InCommon®

IAM Online

Thursday, April 8, 2010

Making Federation Happen

Joel Cooper, Director of Information Technology Services, Carleton College
John O'Keefe, Director of Academic Technology & Network Services, Lafayette College

Questions via Adobe Connect chat
Audio via Adobe Connect – preferred

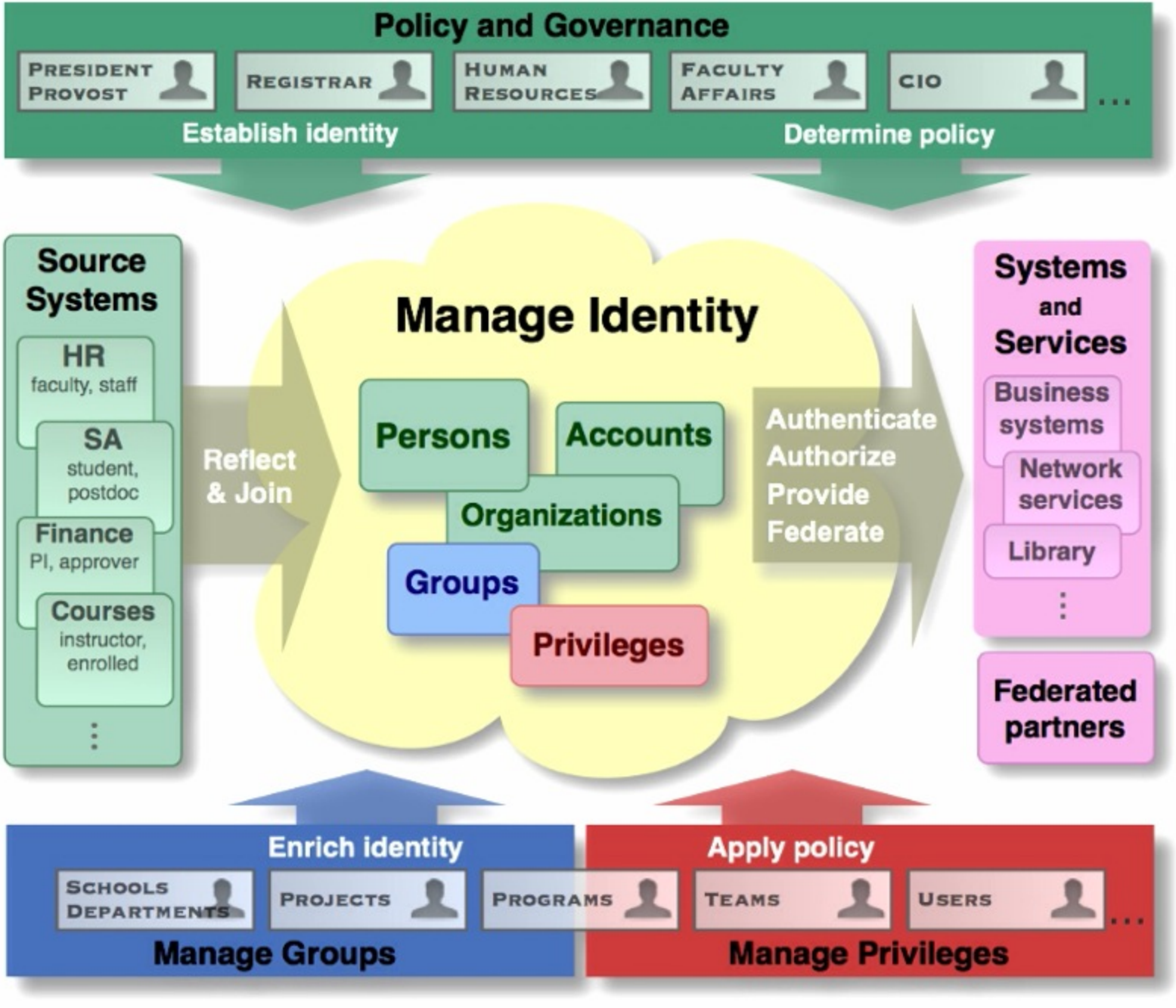
Conference phone bridge also available (listen-only)
Dial-in numbers:
+1-734-615-7474 Preferred (from any phone where long distance has no add'l cost)
+1-866-411-0013 (US/Canada only if you pay for long distance)
Access Code: 0157272#

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

Federated Identity Management Essentials: Making Federation Happen

Joel Cooper, Director of Information Technology Services, Carleton College

John O'Keefe, Director of Academic Technology & Network Services, Lafayette College



Source: Internet2 Middleware Initiative, Tom Barton, Lynn McRae, Steve Carmody, Ann West

The policy side of FIdM

FIdM Policies

- Account provisioning
- Account de-provisioning
- Security of credentials
- Accuracy of information
- Service providing

Account provisioning

- How do you determine who gets NetIDs?
- How do you validate new users?

Account de-provisioning

- How do you remove accounts once users leave?
- How long do you keep NetIDs?

