



# NMI at Work: Case Studies from the NSF Middleware Initiative

David Bantz, University of Alaska System

Mark Crase, California State University

Miguel Soldi, The University of Texas System

Gordon Springer, University of Missouri, Columbia

Ann West, EDUCAUSE/ Internet 2

# EDUCAUSE / Internet 2

## **Introduction**

# NSF Middleware Initiative

- Create a national interoperable middleware infrastructure for education and research
  - Analogous to building NSFNet
- Funded two Teams in 2001
  - Grids Center (Tie resources together)
  - NMI-EDIT (Enable seamless and secure access)

- How do you create a national infrastructure?
  - Solve a problem
  - Create awareness
  - Develop a path
  - Address the gaps and challenges
  - Offer education
  - Provide a community

# Life after Grants: Extending the Reach

## Addressing the deployment support challenge

- Explore bridge support-structure
  - Encourage cohort partnerships
  - Develop diverse models of support
  - Assist a wider scope of schools
- Start with state systems and network service providers

# Extending the Reach

- Funded in 2004
  - Enabling interoperable IdM deployments
  - Exploring diverse business models, services, and products for Identity management training, consulting, and deployment
  - Disseminating information to spur similar activities
  - Informing NMI-EDIT outreach and technology-related products

# Extending the Reach Awards

- California State University System
- Great Plains Network Consortium
- University of Alaska System
- University of Texas System

University of Alaska System

# **Enterprise Directories**

## **Identified Business Needs (~2003):**

- Email addressing
- Unique identifier(s)
- White pages
- Phonebooks
- Directory synchronization

## **Institutional Constraints:**

- UA System has single ERP (Banner)
- Universities expect autonomy
- Individuals have multiple affiliations

## **Pragmatic Goals for Deployment of Directory:**

- **System:** manage IDs for portal
- **Universities:** directory synchronization
- **Campuses:** automate phonebook production
- **Individuals:** end-user self-maintenance

## Project Methodology:

per NMI: Enterprise Directory Implementation Roadmap

- **Strategic** core infrastructure in principle
- **Application** motivated deployment:
  - white pages (online & printed)
  - portal
- **Stealth** built & designed

## **NMI Components Reference:**

- Middleware architecture
- eduPerson, etc objects
- Enterprise Directory Implementation Roadmap
- Identifiers “Best Practices...”
- AuthN with browser cookies examples
- Federation & Shibboleth (longer-term)

California State University

**The Identity Management  
Collaborative: A CSU Identity & Access  
Management Pilot Project**

Cal Poly San Luis Obispo

California State University Stanislaus

The Office of the Chancellor

### **The Project**

- Develop a *middleware service-provider* model whereby one campus supports another campus in designing, implementing and supporting an enterprise directory service.

### **The Project Goals**

- Provide robust Identity Management services by leveraging talent and other system resources
- Strengthen the operations at the *provider* campus
- Improve services at the *client* campus
- Provide test-bed to address issues related to the system-wide Identity & Access Management Project

### **Objectives: Office of the Chancellor**

- Create an inter-campus service/support model
  - Develop *needs assessment* tools to determine programmatic needs and resources required to meet them
  - Develop *service proposal* templates
  - Develop *performance metrics*
  - Conduct *performance assessments*
- Document and disseminate *lessons learned* within the CSU and out to the greater education community

### **Drivers: Stanislaus**

- Need for an Enterprise Directory and Authentication Services
- Integration of Single sign on for:
  - Oracle Portal (for email and Banner)
  - Blackboard
  - PeopleSoft HR 8.0
- Lack of Campus Resources Due to Budget Cuts

### **Goals and Objectives: Stanislaus**

- Authenticating all applications using the Enterprise Directory
  - Applications considered are Help Desk, Imaging, One-Card, Active Directory in labs, Library
  - Formalize procedures for adding applications
  - Create a knowledge base for both the campus community and vendors re: authentication procedures
- Local hosting of the Directory in a couple of years
  - Feasibility study to identify resources needed
  - Identify migration strategies

### **Benefits: Stanislaus**

- Collaboration Process
  - Learning Process for our staff
  - Sharing of best Practices
- Working Directory and Authentication Services with minimal effort
- Working knowledge of implementing an Enterprise Directory

### Drivers: San Luis Obispo

- Value of collaboration
  - Gain an outside perspective
  - Enable knowledge transfer between teams
  - Gain feedback regarding processes, software and tools
  - Enable cross-campus collaboration **not** related to IdM (both campuses using Oracle Collaboration Suite)
- Service Improvement
  - Opportunity to enhance infrastructure
  - Opportunity to improve processes
  - Opportunity to increase services & support
  - Opportunity to achieve greater economies of scale

