Standard attributes in the OpenAthens federation

One of the major advantages of a federation is a standard set of attribute names can be defined so that both IdP and SP can use generic set-ups in most cases and do not need to maintain hundreds of separate configurations.

The following attributes are part of the recommended federation attribute set for the OpenAthens federation and can be used for authorisation unless otherwise stated.

SAML 2

This is the default mode for IdPs in the OpenAthens federation.

urn:oid:1.3.6.1.4.1.5923.1.1.1.10

The targetedID of the user. This is a consistent user ID you can use to recognise individuals when you need to do so.

Example: "159qddg1761rh8d0uo48a2ko5q"

Should always be released by IdP members of the OpenAthens federation.

Single-valued. Unique to the user.

urn:oid:1.3.6.1.4.1.5923.1.1.1.9

The user's role and organisation (scope). Sometimes called scopedAffiliation.

Formed by combining a role and an organisation's scope.

Example: "member@organisation.com"

Standard values for role are:

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

Should always be released by IdP members of the OpenAthens federation (where a value is present).

May be multi-valued.

Authorisation decisions should *usually* be whitelist as a user may have several roles, e.g. both 'staff' and 'student'. The exception would be 'library-walk-in'.

Example pseudocode

```
# Any role from a known organisation

WHEN VALUE OF
        orn:oid:1.3.6.1.4.1.5923.1.1.9
MATCHES
        *@organsation.com
THEN
        AllowAccess

---
# Any user with the 'member' role from subscribing organisations

WHEN VALUE OF
        orn:oid:1.3.6.1.4.1.5923.1.1.9
MATCHES
        member@{subscriber_scopes}
THEN
        AllowAccess
```

urn:oid:1.3.6.1.4.1.5923.1.1.1.7

Any entitlement value that may apply.

Examples: "dental" or "med"

Released by IdP members of the OpenAthens federation when a value applies to a relevant user / service provider combination.

May be multi-valued

Use this for authorisation where you need a greater level of granularity than role - e.g. the difference between regular students and medical students, or if they have a department level subscription.

Legacy shibboleth names

These are returned by OpenAthens IdPs in response to SAML 1.1 requests only so are unlikely to come up in regular usage.

urn:mace:dir:attribute-def:eduPersonTargetedID

A unique identifier for the user that is also unique to the service provider. This attribute is scoped.

Example: "159qddg1761rh8d0uo48a2ko5q@organisation.com"

urn:mace:dir:attribute-def:eduPersonScopedAffiliation

Role. This attribute is scoped.

Example: "member@organisation.com"

urn:mace:dir:attribute-def:eduPersonEntitlement

Anything you need it to be.

Example: "urn:mace:dir:entitlement:common-lib-terms"

OpenAthens specific attributes

These will be retired in the future and are provided only to help you transition from older technologies. They must not be used for authorisation or persistence:

organisationNum

urn:mace:eduserv.org.uk:athens:attribute-def:organisation:1.0:identifier

The OpenAthens organisation ID to help SPs who are moving from old Athens software to federated access map organisations to scopes.

Example: "3032813"

Currently releasable by IdP members of the OpenAthens federation. Newer customers do not release it.

See also:

Extended attributes

Granular authorisation

Migration

For service providers moving to federated access from the older 'Athens Agent' or 'OpenAthens SP1.x' software there will be differences in the user attributes that are available. Updates to your customer records may be necessary, but a benefit is that it simplifies interaction with other federations.

List of retired attributes