

JISC Access Management Animation Script

You may have heard about the introduction of federated access management within the UK. It is promoted as a 'next generation' access management system, but what does that mean, and how does this improve the experience of educational institutions within the UK?

We all know the problem of having multiple usernames. We might use one to access external publisher resources, another to access our e-mail and yet another to access virtual learning environments. Having numerous usernames increases the potential for identity theft and unauthorised exchange of identities.

Even current systems which provide a single identity access to resources, will still require a separate log-in when accessing other domains or when a user wants to access local resources. The difference with Federated access management is that staff and students need use only one institutional username for all of these resources, both internal and external.

In this way multiple passwords and poor security are reduced or eliminated. The single sign on becomes valued by users because it is their entry in to personal resources like e-mail.

The burden on staff having to issue and manage multiple usernames is reduced and frustrated users are less likely to give up on accessing resources.

Because the username is managed by the institution rather than an unknown third party, it can be properly protected and removed when a user no longer has the right to access resources, giving confidence that personal data is secure and not being abused.

So how is this made possible?

Federated access management is made possible by institutions and service providers agreeing to trust the information that they pass to each other and establishing rules and policies to make sure that this trust can be managed. This collaboration of trust is known as a Federation. Federations are being set up on a national basis in many different countries around the world – including the US, Canada, New Zealand, Australia and in over 15 European countries.

The UK service is known as the UK Access Management Federation and is run by UKERNA on behalf of JISC and BECTA. This means that everyone from school children to researchers will be using the same, standards-based, access management system.

There are a number of technological solutions for implementing federated access management. These technologies define a set of protocols for the secure passing of identity information between institutions and service providers and adopt a standards based approach which is SAML compliant. Shibboleth is an example of this technology.

Within the Federation information about users is only held by the institution or organisation to which that user is affiliated, which means there is a single, central point of identity management.

It is the permission to access resources that is shared rather than the user's personal information. This information is known as a set of 'attributes' and can be as simple as declaring that a user is a learner or a tutor at a particular university or college.

This should increase the legitimate use of subscribed services. It facilitates finely-controlled access to services or resources, allowing for subscriptions by department and courseware targeted at individual classes.

Federated access management also reduces the burden that currently exists for library staff in managing usernames, freeing them to concentrate on licenses and subscriptions and selection, management and promotion of resources.

A Federation defines a set of rules that each of the members sign up to. This allows all members to trust each other and means that schools, further and higher education, public sector organisations and commercial partners can all gain the benefits of the federated approach.

So, by allowing users to authenticate through their home institution, the new system will open up a range of other collaboration and access management options not available until now.

In order to adopt federated access management, institutions will have to do a number of things. This includes:

Defining what your institution needs from access management and assess your current ability to manage identities, through an institutional audit.

Developing internal directories to enable effective identity management within institutions.

Selecting an appropriate authentication system.

Implementing identity provider software.

Joining the Federation.

Rolling out staff training, user guidance and support.

More information is available from the JISC website and the UK Federation website.