eduPerson 2012-03

Document: internet2-mace-dir-eduperson-201203 Home: https://wiki.refeds.org/pages/viewpage.action?pageId=38895716	Internet2 Middleware Architecture Committee for Education, Directory Working Group (MACE-Dir)
Released: April 23, 2012	
Copyright © 2012 by Internet2 and/or the respective authors	Comments to: schema-discuss@lists.refeds.org

eduPerson Object Class Specification (201203)

Status of this document

The (201203) 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.

0. Table of Contents

1. Introduction
1.1. General Remarks
1.2. Identifier Concepts
1.3. Scope
2. eduPerson Object Class and Attributes
2.1. eduPerson Object Class Definition
2.2. eduPerson Attribute Definitions
2.2.1. eduPersonAffiliation
2.2.2. eduPersonEntitlement
2.2.3. eduPersonNickname
2.2.4. eduPersonOrgDN
2.2.5. eduPersonOrgUnitDN
2.2.6. eduPersonPrimaryAffiliation
2.2.7. eduPersonPrimaryOrgUnitDN
2.2.8. eduPersonPrincipalName
2.2.9. eduPersonScopedAffiliation
2.2.10. eduPersonTargetedID
2.2.11. eduPersonAssurance
3. Comments on Other Common Person Attributes
3.1. audio
3.2. cn (commonName)
3.3. description
3.4. displayName
3.5. facsimileTelephoneNumber
3.6. givenName
3.7. homePhone
3.8. homePostalAddress
3.9. initials
3.10. jpegPhoto
3.11. l (localityName)
3.12. labeledURI
3.13. mail
3.14. manager
3.15. mobile
3.16. o (organizationName)
3.17. ou (organizationalUnitName)
3.18. pager
3.19. postalAddress
3.20. postalCode
3.21. postOfficeBox
3.22. preferredLanguage
3.23. seeAlso
3.24. sn (surname)
3.25. st (stateOrProvinceName)
3.26. street
3.27. telephoneNumber
3.28. title
3.29. uid
3.30. uniqueIdentifier
3.31. userCertificate
3.32. userPassword
3.33. userSMIMECertificate
3.34. x500uniqueIdentifier
4. Change Log

5. References
6. Acknowledgments

1. Introduction

1.1. General Remarks

The portions of the eduPerson specification intended to support LDAP operations include 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.

It is recommended that person entries have the person, organizationalPerson and inetOrgPerson object classes defined. The former two are included in X.521 (2001) and inetOrgPerson is included in RFC2798 and based in part on RFC4512 and RFC4519. EduPerson attributes would be brought into 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 post 1.0 versions to add the person, orgPerson and inetOrgPerson object classes to the entry.

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 more easily 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/.

1.2. Identifier Concepts

Among the most common and useful personal attributes are identifiers. An identifier is an information element that is specifically designed to distinguish each entry from its peers in a particular set. While almost any information in an entry may contribute to differentiating it from similar entries, identifiers are intentionally designed to do this. It is common for entries to contain several different identifiers, used for different purposes or generated by different information sources. Identifiers have a number of characteristics that help to determine appropriate usage. The following comments are offered to help clarify some points of definition for these various identifiers. These concepts are also referred to in various attribute descriptions.

Persistence

Persistence is a measure of the length of time during which an identifier can be reliably associated with a particular principal. A short-term identifier might be associated with an application session. A permanent identifier is associated with its entry for its lifetime.

Privacy

Some identifiers are designed to preserve the principal's privacy and inhibit the ability of multiple unrelated recipients from correlating principal activity by comparing values. Such identifiers are therefore REQUIRED to be opaque, having no particular relationship to the principal's other identifiers. Note that this definition permits sharing of the identifier among multiple recipients if they are deemed by the attribute provider to be equivalent to a single recipient for privacy purposes.

Uniqueness

Unique identifiers are those which are unique within the namespace of the identity provider and the namespace of the service provider(s) for whom the value is created. A globally-unique identifier is intended to be unique across all instances of that attribute in any provider.

Reassignment

Many identifiers do not specifically guarantee that a given value will never be reused. Reuse would mean assigning an identifier value to one principal, and then assigning the same value to a different principal at some point in the (possibly distant) future. There will be some sets of requirements that dictate a strict no reassignment policy.

