The AAF and Shibboleth

eResearch Australasia 2007

Prof. James Dalziel
james@melcoe.mq.edu.au

Neil Witheridge
nwitheridge@melcoe.mq.edu.au

Dr. Aizhong Lin
alin@melcoe.mq.edu.au

Macquarie E-Learning Centre of Excellence (MELCOE)
Macquarie University

MAMS Background

DEST funded project
  - under Systemic Infrastructure Initiative (SII)
  - seeking to improve national research effectiveness

Initial focus (FRODO projects) covering
  - Repository Projects (ARROW, APSR, ADT)
  - Identity & Access Management (IAM) project (MAMS)

At the heart of the middleware required to unleash research potential is the cluster of services described as “access and identity management”.
Demostration of MAMS Testbed Federation

- Accessing public and protected resources in the Fryer Library collection at the University of Queensland’s ESpace repository

Shibboleth Federated IAM Middleware

- Federation Entities

  - Identity Provider: Secure identity management is a core business requirement
  - Federation Manager
  - Service Provider: Provide Services accessible via the web
  - WAYF Agent
  - Agreement Policies Auditing
  - User: Belongs to an organisation which manages their identity
  - Privacy concerns
  - Want to focus on core business & avoid risks of managing users’ confidential info.
Shibboleth Protocol - User Authentication

1. Access SPA

2. WAYF Where are you From?

3. Authenticate at Identity Provider

4. Redirect User back to Service Provider with 'opaque' user handle

5. Request User Attributes

6. Provide User Attributes

7. Decide what User can Access Based on Attributes

Manages User's 'identity' including 'attributes':
her name, affiliation, role, department...

Shibboleth Protocol - User Attribute Transfer

Implements SAML (an OASIS Standard):
Security Assertion Markup Language
(SAML provides for securely transfer of user attributes)

1. Access SPA

2. WAYF Where are you From?

3. Authenticate at Identity Provider

4. Redirect User back to Service Provider with 'opaque' user handle

5. Request User Attributes

6. Provide User Attributes

7. Decide what User can Access Based on Attributes

(Authenticated) User

SPA

SPb

WAYF

SPa

UserX

Identity Provider

Service Provider
META ACCESS MANAGEMENT SYSTEM

Identity Provider

Within authenticated session, SSO to other service providers in Federation (uses session cookies)

Another Service Provider

Attribute Release Policy for SP for U

Decide what User can Access based on Attributes

SSO !

Redirect Authenticated User back to Service Provider with 'opaque' user handle

You can have these

Gimme attributes

Recap: Shibboleth Protocol - Single Sign On

MAMS deliverables

- MAMS Testbed Federation (Levels 1, 2, 3)
  - Federation Manager
- Roadshows, Workshops for Australian HE
- Shibboleth deployment aids: IdP Easy Installation CD (Knoppix), VMWare image (Debian Linux + IdP/SP)
- MiniGrant Scheme (Rounds 1 and 2)
- ShARP: Shib Attribute Release Policy Editor
- Autograph: User control of their user ARP
MAMS deliverables (cont’d)

- Shibbolized Applications
  - DSpace, Fedora, Zope/Plone, Twiki, Moodle…
  - Authenticated Federated Search service
  - OpenIdP, PeoplePicker (eSecurity funded)
  - Shibboleth protected IM (Online Librarian & generic helpdesk application)
  - Access control using XACML (Fedora)

- Secure VO Infrastructure (IAM Suite)
  - Shib-enabled Gridsphere portal
  - basis of current collaboration with VeRSI

- Shib-enabled MyProxy
  - enabling Shib access to Grid Services

- Delegated Attribute Retriever (DAR) & Authentication State Manager (ASM)
  - Shib-enablement of non-web applications.