Security of credentials

- How do you keep identities secure in the directory?
- How do you keep identities secure in transmission?

Accuracy of information

- What processes do you have to maintain audit trails?
- How reliable is the attribute information?
- How do you update the person registry?
- Who can update the person registry?

Service providing

- What attributes are required to access your service?
- What do you do with attributes you receive as part of a federated identity exchange?
- How do you secure attributes you receive as part of a federated identity exchange?
- How do you notify a federated user if his/her attributes have been compromised?

The technology side of FIdM

FIdM technologies - The special sauce

- Directory service (LDAP, AD, eDirectory)
- eduPerson schema extensions
- Shibboleth
- SAML

Directory Service

- A registry of account information and person attributes
- Common directory services include
  - Active Directory (Microsoft)
  - LDAP (OpenLDAP, Sun LDAP, etc)
  - eDirectory (Novell)

eduPerson

- Standards-based extensions to common directory services to include attributes required by federated services

- Common attributes include

  - eduPersonPrincipleName - institutional NetID (okeefej@lafayette)

  - eduPersonAffiliation - faculty, staff, student, etc

Shibboleth

- Middleware application
- Sits between directory service and web service (Apache, IIS)
- Sends/Receives attributes about users through XML-based “assertions” (SAML)
- Attributes sent/received by College/University determined by either the IdP, SP, or both

Shibboleth's Two Heads

- Identity Provider (IdP) - Sharing authentication and person attributes with others
- Service Provider (SP) - Sharing hosted services with others

SAML

- SAML = Security Assertion Markup Language
- XML-based standard for exchanging authentication and authorization data between security domains
- Contains attribute information sent to service providers

Putting the pieces together

IdM First!

- Planning
- Business Process/Policy Improvement
- Design
- Implementation

Business Process/Policy Improvement

- Align business processes
- When new faculty/staff/students come or leave, how does that work?
- Account creation/deletion must be a rule-based activity!
- Partner with HR, Dean's Office, whoever to change business processes
- Good business processes ensure currency and security

Raise consciousness w/ campus leaders

- In whatever way works with your campus culture
- Make business case
- Establish vision
- Get executive level buy-in

IdM===>FIdM is the critical path

- Begin with the end in mind
- You need a directory service/IdM/provisioning in place
- Automation of provisioning/deprovisioning must be your goal

Design

- Develop IdM strategy if you don't have one
- Involve information systems and systems staff from the beginning
- Pick technologies that work in your environment (AD, LDAP, E-directory)

Plan and implement IdM/directory service

- Policy/business practices--expression of these in automated systems
- Develop policies for data stewardship, password management, helpdesk “I forgot my password issues”
- Implement IdM/directory service based on EduPerson
- Provision and deprovision accounts according to established policies

Prepare to Federate

- Familiarize with Shibboleth
    - Involve technical staff from the beginning
- Set up Shibboleth software
- Familiarize with and join InCommon
- Identify services you want to use or provide (e.g. JSTOR)

Federate!

- Set up pilot application
- Identify and implement other services you want to use or provide
- Identify collaborations that can benefit from federation
- Consider migrating existing internal applications to Shibboleth for SSO

Links & Resources

- eduPerson Extensions - http://middleware.internet2.edu/dir/schema/
- InCommon - http://www.incommonfederation.org/
- Shibboleth - http://shibboleth.internet2.edu/
- TestShib - https://www.testshib.org/
- IdM Roadmap - http://www.nmi-edit.org/roadmap/dir-roadmap_200510/index-set.html

Questions?

John O'Keefe
email: okeefej@lafayette.edu
twitter: @okeefej_62

Joel Cooper
email: jcooper@carleton.edu

InCommon®

InCommon CAMP

Exploring and Supporting Federated Identity and Access Management

June 21-23, 2010 - Raleigh, North Carolina - www.incommon.org/camp

Exploring

•Learn about a roadmap for implementation
•Hear case studies and value propositions
•Link-up with experienced colleagues or corporate partners to help
•Leave with an action plan

Supporting Production

•Attend Technical and Management Tracks
•Learn about advanced practices, working with stakeholders, SAML 2
•Discuss future opportunities, like state federations and federated incident response

Advance CAMP

The Second Identity Services Summit

June 23-25, 2010 - Raleigh, North Carolina - www.incommon.org/camp

- Are you a developer of commercial or open source software?
- Interested in aligning identity implementations with the community to reduce your development and support headaches?
- Join your colleagues and attend Advance CAMP: The Second Identity Services Summit!

www.incommon.org/camp

InCommon®

IAM Online

Please take a few minutes and complete the survey about today's IAM Online:
http://www.surveymonkey.com/s/ZY9FVLK

Upcoming IAM Online:

May 13, 2010, 1 p.m. (ET) Advanced Topics in Federated Identity Management – Toward Common Identity Services (Host: Tom Barton, University of Chicago)

June 10, 2010, 1 p.m. (ET) Hot Topics and Current Issues in Identity and Access Management

Thank you to InCommon Affiliate Unicon for helping to make IAM Online possible.

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