Human Palatability

An identifier that is human-palatable is intended to be rememberable and reproducible by typical human users, in contrast to identifiers that are, for example, randomly generated sequences of bits.

1.3. Scope

The eduPersonPrincipalName and eduPersonScopedAffiliation attribute definitions found below both make use of the concept of scope. The meaning of scope is specific to the attribute to which it is attached and can vary from one attribute to another. In the case of these two attributes, scope conveys the administrative domain or security domain within which the affiliation or principal name holds.

---

2. eduPerson Object Class and Attributes

2.1. eduPerson Object Class Definition

All eduPerson-defined 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 $

eduPersonTargetedID $

eduPersonAssurance)

)

2.2. eduPerson Attribute Definitions

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

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

RFC4512 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

faculty, student, staff, alum, member, affiliate, employee, library-walk-in

Notes

If there is a value in eduPersonPrimaryAffiliation, that value MUST be asserted here as well.

The primary intended purpose of eduPersonAffiliation is to convey broad-category affiliation assertions between members of an identity federation. Given this inter-institutional context, only values of eduPersonAffiliation with broad consensus in definition and practice will have any practical value. The list of allowed values in the current version of the object class is certainly incomplete, especially in terms of local institutional use. The editors felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included in later versions of eduPerson.

"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., they are given institutional calendar privileges, library privileges and/or vpn accounts). It could be glossed as "member in good standing of the university community."

The "member" affiliation MUST be asserted for people carrying one or more of the following affiliations:

faculty orstaff or
student or
employee

Note: Holders of the affiliation "alum" are not typically "members" since they are not eligible for the full set of institutional privileges enjoyed by faculty, staff and students.

Cautionary note: There are significant differences in practice between identity providers in the way they define faculty, staff and employee and the logical relationships between the three. In particular there are conflicting definitions of "staff" and "employee" from country to country that make those values particularly unreliable in any international context.

The "affiliate" value for eduPersonAffiliation indicates that the holder has some definable affiliation to the university NOT captured by any of faculty, staff, student, employee, alum and/or member. Typical examples might include event volunteers, parents of students, guests and external auditors. There are likely to be widely varying definitions of "affiliate" across institutions. Given that, "affiliate" is of dubious value in federated, inter-institutional use cases.

For the sake of completeness, if for some reason the institution carries digital identity information for people with whom it has no affiliation according to the above definitions, the recommendation is simply not to assert eduPersonAffiliation values for those individuals.

"Library-walk-in:" This term was created to cover the case where physical presence in a library facility grants someone access to electronic resources typically licensed for faculty, staff and students. In recent years the library walk-in provision has been extended to cover other cases such as library users on the campus network, or those using on-campus workstations. Licensed resource providers have often been willing to interpret their contracts with licensees to accept this broader definition of "library-walk-in," though specific terms may vary. For a more direct way of using eduPerson attributes to express library privilege information, see the eduPersonEntitlement value "urn:mace:dir:entitlement:common-lib-terms" as defined in the MACE-Dir Registry of eduPersonEntitlement values http://middleware.internet2.edu/urn-mace/urn-mace-dir-entitlement.html.

The presence of other affiliation values neither implies nor precludes the affiliation "library-walk-in."

It is not feasible to attempt to reach broad-scale, precise and binding inter-institutional definitions of affiliations such as faculty and students. Organizations have a variety of business practices and institutional specific uses of common terms. Therefore each institution will decide the criteria for membership in each affiliation classification. What is desirable is that a reasonable person should find an institution's definition of the affiliation plausible.

Semantics

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

A reasonable person should find the listed relationships plausible.

Example applications for which this attribute would be useful

white pages, controlling access to resources

Example (LDIF Fragment)

eduPersonAffiliation: faculty

Syntax: directoryString;*Indexing:*pres,eq

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

RFC4512 definition

(1.3.6.1.4.1.5923.1.1.1.7

NAME 'eduPersonEntitlement'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseExactMatch

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; *Indexing:*No recommendation

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

RFC4512 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 embarrassing 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

white pages

Example (LDIF Fragment)

eduPersonNickname: Spike

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

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

RFC4512 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 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 RFC4512):

(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

white pages

Example (LDIF Fragment)

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

Syntax: distinguishedName;*Indexing:*No recommendation

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

RFC4512 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 RFC4512):

(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

white pages

Example (LDIF Fragment)

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

Syntax: distinguishedName;*Indexing:*eq

2.2.6. eduPersonPrimaryAffiliation (defined in eduPerson 1.0);

*OID:*1.3.6.1.4.1.5923.1.1.1.5

RFC4512 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

faculty, student, staff, alum, member, affiliate, employee, library-walk-in

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.

