person object class (the other is sn). As such it is one of three recommended "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.

This attribute is often overloaded in the sense that many applications act as if this were "their" attribute, and therefore add values to this attribute as they see fit. Because of that it is impossible to give a precise and accurate definition of what this field means.

Example applications for which this attribute would be useful

all

Example (LDIF Fragment)

cn: Mary Francis Xavier

---

12. 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."

Notes

Can be anything.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

description: A jolly good felon

---

13. 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."

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.

Example applications for which this attribute would be useful

directory of directories, white pages, email client

Example (LDIF Fragment)

displayName: Jack Dougherty

---

14. 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."

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

---

15. 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."

Example applications for which this attribute would be useful

Example (LDIF Fragment)

givenName: Stephen

---

16. 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."

Notes

In RFC 1274, this was originally called homeTelephoneNumber.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

homePhone: +1 608 555 1212

---

17. 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."

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

---

18. 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)."

Example applications for which this attribute would be useful

Example (LDIF Fragment)

initials: f x

---

19. 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]."

Semantics

A smallish photo in jpeg format.

Example applications for which this attribute would be useful

directory of directories, white pages

---

20. l (localityName, 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."

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

l: Hudson Valley

---

21. 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."

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

---

22. 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."

Notes

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

Some mail clients will not display entries unless the mail attribute is populated. See the LDAP Recipe for further guidance on email addresses, routing, etc. (http://middleware.internet2.edu/dir/rpr-nmi-edit-mace_dir-ldap_recipe.2.0.html).

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.

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

---

23. manager (defined in inetOrgPerson); *OID:* 0.9.2342.19200300.100.1.10

Application utility class: no recommendation; *# of values:* multi

Definition

Follow inetOrgPerson definition which refers to RFC 1274: "The manager attribute type specifies the manager of an object represented by an entry." The value is a DN.

Notes

This attribute carries the DN of the manager of the person represented in this entry.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

manager: uid=twilliams, ou=people, dc=hobart dc=edu

---

24. 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."

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

---

25. o (organizationName, defined in inetOrgPerson); *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.

Notes

Likely only one value.

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

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

o: St. Cloud State

---

26. ou (organizationalUnitName, defined in inetOrgPerson); *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."

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

ou: Faculty Senate

---

27. 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."

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

---

28. 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."

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

---

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

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

Definition

Follow X.500(2001): "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.

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

---

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

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

Definition

Follow X.500(2001): "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."

Notes

Follow X.500(2001): "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."

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

postOfficeBox: 109260

---

31. 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)

See RFC2068 and ISO 639 for allowable values in this field. Esperanto, for example is EO in ISO 639, and

RFC2068 would allow a value of en-US for US English.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

preferredLanguage: EO

---

32. 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."

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

---

33. sn (surname, 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."

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.

Example applications for which this attribute would be useful

all

Example (LDIF Fragment)

sn: Carson

---

34. st (stateOrProvinceName, defined in orgPerson); *OID:* 2.5.4.8

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

Definition

Abbreviation for state or province name.

Format: The values should be coordinated on a national level and if well-known shortcuts exist - like the two-letter state abbreviations in the US – these abbreviations are preferred over longer full names.

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

Permissible values (if controlled)

For states in the United States, 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. and, as noted in the definition, other nationally coordinated official abbreviations are preferred for province names.

Semantics

Standard two-letter abbreviations for U.S. state names, other standards based abbreviations for provinces where available.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

st: IL

---

35. 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)."

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

street: 303 Mulberry St.

---

36. 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."

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

telephoneNumber: +1 212 555 1234

---

37. title (defined in orgPerson); *OID:* 2.5.4.12

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

Definition

Follow X.520(2001): "The Title attribute type specifies the designated position or function of the object within an organization."

Notes

No controlled vocabulary, may contain anything.

Example applications for which this attribute would be useful

directory of directories, white pages

Example (LDIF Fragment)

title: Assistant Vice-Deputy for Redundancy Reduction

---

38. 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."

Notes

Likely only one value. See the extensive discussion in the "LDAP Recipe" (http://middleware.internet2.edu/dir/rpr-nmi-edit-mace_dir-ldap_recipe.2.0.html).

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'.

Example applications for which this attribute would be useful

controlling access to resources

Example (LDIF Fragment)

uid: gmettes

---

39. uniqueIdentifier (defined in none); *OID:* 0.9.2342.19200300.100.1.44

Application utility class: no recommendation; *# of values:*

Definition

Follows definition of RFC1274: "Specifies a 'unique identifier' for an object represented in the directory."

Notes

Avoid. UniqueIdentifier should not be reused because 1) it is not included in any of the commonly implemented object classes and 2) iPlanet documentation states that its valus is "assigned by the server." Relying on it for other purposes would be overloading of intended uses, something we avoid on principle since iPlanet is a commonly used directory server.

