AAA for IMOS: Australian Access Federation & related components

James Dalziel
Professor of Learning Technology, and Director,
Macquarie E-Learning Centre Of Excellence (MELCOE)
Macquarie University
james@melcoe.mq.edu.au
www.melcoe.mq.edu.au

Presentation for IMOS Data Workshop, University of Tasmania June, 2007

Overview

- Middleware
- Trust Technology
- Shibboleth and the Australian Access Federation
- AAF and trusted services
- Suggested next steps

My Background

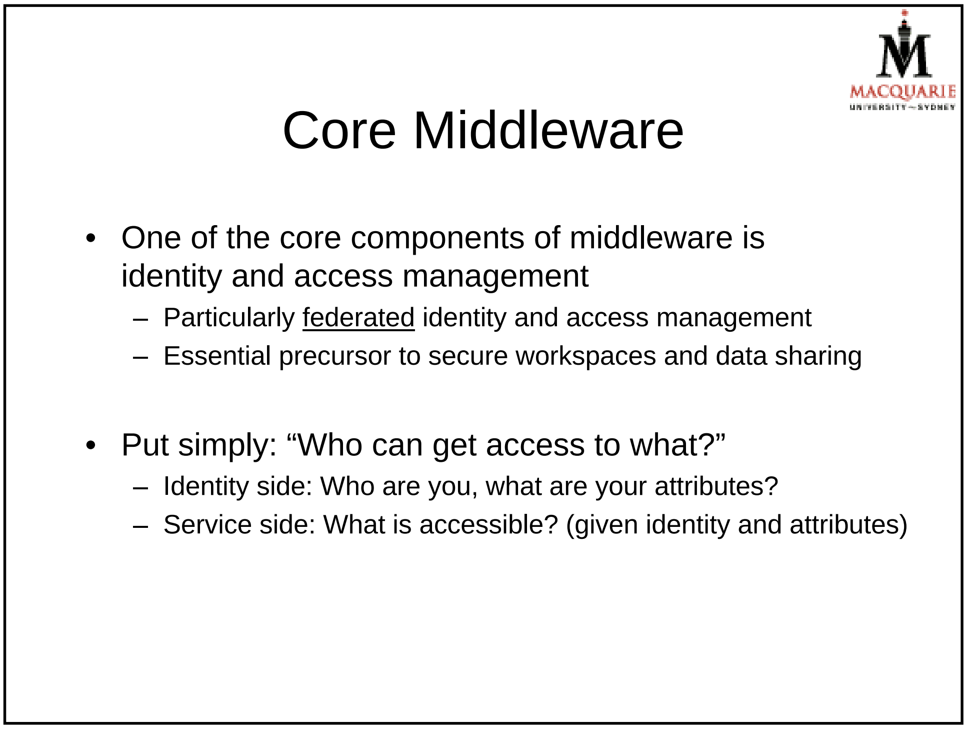
- Lead a research centre in IT infrastructure for the higher education and research sector (MELCOE)
  - Includes eResearch and eLearning
  - All outputs are freely available as open source/open content
- Member of NCRIS 5.16 Steering Committee
- Lead/collaborate on national IT infrastructure projects
  - MAMS for federated identity and access management (“trust federation”) leading to Australian Access Federation (AAF)
  - Secure Repositories (using Fedora) based on access policies
  - Secure Workspaces/Virtual Organisations (“IAMSuite”)
  - Workflow for collaborative activities (“RAMS”)
- Involved in planning for the “Australian National Data Service” (ANDS)

Middleware

- Middleware is a layer of software services that sit above the network, but below individual applications

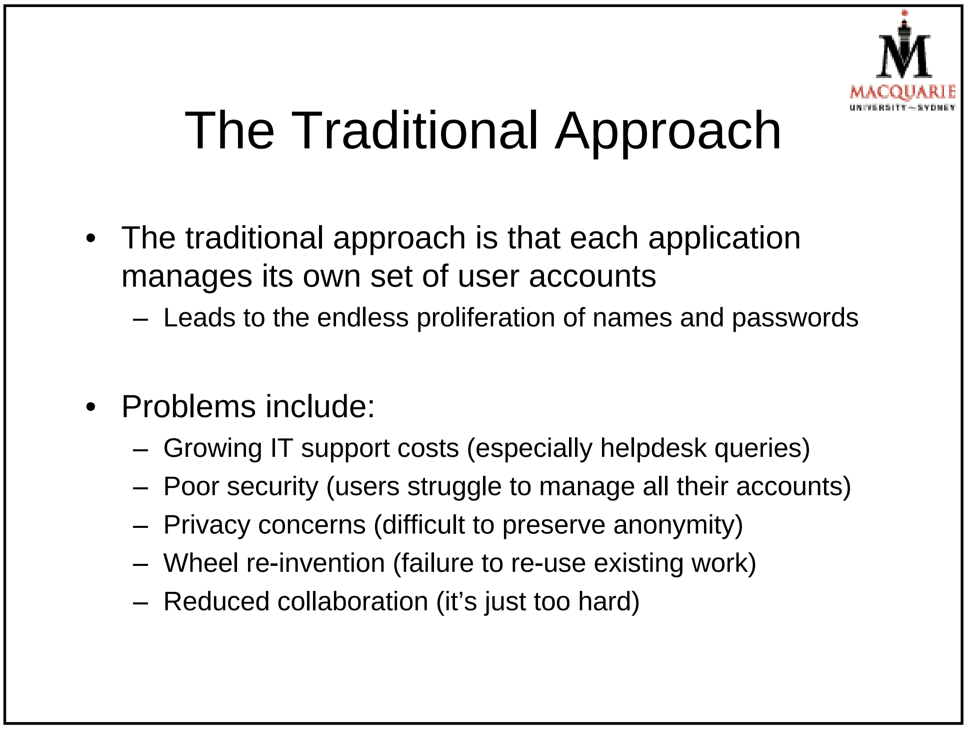
- Middleware helps connect disparate systems; it is the “glue” that overcomes the limitations of isolated systems

- Middleware relies on open standards



Core Middleware

- One of the core components of middleware is identity and access management
  - Particularly federated identity and access management
  - Essential precursor to secure workspaces and data sharing
- Put simply: “Who can get access to what?”
  - Identity side: Who are you, what are your attributes?
  - Service side: What is accessible? (given identity and attributes)



The Traditional Approach

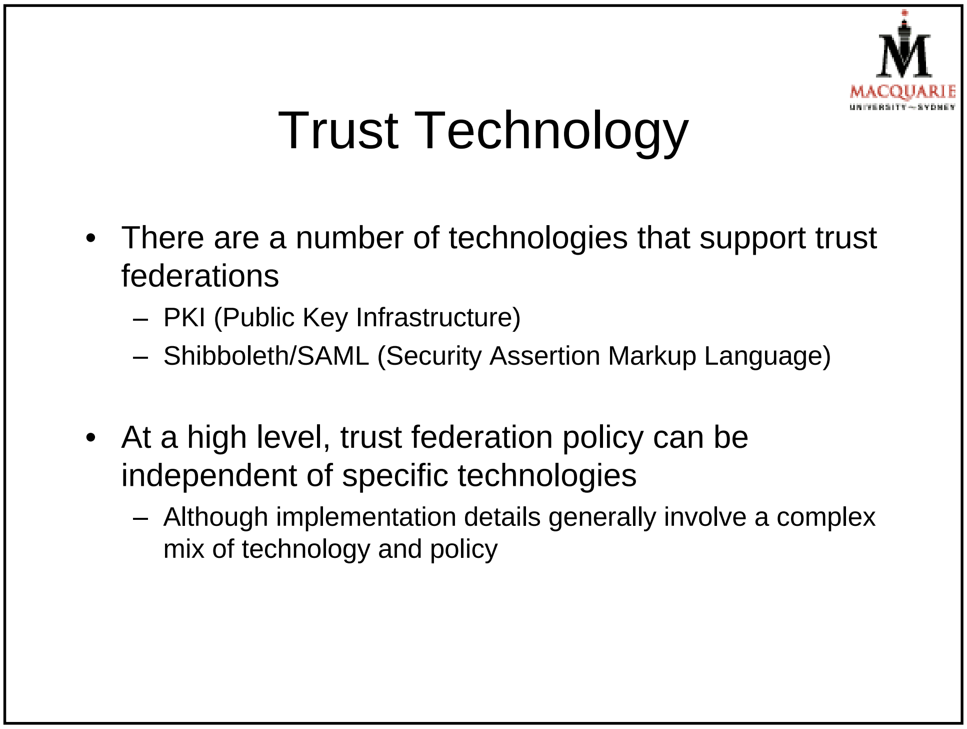
- The traditional approach is that each application manages its own set of user accounts
  - Leads to the endless proliferation of names and passwords
- Problems include:
  - Growing IT support costs (especially helpdesk queries)
  - Poor security (users struggle to manage all their accounts)
  - Privacy concerns (difficult to preserve anonymity)
  - Wheel re-invention (failure to re-use existing work)
  - Reduced collaboration (it’s just too hard)

