Identity Services for Open Source Software
Outline

- TomB - Intro - Identity Services Summit
- Andrew – Layering ID services in Jasig community products
- Eric – Kuali Identity Management and Grouper integration
- TomD – Access management Bable fish
- Bob – ID services and the larger community
- Panelists & attendees - Questions and discussion
• Consortium of Universities building an enterprise-level, easy-to-install open source podcast and rich media capture, processing and delivery system.

• Typical security issues need to be handled
  – User authentication
  – Service authentication
  – Proxy authentication
  – Long-running processes
  – Integration with enterprise services
  – Out-of-box support for enterprises lacking those services
“Is this a problem that the Matterhorn software needs to solve?

... I hope we can come up with a cheap & easy solution in order to get on with our fundamental tasks involving the handling of media.”

Josh Holtzman, Matterhorn Team member
opencast list, May 15, 2009
Enterprise IAM

Policy and Governance

Establish identity

Determine policy

Source Systems

- HR
  - faculty, staff
- SA
  - student, postdoc
- Finance
  - PI, approver
- Courses
  - instructor, enrolled

Reflect & Join

Manage Identity

Persons

Accounts

Organizations

Groups

Privileges

Authenticate

Authorize

Provide

Federate

Enrich identity

Apply policy

Manage Groups

Manage Privileges

Systems and Services

- Business systems
- Network services
- Library
- Federated partners
WANTED:
Domesticated applications

- Integrate collaboration tools into a common platform
- User and collaboration centric identity, not tool-based identity

- COmanage
- SURFGroepen
- Sympa as VO group manager
- Duke’s OZ
The identity services problem

Applications can't be developed that easily integrate with outboard IAM services until there's broadly held agreement on the interfaces between the two.
Everyone’s a Yertle

- Application developers
- Platform developers
- Framework developers
- Standards bodies
  - Too many
  - Not enough
- Communities of practice
  - HE/Research
  - Web 2.0+
- Integrators
- Deployers
Don’t try to solve the general problem!

Focus on a small set of related, constrained use cases and make progress on those
Some action items from the Summit

- Access management glossary and mapping between open source projects
- KIM – grouper service implementation proof of concept
- Shibbolized & CASified .NET
- Bedework & COmanage discovery
- Development frameworks and access management picture
<table>
<thead>
<tr>
<th>Gmail</th>
<th>Unicon Zimbra</th>
<th>Refresh Account</th>
<th>Add/Modify Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Larkspur Hotels &amp; Restaurants</td>
<td>Your recent stay at Larkspur Landing Sacramento</td>
<td>12:56 pm</td>
<td></td>
</tr>
<tr>
<td>REI Gearmail</td>
<td>REI Labor Day Sale and Clearance on Now</td>
<td>12:04 pm</td>
<td></td>
</tr>
<tr>
<td>&quot;StickyMinds.com&quot;</td>
<td>Tap Hidden Savings in the Build and Test Process</td>
<td>11:20 am</td>
<td></td>
</tr>
<tr>
<td>Southwest Click 'n Save</td>
<td>It's not too late for a last-minute getaway for Labor Day</td>
<td>10:08 am</td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td>String of Pearls is now following you on Twitter!</td>
<td>9:46 am</td>
<td></td>
</tr>
</tbody>
</table>
Current Accounts:
- Gmail Username: unicon.sales@gmail.com  
  Password:  
  Update  Delete
- apetro personal gmail Username: microcline  
  Password:  
  Update  Delete
- Unicon Zimbra  

