

Tools & Services for Shibboleth Federations*



* This brochure describes technologies available to the MAMS Testbed Federation. As the Australian Access Federation is yet to be finalised, its technologies may differ.

Introduction

A Shibboleth Federation is a “trust fabric” for members (Identity Providers and Service Providers) to collaborate. It provides the core infrastructure or the “middleware” for supporting federated identity and access management among members.

MAMS has been working on enriching the list of services that can be provided to Shibboleth Federations. These services are used by Identity Providers and Service Providers. These services are being prepared for use by the Australian Access Federation.

Some of these shared services are briefly explored here. They are Federated White Pages, People Picker, Federated Services (Federated Cloud), Federated Entitlement Service (FES), Short-Lived Credential Service (SLCS) and its supporting services such as Federated AueduPersonSharedToken Service (FAST).

It is hoped that these services can be provided in Shibboleth Federations without charge to users. Their designs and implementations have been, and continued to be, subject to community reviews. The provision of Federated Services can reduce workload and maintenance otherwise needed if each Federation member had their own services.

Federated Services provide relevant components to allow IdPs and SPs to enable their end-users to utilise the services. These services may be installed as part of a new Shibboleth IdP/SP installation or added to an existing installation. Installation and integration procedures for most of the services are simple, with most of the complex development, integration and configuration already performed by the Shibboleth Federation Operator.

Federated White Pages

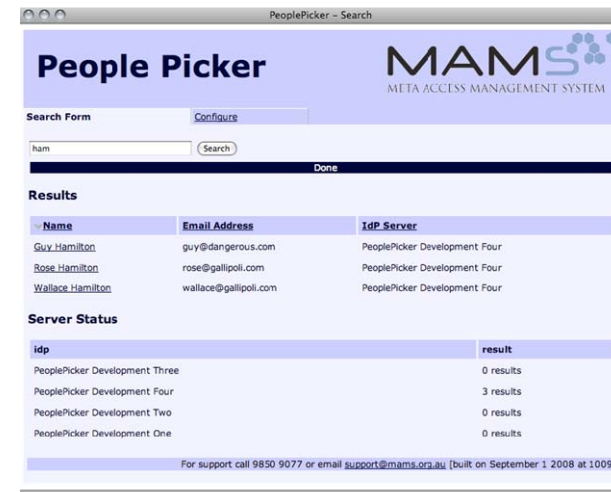
Federated White Pages uses the People Picker tool to allow end-users to discover information about the other end-users in the Federation. This service is a protected resource allowing convenient access to participating IdPs from a single location. Traditionally, discovery of user information requires individual searches being performed on each institutional white pages.

Federated White Pages has been deployed centrally in the Federation and institutional IdPs are encouraged to allow limited information about their staff users to be discoverable via this secure service. The IdP administrator manages allowable parameters of the search such that user’s privacy is managed.

Searches can be performed on all IdPs that have registered with the Federated White Pages server. Controlled and limited information of discovered users is returned, ie, name and email address. Additional information, such as phone number, department or division, are optional information (at the IdP’s discretion) to aid identification of discovered user.

People Picker

People Picker allows SPs to *pick* a federation user and give them access to its resources. Based on trusted IdP records within the Federation, SPs are able to discover authoritative user information (name and email) from People Picker. Information discovered manages the user’s privacy restrictions as well as the restrictions of the institution to which they belong.



The following are some features of People Picker:

- Search for a user across a whole federation with one search.
- Secure – data is encrypted and Attribute Release Policies (ARPs) are enforced. Each IdP controls release of its data.
- Search results are incrementally returned and search progress is clearly indicated as a search proceeds.
- Searches are customisable across the federation
- Custom clients for SP applications can be implemented.
- Ability for SP administrators to invite discovered users to a SP, automatically adding access rules for them.
- Extra details (eg, phone number) can be retrieved for any user where this information is provided by their IdP (optional).

When you use People Picker to invite an end-user to your SP, the invited user gets a digitally signed email linking to a Shibbolised login page. Upon successful authentication at the user’s institutional IdP, the SP adds them as a valid user without the SP administrator needing to take any extra step.

