IAM Online
Thursday, May 13, 2010 – 1 p.m. EDT

Toward Common Identity Services

Questions via Adobe Connect chat
Audio via Adobe Connect – preferred

Conference phone bridge also available (listen-only)
Dial-in numbers:
+1-734-615-7474 Preferred (from any phone where long distance has no add’l cost)
+1-866-411-0013 (US/Canada only if you pay for long distance)
Access Code: 0157272#

Thank you to our InCommon Featured Affiliate for May, AegisUSA, for supporting IAM Online

IAM Online is brought to you by InCommon, in cooperation with Internet2
and the EDUCAUSE Identity and Access Management Working Group
Agenda

• The problem with identity services integration
• uPortal + Grouper
  – Jen Bourey, Chris Hyzer
• Kuali IdM + UW’s Astra & ABR
  – Dan Seibert, Tony Potts

• More steps
  – Advance CAMP 23-25 June
• 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

• Current choices
  – Integration with enterprise services
  – Out-of-the-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
Scientific & scholarly collaborations

• Groups of academics share private drafts of papers, data sets, etc among themselves and eventually release reports, papers, etc to the community

• Typical needs
  – Document sharing
  – Scheduling
  – Email list
  – Domain specific tools
  – Colleagues span several organizations

• Current choices
  – Run own collaboration-specific wikis, tools, and accounts for each
  – Use GoogleApps and gmail accounts, plus tools and tool-specific accounts
Wanted: “domesticated” applications
13-May-2010, IAM Online

Jen Bourey, Unicon, uPortal developer
Chris Hyzer, University of Pennsylvania, Grouper developer

uPortal Integration with Grouper
uPortal integration with Grouper agenda

- What is uPortal
- What is Grouper
- Why integrate the two
- Architecture (with client)
- Existing efforts
- Gaps
- uPortal using Grouper by default
- Architecture
- Related work
- Schedule
About uPortal

- uPortal is the leading open source enterprise portal framework built by and for the higher education community
- Java-based JSR-168 portlet container
- Emphasis on providing an extensible integration platform
Portals and Higher Ed

- Pre-existing identity systems
- Multiple identity systems
- Complex identity rules
uPortal Groups API

- Provide group membership information
- Collect group information from multiple sources
- Optional write API
- Group membership exposed to portlets as roles via portlet API
Common Group Stores

- Local database store
- LDAP
- Dynamic groups based on user attributes
About Grouper

Grouper’s Role in the Identity and Access Management (IAM) Model
About Grouper
About Grouper

- Centrally manage groups and permissions
- Various interfaces: UI, WS, LDAP, CLI, XMPP (coming soon)
- Auditing
- Skinnable simple membership UI
- Notifications
- Composite groups (intersection, complement)
- Fine grained group permissions
- Roles, role inheritance, permissions, permission inheritance
- Rules (on roadmap)
Why integrate uPortal with Grouper

- Leverage features of Grouper not in uPortal
- Ability for institutions to leverage existing Grouper deployments
- Share groups with uPortal and non-uPortal applications
- uPortal can focus on portals and not on group management
Architecture (with Grouper Client)
Existing Integrations - ESUP-Portail / ESCO-Portail

• Read/write access

• Used to delegate content management permissions in a very large portal

• Custom code to communicate with Grouper
Existing Integrations - Northern Arizona University

- Grouper channel
- Read/write Grouper group access
- Allow students to administer their own student groups
- Uses Grouper web services client
Existing Integrations - University of Chicago

• Read-only Groups API implementation

• Uses Grouper web services client

• Assign portal content and permissions based on Grouper membership
Gaps between uPortal groups and Grouper groups

- Dynamic attribute-based groups
- Textfile-based groups
- grouperLoader based on LDAP?
- uPortal uses maven, Grouper uses ant
- Probably more as we start this project
uPortal using Grouper by default

- If things go as hoped
- Look into replacing the default uPortal implementation with Grouper
- Ship the uPortal quick start with Grouper (as it does with CAS authentication)
- Provide migration path
- Share the database in quick start
Architecture (using Grouper by default)
Related work

- Grouper has a similar integration with Kuali Rice
- Can use Grouper for Kuali apps
- Can be used to add workflow to Grouper
  - e.g. will be added to a group or granted a permission if the proper approvals occur
Schedule

- Grouper team, Unicon, and uPortal team
- Hope to start in a month
- Will have progress and more plans by the end of the summer
- Might depend on future Grouper and/or uPortal release
Implementing Kuali Identity Management at your Institution

KIM Introduction
What is KIM?