Add Account:
- Unicon Zimbra
- Unicon Dev Zimbra
- Gmail

Description:  
Username:  
Password:  
Add

Your account information is encrypted and stored in a secure database in order to connect with your external mail account.
<table>
<thead>
<tr>
<th>Att. Name</th>
<th>Att. Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available attributes:</td>
<td></td>
</tr>
<tr>
<td>serverName</td>
<td>build.fluidproject.org</td>
</tr>
<tr>
<td>displayName</td>
<td>Admin User</td>
</tr>
<tr>
<td>givenName</td>
<td>Admin</td>
</tr>
<tr>
<td>user.name.given</td>
<td>Admin</td>
</tr>
<tr>
<td>sn</td>
<td>User</td>
</tr>
<tr>
<td>user.name.family</td>
<td>User</td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:admin.user@example.org">admin.user@example.org</a></td>
</tr>
<tr>
<td>user.home-info.online.email</td>
<td><a href="mailto:admin.user@example.org">admin.user@example.org</a></td>
</tr>
<tr>
<td>uid</td>
<td>admin</td>
</tr>
<tr>
<td>username</td>
<td>admin</td>
</tr>
<tr>
<td>user.login.id</td>
<td>admin</td>
</tr>
<tr>
<td>Unavailable attributes:</td>
<td></td>
</tr>
</tbody>
</table>
# Attribute Swapper Portlet

## Lookup Person

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Original Value</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name (displayName)</td>
<td>Admin User</td>
<td>Admin User</td>
</tr>
<tr>
<td>First Name (givenName)</td>
<td>Admin</td>
<td>Admin</td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:admin.user@example.org">admin.user@example.org</a></td>
<td><a href="mailto:admin.user@example.org">admin.user@example.org</a></td>
</tr>
<tr>
<td>Last Name (sn)</td>
<td>User</td>
<td>User</td>
</tr>
<tr>
<td>user.home-info.online.email</td>
<td><a href="mailto:admin.user@example.org">admin.user@example.org</a></td>
<td><a href="mailto:admin.user@example.org">admin.user@example.org</a></td>
</tr>
<tr>
<td>Last Name (user.name.family)</td>
<td>User</td>
<td>User</td>
</tr>
<tr>
<td>First Name (user.name.given)</td>
<td>Admin</td>
<td>Admin</td>
</tr>
</tbody>
</table>

[Update Attributes] [Reset Attributes]
Attribute Swapper Portlet

New Search
Found 2 users:

• Student User (student)
  • Select User's Attributes · View Details
  • displayName: Student User
  • username: student
  • mail: student.user@example.org

• Student Layout Owner (student-lo)
  • Select User's Attributes · View Details
  • displayName: Student Layout Owner
  • username: student-lo

New Search
Groups Manager

Search

For Channel whose name contains

- search only descendants of the selected group

Browse

- Root Groups
  - All categories
  - Academics
  - Administration
  - Advisor
  - Demonstration
  - Development
  - Entertainment
  - Finances
  - Information
  - Instructors
  - Library
  - News
  - Research
  - Services
  - Testing
  - Work

Group Details

- Edit Group
- Close Group

Information

Informational Portlets

Members

- Bookmarks
  - Show Info

- Calendar
  - Show Info
Groups Manager

Assign By Owner

Assign Permissions for Targets of this Owner:

Target: Information
- Delete this group
- Rename this group
- View this group
- Manage this group's members
- Assign Permissions for this group

Activities:

Principals:
- DENY

Staff (Group):
- DENY
- GRANT
- DENY

Submit  Reset Form
uPortal permissions

• Per OWNER, PRINCIPAL may ACTION on TARGET.

• According to the groups manager, members of the portlet developers group may edit the membership of the portlet testers group.

• According to the framework, members of the portlet testers group may see error messages with full stack traces.
# Groups Manager

## Assign By Owner

### Groups Manager

Assign Permissions for Targets of this Owner:

<table>
<thead>
<tr>
<th>Target: Information</th>
<th>Activities:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete this group</td>
<td>Rename this group</td>
</tr>
</tbody>
</table>

### Principals:

| Staff (Group) | DENY | DENY | GRANT | GRANT | DENY |

**Submit**  **Reset Form**
## Announcements Administration

### Announcements for First Topic

No announcements showing, scheduled or pending.

