About federated access management

Federated access management (occasionally abbreviated to FAM) describes the situation where a group of service providers and identity providers have agreed to share the job of enabling users to access content remotely. This kind of group is called a federation and there is usually a central registry of some type that defines the terminology and organises any necessary trust.

In a federated environment the service providers make the decisions that they are best able to - i.e. whether or not to allow access; in turn the identity providers make the decisions that they are best able to - which is whether a user belongs to their organisation or not. An internet standard called SAML (Security Assertion Mark-up Language) is used to transfer information about the user from the identity provider to the service provider so that the service provider can make the access decision. SAML has come in two main versions - SAML 1.1 was superseded by SAML 2 in 2005 and whilst you shouldn't see any of the old stuff about, it does still pop up occasionally.

The bits of information being passed from identity provider to service provider are called 'attributes' and there are three main ones that can be passed which are called (in federation terms):

- A scoped affiliation
- A targeted ID
- An entitlement

Scoped affiliation just means a user's role and organisation and will look something like member@organisation.example. The first bit is the role and the second is the 'scope' which represents an organisation. The roles that can be passed are specified by the federation and since most federations are academic the roles are slanted that way (e.g. member, employee, staff, student, faculty, alumni). In OpenAthens these roles are configured in permission sets. At the moment, not many resources need you to be more precise than 'member' but this may change in the future. An account can have several roles assigned by multiple permission sets.

Targeted ID means the identifier for the user passed to the service provider and is completely pseudonymous (i.e. strangers cannot know who it represents by looking at it). The targeted part is because each service provider sees a different identifier for the same user. Taken together this means that only you can track users between service providers and connect accesses to individuals. This attribute is scoped in older SAML versions but not in versions since 2005, so might include an organisation identifier. A targeted ID will look something like:

SAML 1.1: ahf8543w0_da33yrYYisyd8@organisation.example

SAML 2.0: ahf8543w0_da33yrYYisyd8

Entitlement is the everything else attribute which can mean different things to different service providers which is why there are functions on permission sets that will let you say different things to different service providers for this attribute. This one is never scoped. This is the attribute that enables you to get very granular indeed and would allow you to identify specific sub-sets of your users to service providers so that they can restrict access to just those users and bill accordingly. At the moment it is not used by many service providers.

Almost all federated resources will require one or both of targeted ID and scoped affiliation to be passed and some an entitlement value. All federated resource suppliers will be able to tell you which attributes they need you to release - some will publish this information on their website whilst others will need you to ask their support teams directly.

OpenAthens will always* ...

- pass a targeted ID for a user.
- pass all roles specified on permission sets that are assigned to a user.
- pass entitlements specified on permission sets to the resources connected with those entitlements.

* When restrictive mode is active, no attributes are passed to resources that are not specified in permission sets assigned to the user.

What this means in practical terms is that whilst you generally do need to set the role on a permission set, the default of 'member' is likely correct. A blank role is a legitimate option in some cases so the interface will let you do that and it's worth checking for this if you have any access problems.

Shibboleth

Shibboleth is a term that is commonly associated with federated access management because, as an open source way to use the SAML standard in a federation, the bodies running federations can talk about it without appearing to endorse any commercial interests. What it means to you is that if a service provider says they support Shibboleth specifically, you can say that you are using something that works with that and carry on. OpenAthens is better than Shibboleth for many reasons, but the most important one is that you don't have to install anything to use OpenAthens.

What happens when a user accesses a resource using federated access management?

Here is what happens, in order, for a typical user access of a resource:

1. The user clicks login link on resource
2. The resource literally asks the user 'Where Are You From?'
3. The user selects their identity provider (home organisation) from the available options
4. The resource looks up the identity provider's metadata (trusted information about the organisation)
5. The resource redirects the user's browser to the identity provider's login page with a signed request for information and some return instructions.
6. The identity provider determines to their own satisfaction that the user is one of theirs
7. The identity provider redirects the user's browser back to the resource with some information about the user.
8. The resource compares that information with its list of valid reasons to let someone in and lets them in, or not, as appropriate

Steps 2 & 3 can be omitted if the link in step 1 is a wayfless URL (i.e. one that includes the home organisation's entity(ID)).
EntityIDs and scopes

When you are arranging access with a federation service provider you will need to provide them with both your entityID and scope and a page to display these can be found under the Management menu. When you tell these to the service provider it is also a good opportunity to ask them what attributes they need, especially if the subscription is only for a sub-set of your accounts.

The scope is what is used to tell organisations apart. Usually there will only be one per domain, but large domains may have several if different organisations within that domain need to subscribe to content separately.

The entityID is the reference used to look up where and how to send the user - e.g., where to log in. There only needs to be one of these per domain.