Strategies for Accelerating Identity and Access Management (IAM) in Higher Education
<table>
<thead>
<tr>
<th>Name</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Barton</td>
<td>Global Access Services for R&amp;E</td>
</tr>
<tr>
<td>Keith Hazelton</td>
<td>IAM Common Foundations, Shareable Solutions</td>
</tr>
<tr>
<td>Bill Yock</td>
<td>IAM Communities Past, Present and Future</td>
</tr>
</tbody>
</table>
We built a global network
But we didn’t include access services!

• The network enables sessions between pairs of endpoints anywhere in the world
  – Move data
  – User activity

• Access policies >> network addresses
  – Users, roles, credentials, attributes, metadata
  – Needed even to manage network access, let alone sensitive data or equipment

• Traditional solutions are specific to each resource
  – Internal user credentials and role management
Maximum pain, minimum gain, impeding science

My email

My cluster

Oh cr*p!!

---

Maximum pain, minimum gain, impeding science

The image depicts two fishbowls: one labeled "My email" with a fish splashing out of the water, and another labeled "My cluster" with three fish swimming in it. A thought bubble above the fish in the "My email" bowl contains the word "Oh cr*p!!", symbolizing discontent with the situation.
Focus on science

- Virtual Organizations and other collaborations
- Research computing provided by campus/lab/facility
- Network providing very high bandwidth
- Types of activities addressed by the NSF CC*IIE program
- Mix of needs for access policies across scientific activities
  - Collaborators spread across organizations and nations
  - Campus/local, Federated, Social, X.509, MFA, higher Level of Assurance credentials
  - Range of applications & services supporting collaboration
  - Specialized computing, storage, and instrumentation resources
- All of the above need to be usable, by scientists, to manage access in support of their work
Everyone else needs this too

- Mix of needs for access policies across scientific academic and administrative activities
  - Collaborators spread across organizations and nations
  - Campus/local, Federated, Social, X.509, MFA, higher Level of Assurance credentials
  - Range of applications & services supporting collaboration
  - Specialized computing, storage, and instrumentation resources
- All of the above need to be usable, by scientists anyone, to manage access in support of their work
So we need global access services. What does that look like?

• University/College, Lab, Facility IAM instances
• Collaboration platforms/portals for Virtual Organizations (VOs)
• On-prem, hosted, and aaS IAM options available to the above
• IAM manages identities, credentials, attributes, groups, roles
• IAM integration with compute/app, storage, and network resources
• All embedded within federation and interfederation to connect people, their credentials, and their attributes and roles with protected resources
Delegate in order to scale

• No one knows what all everyone is permitted to do
• So, access management must be widely distributed
  – Among organizations & VOs
  – Within organizations & VOs
• Hence, access management systems must support delegation in addition to identities, credentials, attributes, groups, roles
• Delegation must happen at many scales
  – Global on down, so that the resulting system works globally
  – At organizations and VOs on up, where access management needs are actually known
Globally distributed network management
Globally distributed access management
Delegated access management for UChicago VPN

Different groups, different authorities
VPN only uses "vpn:authorized"

allowed:
- staff
- student
- postdoc
- IRB

denied:
- closure
- locked

core business systems

IAM system

IRB Office

IT Security Team
Distributed management of Level of Assurance (Silver)

<table>
<thead>
<tr>
<th>Step</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eligibility - Has Proper Affiliations</td>
<td>✔️</td>
</tr>
<tr>
<td>Eligibility - Is Eligible for an ID Card</td>
<td>✔️</td>
</tr>
<tr>
<td>Eligibility - Has claimed a CNetID</td>
<td>✔️</td>
</tr>
<tr>
<td>Submit Address of Record</td>
<td>✔️</td>
</tr>
<tr>
<td>Verified Address of Record</td>
<td>✔️</td>
</tr>
<tr>
<td>Identity has been proven</td>
<td>✔️</td>
</tr>
<tr>
<td>CNet password &lt; 1 year old</td>
<td>✔️</td>
</tr>
<tr>
<td>CNet password &gt;= 12 characters</td>
<td>✔️</td>
</tr>
<tr>
<td>Passed IT Security Audit (no insecure use of AD)</td>
<td>✔️</td>
</tr>
</tbody>
</table>

