# InCommon Federation Attribute Summary

The following is a non-exhaustive list of the attributes commonly encountered in the use of InCommon-enabled services.

### Table Key

| | |
|---|---|
| **Friendly Name** | A short name for the attribute |
| **Formal Names** | The formal name of the attribute when expressed in a SAML assertion in accordance with the MACE-Dir SAML Attribute Profiles { http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200804.pdf} (PDF) |
| **Datatype** | An informal description of the value syntax of the attribute |
| **Multi?** | Indicates whether the attribute is multi-valued |

### Attribute Summary Table

| **Friendly Name** | **Formal Names** | **Datatype** | Multi? |
|---|---|---|---|
| eduPersonScopedAffiliation | SAML1: urn:mace:dir:attribute-def:eduPersonScopedAffiliation<br>SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.9 | Domain-Qualified String Enumeration | Y |
| eduPersonPrincipalName | SAML1: urn:mace:dir:attribute-def:eduPersonPrincipalName<br>SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.6 | Domain-Qualified String | N |
| eduPersonEntitlement | SAML1: urn:mace:dir:attribute-def:eduPersonEntitlement<br>SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.7 | URI | Y |
| eduPersonTargetedID | urn:oid:1.3.6.1.4.1.5923.1.1.1.10 | String, max. 256 characters | N |
| sn | SAML1: urn:mace:dir:attribute-def:sn<br>SAML2: urn:oid:2.5.4.4 | String | Y |

| | | | |
|---|---|---|---|
| givenName | SAML1: urn:mace:dir:attribute-def:givenName<br>SAML2: urn:oid:2.5.4.42 | String | Y |
| displayName | SAML1: urn:mace:dir:attribute-def:displayName<br>SAML2: urn:oid:2.16.840.1.113730.3.1.241 | String | N |
| mail | SAML1: urn:mace:dir:attribute-def:mail<br>SAML2: urn:oid:0.9.2342.19200300.100.1.3 | String | Y |

# Attribute Descriptions

## eduPersonScopedAffiliation

**Formal Definition**
http://middleware.internet2.edu/eduperson/ [see below]

**Description**
Multiple values of the form *value@domain*, where *domain*is (typically) a DNS-like subdomain representing the organization or sub-organization of the affiliation (e.g., "osu.edu") and *value* is one of:

- member
- student
- employee
- faculty
- staff
- alum
- affiliate

Note that these values are NOT case-sensitive, and capital or mixed-case values are permitted (e.g., MEMBER, Member, MeMbEr), though all lower-case is recommended.

**Usage Notes**
Affiliation is a high-level expression of the relationship of the user to the university or organization specified in the domain. A user can possess many affiliations, though some values are mutually exclusive. This attribute is often made available to any Shibboleth service provider, and is a good way to filter or block users of a given general type. In particular, "member" is an indication that the user is somebody with relatively official standing with a university at the present time, and does not apply to guests, other temporary accounts, terminated employees, unpaid/unregistered students, and other exceptional cases.

## eduPersonPrincipalName

**Formal Definition**
http://www.educause.edu/eduperson/

**Description**
A single value of the formuser@domain, wheredomainis (typically) a DNS-like subdomain representing the security domain of the user (e.g., "osu.edu") and user is generally a username, NetID, UserID, etc. of the sort typically assigned for authentication to network services within the security domain.

**Usage Notes**
EPPN is the eduPerson equivalent of a username. It typically has most of the properties usually associated with usernames (such as uniqueness and a naming convention of some sort), with the added property of global uniqueness through the use of a scope. An application that tracks information based on it can therefore interact with users via any number of identity providers without fear of duplicates, although the possibility for recycling/reassignment does still exist within the domain of a given identity provider.Note that at some Identity Providers a user can freely change their local account name (in the case of a name change due to marriage, for example), and the corresponding EPPN will typically change as well. This can cause a loss of service until name changes propagate throughout every application storing the value. For a less dynamic identifier, see also the eduPersonTargetedID attribute.

## eduPersonEntitlement

**Formal Definition**
http://www.educause.edu/eduperson/

**Description**
Muliple values, each a URI, representing a license, permission, right, etc. to access a resource or service in a particular fashion. Entitlements represent an assertion of authorization to something, precomputed and asserted by the identity provider. This attribute is typically used to assert privileges maintained centrally rather than within specific application databases.

**Usage Notes**
Entitlements should not in general be parsed or interpreted based on the structure or content of the values, but simply compared as strings to access-control expressions in the application.

## eduPersonTargetedID

**Formal Definition**
http://www.educause.edu/eduperson/

**Description**
A single string value of no more than 256 characters that uniquely identifiers a user in an opaque, privacy-preserving fashion. In most cases, the value will be different for a given user for each service provider to which a value is sent, to prevent correlation of activity between service providers.

**Usage Notes**
This attribute offers a powerful alternative to the use of eduPersonPrincipalName as a user identifier within applications and databases. Its power lies in the fact that it offers a significant degree of privacy and control for users. It also tends to be more stable than EPPN because it doesn't change merely in response to superficial name changes. It still may change, but generally in a more controlled fashion. It also requires a policy of non-reassignment. That is, while a given user may be associated with more than one value over time, a single value once assigned will never be assigned to any other user. When appropriate, the value can remain consistent across multiple service providers, if those systems have a demonstrated relationship and need to share information about the user's activities. Such sharing must be tightly controlled.

Note that the values are not guaranteed to be unique except within a given identity provider's set of values.

