

## Shibboleth Federation Management Tools\*



\* 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

MAMS is pleased to contribute to the Australian Access Federation, a continuation from MAMS Testbed Federation, by offering a number of tools to allow seamless interactions between the Federation and its members. Members interact with the Federation via a set of automated tools, giving full control and flexibility for the members to manage their entries while allowing the Federation Operator to enforce the Federation's rules of membership.

Automated processes enable near real time updates on information being propagated to all members of the Federation. This allows other set of tools, such as ShARPE and Autograph (privacy management tools for IdPs), to digest the propagated information. The tools communicate further with institutional administrators to enable them make appropriate decision (e.g. applying heuristic configuration options or manually changing configuration to allow institutional users to gain access to new services). Events and news are broadcasted within minutes to members of the Federation.

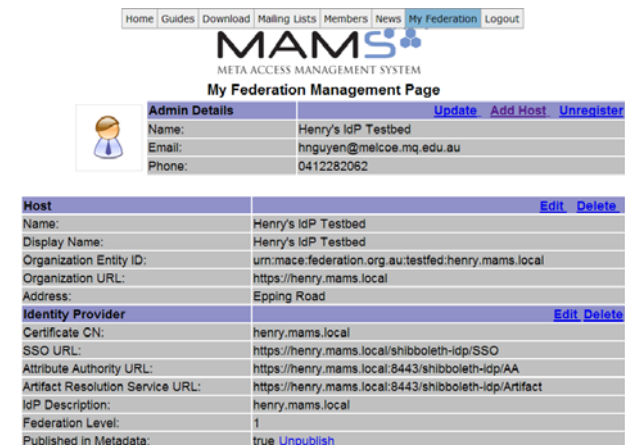
The Federation presents a number of new features to enhance efficiency for deployment and use of Shibboleth:

- Central management of Shibboleth membership through Federation Manager
- Service Descriptions to portray the types of services and service offerings available, and the attributes requirement for end-users in order for service access to be granted
- Customised Metadata provides only the metadata relevant to a particular IdP member (e.g. an IdP needs to know about only the subset of SPs that it collaborates with, not other irrelevant SPs)
- Customised WAYF allows groups of SPs to share the same look and feel. This approach supports powerful user-friendliness feature when this is combined with other features mentioned above.

### Federation Manager

Federation Manager is an easy to use tool to manage centrally institutional participation entry within Shibboleth in the AAF. It offers numerous features giving flexible configuration of entities as well as strong enforcement of the AAF Shibboleth Operational Requirements and Recommendations Document.

Federation Manager is considered the *heart* of the Federation. Other tools and processes are the limbs and body of the Federation. Metadata generation and management are fully controlled by Federation Manager.



Home Guides Download Mailing Lists Members News My Federation Logout

MAMS  
META ACCESS MANAGEMENT SYSTEM  
My Federation Management Page

Admin Details	Update	Add Host	Unregister
Name:	Henry's IdP Testbed		
Email:	hnguyen@melcoe.mq.edu.au		
Phone:	0412282062		

Host	Edit	Delete
Name:	Henry's IdP Testbed	
Display Name:	Henry's IdP Testbed	
Organization Entity ID:	urn:mace:federation.org.au:testfed:henry.mams.local	
Organization URL:	https://henry.mams.local	
Address:	Epping Road	

Identity Provider	Edit	Delete
Certificate CN:	henry.mams.local	
SSO URL:	https://henry.mams.local/shibboleth-ldap/SSO	
Attribute Authority URL:	https://henry.mams.local:8443/shibboleth-ldap/AA	
Artifact Resolution Service URL:	https://henry.mams.local:8443/shibboleth-ldap/Artifact	
IdP Description:	henry.mams.local	
Federation Level:	1	
Published in Metadata:	true <a href="#">Unpublish</a>	

The following are some features of Federation Manager:

- Groups of administrators are able to manage multiple entries for their local organisation (IdPs and/or SPs)
- Administrators can link their accounts to allow shared management of their local organisation's entries.
- Entries are modifiable by administrators but it will only take effect following Federation Operator review and approval
- Two core Levels of Assurance (LoA) are supported, namely Floor of Trust and Level 3.
- IdPs and SPs can be visible to all members of the Federation (default) or restricted to being only visible to some members.
- Each Service Offering (SO) of an SP can be further restricted to a smaller subset of IdPs if desired.
- Attributes required for satisfaction of SOs are fully registered in the Federation. This information is ready to be processed by IdPs so that end-users can be notified ahead of time before the release of attributes for access to a new service.
- Support of AAF core attribute list and creation of custom attributes
- Support for embedded certificates

The complete list of features is available by contacting the MAMS Team.

### Service Description

Service Description is a mechanism for SP administrator to inform other members of the Federation about the services available from the SP. This description includes information regarding the service, its list of service offerings, and its attributes requirements.

IdP administrators use Service Descriptions with Federation tools, such as SHARPE and Autograph, to determine access configurations for their end-users. The Shibboleth Federation Operator ensures that information in Service Descriptions is a valid representation of SP's requirements prior to such information being integrated into the Federation's metadata.