- **core business systems**
- **IAM system**
- **self**
- **ID Card Office**
- **self**
- **IT Security**
Role-backed multi-factor authentication

Service Owner
MFA required

User
MFA opt-in

IT Security
MFA enrolled

IAM System
Silver

MFA Login?
OR

Silver?
AND

Identity Provider with Multi Context Broker

MFA Silver Neither

Service
1. MFA
2. Silver
Foundation for global access services

- Some mature access management tools
- Production deployment at many organizations and some VOs
- Mature federation technologies
- R&E Federations in many countries
- Substantial start on interfederation technologies
- Organizations with experienced people supporting and enhancing all of the above
Major areas of work still ahead

• Federation & interfederation
  – Expand federation – more participants
  – Make it easier for international VOs & other collaborations
  – Make interfederation actually happen
• Lower bar for deployment of these capabilities
  – More open source IAM products with common APIs
  – Hosted and aaS IAM offerings available to R&E sector
• Standards for access management objects to be managed and shared between instances
  – Naming, schema, protocols, bindings
Identity and Access Management (IAM)
Common Foundations, Shareable Solutions

Keith Hazelton
University of Wisconsin
InCommon Technical Advisory Committee
IAM infrastructure matters, but it is only a means.
IAM: Getting people appropriate access to resources
Any sufficiently advanced technology is indistinguishable from magic – A. C. Clarke
IAM: Getting people appropriate access to resources
IAM: Getting people appropriate access to resources
Our IAM solutions are not yet sufficiently advanced

• Paradox: You can’t magically disappear until you’re 100% there
• Tom just reminded us of major areas of work still ahead
• One set of challenges for universities and colleges (enterprises)
• Another set for research collaborations (virtual organizations)
• Shared challenge of getting enterprises and VOs to work well together
Challenges in enterprise IAM

• IAM infrastructure: Enterprise ecosystems are usually hybrid mix of
  – In-house implementations of commercial products
  – Open source packages (CAS, Shib, Grouper,…)
  – Homegrown Custom engineered pieces
    • See the fascinating email thread, “homegrown”, on idm@listserv.educause.edu
    • To subscribe, send email to LISTSERV@LISTSERV.EDUCAUSE.EDU
    • in the body of the message (not the subject line), put: SUBSCRIBE IDM
  – Emerging, but not (yet?) widely adopted: IAMaaS
Challenges in enterprise IAM

• Few of us are in a position to rip and replace the hybrid mix
• We replace outgrown or unsupportable components
• We enhance our capabilities by bringing in new components
• What architectural models might support this enterprise reality?
Architectural models for hybrid IAM ecosystems

• Commercial IAM Suites
  – Monolithic, product-centric architecture
  – Premised on rip and replace (slow motion doesn’t make it less painful)
  – Substantial professional service contracts nearly inevitable for deployment

• Open source offerings (the CIFER vision)
  – Modular – individual packages address a related set of capabilities – adopt what you need when you need it
  – Pluggable – Widely supported protocols (LDAP, SAML), RESTful APIs and/or event-driven messaging as the basis of integration between packages
  – Adaptable – Designed for flexible configuration and local extension
  – Community (and commercial) support for the packages and for those who use them
The current state of open source IAM

- CIFER has a first-cut comprehensive functional model for IAM
- We can show where existing open source packages cover (or don’t cover) the functional model
- We’re wiring up a platform for demo solutions in a virtual testbed leveraging a selection of open source IAM packages
IAM functional model
### Supporting real-world access through composed IAM functions

- **Scenario:** External consultant gets write access to a central IT project wiki and an associated github repository