A Solution

- Recent innovations provide an alternative to the traditional approach of applications managing accounts
- Requires three components:
  - Identity Providers: (the part of) Organisations that can share who their users are and their attributes (eg, role)
  - Service Providers: Services (ie, applications) that are accessible by users from Identity Providers
  - Trust Federation: A trust framework (policy and technical) that connects Identity Providers and Services Providers
- A typical large research organisation (eg, university) contains one Identity Provider (the directory) and may have many Service Providers

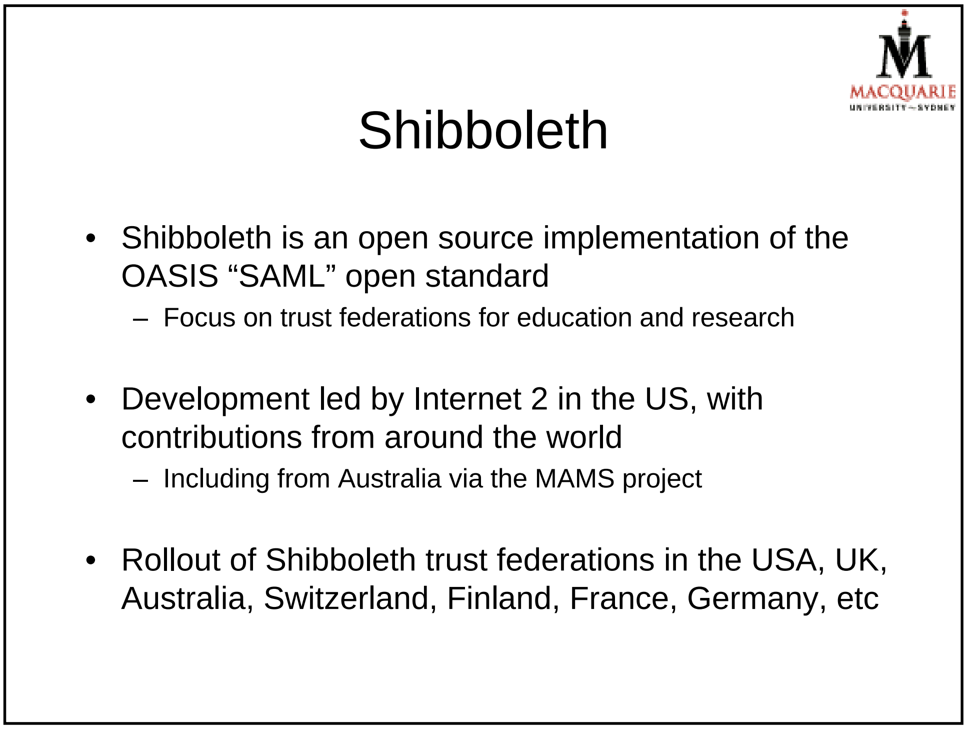
The Process

- Prior Requirements:
  - Identity Provider establishes the identity and attributes of its members (users)
  - Identity Provider joins trust federation, shares attributes
  - Services Provider joins trust federation, uses attributes for access
- Access Process:
  - A user logs in to their home organisation (Identity Provider)
  - The user attempts to access a service (eg, secure workspace)
  - The service requests/uses attributes about the user so as to make a decision about granting/denying access



Trust Technology

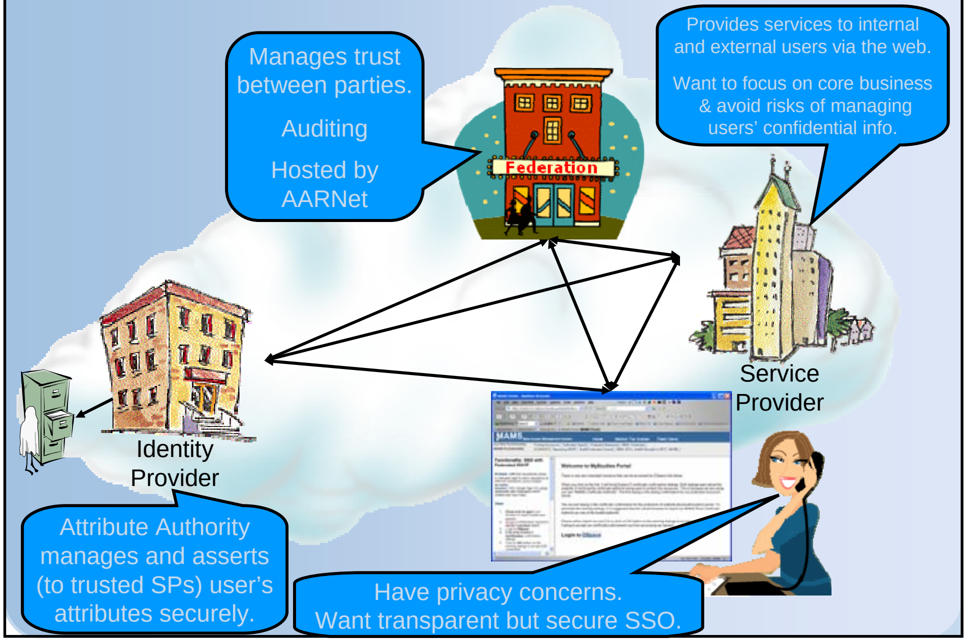
- There are a number of technologies that support trust federations
  - PKI (Public Key Infrastructure)
  - Shibboleth/SAML (Security Assertion Markup Language)
- At a high level, trust federation policy can be independent of specific technologies
  - Although implementation details generally involve a complex mix of technology and policy



Shibboleth

- Shibboleth is an open source implementation of the OASIS “SAML” open standard
  - Focus on trust federations for education and research
- Development led by Internet 2 in the US, with contributions from around the world
  - Including from Australia via the MAMS project
- Rollout of Shibboleth trust federations in the USA, UK, Australia, Switzerland, Finland, France, Germany, etc

Architecture View



Manages trust between parties.

Auditing

Hosted by AARNet

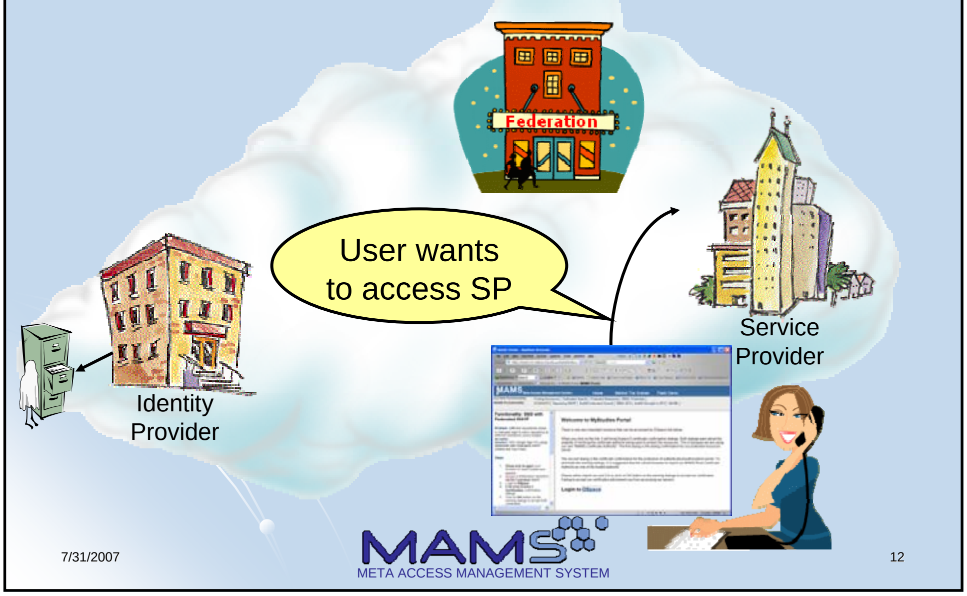
Provides services to internal and external users via the web.