Host		Edit	Delete
Name:	ppk5.mams.local		
Display Name:	PPK Demo Server Five		
Organization Entity ID:	urn:mace:federation.mams.local:testfed:ppk5.mams.local		
Organization URL:	http://www.ppk5.mams.local/index.html		
Address:			
<b>Service Provider</b>	<b>Edit Delete Add ServiceOffering</b>	Authentication/Authorization	
Certificate CN:	ppk5.mams.local		
Artifact Consumer Service URL:	https://ppk5.mams.local/Shibboleth.sso/SAML/Artifact		
Assertion Consumer Service URL:	https://ppk5.mams.local/Shibboleth.sso/SAML/POST		
Service URL:	https://ppk5.mams.local/testapp/demo.jsp		
SP Description:	JSP Application		
Federation Level:	STAGING		
Published in Metadata:	true <a href="#">Unpublish</a>		

Host		Edit	Delete
Name:	ppk staging six		
Display Name:	ppk6		
Organization Entity ID:	urn:mace:federation.mams.local:testfed:ppk6.mams.local		
Organization URL:	http://www.ppk6.mams.local		
Address:	none		

## Customised Metadata

Customised metadata ensures that the IdP and SP only receive information about their respective partner institutions. An IdP need only know about SPs (services) that are potentially applicable to its end-users, and by the same token an SP can restrict the set of IdPs that may be able to access a service.

The Federation allows all of its members to define these relationships. This is reflected in metadata and it forms part of the trust fabric underlying every interaction performed by Federation members.

Select Authentication Level of Assurance

AAF FLOOR OF TRUST 3

LEVEL 3 3

Select Authorized IDPs

By default the Service you are creating is offered/available to all IDPs. If you want this default behaviour just click Save button at the bottom to save the SP. If you want to restrict access and allow access to only a few Idps then select the Idps below and then click Save.

Allow access to only the selected IDPs

Kerberos IdP

PPK Staging Org One

aaf1.mams.local

slcs-vm.mams.local

grid1-vm.mams.local

Autograph1 IdP

These relationships can be restricted to a finer-grained access at the level of service offerings. Individual service offerings from an SP may have different sets of restricted list of IdPs, reflecting the business agreements between the institutions involved.

**Edit Service Offering Details**

Service:

Description:

Restricted to Certain Users:

**Edit Service Offering Availability**

By default the Service Offering you are creating is offered/available to all IDPs available to the related SP. If you want this default behaviour just click Save button at the bottom to save the SP. If you want to restrict access of this offering and allow access to fewer Idps then select the Idps below and then click Save.

Allow access to only the selected IDPs

aaf2 Idp

wfed.com.au Idp

Kerberos IdP

## Customised WAYF

Where Are You From (WAYF) is a Federation service that aids users to choose their IdP within the large number of IdPs available in the Federation. The WAYF is also referred as *Home Institution Discovery Service*, or simply Discovery Service. As the SP has no knowledge regarding the user's IdP location, it uses the WAYF to redirect user to select the correct IdP.

The Federation typically provides one generic interface for the WAYF, however this interface has been considered too generic and does not reflect consistent look and feel from the initial SP, hence may confuses the end-user during transition from the visited SP to the login look and feel at the IdP.

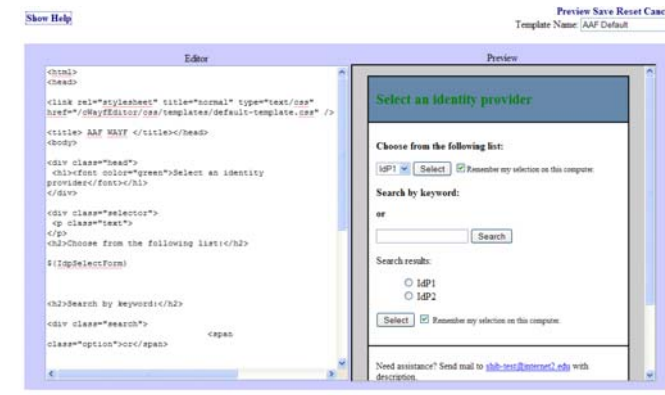
Customised WAYF is an optional central service provided by the Federation to allow SP administrators to tailor the look and feel of his SP's associated WAYF. Administrators can perform the necessary customisation through simple interface and subsequently manage the list of customised templates created.

Available Templates for SP *urn:mace:federation.org.au:testfed:slcs-vm.mams.*

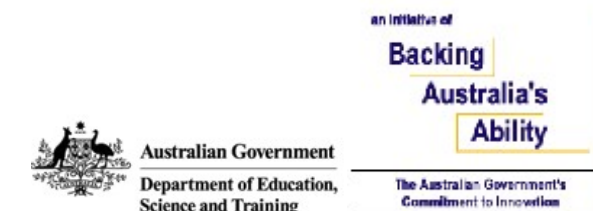
Name	Set for SP Author	Created Date	Last Modified
<a href="#">BlueTheme</a> <a href="#">Copy</a> <a href="#">Remove</a> <a href="#">Edit</a>	<input checked="" type="checkbox"/>	znguyen 12/09/2008	12/09/2008
<a href="#">AAF Default</a> <a href="#">Copy</a> <a href="#">Remove</a> <a href="#">Edit</a>	<input type="checkbox"/>	znguyen 12/09/2008	12/09/2008
<a href="#">AAF Default</a> <a href="#">Copy</a>	<input type="checkbox"/>	admin 12/09/2008	12/09/2008
<a href="#">BlueTheme</a> <a href="#">Copy</a>	<input type="checkbox"/>	admin 12/09/2008	12/09/2008

Administrators will be able to pick and modify existing templates contributed by the Shibboleth Federation Operator or choose to manage his/her own templates. The tool provides a simple HTML WYSIWYG editor to help in visualisation.

Customisation of the centralised WAYF can be embedded into applications at the SP. This feature, coupled with the Customised Metadata, can provide a much-simplified interface to the overall user experience with the Federation while maintaining strong security of access.



All systems described here are developed by the Meta Access Management System (MAMS) Team 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.



## References

AAF Features info: <http://www.federation.org.au>

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

Contact: Bruc Liong, [bliong@melcoe.mq.edu.au](mailto:bliong@melcoe.mq.edu.au)