EDUCAUSE 2014
ANNUAL CONFERENCE

InCommon and Your Identity Management Infrastructure: Strategies from CIOs

Joel Cooper, CITO Swarthmore College
John O'Keefe VP for ITS and CIO Lafayette College
What is Identity Management?

Identity and access management is a way to enable a person to access information and services based on their roles with the institution while ensuring data security.

An identity and access management system (IAM) should facilitate everything from student enrollment and course rosters, lab access and grant reporting, email and ticketing systems to secure and efficient collaborations with colleagues across the globe.
Federated Identity Management

- Parties agree to leverage the identity provider’s database, rather than creating separate data stores
- Users no longer register with the service provider, using their university credentials for transactions
- Single sign-on convenience for users
- Identity provider does the authentication; service provider does the authorization
- Attributes are the key – maintain privacy and security
Technology and Policy

- Technology - Shibboleth, SAML, eduPerson
- Policy – InCommon Federation
So, what is Shibboleth?

- Middleware application
- Sits between IdM (e-Directory, OpenLDAP, AD) and Web (Apache, IIS)
- Sends/Receives attributes about users through XML-based “assertions”
- Attributes sent/received by institution 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
What is InCommon?

• The organization that manages the trust relationships
• Issues certificates
• Manages standards and best-practices required by members
• Negotiates inter and intra-federation relationships
Federated Identity: Why?

- Trusted Identity in Education and Research (TIER), part of the cyberinfrastructure Internet2 is building out
- Trust relationship between identity provider (you) and service provider (cloud service)
- Better security for access to cloud services
- Single sign-on, no multiple username/password silos
- Service providers don’t need to provision or de-provision accounts
- Important to our faculty (research teams, virtual organizations…) students, and administrators (lots of cloud services)
Challenges/Opportunities

• Lots of organizational heavy lifting
• It’s not just an IT project—involving other campus stakeholders
• Auditors and risk management folks can be allies
• Easier than it used to be?
• HR employee intake procedures
• Provost requiring signed contracts
Implementing IdM

- Business process reengineering
- Buy or build IdM provisioning software or service
- Automate provisioning and deprovisioning processes
- Implement EDUPERSO directory schema (LDAP, AD)
- Do nothing more and you’ll have achieved a lot
- Implement Shibboleth (identity attributes fed by LDAP, AD)—authentication and authorization
- And federate…
Join InCommon

• THE organization in higher education providing the trust framework between educational institutions, research organizations, and service providers
• 450 higher education participants
• 32 labs, research organizations
• 185 commercial partners (see http://www.incommonfederation.org/participants/)
• Having the InCommon framework in place eliminates lots of work for everyone, improves service and security
Join InCommon

• Once federated, setting up the service is straightforward
• Attribute information superior to CAS
• Improved security of cloud services
• Improved security of campus credentials and identity
• Service providers are starting to “get” the benefits of federation
Swarthmore’s Journey

• Got involved in identity management project to solve internal problem
• Adopted cloud-based identity management system
• Did massive business process reengineering
• Implemented IdM strategy
• And then…
Federation!

- IdM project prepared us for next steps…
- Implement Shibboleth
- Join InCommon
- Documentation from IdM project=POP document for InCommon
- We did our own Shibboleth implementation
- Set up 4 service providers this past summer
- Planning underway with TriCo library consortium and Moodle CMSes
Swarthmore Use Cases

- student judicial (cloud service)
- IRB administration (cloud service)
- JSTOR (especially alumni access)
- see Lafayette’s list of service providers
- evolving Net+ services
Lafayette’s IAM Journey
About the College

- Approximately 2,350 Students, 218 Faculty, about 534 Staff
- Small, residential, private liberal arts college with Engineering
- Endowment driven ($870M as of July 2014)
About ITS

- Centralized IT with 36 staff
- Open-source centric
- 2 FTE dedicated to IAM
- IT Budget - $1.9M Opex, $2.3M Capex
ITS Strategy

- Integrate with best-of-breed
- Web services architecture
- Private and public cloud integration
- Own the data!
- Authentication is the glue
“On the Internet, nobody knows you’re a dog.”
The Problems

- Access to college-run services did not scale
- Too many user accounts to manage
- Decentralized authorization
- Security and privacy varied from service to service
- Poor accuracy and timeliness of account provisioning
More problems!

• Access to new outsourced services did not scale
• Still too many user accounts to manage
• Authorization was managed by the Service Provider without institutional verification
• Security and privacy varied from hosted service to hosted service
• Poor accuracy and timeliness of account provisioning for hosted services
What We Do With Federated Identity
InCommon Federation Benefits

**Convenience** – Single sign-on with higher education credentials

**Safety** – Enhanced security with fewer data spills

**Privacy** – Release of only the minimum information necessary to gain access to resources

**Scalability** – Once implemented, federated access relatively simple to extend

**Authentication** – Campus does the authentication, maintaining control of user information

**Authorization** – Service provider makes access decisions based on attributes
How Good FIdM Helps Us Sleep

- Used InCommon’s guidelines as a cookbook
- Effective attribute collection and maintenance has enabled other projects
- Secure and automated credentialing
I'm just outside town, so I should be there in fifteen minutes.

Actually, it's looking more like six days.

No, wait, thirty seconds.

The author of the Windows file copy dialog visits some friends.
Is It Better Yet?

• College-hosted information and services co-mingled with cloud-hosted information and services
• Non-federated internal and external use cases for SSO
• Increasing complexity of SSO
So why involve CAS?

- Instances where there are no federated use cases
- Not all systems have Shibboleth SP capabilities
- More deterministic control over user experience
What we do with CAS

Drupal™

Zimbra™

qualtrics.com®

medicat®

ellucian

TouchNet®

PCi Driving Engagement and Contributions

ADIRONDACK SOLUTIONS

DegreeWORKS
CAS and Shibboleth Together

- Comprehensive single sign-on for web applications
- Seamless transition from internal to external services
- Better UX for the users
- Provides SSO mechanism for institutional web apps regardless of federating
- Federated when needed, CAS when not
Lessons Learned

• Require use of CAS or Shibboleth in RFPs
• Sponsor partners to join InCommon
• Both federated and non-federated services is a reality
• Standards all the way
• Centralize and close off external access to directory services
• IDENTITY IS INFRASTRUCTURE!
What’s Next

• Group management
• High availability
• Standard attribute release policy (R&S)
• Automation never ends!
• Service Providing
Questions?

Joel Cooper
jcooper2@swarthmore.edu

John O’Keefe
okeefej@lafayette.edu
Help Us Improve and Grow

Thank you for participating in today’s session.

We’re very interested in your feedback. Please take a minute to fill out the session evaluation found within the conference mobile app, or the online agenda.