- A module of Kuali Rice
- Common Interface and Service Layer
- Integrated Reference Implementation
- Set of User Interfaces
- KIM is not just “Identity Management”, it’s also “Access Management”
What KIM is Not

• A Full-Fledged Identity Management System
  • Provisioning
  • Hooks to update other systems
  • Duplication Management

• An Identity Aggregator
• An Authentication Implementation
KIM Services
KIM Core Services

- Identity Service
- Group Service
- Role Service
- Permission Service
- Responsibility Service
- “Authentication” Service
KIM Service Architecture

Java Client Application

KIM Client-side Services
- Authentication Service
- Identity Management Service
- Role Management Service
- Person Service

Kuali Rice Standalone Server
- Rice Graphical User Interfaces (for KIM, this includes Person, Role, Group)

KIM Server-side Services
- Identity Service
- Group Service
- Permission Service
- Role Service
- Responsibility Service

KNS
KEW
KSB
KEN

Kuali Service Bus

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

SOAP Client Application

web service integration

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

Institutional Service Overrides

Services can be overridden to integrate with other IDM solutions
Remember...

• The primary goal of KIM was to build a service-oriented abstraction layer for Identity and Access Management

• Integration with other IDM services was acknowledged, expected, and designed for!
KIM Integration

Integration with various Identity Management Systems

- CAS
- OpenLDAP
- Grouper
- Shibboleth
- Windows Server
- Active Directory
- Identity Lifecycle Manager 2007

Kuali Foundation: open source administration software for education
KIM Integration with other IdM products

Determine an integration plan that fits your institution.

• Use reference implementations for all core KIM services
• Override all KIM services
• Hybrid approach – override those services where solutions are provided by other systems at your institution. Use reference implementation to fill the gaps.
KIM Out of the Box

KIM Service Layer

Identity Service  Group Service  Role Service  Permission Service  Responsibility Service

Reference Implementations

Rice Database
Override KIM Identity Service with LDAP
Override KIM Identity Service with Shibboleth

KIM Service Layer

- Identity Service
- Group Service
- Role Service
- Permission Service
- Responsibility Service

Reference Implementations

Shibboleth

Rice Database
Override Identity and Group Services with Grouper

KIM Service Layer

Identity Service  Group Service  Role Service  Permission Service  Responsibility Service

Grouper™ Reference Implementations

Rice Database
Using Shibboleth For Authorization?

KIM Service Layer

- Identity Service
- Group Service
- Role Service
- Permission Service
- Responsibility Service

Shibboleth
University of Washington KIM Integration

KIM Service Layer

- Identity Service
- Group Service
- Role Service
- Permission Service
- Responsibility Service

OpenLDAP

University of Washington
ASTRA
Implementation and Kuali Identity Management at your Institution

Proof-of-Concept Experience at UW
Overview

• University of Washington & .NET
• Homegrown systems
• Long-term interest in Rice/KS/KFS
• Community partner
• Several points of integration
Proof-of-Concept

• Training
• Minimal investment
• Deep enough dive
• Not throw-away work
• Community involvement
UW Requirements

- LDAP integration
- KIM integration with home-grown system
  - Hybrid solution
  - Secure web services
- Developers trained
- Understanding of staffing needs
- Source control and build process
### Workflow Requirements

