Supported Attribute Summary

Deprecated

Note that this page has been deprecated; the information they contain is no longer current. The page has been retained for historical purposes only.

This document contains **DRAFT** material intended for discussion and comment by the InCommon participant community. Comments and questions should be sent to the InCommon participants mailing list.

InCommon Attribute Overview

Note that detailed recommendations regarding specific attributes can be found in the Attribute Summary section, below. It is strongly recommended that InCommon participants or prospective participants familiarize themselves with the standard set of attributes below. The information offered here is a non-normative illustration of the typical use of attributes in InCommon (and more broadly, Research and Education federations.)

Federation and Identity Attributes

The InCommon Federation provides the trust foundation to enable Service Providers and Identity Providers to work together to manage access to protected resources. InCommon participant sites use federation-enabled software products, such as the Shibboleth suite or other products supporting the Security Assertion Markup Language (SAML) to accomplish this.

In a federation scenario, when someone attempts to access a resource protected by a SAML “Service Provider” (SP) implementation , an “Identity Provider” (IdP) is asked to provide information called "identity attributes" to the Service Provider. These attributes might include a unique identifier (traditionally a "user ID") and sometimes other information such as organizational affiliation, entitlement to access a service, email address, etc. (this information is also referred to as a "claim" or "claims" in some federation scenarios). In many cases, identity attributes are very useful to services for use in identification of users, access control, personalization, and other purposes. InCommon encourages the support of identity attributes by its participants to improve academic and business processes through the use of federated services at scale.

An identity attribute, as asserted by an IdP, consists of an attribute name (such as "eduPersonScopedAffiliation"), and one or more values (such as "student@example.edu"). Values are usually simple strings, but more complex values may be negotiated between IdPs and SPs for specific uses. A number of identity attributes may be sent at one time, and in the federation model, this is usually every time a person accesses a service. Identity attributes can express things specific to a particular user, such as a unique identifier, or things shared among many users, such as group membership or affiliation. Identity attribute values are based on information maintained in the identity management system which backs an IdP, often using existing technology such as LDAP-based directory services or relational databases. The IdP sets policies about which attributes and values are sent to which SPs, often in collaboration with Service Provider requests for attributes, or in alignment with federation attribute release recommendations such as the Research and Scholarship category, which automates attribute release for services that qualify.

InCommon Attribute Recommendations

To obtain the benefits of interoperable identity attributes, InCommon participants must broadly adopt a common set of attribute release policies. InCommon Operations strongly recommends that participants adopt the following behavior with regard to attribute release:

1. Support the attributes defined in the Attribute Summary section, below.
2. Release either a non-reassigned and permanently unique to an individual eduPersonPrincipalName (preferred) or eduPersonTargetedID (if a non-reassigned eduPersonPrincipalName is not available at your institution) to all Service Providers globally, if your institution does participate in eduGAIN.
3. Release either a non-reassigned and permanently unique to an individual eduPersonPrincipalName (preferred) or eduPersonTargetedID (if a non-reassigned eduPersonPrincipalName is not available at your institution) to all Service Providers registered by InCommon if your institution does not participate in eduGAIN.
4. Support the International Research and Scholarship Entity Category

Failure to support these practices results in an Identity Provider implementation which is not ready for collaboration and does not meet the needs of users at your institution or collaborative services globally. Identity Providers are strongly encouraged by InCommon to support these recommendations, some of which may become requirements over time.

InCommon Federation Attribute Summary

A *supported attribute* is one that the IdP is **able** to release; that is, a *supported attribute* is a technical capability of a given IdP deployment. Whether or not an IdP **will** release any given attribute is a local policy decision.

As noted in the InCommon Participation Agreement, IdPs are expected to support the following attributes:

- *Identifiers*
  - `eduPersonUniqueId`
  - `eduPersonPrincipalName`
  - `eduPersonTargetedID` (a.k.a. SAML2 Persistent NameID)
- *Mail attribute*

    - `mail`
- *Person name attributes*
    - `displayName`
    - `givenName`
    - `sn` (surname)
- *Authorization attributes*
    - `eduPersonScopedAffiliation`
    - `eduPersonEntitlement`

See the eduPerson Object Class Specification for the formal definitions of each of the above attributes.

Summary of Attributes Supported by IdPs in the InCommon Federation

Friendly Name	Protocol-level Names	Datatype	Multi?
eduPersonScopedAffiliation	SAML1: urn:mace:dir:attribute-def:eduPersonScopedAffiliation 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 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 SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.7	URI	Y
eduPersonTargetedID	SAML2: 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 SAML2: urn:oid:2.5.4.4	String	Y
givenName	SAML1: urn:mace:dir:attribute-def:givenName SAML2: urn:oid:2.5.4.42	String	Y
displayName	SAML1: urn:mace:dir:attribute-def:displayName SAML2: urn:oid:2.16.840.1.113730.3.1.241	String	N
mail	SAML1: urn:mace:dir:attribute-def:mail SAML2: urn:oid:0.9.2342.19200300.100.1.3	String	Y

Attribute Descriptions

eduPersonScopedAffiliation

Formal Definition

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
- library-walk-in

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

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

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

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

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

givenName

Formal Definition

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

displayName

Formal Definition

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

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.

Useful Links

- REFEDS website
- NET+ Identity Guidance for Services
- MACE-Dir Working Group
- MACE-Dir Uniform Resource Name (URN) Registry
- SAML V2.0 LDAP/X.500 Attribute Profile
- EduPerson specification
- Attribute naming in Shibboleth