See eduPersonAffiliationfor further details.

Example applications for which this attribute would be useful

controlling access to resources

Example (LDIF Fragment)

eduPersonPrimaryAffiliation: student

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

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

RFC4512 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

white pages

Example (LDIF Fragment)

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

Syntax: distinguishedName;*Indexing:*eq

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

RFC4512 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

A scoped identifier for a person. It should be represented in the form "user@scope" where 'user' is a name-based identifier for the person and where 'scope' defines a local security domain. Each value of 'scope' defines a namespace within which the assigned identifiers MUST be unique. Given this rule, if two eduPersonPrincipalName (ePPN) values are the same at a given point in time, they refer to the same person.

Notes

Syntactically, ePPN looks like an email address but is not intended to be a person's published email address or be used as an email address. In general, name-based identifiers tend to be subject to some degree of expected change and/or reassignment.

Values of eduPersonPrincipalName are often, but not required to be, human-friendly, and may change as a result of various business processes. They may also be reassigned after a locally-defined period of dormancy. Applications that require a guarantee of non-reassignment and more stability, but can tolerate values unfriendly (and unknown) to humans should refer to the eduPersonTargetedIDattribute.

Example applications for which this attribute would be useful

controlling access to resources and other cases where a human friendly identifier is needed

Example (LDIF Fragment)

eduPersonPrincipalName: hputter@hsww.wiz

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

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

RFC4512 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.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. Multiple "@" signs are not recommended, but in any case, the first occurrence of the "@" sign starting from the left is to be taken as the delimiter between components. Thus, user identifier is to the left, security domain to the right of the first "@". This parsing rule conforms to the POSIX "greedy" disambiguation method in regular expression processing.

Permissible values

See controlled vocabulary for eduPersonAffiliation. Only these values are allowed to the left of the "@" sign. The values to the right of the "@" sign shouldindicate a security domain.

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

white pages, controlling access to resources

Example (LDIF Fragment)

eduPersonScopedAffiliation: faculty@cs.berkeley.edu

Syntax: directoryString;*Indexing:*pres,eq

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

RFC4512 definition

(1.3.6.1.4.1.5923.1.1.1.10

NAME 'eduPersonTargetedID'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseExactMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

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

Definition

A persistent, non-reassigned, opaque identifier for a principal.

eduPersonTargetedID is an abstracted version of the SAML V2.0 Name Identifier format of "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" (see http://www.oasis-open.org/committees/download.php/35711). In SAML, this is an XML construct consisting of a string value inside a <saml:NameID> element along with a number of XML attributes, of most significance NameQualifier and SPNameQualifier, which identify the source and intended audience of the value. It is left to specific profiles to define alternate syntaxes, if any, to the standard XML representation used in SAML.

In abstract terms, an eduPersonTargetedID value is a tuple consisting of an opaque identifier for the principal, a name for the source of the identifier, and a name for the intended audience of the identifier. The source of the identifier is termed an identity provider and the name of the source takes the form of a SAML V2.0 entityID, which is an absolute URI. The name of the intended audience also takes the form of an absolute URI, and may refer to a single service provider or a collection of service providers (for which SAML V2.0 uses the term "Affiliation", not to be confused with the ordinary eduPerson use of the term).

Per the SAML format definition, the identifier portion MUST NOT exceed 256 characters, and the source and audience URI values MUST NOT exceed 1024 characters.

In SAML, a service provider is an abstract designation and may or may not refer to a single application or physical system. As a result, and because service providers may be grouped arbitrarily into "Affiliations" for policy purposes, the intended audience of an eduPersonTargetedID may be (and often is) limited to a single "target" application, or may consist of a large number of related applications. This is at the discretion of the identity provider. The value of the principal identifier SHOULD be different for different "audience" values, but this is also at the discretion of the identity provider.