Want to focus on core business & avoid risks of managing users' confidential info.

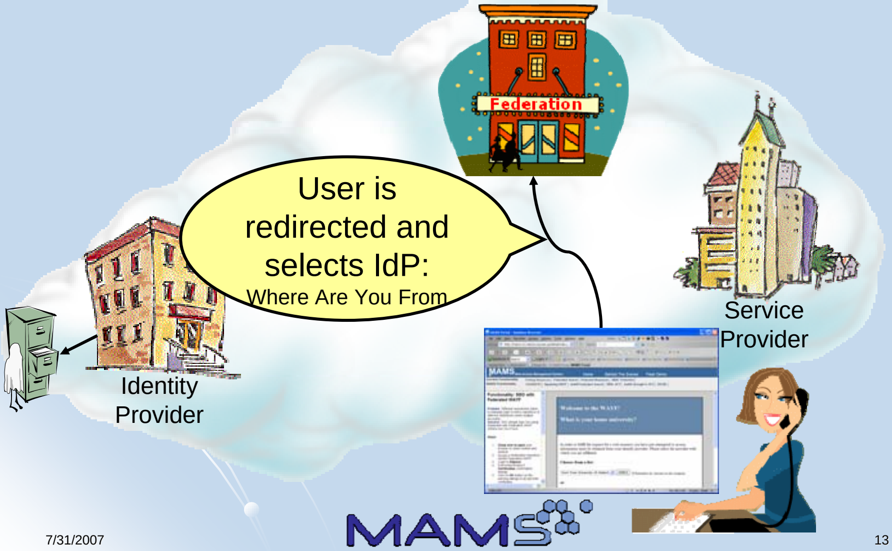
Attribute Authority manages and asserts (to trusted SPs) user's attributes securely.

Have privacy concerns.
Want transparent but secure SSO.

Typical SAML Access Scenario



Typical SAML Access Scenario



MAMS

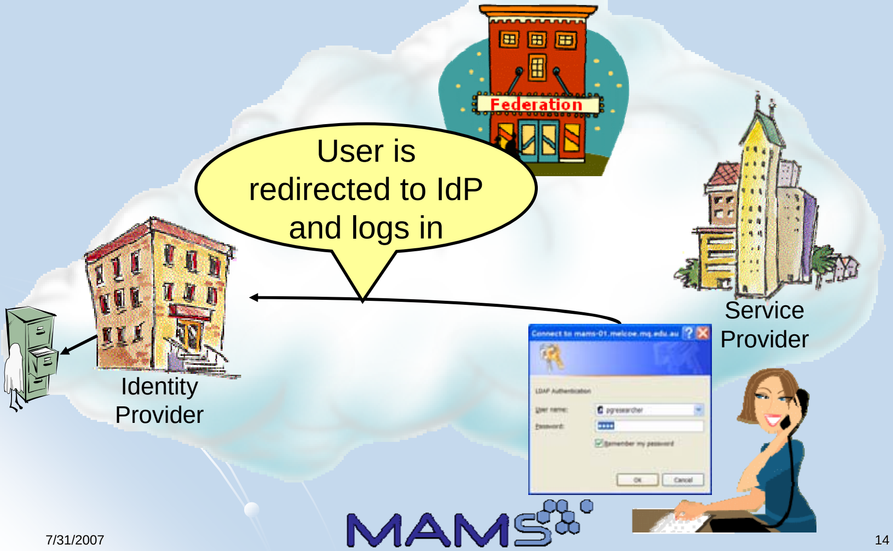
Welcome to the WAYF!

What is your home university?

7/31/2007

MAMS
META ACCESS MANAGEMENT SYSTEM

Typical SAML Access Scenario



Connect to mams-01.melcoe.mq.edu.au

LDAP Authentication

User name: pgresearcher

Password: ••••

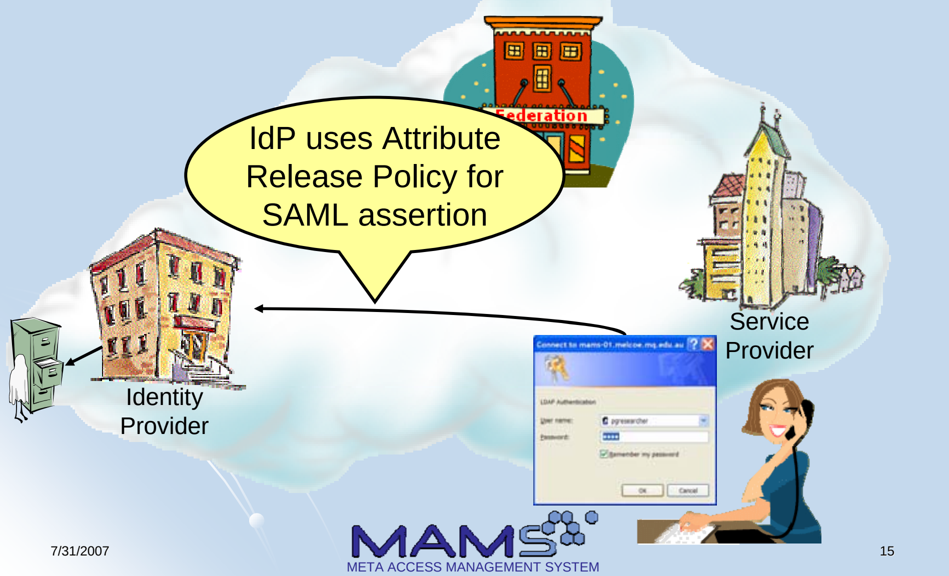
☑ Remember my password

OK Cancel

7/31/2007

MAMS
META ACCESS MANAGEMENT SYSTEM

Typical SAML Access Scenario

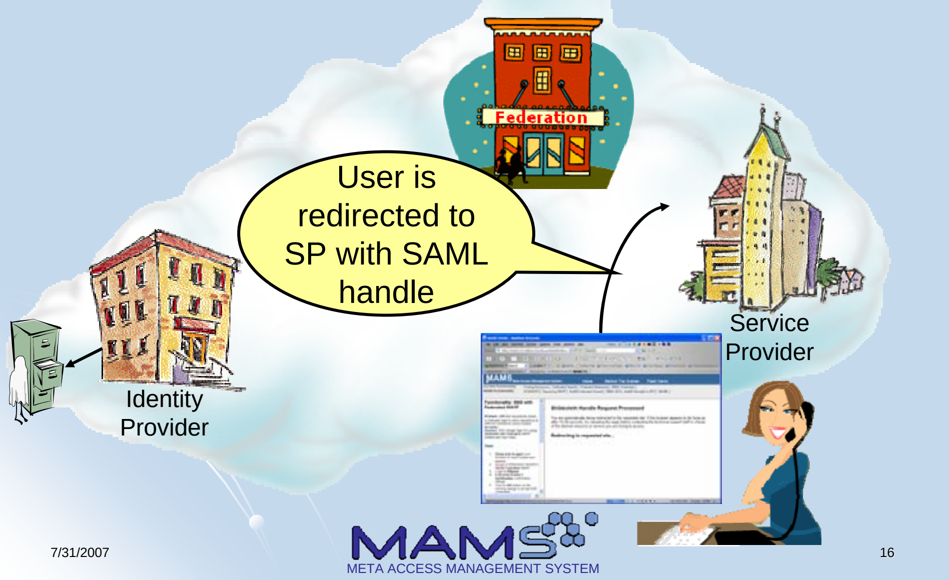


7/31/2007

META ACCESS MANAGEMENT SYSTEM

15

Typical SAML Access Scenario

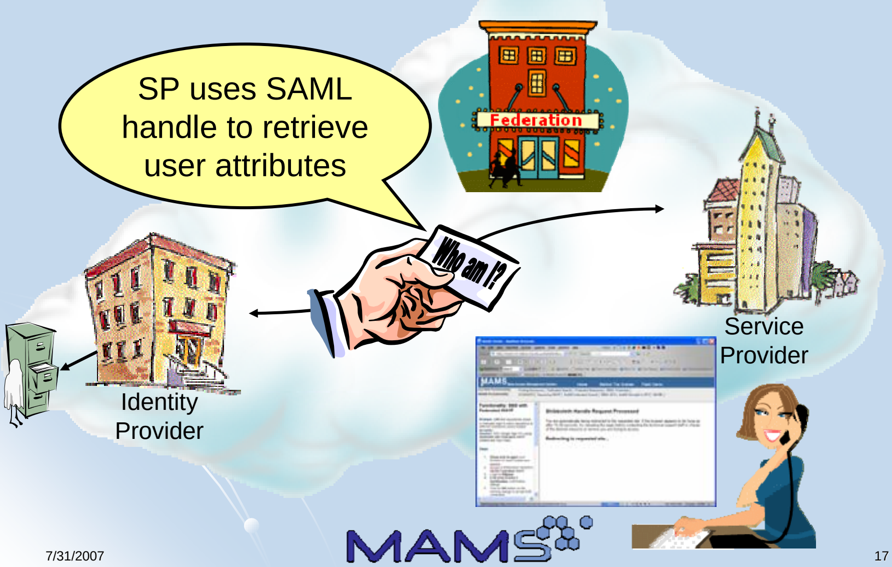

Federation
User is redirected to SP with SAML handle
Service Provider
Identity Provider
MAMS
Shibboleth Handle Request Processed
Redirecting to requested site...