---

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

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

Definition

A user's X.509 certificate

Notes

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

Note that userSMIMECertificate is in binary syntax (1.3.6.1.4.1.1466.115.121.1.5) whereas the userCertificate attribute is in certificate syntax (1.3.6.1.4.1.1466.115.121.1.8).

Example applications for which this attribute would be useful

email clients, controlling access to resources

---

41. userPassword (defined in person); *OID:* 2.5.4.35

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

Definition

This attribute identifies the entry's password and encryption method in the following format:

{encryption method}encrypted password.

Notes

The user pw is hidden, and is used in the bind operation in LDAP. The bind operation must be done over SSL to avoid sending clear text passwords over the wire or through the air.

Example applications for which this attribute would be useful

controlling access to resources

---

42. 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).

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 2798 states that this attribute is to be stored and requested in the binary form, as 'userSMIMECertificate;binary.'

Semantics

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

Example applications for which this attribute would be useful

email clients

---

43. x500uniqueIdentifier (defined in inetOrgPerson); *OID:* 2.5.4.45

Application utility class: no recommendation; *# of values:*

Definition

Defined originally in X.509(96) and included in RFC2256.

Notes

Avoid. X500UniqueIdentifier syntax is specified as bit string, and that is not likely to be a good fit for many of the institutional attribute value choices, especially as part of the DN.

□

Other eduPerson Attribute Definitions

1. eduPersonTargetedID (defined in eduPerson 200312); *OID:* 1.3.6.1.4.1.5923.1.1.1.10

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

Definition

A persistent, privacy-preserving identifier for a principal shared between a pair of coordinating entities, denoted by the Liberty Alliance architecture overview [1] as identity provider and service provider, and by the Shibboleth architecture document as an origin site and a target application [2]. An identity provider uses the appropriate value of this attribute when communicating with a particular service provider, and does not reveal that value to any other service provider except in limited circumstances.

A given value is intended only for consumption by a specific requester, and may be derived from some function over the requester's identity and other principal-specific input(s). It might not itself be stored by the identity provider, but usually is in order to support changes to or revocation of the value. It should be considerably difficult for an observer to guess the value that would be returned to any given requester, even given knowledge of the principal-specific input(s) to that value.

This attribute is typically used to represent a long-term account linking relationship between an identity provider and a service provider. Note that such a service provider might itself also be an identity provider.

[1] http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf

[2] http://shibboleth.internet2.edu

Example applications for which this attribute would be useful

Shibboleth targets with need to maintain a persistent but opaque identifier for a given user for purposes of personalization or record-keeping.

Change Log

This section lists the changes that have been made from version to version of eduPerson. The first list below shows changes in the current version (200312) relative to the previous version (200210).

1. EduPersonScopedAffiliation added.
2. Substring indexing recommendation removed from eduPersonAffiliation
3. New section added for attributes not included in the eduPerson object class. Includes one attribute in this version: eduPersonTargetedID.
4. Introduction altered to include description of this new section.

The following lists the changes (other than typographical corrections) that were made between version 1.0 of the eduPerson object class definition and version 200210.

1. Document Status and Introductory sections have been added.
2. Attention called to the change of the eduPerson object class from structural to auxiliary
3. Subsection headings for empty fields deleted..
4. Indexing recommendations for the eduPerson attributes has been improved and corrected in many cases.
5. The syntax notes for the eight eduPerson attributes have been corrected and they now match the LDIF file. DirectoryString is used for five eduPerson attributes. The other three contain distinguished names, so they use distinguishedName syntax.
6. RFC2252 style definitions have been included for the eduPerson object class itself and for each of the eduPerson attributes.
7. Two new attributes are defined: eduPersonEntitlement and eduPersonPrimaryOrgUnitDN.
8. The notes on the c (country) attribute have been deleted since c is not contained in any of the referenced object classes.
9. Notes have been added for several additional attributes from the standard person object classes. These include audio, manager, title, uniqueIdentifier and x500UniqueIdentifier.
10. Notes on userCertificate and userSMIMECertificate have been rewritten.

Acknowledgments

MACE members and others who contributed many hours to the definition of this object class include Rob Banz, Tom Barton, Brendan Bellina, Scott Cantor, Steven Carmody, Michael Gettes, Paul Hill, Ken Klingenstein, RL"Bob" Morgan, Todd Piket, David Wasley and Ann West. The editor of the MACE-Dir working group, Keith Hazelton, would like to thank them and the many others who helped bring this effort to completion. This version also had the benefit of comments from several of the NMI Testbed institutions. Three that deserve special mention are Georgia State University, the University of Alabama at Birmingham and the University of Michigan. Special thanks to Internet2 staff members for their invaluable assistance, Ben Chinowsky, Renee Frost, Lisa Hogeboom, Nate Klingenstein, Steve Olshansky and Ellen Vaughan.

This material is based in whole or in part on work supported by the National Science Foundation under the NSF Middleware Initiative - NSF 02-028, Grant No. ANI-0123937. The MACE-Dir working group (http://middleware.internet2.edu/dir/) gratefully acknowledges the support of Internet2 and NSF. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).