This attribute may or may not be stored in a typical Directory Service because of its potential variance by relying party, but it is defined here for use in other service contexts such as Security Assertion Markup Language (SAML) assertions. It is typically used in federated scenarios in which more typical opaque identifiers lack appropriate uniqueness guarantees across multiple identity providers.

More specific requirements and guidance follows.

Persistence

As defined by SAML, eduPersonTargetedID values are not required to have a specific lifetime, but the association SHOULD be maintained longer than a single user interaction and long enough to be useful as a key for consuming services. Protocols might also be used to refresh (or "roll-over") an identifier by communicating such changes to service providers to avoid a loss of service. (SAML V2.0 includes one such example.) This may be needed in the event that the association between the principal and the identifier becomes public, if privacy requirements are involved.

Privacy

This attribute is designed in part to aid in the preservation of user privacy. It is therefore REQUIRED to be opaque, having no particular relationship to the principal's other identifiers, such as a local username. It MAY be a pseudorandom value generated and stored by the identity provider, or MAY be derived from some function over the audience's identity and other principal-specific input(s), such as a serial number or UUID assigned by the identity provider.

This attribute is also designed to inhibit, when appropriate, the ability of multiple unrelated services to correlate user activity by comparing values. This is achieved when desired by varying the identifier based on the intended audience.

In other words, there is no guarantee of non-correlation, but there is an assumption of non-correlation from the relying party's perspective outside of explicitly arranged "Affiliations" of relying parties and cooperating identity providers prepared to recognize them.

Uniqueness

A value of this attribute is intended only for consumption by a specific audience of services (often a single one). Values of this attribute therefore MUST be unique within the namespace of the identity provider and the namespace of the service provider(s) for whom the value is created. The value is "qualified" by these two namespaces and need not be unique outside them; the uniqueness of the identifier therefore depends on all three pieces of information.

Reassignment

A distinguishing feature of this attribute inherited from SAML is that it prohibits re-assignment. Since the values are opaque, there is no meaning attached to any particular value beyond its identification of the principal. Therefore particular values created by an identity provider MUST NOT be reassigned such that the same value given to a particular relying party refers to two different principals at different points in time. It is allowable (though perhaps confusing) for a given value to refer to two or more different principals when scoped to different audiences.

Human Palatability

This attribute does not meet requirements for human palatability or readability. It is ill-suited for display to end users or administrators, and is not useful for provisioning accounts ahead of initial access by users since the value will rarely be known by users or administrators. It may be accompanied by other attributes more suited to such purposes, in which case its privacy properties are presumably of no interest, but the lack of reassignment often is.

Example applications

Service providers or directory-enabled applications with the need to maintain a persistent but opaque identifier for a given user for purposes of personalization or record-keeping.

Identity or service providers or directory-enabled applications with the need to link an external account to an internal account maintained within their own system. This attribute is often used to represent a long-term account linking relationship between an identity provider and service provider(s) (or other identity/attribute provider).

2.2.11. eduPersonAssurance (defined in eduPerson 200806);*OID:*1.3.6.1.4.1.5923.1.1.1.11

RFC4512 definition

(1.3.6.1.4.1.5923.1.1.1.11

NAME 'eduPersonAssurance'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseExactMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

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

Definition

Set of URIs that assert compliance with specific standards for identity assurance.

Notes

This multi-valued attribute represents identity assurance profiles (IAPs), which are the set of standards that are met by an identity assertion, based on the Identity Provider's identity management processes, the type of authentication credential used, the strength of its binding, etc. An example of such a standard is the InCommon Federation's proposed IAPs.

Those establishing values for this attribute should provide documentation explaining the semantics of the values.

As a multi-valued attribute, relying parties may receive multiple values and should ignore unrecognized values.

The driving force behind the definition of this attribute is to enable applications to understand the various strengths of different identity management systems and authentication events and the processes and procedures governing their operation and to be able to assess whether or not a given transaction meets the requirements for access.

Example applications for which this attribute would be useful

Determining strength of asserted identity for on-line transactions, especially those involving more than minimal institutional risk resulting from errors in authentication.

A system supporting access to grants management in order to provide assurance for financial transactions.

Example (LDIF Fragment)

eduPersonAssurance: urn:mace:incommon:IAQ:sample
eduPersonAssurance: http://idm.example.org/LOA#sample

Syntax: directoryString;*Indexing:*No recommendation

---

3. Comments on Other Common Person Attributes

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.