7/31/2007

META ACCESS MANAGEMENT SYSTEM

16

Typical SAML Access Scenario



7/31/2007

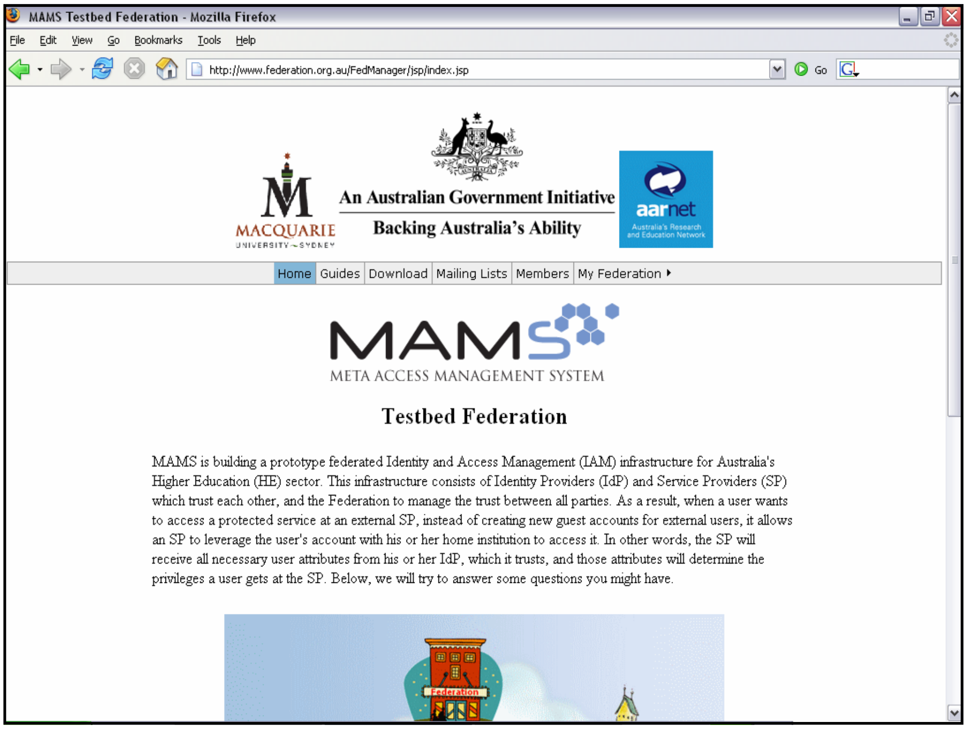
MAMS
META ACCESS MANAGEMENT SYSTEM

17

Benefits

MACQUARIE UNIVERSITY~SYDNEY

- Enhanced collaboration via easy sharing of secure resources and services
- Potential for less duplication of research (and new discoveries building on existing data)
- Home institution login reduces account management, and home institutions can better manage user accounts and security
- Identity assertions are backed by trusted institutions
- Strong privacy management, including “trusted anonymous” option


MAMS Testbed Federation - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.federation.org.au/FedManager/jsp/index.jsp
Go
MACQUARIE
UNIVERSITY~SYDNEY
An Australian Government Initiative
Backing Australia's Ability
aarnet
Australia's Research and Education Network
Home
Guides
Download
Mailing Lists
Members
My Federation
MAMS
META ACCESS MANAGEMENT SYSTEM
Federation

Testbed Federation

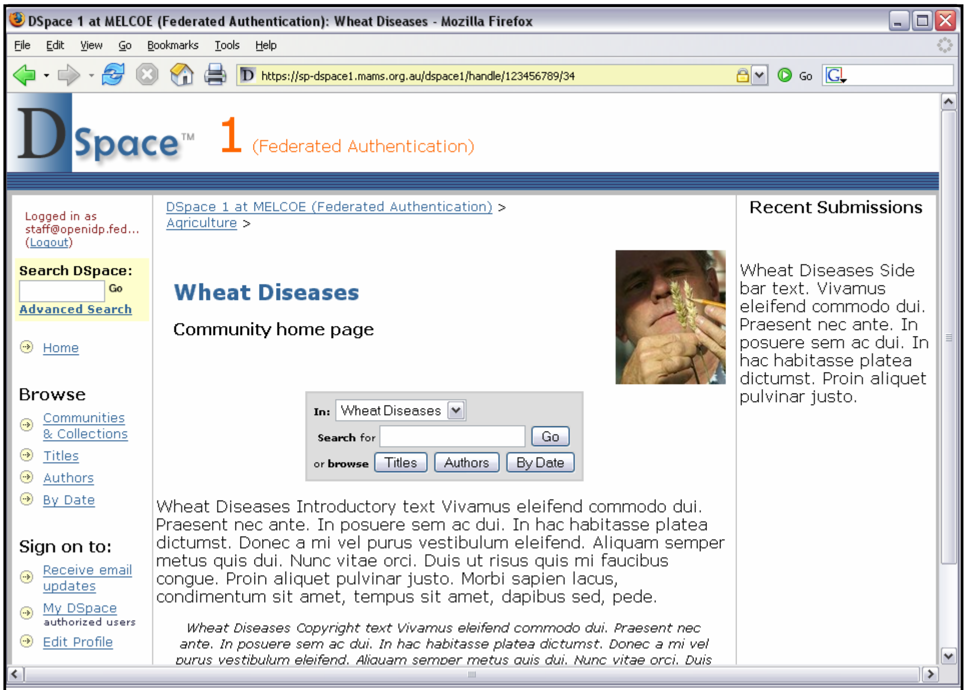
MAMS is building a prototype federated Identity and Access Management (IAM) infrastructure for Australia's Higher Education (HE) sector. This infrastructure consists of Identity Providers (IdP) and Service Providers (SP) which trust each other, and the Federation to manage the trust between all parties. As a result, when a user wants to access a protected service at an external SP, instead of creating new guest accounts for external users, it allows an SP to leverage the user's account with his or her home institution to access it. In other words, the SP will receive all necessary user attributes from his or her IdP, which it trusts, and those attributes will determine the privileges a user gets at the SP. Below, we will try to answer some questions you might have.

Australian Access Federation

- The Australian Access Federation project is taking forward the work of the MAMS (Shibboleth) and e-Security (PKI) projects to develop a unified trust federation for higher education and research
  - Policy and governance
  - PKI and Shibboleth production rollout
  - Adoption support, workshops, supporting systems, etc

Examples of trusted services

- Trusted (secure) repositories (documents, data, media)
  - DSpace (integration of “traditional” application)
  - Fedora (native support for SAML, XACML for authorisation)
  - Others to come
- Secure Real-Time Text Chat
  - Example: Online Librarian
- Trusted Gridsphere portal and Virtual Organisation management (“IAMSuite”)
  - Including access to Grid services via Shibboleth/PKI bridge
- Workflow for collaborative research (“RAMS”)


DSpace 1 at MELCOE (Federated Authentication): Wheat Diseases - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://sp-dspace1.mams.org.au/dspace1/handle/123456789/34
Go
DSpace™ 1 (Federated Authentication)
Search DSpace:
Go
Advanced Search
Home
Browse
Communities & Collections
Titles
Authors
By Date
Sign on to:
Receive email updates
My DSpace
authorized users
Edit Profile
In: Wheat Diseases
Search for
Go
or browse
Titles
Authors
By Date
Recent Submissions

Logged in as staff@openidp.fed... (Logout)

