



Australian Access Federation



The Australian Access Federation (AAF) is currently being established to provide a framework and supporting infrastructure to facilitate trusted electronic communications and collaboration within and between universities and research institutions in Australia and overseas. The AAF will rely on cutting edge technologies to automatically provide a range of authentication services, which will allow authentication of people (Researchers, Teachers and Students) and resources (servers, services, networks, instruments and data). It will enable resource owners to authorise a researcher to access on-line resources, such as compute facilities, data and other research infrastructure, across their home institution, other institutions around Australia or around the world.

The Australian Access Federation will provide the means of allowing a member institution and/or a service provider to trust the information it receives from another member. This will provide seamless access to resources and secure communication to support effective collaboration between users.

Similar federations are emerging in the international community as institutions around the world seek a common approach for managing and sharing resources. A key driver of AAF is to reduce the risk of accidental or malicious exposure of data and other resources in a collaborative environment.

What's in it for me?

For researchers, other staff members, and students

If you are a researcher, staff member, or student at a university or research institution, the most immediate benefit is that the AAF will enable you to log in using the credentials issued by your own institution, and seamlessly access a wide range of resources both internal and external to your institution, such as:

- Data collections and data grids;
- Scientific instruments, modelling and visualisation tools, and computing resources;
- Collaboration environments and workspaces for virtual teams;
- Scholarly resources and publications;
- eLearning resources and learning object collections;
- National higher education and research administrative systems.

This means:

- You do not have to request and remember individual accounts from each of these different resource providers, only the one account from your own institution.
- You can collaborate more easily with colleagues because it is easier to share access to tools and resources.
- You can use trusted ad-hoc communication via secure email, enabling confidentially through encryption and providing confidence in the sender.
- You may be able to receive electronically signed academic transcripts, streamlining international and domestic study and work application processes.

For resource providers

If you manage resources such as those listed above, the AAF will enable you to provide access to your resource or service to authorised users in a secure way without you having to issue individual accounts. Under the AAF, institutions and resource providers agree to abide by the Federation policies and to trust the information that each passes to the other. This means you can focus on managing your resource or service and the rules for authorising access, rather than on managing user accounts.

For institutions

Institutions will benefit from the AAF by enabling their research, academic, and administrative users to access a wide range of resources and to collaborate more easily with colleagues in Australia and in other countries with which the AAF peers.

Other ways in which institutions may make use of the AAF framework and infrastructure include:

- AAF membership can be used as a driver for improving institutional identity management practices;
- Institutions can better manage student access to administrative systems, such as enrolment information and examination results;
- Institutions would be able to provide improved access services for cross institutional enrolments;
- Institutions will have the opportunity to use AAF services to provide a more efficient means of delivering encrypted information; and
- The Public Key Infrastructure (PKI) and Shibboleth technologies used with the AAF can be used for other institutional purposes, such as allowing the use of digital signatures on email and documents.

What do you need to do?

There will be a significant amount of work required for an institution to join the AAF and deploy the technologies; however some aspects can be managed by the AAF if an institution does not wish to manage them internally.

Directors of Information Technology

- Identify an authoritative source of information about your institution's users.
- Deploy the Shibboleth Identity Provider component at your institution.
- Determine who is responsible for the role of requesting server and appliances certificates to the AAF from your institution.

Resource owners and service providers

- Identify which resources you would like to make available to AAF members.
- Determine the business criteria for providing services
- Identify authentication and access rules to be used with your resources.
- Integrate the Shibboleth Service Provider component and/or PKI authentication.

Universities

- Identify an authoritative source of information about your institution's users.
- Identify your institution's identity management processes.

Senior management (DVCs Research etc)

- Analyse AAF integration in terms of the strategic plan for your institution or area.

Researchers, other staff members, and students

- Identify which resources available at the federation you would like to use.

When will AAF be available?

It is expected that the AAF will commence operations by the end of 2008 and Institutions and service providers will seek to join the AAF progressively during 2009. Once established, the AAF will continue to consider applications for membership into the future.

Public Key Infrastructure and the AAF

The AAF is supported by two technologies: Shibboleth and Public Key Infrastructure (PKI).

PKI

The use of PKI technology in the AAF will assist in minimising the exposure to accidental or malicious use of collaborative resources. For example:

- PKI can be used to support authentication via stronger mechanisms than the traditional "username and passwords".
- It can also be used for signing of email and other documents proving the originator's identity and ensuring that the data has not been modified intentionally or unintentionally without being detected. Signing of emails and documents can support more efficient, paper free business processes.
- PKI also provides the cryptographic means to ensure confidentiality of sensitive data is preserved. For example widely adopted email clients enable average users to sign and encrypt emails.
- PKI is actively used today to support high performance computing (GRID) access control and job authorisation in the higher education and research sector. The authentication system is based on x509 certificates.
- PKI is also used across the higher education and research sector for server certificates, to enable end users to have confidence that their information in transit is encrypted and that they are connected to the correct organisation.

The Australian Access Federation Project is supported by:

For more information please visit:

www.aaf.edu.au