3.1. audio (defined in RFC2798, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.55

*Application utility class:*no recommendation;

Definition

RFC1274 notes that the proprietary format they recommend is "interim" only.

Notes

Avoid. Not clearly defined, no de facto standard.

3.2. cn (commonName, included in person); *OID:*2.5.4.3

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

Definition

Common name.

According to RFC4519, "The 'cn' ('commonName' in X.500) attribute type contains names of an object. Each name is one value of this multi-valued attribute. 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 associated. 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

3.3. description (included 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 RFC4519, "The 'description' attribute type contains human-readable descriptive phrases about the object. Each description is one value of this multi-valued attribute."

Notes

Can be anything.

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

description: A jolly good felon

3.4. displayName (defined in RFC2798, 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 RFC2798 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

white pages, email client

Example (LDIF Fragment)

displayName: Jack Dougherty

3.5. facsimileTelephoneNumber (defined in RFC4519, included in orgPerson); *OID:*2.5.4.23

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

Definition

According to RFC4519: "The 'facsimileTelephoneNumber' attribute type contains telephone numbers (and, optionally, the parameters) for facsimile terminals. Each telephone number is one value of this multi-valued attribute."

Notes

Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."

Semantics

A fax number for the directory entry.

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

facsimileTelephoneNumber: +44 71 123 4567

3.6. givenName (defined in RFC4519, inetOrgPerson); *OID:*2.5.4.42

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

Definition

From RFC4519 description:"The 'givenName' attribute type contains name strings that are the part of a person's name that is not their surname. Each string is one value of this multi-valued attribute."

Example applications for which this attribute would be useful

Example (LDIF Fragment)

givenName: Stephen

3.7. homePhone (defined in RFC2798, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.20

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

Definition

From RFC1274 description: "The [homePhone] attribute type specifies a home telephone number associated with a person."

Notes

Attribute values should comply with the ITU Recommendation E.123: i.e., "+44 71 123 4567."

In RFC1274, this was originally called homeTelephoneNumber.

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

homePhone: +1 608 555 1212

3.8. homePostalAddress (defined in RFC2798, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.39

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

Definition

From RFC1274 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

white pages

Example (LDIF Fragment)

homePostalAddress: 1212 Como Ave.$Midton, SD 45621

3.9. initials (defined in RFC4519, inetOrgPerson); *OID:*2.5.4.43

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

Definition

From RFC4519 description: "The 'initials' attribute type contains strings of initials of some or all of an individual's names, except the surname(s). Each string is one value of this multi-valued attribute."

Example applications for which this attribute would be useful

Example (LDIF Fragment)

initials: f x

3.10. jpegPhoto (defined in RFC2798, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.60

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

Definition

Follow inetOrgPerson definition of RFC2798: "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

white pages

3.11. l (localityName, defined in RFC4519, included in orgPerson); *OID:*2.5.4.7

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

Definition

locality name.

According to RFC4519, "The 'l' ('localityName' in X.500) attribute type contains names of a locality or place, such as a city, county, or other geographic region. Each name is one value of this multi-valued attribute."

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

white pages

Example (LDIF Fragment)

l: Hudson Valley

3.12. labeledURI (defined in RFC2798, inetOrgPerson); *OID:*1.3.6.1.4.1.250.1.57

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

Definition

Follow inetOrgPerson definition of RFC2079: "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 RFC2079: "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

white pages

Example (LDIF Fragment)

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

3.13. mail (defined in RFC4524, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.3

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

Definition

From RFC4524: The 'mail' (rfc822mailbox) attribute type holds Internet mail addresses in Mailbox [RFC2821] form (e.g., user@example.com).

Notes

Preferred address for the "to:" field of email to be sent to this person. Usually of the form localid@univ.edu. Though multi-valued, there is often 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/docs/ldap-recipe.htm).

Semantics

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

Example applications for which this attribute would be useful

white pages, email client

Example (LDIF Fragment)

mail: dumbledore@hsww.wiz

3.14. manager (defined in RFC4524, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.10

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

Definition

From RFC4524: "The 'manager' attribute specifies managers, by distinguished name, of the person (or entity).

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

white pages

Example (LDIF Fragment)

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

3.15. mobile (defined in RFC4524, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.41

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

Definition

From RFC4524: "The 'mobile' (mobileTelephoneNumber) attribute specifies mobile telephone numbers (e.g., "+1 775 555 6789") associated with a person (or entity)."

