CIFER: An IAM Solution For the Community From the Community

Wednesday, November 14, 2012 – 3 p.m. ET

Keith Hazelton, University of Wisconsin-Madison

Dedra Chamberlin, University of California San Francisco and University of California Berkeley

Tom Barton, University of Chicago

Thank you to InCommon Affiliates for helping to make IAM Online possible.
IAM in a university environment

- Which people?
- What systems & business processes?
- What policies?
- What purposes?
- Whose authority?

No off the shelf toolset does this completely.
Community Identity Framework for Education and Research (CIFER)

- Comprehensive
- Federation- and cloud-ready
- Adds to current open source components
- Delivered by and for the higher education community

- Supported by
  - Kuali Foundation
  - Jasig
  - Internet2
  - Campuses
How we’ll mash these up today

1. Keith Hazelton, CIFER backgrounder
2. Questions for you, webinar participants, to ponder while
3. Dedra Chamberlin looks at this through lens of IAM renewal project at UC
4. Online polling for your responses to questions
5. Discussion of those
Community Identity Framework for Education and Research -- CIFER

CIFER Goal:

To make radical improvements in higher education Identity and Access Management (IAM) in terms of

- Capability,
- Ease of integration
- Affordability
CIFER – Community Identity Framework for Education and Research

**IAM Console**

- **KEW**
- **OpenReg**
- **Identity Registry**
- **Kuali KIM**
- **Access Management**
- **Grouper**
- **Authentication**
- **Shibboleth**
- **Provisioning & Integration**
- **Grouper**
- **Kuali KRMS**

**Systems of Record**
- Human Resources
- Student Information System

**Target Systems**
- Learning Mgmt Systems
- Cloud Apps

**Other IAM Components**
- No Reinvention Zone

**Directories**
- LDAP, AD
- Middleware like ServiceMix, Jboss

Legend:
- = In scope
- = Out of scope
There are CIFER teams already hard at work rolling out open source solutions that fill critical gaps in the open source IAM space.

Open source, Identity Registries (IdReg) are now out there for adoption.

- **Open Registry (OR: Rutgers, Jasig):** UC Berkeley, UCSF, U Utah, Unicon kicking tires

- **Central Person Registry (CPR: Penn State):** Foundation for Kuali KIM; CMU, U Utah kicking tires

- **OR-CPR Deep Collaboration is ongoing**
  - Active design convergence around APIs, core schema, protocols
There are CIFER teams already hard at work rolling out open source solutions that fill critical gaps in the open source IAM space.

Provisioning and Integration (P&I)

- Tools to enable Systems of Record getting information into an Identity Registry

- Developing core schema and identity info APIs and protocols (SCIM?)

- Tools to propagate changes in Identity Registry information into consumer systems that need it for user profile purposes and for access management
There are CIFER teams already hard at work rolling out open source solutions that fill critical gaps in the open source IAM space

Access Management

- Tools to manage groups, roles and permissions
  - Grouper Project
  - Kuali KIM APIs
- Provisioning tools to enable groups, roles, permissions to affect access control decisions in real running services
  - Grouper Provisioning Service Provider (PSP)
  - Toolkits to support provisioning from Grouper for Spring, .NET, Shiro
  - ForgeRock OpenIDM, OpenICF
State of CIFER, “Get Real” Version

• Authentication
  – Identity proofing, Credential issuance, Password management
    • Identity Registry integration is crucial
  – Social to SAML services
    • MACE Social Identity working group and trial Soc2SAML gateway service
  – Mobile Application and Non-Browser authentication
    • InCommon and peers around the world
    • Tech development: Moonshot and SAML ECP GSS-API mechanism

• Cross-component Shared Services (*work has begun*)
  – IAM Console
    • Prerequisite: Instrumentation of the CIFER components
    • UIs For self service
    • UIs For admins
  – Quality Assurance across CIFER work streams
  – Packaging, Documentation, Training
Growing roster of campuses and organizations directly involved in CIFER workstreams
- Supporting local projects while contributing to CIFER
  - UC Berkeley, UC SF, Penn State, Rutgers, Duke, U Virginia, ...
  - Contributing significant labor
    - U Washington, UC Davis, U Chicago, UW-Madison, Kuali,…

Key commercial affiliate has joined the team: Unicon

Work proceeding on a formal strategic alignment between Internet2, Kuali and Jasig around CIFER
- Discussions around significant resources for CIFER from Internet2 and Kuali
- Administrative services (CIFER will NOT be another open source org)
- Support for software development and community development
• The doors are open
  – [http://ciferproject.org](http://ciferproject.org) has a subscription link for all things CIFER
  – [community@ciferproject.org](mailto:community@ciferproject.org) or subscribe directly at

• The CIFER Teams are always recruiting through their shared wiki:
  – [https://spaces.internet2.edu/display/cifer/Home](https://spaces.internet2.edu/display/cifer/Home)
At a few points during this session we will post instant polling questions for YOU the participants.