DSpace 1 at MELCOE (Federated Authentication) > Agriculture >

Wheat Diseases

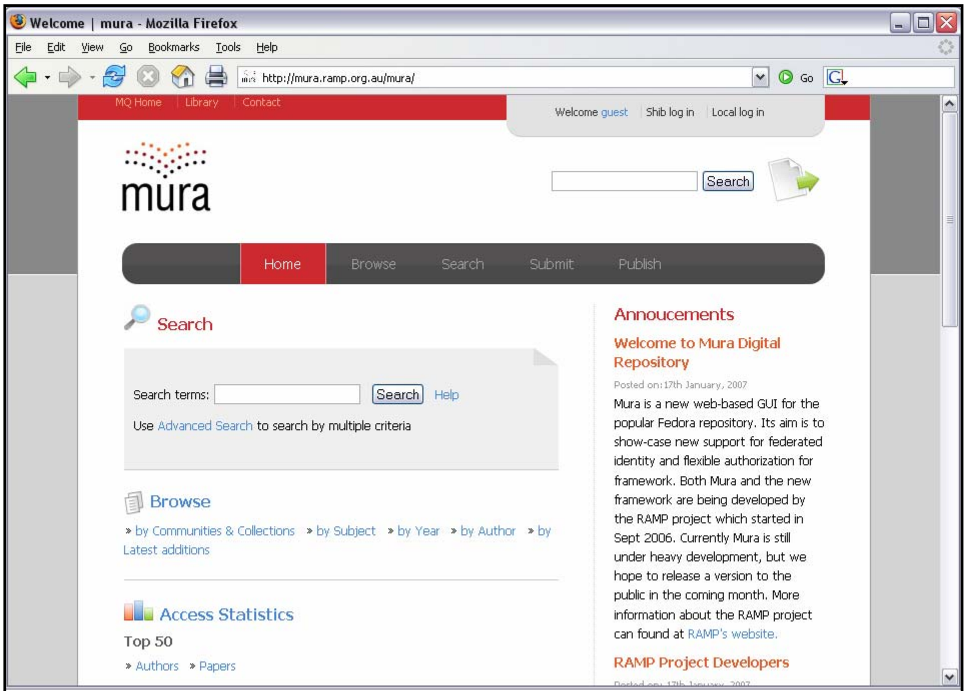
Community home page

Wheat Diseases Introductory text Vivamus eleifend commodo dui. Praesent nec ante. In posuere sem ac dui. In hac habitasse platea dictumst. Donec a mi vel purus vestibulum eleifend. Aliquam semper metus quis dui. Nunc vitae orci. Duis ut risus quis mi faucibus congue. Proin aliquet pulvinar justo. Morbi sapien lacus, condimentum sit amet, tempus sit amet, dapibus sed, pede.

Wheat Diseases Copyright text Vivamus eleifend commodo dui. Praesent nec ante. In posuere sem ac dui. In hac habitasse platea dictumst. Donec a mi vel purus vestibulum eleifend. Aliquam semper metus quis dui. Nunc vitae orci. Duis

Wheat Diseases Side bar text. Vivamus eleifend commodo dui. Praesent nec ante. In posuere sem ac dui. In hac habitasse platea dictumst. Proin aliquet pulvinar justo.

Shibboleth-enabled DSpace repository


Welcome | mura - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://mura.ramp.org.au/mura/
Go
MQ Home | Library | Contact
Welcome guest | Shib log in | Local log in
mura
Search
Home Browse Search Submit Publish

Search

Search terms: Search Help

Use Advanced Search to search by multiple criteria

Browse

» by Communities & Collections » by Subject » by Year » by Author » by Latest additions

Access Statistics

Top 50

» Authors » Papers

Annoucements

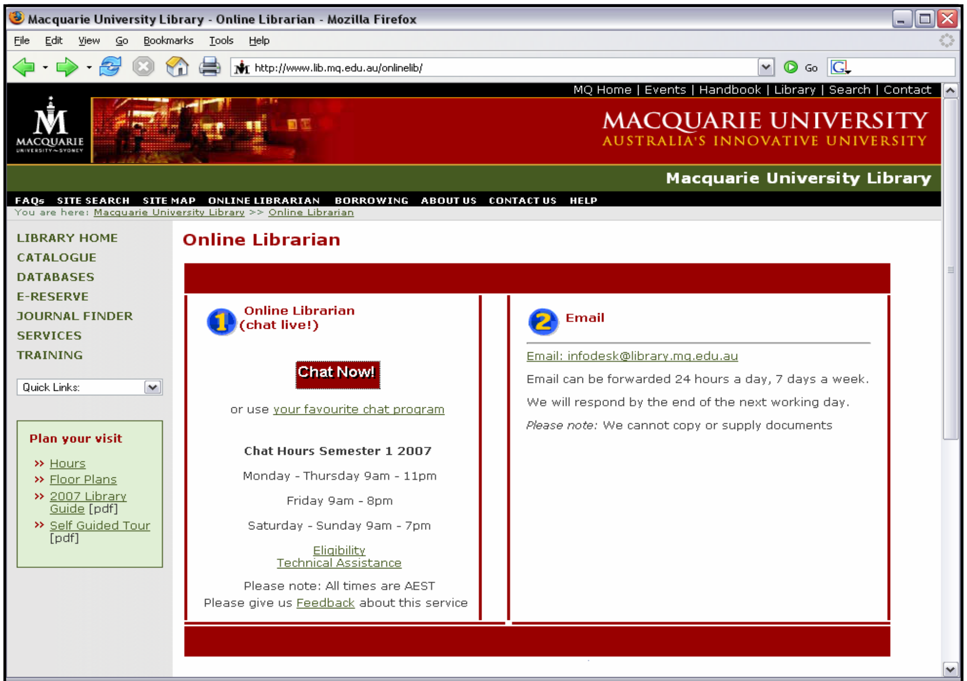
Welcome to Mura Digital Repository

Posted on: 17th January, 2007

Mura is a new web-based GUI for the popular Fedora repository. Its aim is to show-case new support for federated identity and flexible authorization for framework. Both Mura and the new framework are being developed by the RAMP project which started in Sept 2006. Currently Mura is still under heavy development, but we hope to release a version to the public in the coming month. More information about the RAMP project can found at RAMP's website.

RAMP Project Developers

Shibboleth and XACML-based Fedora Repository


Macquarie University Library - Online Librarian - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.lib.mq.edu.au/onlinelib/
Go
MQ Home | Events | Handbook | Library | Search | Contact
MACQUARIE UNIVERSITY~SYDNEY
MACQUARIE UNIVERSITY
AUSTRALIA'S INNOVATIVE UNIVERSITY
Macquarie University Library
FAQs SITE SEARCH SITE MAP ONLINE LIBRARIAN BORROWING ABOUT US CONTACT US HELP
You are here: Macquarie University Library >> Online Librarian
LIBRARY HOME
CATALOGUE
DATABASES
E-RESERVE
JOURNAL FINDER
SERVICES
TRAINING
Quick Links:

Plan your visit

- Hours
- Floor Plans
- 2007 Library Guide [pdf]
- Self Guided Tour [pdf]

Online Librarian

1 Online Librarian (chat live!)

Chat Now!

or use your favourite chat program

Chat Hours Semester 1 2007

Monday - Thursday 9am - 11pm

Friday 9am - 8pm

Saturday - Sunday 9am - 7pm

Eligibility
Technical Assistance

Please note: All times are AEST
Please give us Feedback about this service

2 Email

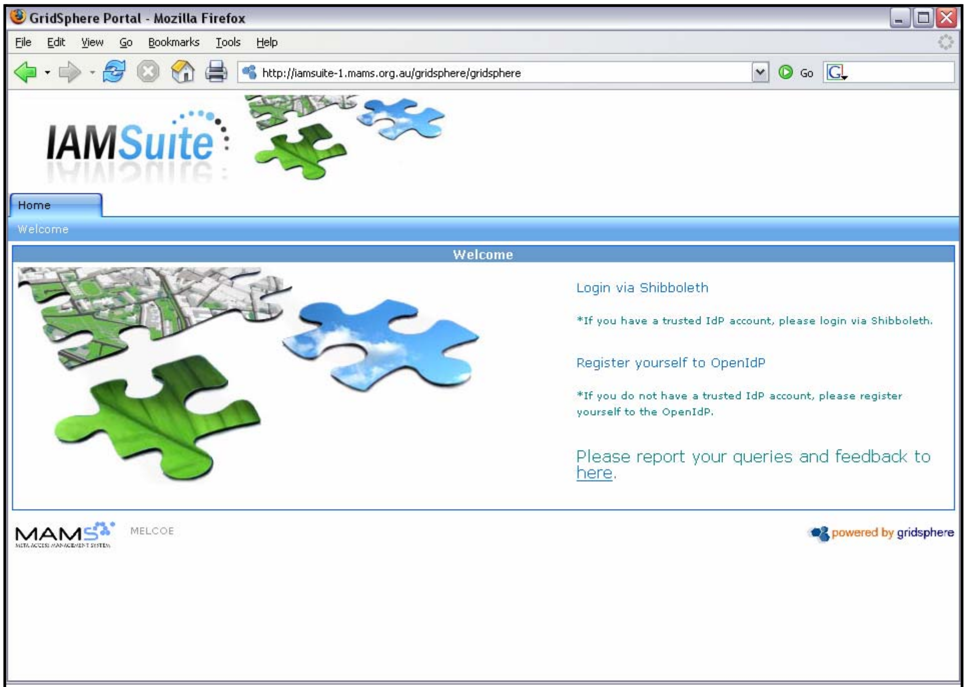
Email: infodesk@library.mq.edu.au

Email can be forwarded 24 hours a day, 7 days a week.