Notes

cellular or mobile phone number. Attribute values should comply with the ITU Recommendation E.123: i.e., "+44 71 123 4567."

Semantics

cellular or mobile phone number.

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

mobile: +47 22 44 66 88

3.16. o (organizationName, defined in RFC2798, 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

white pages

Example (LDIF Fragment)

o: St. Cloud State

3.17. ou (organizationalUnitName, included in orgPerson); *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

white pages

Example (LDIF Fragment)

ou: Faculty Senate

3.18. pager (defined in RFC4524, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.42

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

Definition

From RFC4524: "The 'pager' (pagerTelephoneNumber) attribute specifies pager telephone numbers (e.g., "+1 775 555 5555") for an object."

Notes

Attribute values should comply with the ITU Recommendation E.123: i.e., "+44 71 123 4567."

Semantics

pager number.

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

pager: +1 202 555 4321

3.19. postalAddress (included 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

white pages

Example (LDIF Fragment)

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

3.20. postalCode (included 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

white pages

Example (LDIF Fragment)

postalCode: 54321

3.21. postOfficeBox (RFC4519, included in orgPerson); *OID:*2.5.4.18

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

Definition

From RFC4519: "The 'postOfficeBox' attribute type contains postal box identifiers that a Postal Service uses when a customer arranges to receive mail at a box on the premises of the Postal Service. Each postal box identifier is a single value of this multi-valued attribute."

Notes Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

postOfficeBox: 109260

3.22. preferredLanguage (defined in RFC2798, inetOrgPerson); *OID:*2.16.840.1.113730.3.1.39

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

Definition

Follow inetOrgPerson definition of RFC2798: "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

white pages

Example (LDIF Fragment)

preferredLanguage: EO

3.23. seeAlso (RFC4519, included in person); *OID:*2.5.4.34

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

Definition

From RFC4519: The 'seeAlso' attribute type contains the distinguished names of objects that are related to the subject object. Each related object name is one value of this multi-valued attribute."

Semantics

The distinguished name of another directory entry.

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

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

---

3.24. sn (surname, RFC4519, included in person); *OID:*2.5.4.4

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

Definition

Surname or family name. From RFC4519: "The 'sn' ('surname' in X.500) attribute type contains name strings for the family names of a person. Each string is one value of this multi-valued attribute."

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 both 1) the whole surname including hyphens if present and 2) each component of a hyphenated surname 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-Smith
sn: Carson
sn: Smith

3.25. st (stateOrProvinceName, RFC4519, included 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. If well-known shortcuts exist, like the two-letter state abbreviations in the US, these abbreviations are preferred over longer full names.

From RFC4519: "The 'st' ('stateOrProvinceName' in X.500) attribute type contains the full names of states or provinces. Each name is one value of this multi-valued attribute."

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 RFC4519 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

white pages

Example (LDIF Fragment)

st: IL

3.26. street (RFC4519, included in orgPerson); *OID:*2.5.4.9

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

Definition

From RFC4519: "The 'street' ('streetAddress' in X.500) attribute type contains site information from a postal address (i.e., the street name, place, avenue, and the house number). Each street is one value of this multi-valued attribute."

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

street: 303 Mulberry St.

3.27. telephoneNumber (included in person); *OID:*2.5.4.20

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

Definition

Office/campus phone number. Attribute values should comply with the ITU Recommendation E.123: i.e., "+44 71 123 4567."

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

telephoneNumber: +1 212 555 1234

3.28. title (RFC4519, included in orgPerson); *OID:*2.5.4.12

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

Definition

From RFC4519: "The 'title' attribute type contains the title of a person in their organizational context. Each title is one value of this multi-valued attribute."

Notes

No controlled vocabulary, may contain anything.

Example applications for which this attribute would be useful

white pages

Example (LDIF Fragment)

title: Assistant Vice-Deputy for Redundancy Reduction

3.29. uid (defined in RFC4519, inetOrgPerson); *OID:*0.9.2342.19200300.100.1.1

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

Definition

From RFC4519: "The 'uid' ('userid' in RFC1274) attribute type contains computer system login names associated with the object. Each name is one value of this multi-valued attribute."