### sn

**Formal Definition**
http://www.educause.edu/eduperson/

**Description**
Multiple string values containing components of the users's "family" name or surname.

## givenName

**Formal Definition**
http://www.educause.edu/eduperson/

**Description**
Multiple string values containing the part of the user's name that is not their surname or middle name.

## displayName

**Formal Definition**
http://www.educause.edu/eduperson/

**Description**
A single string value indicating the preferred name of a person to be used for display purposes, for example a greeting or a descriptive listing.

## mail

**Formal Definition**
http://www.educause.edu/eduperson/

**Description**
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.

**Usage Notes**
The address in this attribute cannot be assumed to represent an organizationally-assigned contact address for a user established as part of a strong identity-proofing process. This may be true of some organizations that assert this attribute, but some organizations may permit users to provide their own preferred address, e.g. an email account at an Internet mail service.

***Ths page last updated November 2, 2010***

*Editor's note – Only the latest version of documentation is included; older versions are omitted. URLs have been added to comply with the PDF/A specification where the reference is consider important to understanding the text..*

# eduPerson & eduOrg Object Classes

eduPerson and eduOrg are LDAP schema designed to include widely-used person and organizational attributes in higher education. They were developed, and are maintained, by the Internet2 MACE-Directories Working Group (MACE-dir), a project of the Internet2 Middleware Initiative. These middleware activities are supported by Internet2 and EDUCAUSE.

Comments to i2mi-info@internet2.edu.

The problem: There are no established patterns for building general-purpose institutional directories. Each institution has to start from scratch, and no two higher education directories look alike.

The eduPerson object class would provide a common list of attributes and definitions. The task force plans to draw on the existing standards work in higher education, select items that are of broad utility, and define a common LDAP representation for each of them.

## Documentation

- **eduPerson/eduOrg Object Identifier (OID) Registrations**
  - MACE administers OIDs for Internet2. This page lists OIDs currently assigned to eduPerson and eduOrg. General information about the registry, and the complete list of MACE-administered OIDs, is available here.

- **eduPerson (200806)**

  HTML http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html

  - Platform-Specific eduPerson LDIFs*

  The Internet2 MACE-Dir Working Group has released this new (200806) version of the eduPerson specification. This principal change in this version is the addition of a new attribute: eduPersonAssurance. 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.

Development of this specification was supported with funding from Internet2, EDUCAUSE, and the NSF Middleware Initiative (Cooperative Agreement No. ANI-0330626). For more details please see the NMI Enterprise and Desktop Integration Technologies (EDIT) site.

*LDIF (Lightweight Directory Interchange Format) is an ASCII file format that LDAP servers can import and export. The above LDIF files, when imported into an LDAP server will define the object class and its attributes so that the directory administrator can use them with new directory entries.

- ***A Recipe for Configuring and Operating LDAP Directories***, Michael Gettes, MIT
- **Letter to Implementers, 12 Feb 2001**


[7 KB PDF]
http://middleware.internet2.edu/eduperson/docs/Implementers_010209.pdf

- **FAQ for eduPerson 1.0, 12 Feb 2001**


[38 KB PDF]
http://middleware.internet2.edu/eduperson/docs/faq.pdf

## Background Materials

- **eduPerson Task Force Charter**


[25 KB DOC]
http://middleware.internet2.edu/eduperson/docs/charter.doc

- **K. Hazelton Presentation to the Net@EDU PKI Working Group, Tempe AZ, 8 Feb 2000**


[37 KB PPT]
http://middleware.internet2.edu/eduperson/docs/hazelton.ppt

# eduPerson/eduOrg Object Identifier (OID) Registrations

MACE administers OIDs for Internet2. This page lists OIDs currently assigned to eduPerson and eduOrg. General information about the registry, and the complete list of MACE-administered OIDs, is available here. **1.3.6.1.4.1.5923** is the Internet2 OID arc.

| **eduPerson (200312) OIDs 1.3.6.1.4.1.5923.1.1.*** | **Allocation** |
|---|---|
| 1.3.6.1.4.1.5923.1.1.2 | eduPerson |
| 1.3.6.1.4.1.5923.1.1.1.1 | eduPersonAffiliation |
| 1.3.6.1.4.1.5923.1.1.1.7 | eduPersonEntitlement |
| 1.3.6.1.4.1.5923.1.1.1.2 | eduPersonNickname |
| 1.3.6.1.4.1.5923.1.1.1.3 | eduPersonOrgDN |
| 1.3.6.1.4.1.5923.1.1.1.4 | eduPersonOrgUnitDN |
| 1.3.6.1.4.1.5923.1.1.1.5 | eduPersonPrimaryAffiliation |
| 1.3.6.1.4.1.5923.1.1.1.8 | eduPersonPrimaryOrgUnitDN |
| 1.3.6.1.4.1.5923.1.1.1.6 | eduPersonPrincipalName |
| 1.3.6.1.4.1.5923.1.1.1.9 | eduPersonScopedAffiliation |
| 1.3.6.1.4.1.5923.1.1.1.10 | eduPersonTargetedID |
| **eduOrg (200210) OIDs 1.3.6.1.4.1.5923.1.2.*** | **Allocation** |
| 1.3.6.1.4.1.5923.1.2.2 | eduOrg |
| 1.3.6.1.4.1.5923.1.2.1.2 | eduOrgHomePageURI |
| 1.3.6.1.4.1.5923.1.2.1.3 | eduOrgIdentityAuthNPolicyURI |
| 1.3.6.1.4.1.5923.1.2.1.4 | eduOrgLegalName |
| 1.3.6.1.4.1.5923.1.2.1.5 | eduOrgSuperiorURI |
| 1.3.6.1.4.1.5923.1.2.1.6 | eduOrgWhitePagesURI |