We will respond by the end of the next working day.

Please note: We cannot copy or supply documents

Shibboleth-based Secure chat service – Online Librarian


GridSphere Portal - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://iamsuite-1.mams.org.au/gridsphere/gridsphere
Go
IAMSuite
Home
Welcome
MAMS
METADATA ACCESS MANAGEMENT SYSTEM
MELCOE
powered by gridsphere

Welcome

Login via Shibboleth

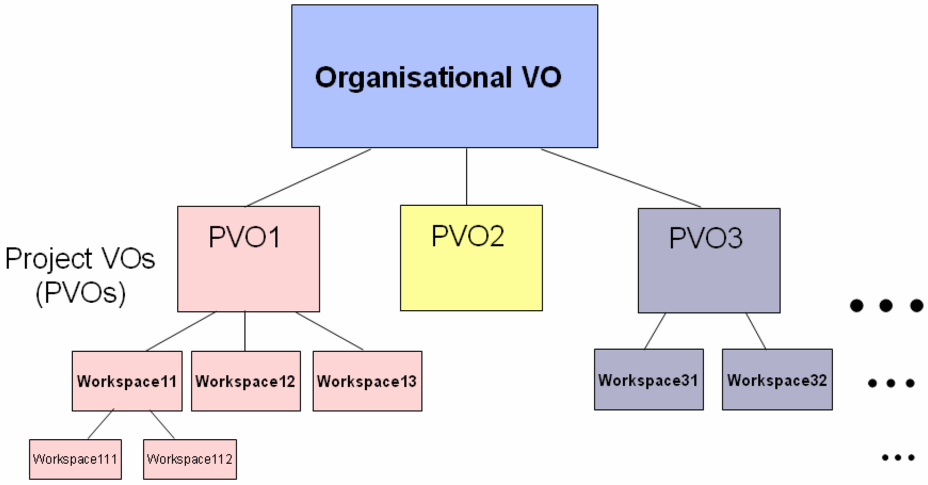
*If you have a trusted IdP account, please login via Shibboleth.

Register yourself to OpenIdP

*If you do not have a trusted IdP account, please register yourself to the OpenIdP.

Please report your queries and feedback to here.

Shibboleth-based Virtual Organisation system - IAMSuite


Organisational VO

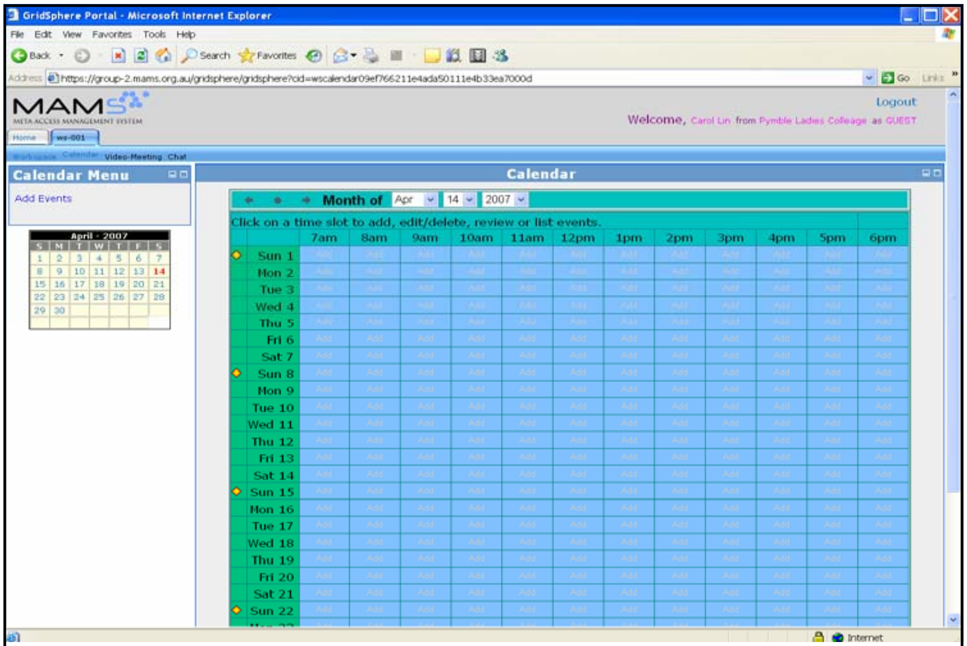
Project VOs (PVOs)

PVO1 · PVO2 · PVO3 · • • •

Workspace11 · Workspace12 · Workspace13 · Workspace31 · Workspace32 · • • •

Workspace111 · Workspace112 · • • •

IAMSuite Toolkit for management of Virtual Organisations (secure workspaces)


GridSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://group-2.mams.org.au/gridsphere/gridsphere?cid=wscalendar09ef766211e4ada50111e4b33ea7000d
Go Links
MAMS
META ACCESS MANAGEMENT SYSTEM
Logout
Welcome, Carol Lin from Pymble Ladies Colleage as GUEST
Home ws-001
Workspace Calendar Video-Meeting Chat
Calendar Menu
Add Events
Calendar
Month of Apr 14 2007
Internet

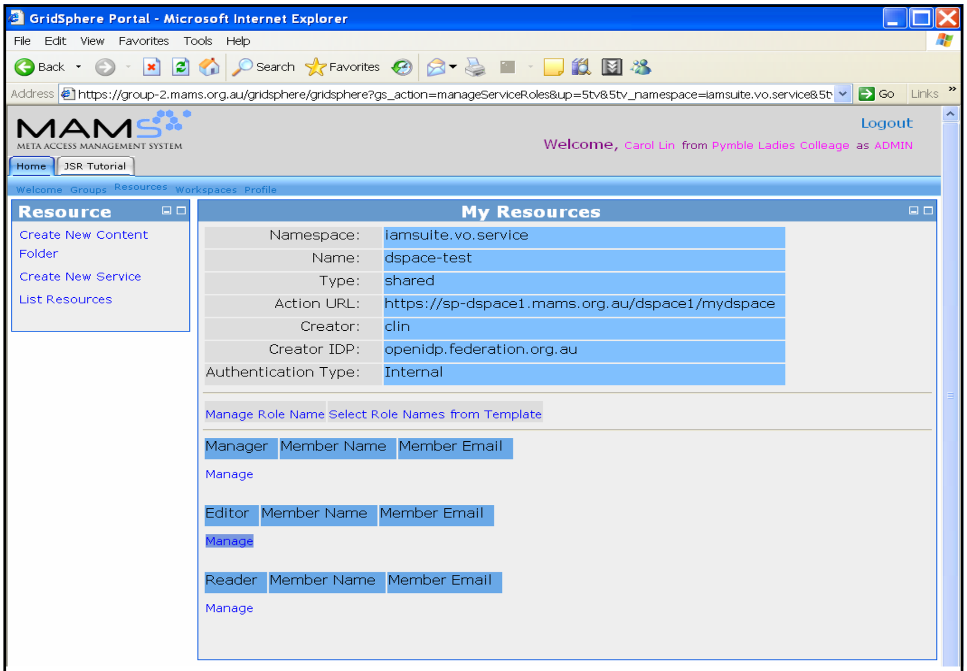
April - 2007

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Click on a time slot to add, edit/delete, review or list events.