Notes

Likely only one value. See the extensive discussion in the "LDAP Recipe" (http://middleware.internet2.edu/dir/docs/ldap-recipe.htm).

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

RFC1274 uses the longer name 'userid'.

Example applications for which this attribute would be useful

controlling access to resources

Example (LDIF Fragment)

uid: gmettes

3.30. uniqueIdentifier (RFC4524); *OID:*0.9.2342.19200300.100.1.44

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

Definition

From RFC4524: "The 'uniqueIdentifier' attribute specifies a unique identifier for an object represented in the Directory. The domain within which the identifier is unique and the exact semantics of the identifier are for local definition. For a person, this might be an institution- wide payroll number. For an organizational unit, it might be a department code."

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 value 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.

3.31. userCertificate (defined in RFC2798, inetOrgPerson); *OID:*2.5.4.36

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

Definition

A user's X.509 certificate

Notes

RFC2256 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

3.32. userPassword (RFC4519, included 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

3.33. userSMIMECertificate (defined in RFC2798, 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 RFC2798, "If available, this attribute is preferred over the userCertificate attribute for S/MIME applications."

RFC2798 states that this attribute is to be stored and requested in the binary form, as 'userSMIMECertificate;binary.'

Semantics

Following userSMIMECertificate in RFC2798, "A PKCS#7 [RFC2315] SignedData."

Example applications for which this attribute would be useful

email clients

3.34. x500uniqueIdentifier (defined in RFC2798, 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.

---

4. Change Log

This section lists changes that have been made from version to version of eduPerson.

The following list shows changes in version (201203) relative to version (200806).

- 1. Section 2.2.1 "eduPersonAffiliation"text updated to clarify its definition and comment on its usage
- 2. Section 2.2.6 "eduPersonPrimaryAffiliation"text updated to point to eduPersonAffiliation for detailed definitions
- 3. Section 2.2.10 "eduPersonTargetedID"text updated to better describe properties and uses of eduPersonTargetedID
- 4. Section 2.2.8 "eduPersonPrincipalName"text significantly edited and shortened to update content and to eliminate guidelines that are more properly defined by identity federations.

The following list shows changes in version (200806) relative to version (200712).

- 1. In section 1.1, changed RFC2256 to RFC4512.
- 2. In section 1.1, removed paragraph explaining upgrade process from 200312 to 200604.
- 3. In section 1.2, removed reference to an "upcoming MACE-Dir document on information models"
- 4. In section 2.1, restructured attribute list to one per line for improved readability and added attribute eduPersonAssurance
- 5. Add named anchors and linked Table of Contents. This is document enhancement, not a specification change.
- 6. Added subsection 2.2.11 "eduPersonAssurance".
- 7. In all subsections of 2.2, changed "RFC2252 definition" to "RFC4512 definition".
- 8. In section 2.2.5, changed reference from "RFC2252" to "RFC4512".
- 9. In section 3.2, 3.3, changed reference from "RFC2256" to "RFC4519" and updated text.
- 10. In section 3.5, added reference to RFC4519 and updated text. Added notes section.
- 11. In section 3.6, changed reference from "RFC2798" to "RFC4519" and updated text.
- 12. In section 3.7, added note "Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567.""
- 13. In section 3.9, changed reference from "RFC2798" and "RFC2256" to "RFC4519" and updated text.
- 14. In section 3.11, changed reference from "RFC2256" to "RFC4519" and updated text.
- 15. In section 3.13, changed reference from "RFC2798" to "RFC4524" and updated text.
- 16. In section 3.13, changed wording of "Likely to be only one value" to "Though multi-valued, there is often only one value."
- 17. In section 3.13, updated location of the LDAP Recipe from "http://www.duke.edu/~gettes/giia/ldap-recipe" to "http://middleware.internet2.edu/dir/docs/ldap-recipe.htm".
- 18. In section 3.13, removed notation about RFC1274 and rfc822Mailbox
- 19. In section 3.14, 3.15, changed reference from "RFC2798" to "RFC4524" and updated text.
- 20. In section 3.15, removed notation regarding RFC1274. Added note "Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567.""
- 21. In section 3.18, changed reference from "RFC2798" to "RFC4524" and updated text. Removed notation regarding RFC1274. Added notation that ITU Recommendation E.123 should be used.
- 22. In section 3.21, changed to RFC4519 and removed redundant notation.
- 23. In section 3.23, added reference to RFC4519
- 24. In section 3.24, added reference to RFC4519. Changed example to show recommended usage with a hyphenated name.
- 25. In section 3.25, added reference to RFC4519
- 26. In section 3.26, changed reference from RFC2256 to RFC4519 and updated text.
- 27. In section 3.27, changed international format recommendation to "Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."".
- 28. In section 3.28, added reference to RFC4519 and updated text.
- 29. In section 3.29, changed reference from "RFC2798" to "RFC4519" and update text.
- 30. In section 3.29, updated location of the LDAP Recipe from "http://www.duke.edu/~gettes/giia/ldap-recipe" to "http://middleware.internet2.edu/dir/docs/ldap-recipe.htm".
- 31. In section 3.30, changed reference from "RFC1274" to "RFC4524" and updated text.
- 32. In section 3.32, added reference to RFC4519. Text was not updated because it is significantly different than RFC4519.
- 33. In section 4, added indention to all subsections to improve readability and added line break after section.
- 34. In section 2.2.2 change EQUALITY caseIgnoreMatch to caseExactMatch, matching the eduPerson LDIF.