Federated Services

This is an umbrella for a range of collaborative services that can be offered centrally in a Shibboleth Federation. These services

are shared across multiple servers. Federation members use the *tools as service*, without knowledge of, or the need to own, the infrastructure.

Federated Services is also known as *Federated Cloud* or *Shibboleth Cloud* to signify its association with Cloud Computing and Web 2.0 technology in the context of secure and trusted end-user identities from the Federation.



Users could sign up for their choice of a growing number of Shibbolised services such as wikis, learning and content management tools, mailing lists, repositories, blogs, chats, forums, software development tools (SCM viewers, issue trackers, project management), news feeds, with more being available in the future. All of these services are built by different vendors and a Federation can providing them as part of a suite, allowing seamless integration without the need for every member to do the hard work of installation and management.

A Federated Cloud of Services allows a Federation to employ various technologies such as distributed infrastructure, backup, load balancing, etc, to help foster availability of Services to members of a Federation.

Notable features of Federated Services are:

- Availability of many popular tools - full versions of the tools the user knows and loves.
- Ability to invite other users in the Federation to join the group using simple invitation mechanisms such as People Picker.
- Share resources with restricted set of users within the group.
- Ability to mix and match tools as you see fit to achieve optimal collaboration amongst different end-user groups.

SLCS and FAST

As part of the integration of Shibboleth into Grid Computing, a Federation can provide a centralised SLCS server that issues proxy certificates upon successful authentication at the IdP. It converts user's information received from their IdP to the appropriate certificate that is used to access resources in the Grid. This would often require strong authentication at the IdP

Furthermore, the MAMS Team provides the FAST service to allow institutions to issue and manage their users' `aueduPersonSharedToken` via a central service. `aueduPersonSharedToken` is one of attributes required for accessing various Grid services in Australia.

Members can use a Federation SLCS service and FAST, removing the necessity for the institutions to manage their own.

As with other services offered in a Federation, SLCS and FAST can come with additional support in the form of future enhancements, additional tools to maximise its usage, and other features that make adoption simpler for end-users and administrators.

Federated Entitlement Service (FES)

The MAMS Team is investigating implementation of Federation Entitlement Service. FES is a centralised service in a Federation that allows both IdP and SP administrators to share and assign a range of entitlements to their users to help a SP enforce its authorisation. The SP receives acceptable user's entitlements from which it can perform checking and mapping to authorisation rules to see whether the user is allowed to gain access to the particular resources in question.

There are two modes of usage for FES, namely IdP-push and SP-pull model.

IdP-push requires the IdP to connect to FES and to retrieve relevant entitlements associated to its user. The IdP is then going to *push* the entitlement as part of user's other attributes to the SP.

SP-pull means that the SP needs to do the work of querying FES (*pull*) to gather for user's entitlements prior applying authorisation on access attempts to the protected resources.

FES allocates entitlement namespaces to different entities to ensure that namespace collision does not happen. At the same time, it also allows some common namespaces to be shared across different domains (IdPs and/or SPs).

User's privacy is maintained by FES by ensuring that only authorised Federation members (whether IdP or SP) are allowed to retrieve a specific end-user's entitlements. At any given time, a user can have a large number of entitlements from

which only a very small numbers are to be shared to a specific SP.

Communication between Federation members and FES is secured. Only trusted Federation members are allowed to query FES.

Federation Services Development

These software programs are developed by the Meta Access Management System (MAMS) project at Macquarie University, Sydney, Australia. The MAMS project is funded by the Australian Federal Government's Department of Education, Science, and Training (DEST) as part of "Backing Australia's Ability" program. The development of these tools and services are further continued under Australian Access Federation project.



australian access
federation



Australian Government
Department of Education,
Science and Training

an initiative of

Backing
Australia's
Ability

The Australian Government's
Commitment to Innovation

References

Federation Services info: <http://www.mams.org.au>

MAMS: <https://mams.melcoe.mq.edu.au>

MAMS Federation : <http://federation.org.au>

Contact: Bruc Liong, bliong@melcoe.mq.edu.au