		7am	8am	9am	10am	11am	12pm	1pm	2pm	3pm	4pm	5pm	6pm
◆	Sun 1	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Mon 2	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Tue 3	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Wed 4	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Thu 5	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Fri 6	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Sat 7	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
◆	Sun 8	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Mon 9	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Tue 10	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Wed 11	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Thu 12	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Fri 13	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Sat 14	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
◆	Sun 15	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Mon 16	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Tue 17	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Wed 18	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Thu 19	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Fri 20	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
	Sat 21	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add
◆	Sun 22	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add	Add

IAMSuite: Example of VO tools – shared calendar service


GridSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://group-2.mams.org.au/gridsphere/gridsphere?gs_action=manageServiceRoles&up=5tv&5tv_namespace=iamsuite.vo.service&5t
Go Links
MAMS
META ACCESS MANAGEMENT SYSTEM
Logout
Welcome, Carol Lin from Pymble Ladies Colleage as ADMIN
Home JSR Tutorial
Welcome Groups Resources Workspaces Profile
Resource
Create New Content Folder
Create New Service
List Resources
My Resources

Namespace:	iamsuite.vo.service
Name:	dspace-test
Type:	shared
Action URL:	https://sp-dspace1.mams.org.au/dspace1/mydspace
Creator:	clin
Creator IDP:	openidp.federation.org.au
Authentication Type:	Internal

Manage Role Name Select Role Names from Template

Manager	Member Name	Member Email

Manage

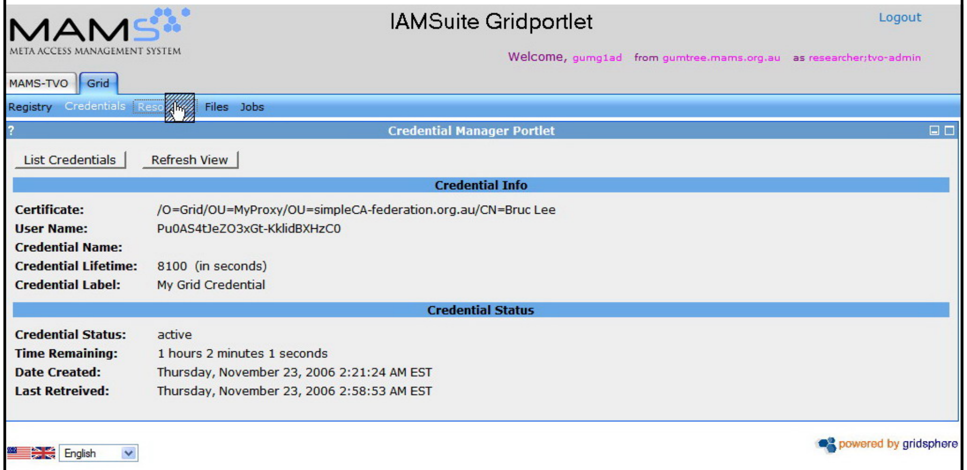
Editor	Member Name	Member Email

Manage

Reader	Member Name	Member Email

Manage

IAMSuite VO: Configuring User Authorisation for Trusted Services



IAMSuite Gridportlet

Welcome, gumg1ad from gumtree.mams.org.au as researcher:tvo-admin

Credential Manager Portlet

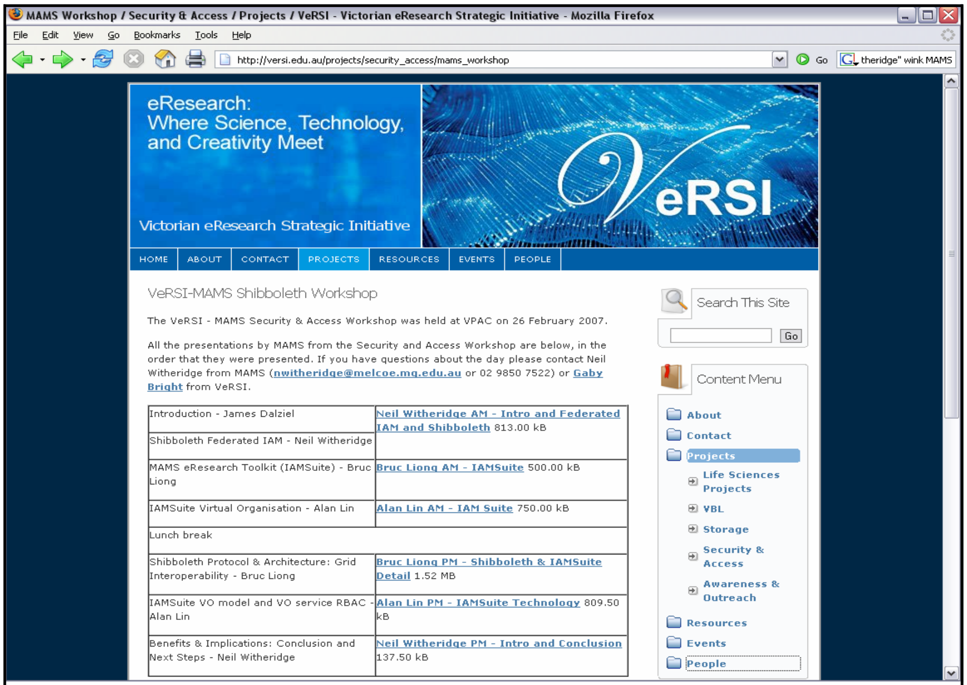
Credential Info

Certificate: /O=Grid/OU=MyProxy/OU=simpleCA-federation.org.au/CN=Bruc Lee
User Name: Pu0AS4tJeZO3xGt-KklidBXHzC0
Credential Name:
Credential Lifetime: 8100 (in seconds)
Credential Label: My Grid Credential

Credential Status

Credential Status: active
Time Remaining: 1 hours 2 minutes 1 seconds
Date Created: Thursday, November 23, 2006 2:21:24 AM EST
Last Retreived: Thursday, November 23, 2006 2:58:53 AM EST

IAMSuite integration with Grid Portlet for Certificates



MAMS Workshop / Security & Access / Projects / VeRSI - Victorian eResearch Strategic Initiative - Mozilla Firefox

VeRSI-MAMS Shibboleth Workshop

The VeRSI - MAMS Security & Access Workshop was held at VPAC on 26 February 2007.

All the presentations by MAMS from the Security and Access Workshop are below, in the order that they were presented. If you have questions about the day please contact Neil Witheridge from MAMS (nwitheridge@melcoe.mq.edu.au or 02 9850 7522) or Gaby Bright from VeRSI.

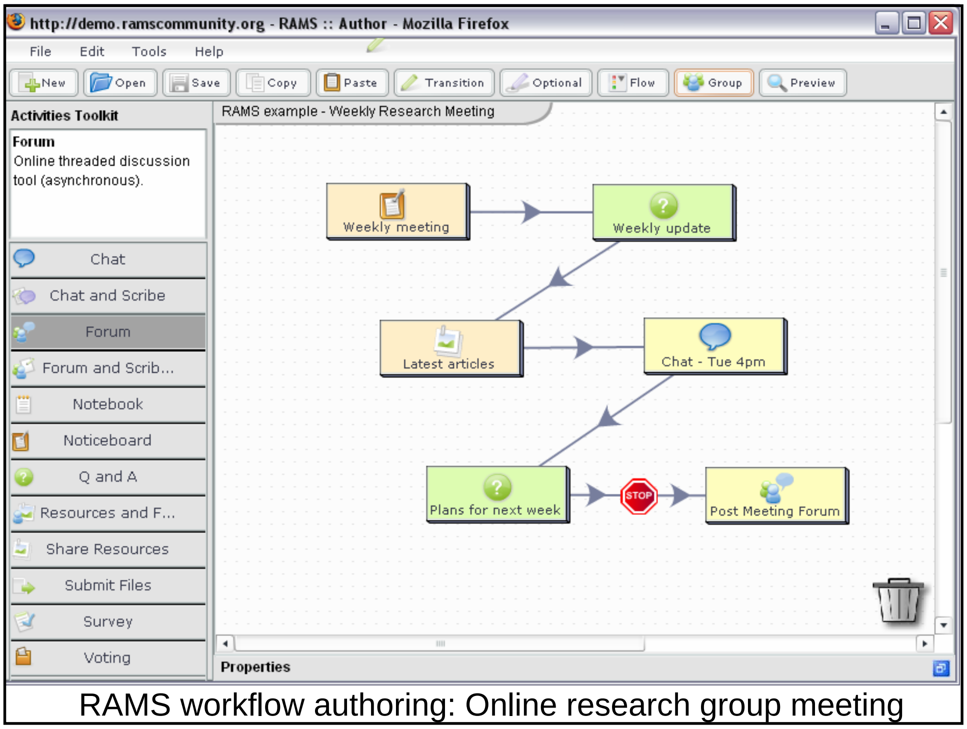
Introduction - James Dalziel	Neil Witheridge AM - Intro and Federated IAM and Shibboleth 813.00 kB
Shibboleth Federated IAM - Neil Witheridge	
MAMS eResearch Toolkit (IAMSuite) - Bruc Liong	Bruc Liong AM - IAMSuite 500.00 kB
IAMSuite Virtual Organisation - Alan Lin	Alan Lin AM - IAM Suite 750.00 kB
Lunch break	
Shibboleth Protocol & Architecture: Grid Interoperability - Bruc Liong	Bruc Liong PM - Shibboleth & IAMSuite Detail 1.52 MB
IAMSuite VO model and VO service RBAC - Alan Lin	Alan Lin PM - IAMSuite Technology 809.50 kB
Benefits & Implications: Conclusion and Next Steps - Neil Witheridge	Neil Witheridge PM - Intro and Conclusion 137.50 kB