MAMS Testbed Federation

http://federation.org.au/FedManager/listMembers.do

“Level-2” Federation (at 26/6/07):

21 Service Providers
19 Identity Providers (~900,000 identities)
MAMS Mini-Grant Program
(2 rounds of 5 projects, AUS$40k per project)

Round 1 (Feb 2006):
- AARNet: IdP, ENUM IdP, ENUM SP
- Griffith Uni: IdP, IT Department Wiki SP
- Uni of Qld: IdP, eSpace Fedora+Fez SP
- Qld Uni of Technology: ATN IdPs, eGrad School SP
- Uni of Sydney: IdP, NANO image database SP

Round 2 (Jul 2006):
- Deakin Uni:* IdP, eLectures SP
- James Cook Uni: IdP, JCU/AlMS data access SP
- Melbourne Uni: IdP, LIGO data access SP
- Monash Uni:* IdP, Shibbolised SRB SP
- Murdoch Uni: IdP, Online Librarian SP
- Curtin Uni: 5 IdPs (WAGUL), Reciprocal Borrowing SPs

* Shared project funding

Demo: Shibboleth SP examples
- Information Repository Service
  - accessing using Macquarie University identity
  - UQ ePrints Service (https://espace.library.uq.edu.au/)
- Collaborative Tools
  - Shibboleth Wiki
- Sharing Library Service
  - WAGUL Reciprocal Borrowing
  - Borrower Registration, Workstation Authentication
- Database Access Service
  - UQ/USyd NANO Project
  - Image database

One name and password = access to many services.
Australian Access Federation

- DEST funded project to develop an operational Trust Federation for Australian HE and Research sector - the Australian Access Federation (AAF)
- Led by the University of Queensland, with Macquarie University and AusCERT as partners.
- AAF sub-projects:
  - AAF Governance & Policy (UQ)
  - PKI for Australian HE (UQ, AusCERT)
  - Shibboleth Trust Federation (MAMS)

AAF Shibboleth Trust Fed Schedule

- Deployment & Integration (2007)
  - Technology
    - Federation Management interfaces
    - PKI Interfaces
    - Shared ('Federation level') Services
    - Grid Services interfaces
    - High-availability infrastructure
    - SP/IdP Deployment aids
  - Policy Development
  - Outreach (workshops, roadshows)
  - Minigrants
- First release (early 2008)
  - Bootstrapping phase
  - IdP auditing
- Second Release (late 2008)
AAF Shibboleth Trust Federation

Services & Shib-enabled App’s

- Shared/Hosted Services
  - Federated Directory Search
- Shibboleth enabled applications & collaboration tools
  - DSpace, Fedora repositories
  - Confluence (& other wiki’s)
  - JIRA (action/defect tracking)
  - Secure Instant Messaging (e.g. for HelpDesk)
  - eResearch VO Toolkit (IAMSuite)
- Grid Services Interoperability
Solution: IAMSuite
A Shibboleth-based Identity and Access Management Suite

IAMSuite Objectives

- Provide a **Shibboleth-enabled Single-Sign-On VO infrastructure** for secure inter-institutional collaboration.
- Provide an **integrated and shared environment** for accessing protected resources (e.g. research data) and services (e.g. generic or research-specific collaboration tools).
- Provide a **portal** for accessing VO resources and services (portlets, stand-alone web applications, or Grid services)
- Provide a **general framework** for developers to build and contribute collaborative applications
**Federation Architecture + IAMSuite**

**Federation Level**
- WAYF
- MyProxy server
- CA?
- Gateway (CTS)

**Institutions Level**
- IdP1@UQ
- IdP2@MQ
- IdPn@UTS
- IR
- GTK: Grid
- GTK: HPC
- GTK: Store
- MyProxy Client
- VO IdP

**Virtual Org. Level**
(e.g. inter-institution eResearch project)
- CTS
- VO Portal
- Gridsphere (based)
- SP: Forum
- SP: Wiki
- SP: CMS

**VO, Sub-VO’s & Workspaces**

**Organisational VO**

**Project VOs (PVOs)**
- PVO1
- PVO2
- PVO3

**Workspaces**
- Workspace11
- Workspace12
- Workspace13
- Workspace31
- Workspace32
- Workspace33

(Gridsphere-based)
Home Institution Authentication

Click here
**VO Service**

External Service Integration

![VO Service](image1)

Add the Integrated Service to Workspace

![Add the Integrated Service to Workspace](image2)
Successfully accessed with SSO

Thank you

Questions?