

Federated Identity Management and Shibboleth: Policy and Technology for Collaboration

Marianne Colgrove, Deputy CTO, Reed

Joel Cooper, Director of Information Technology Services,
Carleton

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

Introduction to Federated Identity Management

Federated Identity Management

- It's not just for big schools
- NITLE Federated Identity Management Working Group
- Marianne Colgrove, Joel Cooper, Eric Jansson, Robert Johnson, John O'Keefe, Kenneth Pflueger, Chris Sellers, Ann West

What is Federated Identity Management?

- Policy = federation agreements
- “An association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions” (Internet 2)
- Examples include InCommon, eAuthorization

What is Federated Identity Management?

- Technology = systems to implement federation, eg, Shibboleth
 - Enable your users to use services outside your school (identity provider)
 - Provide services that other communities can use (service provider)

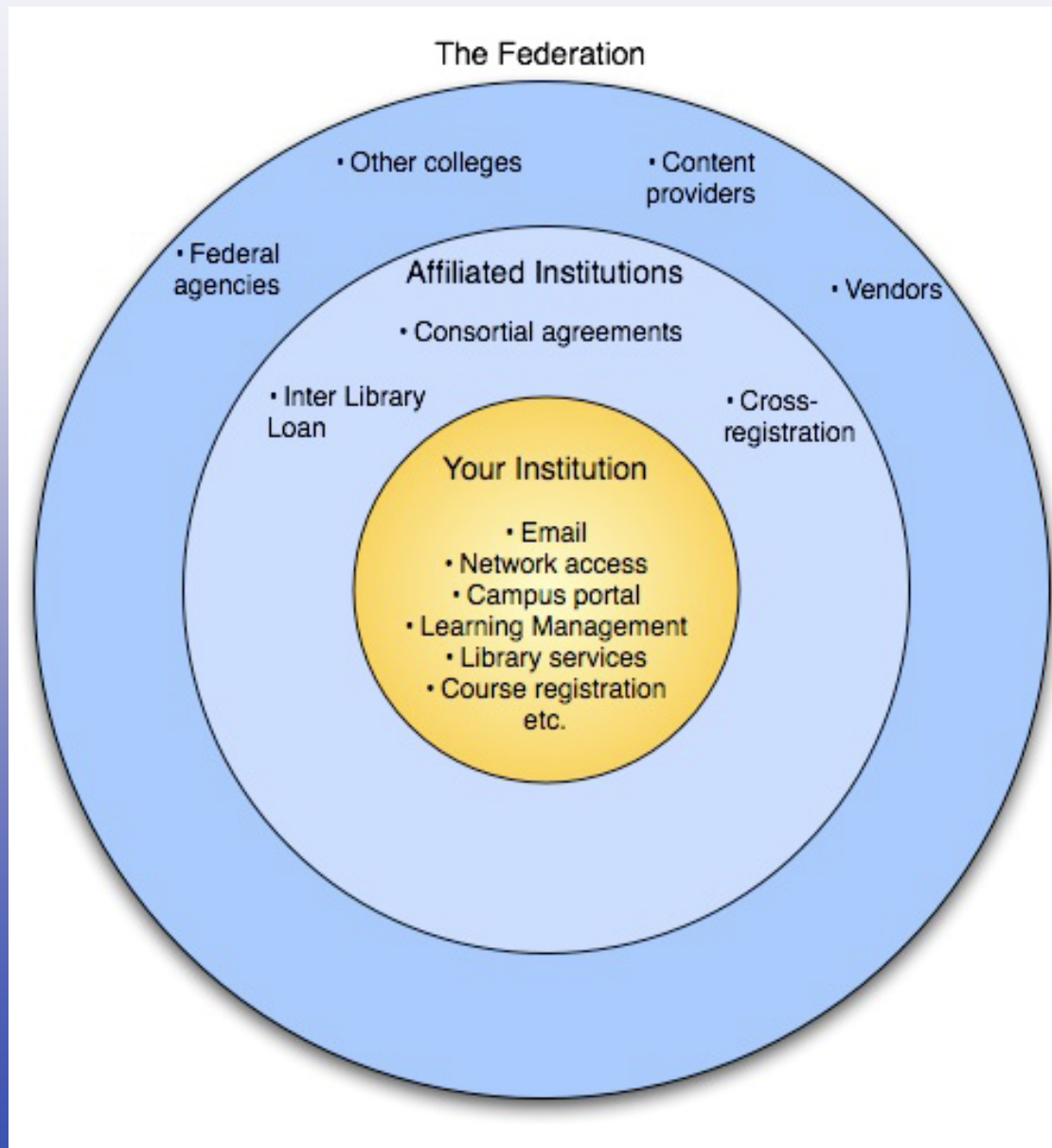
What is Federated Identity Management?

- Practices = solid internal mechanisms
 - Enterprise directory infrastructure
 - Mechanisms for creating and terminating user identities
 - Knowledge of where identity data is stored
 - Buy-in from key administrative units

Benefits of Federation

- Easier access to content and services
- Facilitate collaboration
- More secure
- The benefits of Single Sign On, extended beyond your institution

Extended Single Sign On



Access to Content & Services

- Library content (JSTOR)
- Federal Agencies (NSF, Dept. of Ed)
- Student Enrollment Verification
 - Microsoft DreamSpark
 - Student discounts
 - Financial aid

Facilitate Collaboration

- Google apps
- Inter-institutional
- Intra-institutional (single sign on)

"Ducks In A Row" for Securing Sharing of
Resources

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

IdM First!

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

Raise consciousness w/ campus leaders

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

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

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

Federation Second!

- Second on critical path for implementation

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

Case Study @ Lafayette College

The Beginning

- Net@EDU 2003
- Many Systems, Many Logins (2005: 11 different username/password combinations)
- Moved to single identity store for all systems
- Developed account creation/termination procedures
- Extend schema as desired/necessary (L-numbers, others)

Moving Towards Federated Identity Management

- Implemented eduPerson schema extensions (for Moodle, iTunesU)
- Used Shibb/InCommon as a guide
- Implement Shibboleth March 2007
- Joined InCommon June 2007

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 College determined by either the IdP, SP, or both
- Common attributes include authenticated (y/n), PrincipleName, Affiliation (from eduPerson)
- Where are you from/WAYF?

Then what is InCommon?

- The organization that manages the trust relationships
- Issues certificates
- Manages standards and best-practices required by members
- Negotiates intra-federation relationships

What We Do With Federated Identity Today

- Jstor
- RefWorks
- I2 wiki resources
- [DreamSpark](#)

What's Next: Single Sign-On for LC Web Applications

- Network Management Applications
- Moodle
- iTunesU
- Blogging/Drupal
- Zimbra/email

What's Next: Outside Services Using Federated IdM

- University Tickets
- Collaborations with other schools (Carleton!)
- NITLE Services/CLAC?
- NSF & Grant Application/Management
- Financial Aid Application
- Google Apps
- GridShibb

Projects On The Horizon

- Shibboleth 2.0 under way
- Examine Silver LoA and explore what needs to be done
- Automate account creation/termination procedures
- Encourage others to implement Shibboleth
- More hooks and info into identity vault
- [Federated IdM Conference](#)@Lafayette College: October 6-8, 2008

Links & Resources

- LC InCommon PoP - <http://its.lafayette.edu/about/policies/InCommonPoP>
- LC Account Management Policies - <http://its.lafayette.edu/about/policies/accounts>
- 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