As you listen to Dedra’s remarks about progress at a couple of University of California campuses, think about your answers to the questions on the following slide.

We will make the poll available at the close of her presentation.
• Are you looking at new IAM-related projects now/within the next year? (Yes or No)

• What are your immediate or near-term challenges in IAM?

• What most puzzles or interests you about CIFER?

• What factors would bear on your decision to adopt or participate in CIFER?
UC Berkeley / UCSF
Identity and Access Management
Strategy and CIFER

Dedra Chamberlin
Deputy Director, Identity and Access Management
UCB/UCSF

November 2012
IAM State at UCSF and UCB

• Key Strategic Drivers for IAM solutions
  – Cost Reduction
  – Security
  – User experience

• Improvements to IAM infrastructure are critical to support new enterprise initiatives
  – Operational Excellence initiatives on both campuses
  – Cloud Service integration – Google, Box, Salesforce, Service Now, etc.
  – System-wide initiatives – New UC-wide HR system

• Current IAM infrastructure at UCB and UCSF will not meet upcoming demands
Qualities of our Preferred Solution?

• Scalable
• Modular - designed to allow upgrades/modifications to one component without impact to the others
• Interoperable - with other IAM components and other local and cloud-hosted systems/applications
• User-friendly – unified design, intuitive user experience
• Secure
• Affordable
Why Modular Architecture?

• Leverage current investment
• Leverage existing and well-supported higher ed open/community source solutions
• Because even if you buy a big commercial product, it’s still a group of components that interoperate
  • Loose coupling is better than tight integration
  • Allows more flexibility and incremental investment and re-factoring over time
• Standards-based, not proprietary – easier and cheaper to find skilled labor to support services and integrations
Other Thoughts on Packaged Solutions

- UCSF and UCB both invested in commercial IAM products (IBM Tivoli and Sun IdM)
- Both campuses did not deliver to expectations with those solutions
- We have strong anecdotal evidence from other campuses with similar experiences
- Packaged solutions work well in highly centralized environments dominated by a standard platform for all ERP and IAM systems
- UCB and UCSF have very heterogeneous IT environments
- Commercial products come with significant risks of vendor lock-in on pricing and product conversion timetables
How to Get to Our New, Modular, Standards-based, Open Source Identity Management Solution Tailored to Higher Ed?
What are the Modules?
Key Identity and Access Management Components

Systems of Record
- HR
- Student System
- Guests/ Affiliates
- Alumni
- ...

Provisioning/ Integration
- Possible options:
  - REST
  - SOAP
  - SCIM
  - OpenICF
  - Camel
  - Batch

Identity Registry
- Identity Match Engine
- Admin UI
- Identity Registry
- Admin/Self-Service UI

Digital Identity
- Credential Mgmt. UI
- Credential Management: Password Sync

Campus Directory
- Admin/Self-Service UI
- Directory

Central Authorization Services
- Access Request and Approval Workflow
- Group Management
- Authorization Management
- Access Request: Approval Workflow Engine
- Group Mgmt. UI
- Group Mgmt.

Provisioning/ Integration
- Connectors
- Batch
- Web Services

Credential Store
- (Kerberos/ AD/LDAP)

Web SSO
- CAS
- Shib
- Other SSO

Additional Services
- Google Apps
- ServiceNow
- Box
- LMS
- Wiki
- Travel
- ...
Next Generation IAM Infrastructure

- Existing Open Source products – CAS, Shib, Grouper
- New Community Development – Registry, Identity Console
- Open Source solutions with Commercial Support - Forgerock
Immediate “CIFER” investments

- ID Match Engine
- Registry
- Credential Management self-service and admin tools
- Central Access/Group Management at UCB
UCB, UCSF, and CIFER - Next Steps

- Approval of strategic technology plan by campus leadership
- Signing “letter of intent” to formalize CIFER contributions
- Keep writing software – always with generic requirements and community development in mind
- As soon as appropriate, set up new development projects as community efforts
- Establish ID Match engine as a community project and deploy it at UCB
- Join and contribute to the Open Registry community – stand up the product at two campuses
- Always be on the look out for campuses that might want to build and support products with us
When Can We Start Working Together?

dedra.chamberlin@ucsf.edu
dedra@berkeley.edu
Evaluation
Please complete the evaluation of today’s IAM Online: http://www.surveymonkey.com/s/IAMOnline_November_2012

Next IAM Online – December 12, 2012 (3 pm ET)
Social Identity and a Social2SAML Gateway
www.incommon.org/iamonline

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline
Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by Internet2’s InCommon, in cooperation with the EDUCAUSE Identity and Access Management Working Group