<table>
<thead>
<tr>
<th>Action</th>
<th>Supporting IAM functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Consultant (C) gets an email invitation from Project Manager (PM) to self-register for a university account</td>
<td>Guest account mgmt.; Notification service</td>
</tr>
<tr>
<td>2) C self-registers, gets credentials</td>
<td>Guest acct. mgmt.; Enrollment; Source IdM; Registry IdM; Credential Issuance</td>
</tr>
<tr>
<td>3) PM assigns C to project X as team member</td>
<td>Role/Group mgmt.</td>
</tr>
<tr>
<td>4) PM gives Project X team members access to a project wiki space and to a project code repository on github</td>
<td>Permission mgmt; Provisioning;</td>
</tr>
<tr>
<td>5) C edits wiki, contributes code to repository</td>
<td>AuthN; Policy Decision/Enforcement (AuthZ);</td>
</tr>
</tbody>
</table>
Plugging one of the gaps

- Two years ago there were no open source identity registries
  - For source and registry IdM; enrollment;

- Now we have three at various stages of maturity
  - Enterprise: Open Registry (an Apereo Incubation Project)
  - Enterprise: Central Person Registry (currently based at Penn State)
  - Virtual Organizations: COmanage – Includes an identity registry among other components
One overlay of open source packages on the functional model

- **uPortal™**
- **CPR**
- **Identity Registry**
- **Grouper™**
- **Access Management**
- **Shibboleth**
- **Authentication**
- **CAS**
- **389 directory server**
- **ActiveMQ™**
- **Apache Camel™**
- **Provisioning & Integration**
- **REST**
IAM Testbed as Demo Platform: Early Days

- Potential adopters of one or more open source packages need to see working solutions to problems they are trying to solve
- Here are some of the building blocks already in place
  - Penn State's Open Source version of the Central Person Registry
  - An instance of 389 Directory Server (LDAP)
  - An instance of the Grouper group and permission management package from Internet2
  - A full installation of Apache ActiveMQ
  - The Apache CAMEL integration package (implementing all the integration patterns found in the Enterprise Integration Patterns book)
  - An instance of uPortal
  - Coming next: CAS, Shib and the Confluence wiki
IAM Testbed as Demo Platform

- First goal will be an end-to-end demo of the external consultant scenario described above
- “The only way of discovering the limits of the possible is to venture a little way past them into the impossible” – A. C. Clarke
IAM Communities Past, Present and Future

Bill Yock
University of Washington
InCommon Steering Committee, Program Committee
Chair, Kuali Rice Middleware Project
Agenda

- What “Community Developed” means to me
- The Marketecture of Community
- Community Areas of Concentration
- Coordination across Concentrations
- Emerging Birth of a New Community?
- The ROI of Getting Involved
What “Community Developed” Means to Me

Many Hands Make Light Work - John Heywood
What “Community Developed” Means to Me

Sometimes confusing, often daunting, hard to imagine end result!

Finished products may not look pretty but are extremely versatile!
The Marketecture of Community

Communities and Areas of Concentration

**Internet2**
- Network / InCommon Federation Oriented
  - Grouper, COManage, Net+, Shibboleth
  - Buyers Club, Cooperative

**Apereo**
- Teaching / Learning Oriented
  - CAS, OpenReg
  - Cooperative

**KIM**
- Collaborative
  - Administration / ERP Oriented
  - Kuali

**Solo**
- CPR, OYSTER

**COManage**, **Net+**
How Do We Get These Communities Working Together?

Internet2
Network / InCommon Federation Oriented

Apereo
Teaching / Learning Oriented

CIFER
Administration / ERP Oriented

Kuali
Coordination is Key

- Roadmap Alignment
- Shared Support
- Resource Augmentation

Interfaces & APIs
Reference Architectures
Test Drive Reference Implementations
Birth of a New Community Structure?

Aligned Comprehensive Governance (and Strategy) for all higher education middleware and services by TIER

InCommon®
The ROI of Getting Involved

\[2 + 2 + 2 + 2 + 2 = 5\]
Please Help Maximize our Community ROI!
Get Involved!

Join a CIFER Coordination Work Group

https://spaces.internet2.edu/display/cifer/CIFER+Home

Join (or increase your participation in) one of the existing communities:

http://www.incommon.org
http://www.internet2.edu/communities-groups/groups/middleware/
http://www.apereo.org
http://shibboleth.net
http://www.kuali.org
Thank You!