

Script for AAF animation on federated access management

Video location: <http://www.aaf.edu.au/index.php/about/>

You may have heard about the introduction of the Australian Access Federation for the higher education and research community. But what is it, and how may it improve the experience of staff and students at your institution?

We all know the problem of having multiple credentials to access different systems. We might use one to access our email, another for the university financial system, and yet another for an external publisher resource.

To solve this problem, many institutions have been introducing a single sign-on to their systems, using one authoritative directory. This means there are fewer credentials for users to remember, and user accounts can be properly protected and removed when a user no longer has the right to access resources. It also frees resource managers, such as library staff, from the burden of issuing and managing user accounts.

Federated access management takes this concept further, so that users can use the credentials issued by their own institution to access resources *outside* their institution.

So why is this important for research and higher education?

Just as in other facets of life, information and communication technologies are radically transforming the way research communities across the world are operating, in fields as diverse as medicine, genetics, linguistics, and finance.

Increasingly, research teams are made up of people from different institutions. These teams need to access and share resources that are spread around the world -- resources such as data, scientific instruments, and computing capability.

And as more scholarly and administrative tasks are done online, these functions also require access to external systems and resources.

If it is difficult to manage accounts for users who officially belong to your institution, it is much harder to manage accounts for users who don't. For one thing, there may be many more of them. And how do you know they are who they claim to be, and that they are authorised to access the resources they are requesting?

This is where federated access management comes in. A federation is a framework for trust and collaboration, where institutions and resource providers agree to trust the information they pass to each other and establish rules and policies to make sure this trust can be managed.

Under this model, a user's credentials are managed at his own institution, providing a central authority for identity management. When the user wants to access an external resource, the home institution passes information about him to the resource provider, according to the policies agreed upon by the federation.

Federations are being set up on a national basis in many different countries around the world. The Australian Access Federation is funded by the Australian Government Department of Education, Science and Training and is for the higher education and research community. Peer federations may also be established for Australian government organisations. Consideration is being given to the needs of vocational education and training institutions, and schools.

There are a number of technological solutions for implementing federated access management. These technologies define a set of standards-based protocols for the secure passing of identity information between institutions and service providers. The Australian Access Federation uses two technologies. One is Shibboleth. The other is Public Key Infrastructure, or PKI.

Using Shibboleth an agreed set of attributes about a user is shared to enable access to resources. These attributes can be as simple as declaring that a user is a student or a staff member at a particular university. This facilitates finely controlled access to resources, while still protecting the privacy of the user's personal details.

PKI provides the underlying trust in the Australian Access Federation and can also be used for authentication when there is a requirement for highly secure access to resources, such as sensitive data, some scientific instruments, or high performance computing resources. There are other uses as well; PKI can be used to encrypt email so that it is secure, to allow the use of digital signatures and to make web transactions secure by encrypting them. It is PKI, for example, that is behind the secure padlock on web browsers.

Whether using PKI, Shibboleth, or a combination of the two, the important point is that the Australian Access Federation provides the means of allowing a member institution to trust the information that it receives from another member so that access to resources and secure communication can be conducted seamlessly. This may support effective collaboration between member institutions and also with users in other federations.

So what will your institution need to do in order to join the Australian Access Federation?

Institutions need to do a number of things. These include:

- Assessing your current ability to manage identities and determining the authoritative source of identity information for your institution.
- Identifying services or resources at your institution to make available to the federation community.
- Taking advantage of the Australian Access Federation's workshops and seminars to become familiar with the policies and technologies and how they are managed at the institutional level.
- Determining what you would like to manage locally and what you would like the Australian Access Federation to manage for you.
- Implementing federation policies and services.

More information is available from the Australian Access Federation website: www.aaf.edu.au