### Add Announcement

### Permissions for First Topic

<table>
<thead>
<tr>
<th>Administrators</th>
<th>Editors</th>
<th>Contributors</th>
<th>Audience Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edit</td>
<td>Edit</td>
<td><strong>Edit</strong></td>
</tr>
</tbody>
</table>

### Assigning Audience Members

#### Available Roles
- All_Logged_In_Users
- Alumni
- Everyone
- Faculty
- Grad_Students
- Portal_Administrators
- Staff
- Students

#### Specific Users

- Add new username:

#### Actions
- Add User
- Update

#### Navigation
- Back to Topic
- Admin Home
Announcements Administration

Announcements for First Topic
No announcements showing, scheduled or pending.

Add Announcement

Permissions for First Topic

<table>
<thead>
<tr>
<th>Administrators</th>
<th>Editors</th>
<th>Contributors</th>
<th>Audience Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edit</td>
<td>Edit</td>
<td>Edit</td>
</tr>
</tbody>
</table>

Admin Home

Assigning Audience Members

Available Roles | Specific Users

- All_Logged_In_Users
- Alumni
- Everyone
- Faculty
- Grad_Students
- Portal_Administrators
- Staff
- Students

Add User
Update

Back to Topic  Admin Home
http://confluence.sakaiproject.org/x/RQAAAB
Kuali Identity Management (KIM)

• A new module of the Kuali Rice middleware framework (http://rice.kuali.org)
• Implemented as a set of services for identity and access management
• Designed with the needs of the other Kuali applications in mind (financials, research administration and student system)
• But also meant to be general enough to be used by other applications as well
KIM Services

- IdentityService
  - Principals and entities
- GroupService
  - Group data, group membership checks
- PermissionService
  - Authorization checks
- RoleService
  - Role data
- ResponsibilityService
  - Resolve responsibilities for certain actions (integration point with the workflow engine)
- AuthenticationService
  - Establishes an authenticated user’s session
KIM Architecture

Java Client Application

Kuali Rice Standalone Server

Kuali Service Bus

CAS

Client-side services provide caching and user-friendly service facades

SOAP Client Application

Reference implementation of KIM services will write and read from Rice database

Services can be overridden to integrate with other IDM solutions
Where does it fit?

• Topic of discussion at Advanced CAMP on identity management in June
  – Where does Kuali Identity Management fit into the broader identity and access management space in higher education?

• A few possibilities
  – Can be used solely for implementation of specific Kuali applications
  – Can be positioned as the primary identity and access management services at an institution
  – Certain pieces of the reference implementation can be used, while others can be integrated with or replaced with other solutions (i.e. LDAP, Grouper, Active Directory)

• Working on some projects surrounding the last item, specifically working with Grouper team on a proof of concept for integration with KIM.
KIM Service Layer

Service Implementations

Identity Service
Group Service
Role Service
Permission Service
Responsibility Service

Reference Impl
Reference Impl
Reference Impl
Reference Impl

Kuali Rice Database

Grouper Adapter Impl

Call Grouper via the Java API or web service API

Possible future project to look at integrating KIM permission service with Grouper privileges
MACE-Paccman: some problems

- Access Management terminology is confusing e.g. privilege, permission, entitlement, authorization
- Access Management is often embedded in applications and so is reinvented often
- Access Management often does not account for federations
- Provisioning is easier than de-provisioning
- Audit trails are often per application if they exist at all
MACE-Paccman Deliverables

- Glossary and models for Access Management
  - How to use groups
  - How to use privileges
  - How to provision embedded Access Management software
  - Audit Considerations
- Comparative glossary with major access management endeavors and Open Source Higher ED projects e.g. Sakai, uPortal, Kuali
- Use Cases in Access Management
- Mapping use cases to existing efforts
  - Kuali KIM
  - MIT’s perMIT
  - Grouper
Identity Services for Open Source Software

For more information, visit https://spaces.internet2.edu/display/IdSrvcClearhouse