<table>
<thead>
<tr>
<th>All Organizations</th>
<th>ORF</th>
<th>PSD</th>
<th>PAH</th>
<th>CS</th>
<th>Joint</th>
<th>TBA</th>
<th>Space</th>
<th>FG9</th>
<th>Centers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORGANIZATION</td>
<td>Div</td>
<td>Dept</td>
<td>Dean</td>
<td>Div</td>
<td>Dept</td>
<td>Dean</td>
<td>Div</td>
<td>Dept</td>
<td>Dean</td>
</tr>
<tr>
<td>SEATTLE CAMPUS GEN U</td>
<td></td>
<td></td>
<td></td>
<td>2000000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>ATTORNEY GENERAL</td>
<td></td>
<td></td>
<td></td>
<td>2010000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>PROVOST</td>
<td></td>
<td></td>
<td></td>
<td>2020000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>EQUAL OPPORTUNITY OFC</td>
<td></td>
<td></td>
<td></td>
<td>2020011000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>PLANNING &amp; BUDGETING</td>
<td></td>
<td></td>
<td></td>
<td>2030000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>VP MINORITY AFFAIRS</td>
<td></td>
<td></td>
<td></td>
<td>2060000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>DEAN OF LIBRARIES</td>
<td></td>
<td></td>
<td></td>
<td>2070000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>HEALTH SCIENCES LIBRAR</td>
<td></td>
<td></td>
<td></td>
<td>2070003000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>W</td>
</tr>
<tr>
<td>UW FINANCE &amp; FACILITIES</td>
<td></td>
<td></td>
<td></td>
<td>2080000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>W</td>
</tr>
<tr>
<td>UW INFO TECH</td>
<td></td>
<td></td>
<td></td>
<td>2100000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>VP STUDENT LIFE</td>
<td></td>
<td></td>
<td></td>
<td>2120000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
<tr>
<td>STUDENT ACTIVI &amp; SUE</td>
<td></td>
<td></td>
<td></td>
<td>2120102000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>SEDNT DISABLY RESOURCES</td>
<td></td>
<td></td>
<td></td>
<td>2120103000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>STUDENT FINANCIAL AID</td>
<td></td>
<td></td>
<td></td>
<td>2120105000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>COUNSELING CENTER</td>
<td></td>
<td></td>
<td></td>
<td>2120109000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>CAREER SERVICES</td>
<td></td>
<td></td>
<td></td>
<td>2120111000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>ENROLLMENT SERVICES</td>
<td></td>
<td></td>
<td></td>
<td>2120115000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>HOUSING &amp; FOOD SERVICE</td>
<td></td>
<td></td>
<td></td>
<td>2121800000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>EXTERNAL AFFAIRS</td>
<td></td>
<td></td>
<td></td>
<td>2140000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>VP FOR DEVELOPMENT</td>
<td></td>
<td></td>
<td></td>
<td>2150000000</td>
<td></td>
<td>A</td>
<td>A</td>
<td>W</td>
<td>A</td>
</tr>
</tbody>
</table>

*Kuali Foundation*: open source administration software for education
LDAP Integration

• Spring LDAP & Spring Security Modules
• Encryption methods
• Configuration
  • Spring
  • System parameters
  • Mapping
• Issues
UW RICE WORKFLOW ARCHITECTURE

create() route()
approve() disapprove()
getWorkflowActionSummary()
requestAdHocApproveToPrincipal()
Workflow Integration

• **SimpleDocumentService**
  • Routing calls (create, route, approve, etc)

• **Post Processor**
  • Callbacks through web services
  • Notification to external system
    • Route status changes (saved, initiated, enroute, final, etc)
    • Route node changes (who has responsibility now)

• **Qualifiers**
Role & Group Service Integration

• JAX-WS used to generate Java classes
• Roles
  • Mapped directly to ASTRA roles using convention
  • ASTRA “span of control” mapped to KIM qualifiers
• Groups
  • Mapped to specific roles within ASTRA
• Issues
Outcomes

• Highly functional
• All major integration points completed
• Minimal core-rice changes
• Code contributions
• Team confidence
• What’s Next?
Advance CAMP
The Second Identity Services Summit
June 23-25, 2010 - Raleigh, North Carolina - www.incommon.org/camp

Outcomes of this discussion-oriented, participant-driven meeting are to:

• Develop new IAM requirements for current projects, products, and development frameworks
• Identify opportunities for new IAM-oriented projects, align complimentary work, and collaborate on solutions
• Set the direction for the community on what's next for identity-related activities and resources

www.incommon.org/camp
IAM Online

Please take a few minutes and complete the survey about today’s IAM Online: http://www.surveymonkey.com/s/F8TPYKD

Upcoming IAM Online:

June 10, 2010, 1 p.m. (ET)  Handling Affiliate Populations
July 8, 2010 – 1 p.m. (ET)  Federated Identity Management Essentials

Thank you to InCommon Affiliates for helping to make IAM Online possible.