- 35. In sections 2.2.2 and 2.2.4 specify indexing as "No recommendation". No indexing recommendation has ever been specified for these attributes, this language is just for clarification.

The following list shows changes in version (200712) relative to version (200604).

- 1. In section 2.2.1, "eduPersonAffiliation" and section 2.2.6, "eduPersonPrimaryAffiliation," added "library-walk-in" to *Permissible values*
- 2. In section 2.2.1, "eduPersonAffiliation" and section 2.2.6, "eduPersonPrimaryAffiliation," added the new paragraph explaining "library-walk-in."

The following list shows changes in version (200604) relative to version (200312).

- 1. Definition of eduPersonPrincipalName and eduPersonScopedAffiliation modified. A "first match from the left" rule is invoked such that the two components are the substrings found on either side of the first "@" sign.
- 2. Definition of eduPersonTargetedID revised to align with current recommended practice in Shibboleth applications.

The following list shows changes in version (200312) relative to 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.
- 5. Comments on identifiers and their properties consolidated into an introductory note, corresponding edits in the eduPersonTargetedID section.
- 6. Recommendation on the "sn" attribute amended to suggest including the whole surname as well as the components in cases of hyphenated surnames.
- 7. Various typographical errors corrected.

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.
- 11. Clarifying text added in sections 1.3 and 2.2.8

---

5. References

E.123	http://www.itu.int/rec/T-REC-E.123/en
ISO 639	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22109
RFC822	http://tools.ietf.org/html/rfc822
RFC1274	http://tools.ietf.org/html/rfc1274
RFC2068	http://tools.ietf.org/html/rfc2068
RFC2079	http://tools.ietf.org/html/rfc2079
RFC2119	http://tools.ietf.org/html/rfc2119
RFC2256	http://tools.ietf.org/html/rfc2256
RFC2315	http://tools.ietf.org/html/rfc2315
RFC2632	http://tools.ietf.org/html/rfc2632
RFC2633	http://tools.ietf.org/html/rfc2633
RFC2634	http://tools.ietf.org/html/rfc2634
RFC2821	http://tools.ietf.org/html/rfc2821
RFC4512	http://tools.ietf.org/html/rfc4512
RFC4519	http://tools.ietf.org/html/rfc4519
RFC4524	http://tools.ietf.org/html/rfc4524

---

6. 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, Ann West, Ignacio Coupeau, Leif Johannson, Hallvard Furuseth, Diego Lopez, Roland Hedberg, Ingrid Melve, Alistair Young, Peter Gietz, Mark Jones, Nathan Dors, Tom Scavo, Lynn McRae, Chad La Joie, Katheryn Strojny, Kathryn Huxtable, Digant Kasundra, Gabriel Sroka, Jon Saperia, David Bantz and others. 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 over the years, Ben Chinowsky, Renee Frost, Lisa Hogeboom, Nate Klingenstein, Steve Olshansky, Jessica Bibbee, Ellen Vaughan and Emily Eisbruch.

This material is based in whole or in part on work supported by EDUCAUSE, Internet2, and the National Science Foundation under the NSF Middleware Initiative - NSF 02-028, Grant No. ANI-0123937. 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).