Recipe for Federation: Policy, Governance, Infrastructure

Tom Jordan <tom.jordan@wisc.edu>
Ty Letto <ty.letto@wisc.edu>
Background

UW System Structure

• Common Systems – 13 campuses, UWEX, UWSA
History

• UWSA started the IAA initiative in 1996
  – Impetus was to track a person with a unique identifier throughout their student/employee lifecycle regardless of what system they were in
  – Madison UDS work created foundation through a replacement of the Card ID system for Y2K

• Infrastructure and proof of concept pilot for the Whitepages (system-wide directory never deployed) began in 2001
  – Name search would provide a comprehensive view of the individuals roles throughout UW System
  – Recognize single individual with multiple roles throughout UW System
  – UDS V.2 was template for current IAA Registry

• Began deployment of the IAA AuthHub in 2002 which provided authentication for system-wide apps
• **History – cont.**
  
  – **IAA Working Group** formed in December **2003**
    
    • Sponsored and charged by UWSA
    • Protect integrity of campus data
    • Enforce proper use of system data
    • Only way campuses would agree to provide feeds
  
  – **Three key governance principals**
    
    • May use education & HR data obtained from campus electronic data submission for the sole purpose of providing the identity and access management services (not for reporting). UWSA has no authority to make any other use or disclosures of such data
    • Responsible for maintaining and protecting the integrity and security of data while maintained in the IAA system
    • Data is for the purpose of software applications, not individual computer users
      
      – IAA Governance Working Group approves requests
      – They have the ability to query, access or obtain data from IAA
2003 IAA Memorandum of Understanding created

- Governs and protects data submitted to the IAA systems by UW System campuses and any use of that data
- Executed between each campus and UWSA
- Created by IAA Working Group
Background Cont.

UW System Structure Today

• 2008 launched new IAM infrastructure in support of HRS

• 2010 new IAM Steering Committee formed with expanded responsibilities:
  – Governance of data
  – Governance of infrastructure
  – Governance of budget and resources
Background Cont.

IAM Steering Committee representation

- CIO
- Campus
- ERPs
- Libraries
- UWSA Legal
- UW System Security

IAM Technical Advisory Group

IAM Support Team
The Wisconsin Identity Federation

• Architecture
  – Identity Registry
    • Batch or Near-Real-Time submissions from campuses
    • Central Identity Reconciliation – “the join”
  – Federation Infrastructure
    • Discovery service
    • Reverse Proxy Service
    • Metadata update / distribution
  – Federation Identity Providers
    • Centrally hosted IdPs (on behalf of some campuses)
    • Campus-operated IdPs
  – Federation Service Providers
    • Common Systems Applications
The Wisconsin Identity Federation

Provisioning flow:
- Campus Identity Sources
- System-wide Identity Registry

Login flow:
- Campus AuthN Sources
- System-hosted IdPs
- Campus IdPs

Common Systems Applications

DoIT DIVISION OF INFORMATION TECHNOLOGY
The Wisconsin Identity Federation

Campus Hosted
- UW Milwaukee
- Stout University of Wisconsin
- UW Madison
- UW Whitewater

Federation Infrastructure
- Federation Metadata
- WAYF

Centrally Hosted
- University of Wisconsin Eau Claire
- UW Extension
- University of Wisconsin Oshkosh
- University of Wisconsin Parkside
- University of Wisconsin Green Bay
- University of Wisconsin Platteville
- University of Wisconsin La Crosse
- University of Wisconsin River Falls
- University of Wisconsin Stevens Point
- University of Wisconsin Superior

Federation Applications
- Oracle HCM
- Oracle Peoplesoft
- Perceptive Software
- Symantec
- Ex Libris Alma
- Kaltura
- Blackboard
- Cherwell Software
- Primo
- Desire2Learn
- WebCheckout

DoIT DIVISION OF INFORMATION TECHNOLOGY
Wisconsin Federation Operations

- **Central Infrastructure Operations**
  - Identity Registry
  - Discovery Service
  - Hosted IdP services
- **Campus Operations**
  - Feed submission / troubleshooting
  - Local credentialing & support
- **Common Systems Application Support**
  - Application-specific troubleshooting
- **Tools and Techniques**
  - Data investigation (lookup, FADD)
  - Distributed troubleshooting processes
Wisconsin Federation Operations

• **Business Operations**
  – Data governance and oversight (IAM-Steering)
  – Budget and resource management (IAM Support Team)

• **Application Onboarding**
  – Data request
  – Technical assessment
  – Technical & Architectural Oversight

• **Infrastructure Strategy and Direction**
Wisconsin Federation Business Value

• Helping UW System collaboration happen
• Enables shared management
• Makes operations transparent
• Federates globally
• Common gateway
• Increased efficiencies
Wisconsin Federation Futures

- **Evolving the Infrastructure:**
  - Enhancing cloud integration capacity for hosted IdPs
  - Exploring Virtual / Federated Directory Services
    - Cross-campus Active Directory Integration
    - Azure AD / Office 365 Integrations
  - Enabling Social authentication for campuses
  - Expanding multi-factor authentication support
Wisconsin Federation Futures

- **Supporting strategic initiatives:**
  - Flex degree
  - K12 / Tech Colleges / Privates
  - CommIT
  - EduROAM
  - Others?

- **Enhancing operations:**
  - Attribute release
  - Procurement / onboarding
  - Tools for distributed support (iaa lookup, etc)
Questions?