MAMS is leading the Security and Access stream for VeRSI eResearch projects

MACQUARIE
UNIVERSITY~SYDNEY

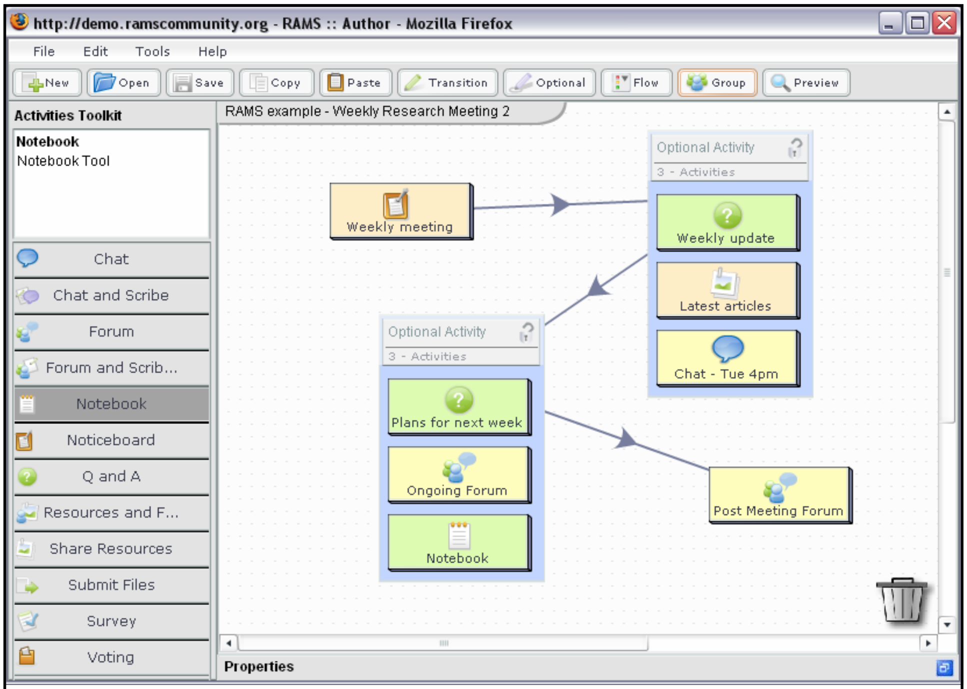
RAMS

- Research Activity Management System is a new workflow system for collaborative research activities
- Focus on research workflows that involve groups of researchers colalborating over multiple steps
  - New data processing and branching functions in V2.1
- For information, downloads and demo accounts, see
  - http://rams.ramp.org.au/


http://demo.ramscommunity.org - RAMS :: Author - Mozilla Firefox

Forum
Online threaded discussion tool (asynchronous).

RAMS workflow authoring: Online research group meeting



RAMS workflow authoring: Alternative example of online research group meeting

Australian National Data Service

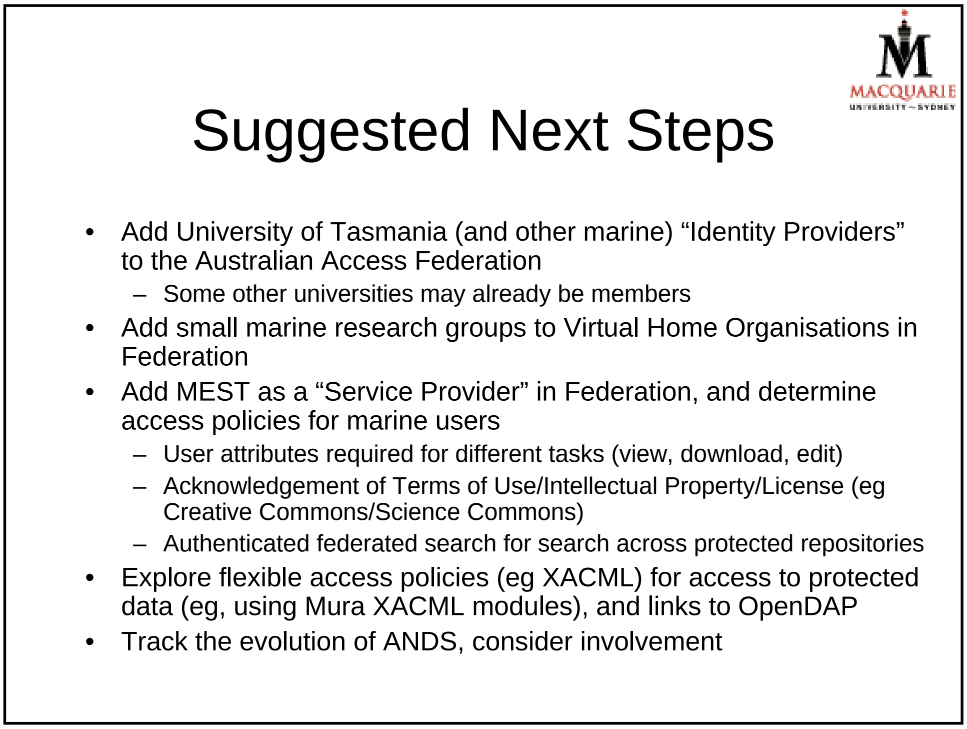
- ANDS is one of the major components of NCRIS 5.16
- Three major components:
  - Federation services – infrastructure to support federated repositories for research data and related common services
  - Stewardship services – support for metadata, curation, archival,
  - Outreach services – support services for data management, choice of software – to be available around the country
- ANDS currently being finalised, planned for launch late 2007/early 2008
- For current details, see 5.16 Investment Plan

Implications for IMOS - Authentication

- The Australian Access Federation provides the foundations for trusted identities from trusted partners
  - Trusted collaboration across organisational boundaries
- Large research organisations (Unis, CSIRO) join the Australian Access Federation as an Identity provider directly (ie, install Shibboleth IdP linked to directory)
- Smaller organisations, or large organisations with a small number of researchers, can join via the “Virtual Home Organisation”
  - Facility provided by Federation as a proxy for own IdP

Implications for IMOS – Authentication (data access)

- The combination of Australian Access Federation and flexible access control policies (eg, XACML) provides the foundation for management of secure data
  - Completely open data can be directly available on the internet
- Different policies for different datasets – controlled by:
  - Identity, user role, organisation
  - Location
  - Time (eg, closed at first, open later on)
  - Actions (eg, open to view, closed to analyse, edit, etc)
- Explore integrating OpenDAP with Shibboleth & XACML
- “Authenticated Federated Search” – potential to search across secure datasets according to access rights



Suggested Next Steps

- Add University of Tasmania (and other marine) “Identity Providers” to the Australian Access Federation
  - Some other universities may already be members
- Add small marine research groups to Virtual Home Organisations in Federation
- Add MEST as a “Service Provider” in Federation, and determine access policies for marine users
  - User attributes required for different tasks (view, download, edit)
  - Acknowledgement of Terms of Use/Intellectual Property/License (eg Creative Commons/Science Commons)
  - Authenticated federated search for search across protected repositories
- Explore flexible access policies (eg XACML) for access to protected data (eg, using Mura XACML modules), and links to OpenDAP
- Track the evolution of ANDS, consider involvement