Implementing Authorised Access

Dr. Erik Vullings
MAMS Programme Manager
Erik.Vullings@melcoe.mq.edu.au
DEST founded ARIIC to guide:
- Australian Digital Thesis (ADT)
- Australian Partnership for Sustainable Repositories (APSR)
- Australian Research Repositories Online to the World (ARROW)
- Meta Access Management System (MAMS)
  - Financed by DEST till the end of 2006 ($4.2 million)

FRODO (Federated Repositories of Digital Objects)
META ACCESS MANAGEMENT SYSTEM

Single Sign-On

Digital Identity Mgmt

Federated Identity Mgmt

Access Control

Provisioning

Legacy plug-ins

Federated search

Single Sign-On

Digital Identity Mgmt

thomaslornsen@gmx.de
How open is your IR really?

My institutional repository is open:

- Submissions use separate client
- For internal members, but external people have to wait some time
- And staff can self submit
- But only peers can rank & annotate
- Except for some special content (e.g. data/source files) – my faculty only
- Except for reviewing prepublications, which are only for some colleagues
What Access Control do you need?

- None
- IP-based is sufficient
- With Authentication
  - Access Control Lists:
    - If you are on the list, you are in
  - Role-Based Access Control:
    - Your role gives you certain rights
  - Attribute Based Access Control:
    - Your attributes give you certain rights
Which attributes does the IR need?

When I visit an IR, how do I present myself?

Reference #123456
Staff at Macquarie Uni

Erik Vullings
ICT Staff at Macquarie

Erik Vullings
Erik@mq.edu.au
ICT Staff at Macquarie
+61-(0)2-9850.6537

MQ
Different cards open different doors

- Services & Service Level -

Reference #123456
Staff at Macquarie Uni

Enables access to some of the IR

Erik Vullings
ICT Staff at Macquarie

Enables access to all of the IR

Erik Vullings
Erik@mq.edu.au
ICT Staff at Macquarie
+61-(0)2-9850.6537

Allows me to submit content
How do I get your attributes?

- Solution: Use local LDAP
- Problem: What about external users?
- Solution: Create guest account
- Problem: Users have too many passwords
- Solution: Use MAMS Testbed Federation based on Shibboleth
- Problem: Huh???
Federation Components

- **Manages trust between parties.**
- **Auditing**

**Identity Provider**
- Attribute Authority manages and asserts (to trusted SPs) user’s attributes securely.

**Service Provider**
- Provides services to internal and external users via the web.
- Want to focus on core business & avoid risks of managing users’ confidential info.

- Have privacy concerns.
- Want transparent but secure SSO.
Typical SAML Access Scenario

User wants to access IR

Identity Provider

Institutional Repository

Federation
Typical SAML Access Scenario

- Identity Provider
- Shibboleth
- Apache filter intercepts
- Federation
- Institutional Repository

MAMS
META ACCESS MANAGEMENT SYSTEM
Typical SAML Access Scenario

User is redirected and selects IdP: Where Are You From

Identity Provider

Federation

Institutional Repository
Typical SAML Access Scenario

User is redirected to IdP and logs in
Typical SAML Access Scenario

Identity Provider

IdP uses Attribute Release Policy for SAML assertion

Institutional Repository

Federation
Typical SAML Access Scenario

User is redirected to IR with SAML handle

Identity Provider

Institutional Repository

Federation
Typical SAML Access Scenario

IR uses SAML handle to retrieve user attributes
Typical SAML Access Scenario

Shibboleth validates assertion and maps user to IR role
Shibboleth and SSO

- The previous example illustrates INTER-institutional SSO
- However, it can also be used for INTRA-Institutional SSO
  - Not only for IR, but potentially any application (like E-Learning systems or dataset repositories)
What about Access Control?

— One Language to Rule Them All —

- eXtended Access Control Markup Language (XACML)

Enable Shibboleth Access

- IR 1 Fedora
- IR 2 DSpace
- Institutional XACML Policy Store
- Federation XACML Policy Store
XACML in Action

JOE wants to EDIT his PREPRINT

Policy Enforcement Point (PEP)
Create XACML request
Respond with Permit/deny/obligation

Policy Access Point (PAP)
Retrieve Policies

Policy Decision Point (PDP)

Policy Information Point (PIP)
Retrieve Information
XACML and Rights Expression

- XACML for fine-grained access control
- Digital Rights Expression Languages (DRELs) manage a wide range of digital rights
- MAMS view:
  - Leave the legal bit to the lawyers
  - Just focus on access control
Testing XACML with Fedora

MAMS XACML-Based Repository

Welcome to MAMS repository utilizing Fedora, XACML and Shibboleth technology.

You are currently logged in as staffmams@gmail.com
You have the following roles: Staff

- **Search** Search allows you to perform simple search on our repository
- **Submit** Submit allows you to add a new item to the repository
- **Publish** Publish allows you to change a previously submitted item to be visible during search.

Powered By:

[Shibboleth logo]
MAMS activities in Authorization

- **Existing work to date**
  - Web-based XACML demo
  - Authenticated Federated Search (XACML)
  - Testing XACML with Fedora

- **New work for 2006**
  - Defining key XACML policies for IR
  - Further develop MAMS Fedora+XACML IR
  - Visual XACML editor (XML-free)