### **Goals and Objectives: San Luis Obispo**

- Enhance Identity Management Infrastructure
  - Upgrade software to newer versions
    - Oracle Internet Directory 10g and CAS 2.012
  - Implement LDAP replication
  - Implement EduPerson/CalStateEduPerson directory schema
  - Enhance documentation
    - Technical and procedural
- Enhance cross-campus collaboration
  - Facilitate sharing between campuses

### **Benefits: San Luis Obispo**

- Improved campus buy-in regarding middleware
  - CSU sanctioned initiative
  - Other CSU's moving forward
  - Supports future interaction within CSU system
- Input from other middleware teams regarding Cal Poly's implementation
  - What would another team have done differently?
- Collaboration process
  - What can we share? How can we share?
  - What did we do right? What needs improvement?
  - What did we miss?

### **Project Structure: Stanislaus**

- Role: Client
- Identify service requirements
- Gain campus buy-in for a remote LDAP directory
- Identify applications to be supported
- Identify pilot group for training
- Communicate the advantages of a secure identity management system on Campus
- Documentation:
  - Policy statements and agreements
  - Creation of knowledge base of Frequently Asked Questions

### **Project Structure: San Luis Obispo**

- Role: Service Provider
- Provide a Service Proposal
- Define Security and Reliability Metrics
  - Transmission of directory information
  - Storage of directory information
- Build and populate an enterprise LDAP-compliant directory
- Enable authentication services
- Provide remote support for enterprise directory and authentication services

## Challenges and Lessons Learned:

- Challenges
  - Campus and Staff buy-in
    - Concept of remote directory services
    - Security and reliable access
  - Staff resources
    - Resources for the project
      - Conflicts with local projects
- Synchronizing activities at two campuses is not trivial
- External forces are also at play
- Receiving help from a *provider* campus does not negate the need to do significant preparation at *client* campus

### **How NMI Helped:**

- LDAP Recipe
- eduPerson Object Classification →
- calstateEduPerson
- Local Domain Object Class Survey
- Directory Implementation Roadmap
- All the meetings and conferences where we get to meet people and talk about this stuff

The University of Texas System

**Federated Version of Benefits  
Enrollment Application**

## **Background:**

- The UT System Administration Office of Employee Group Insurance (EGI) manages the insurance benefits of all employees and retirees of the 16 UT System institutions.
- Every year, EGI allows all employees and retirees to participate in the benefits open enrollment via the benefits annual enrollment application.
- During the year, employees can use the benefits annual enrollment application to view their current coverage.

## **Business Problem:**

- Use of Social Security Numbers (SSN) as credentials.
- The use of social security numbers as identifiers will be prohibited by UT System policy by 2007.

## **Proposed Solution:**

- Leverage UT System Federation
- A federated version of the benefits annual enrollment application that allows employees and retirees to access the application using their home institution-provided identity credentials.

## **Project Goals:**

- Create a federated version of UTTouch - benefits annual enrollment mainframe application.
- Pilot year-round availability of the federated version of UTTouch with new hires and active employees at four institutions – UT System Administration, UT Dallas, UT Tyler, and UT Permian Basin – by Fall 2005
- Release the federated version to production for new hires and active employees at all institutions by July 2006.

## **NMI Components at Work:**

- Shibboleth and Specifications
- eduPerson Object Classification
- NMI Outreach and sponsored events
  - Federations

## **Project Objectives:**

- Allow employees to access UTTouch using their home institution-provided identity credentials
- Each institution identity provider shall assert via Shibboleth the appropriate attributes to UTTouch to authorize access to the application.
- Modify scripting environment to integrate with mainframe.
- Provide new and current employees year-round access to UTTouch to make their initial insurance selections or view their current coverage.

## Project Structure:

- **Technical:**

- Configure and implement Shibboleth SP server (UT Austin)
- **Modify web agent**
- Base install of UTTouch application in SP server
- Configure environment variables with clients
- Implement application changes for receiving user data via Shibboleth target/http assertion headers and accessing them in Natural
- Define application indexes to access ADABAS database
- Modify login verification modules
- Create proper authorizations for new Shibboleth SP server

## Project Structure:

- **Policy:**
  - Short Term
    - Issues surrounding the population, release, transmittal, and use of SSN data (since SSNs could be communicated in the background over the encrypted connection for the assertion from the Shibboleth Attribute Authority)
  - Long Term
    - Levels of Assurance
    - Investigate ways to modify the application to not require SSN but use an institution's local identifier

## Challenges:

- Retirees
  - Most institutions do not maintain data about their retirees much less do they maintain identity credentials for them.
  - Will require business process considerations
- Staff Resources
  - Conflicts with local institution projects

## Benefits:

- First large-scale, system-wide deployment of a federated application using Shibboleth
  - ...and the working knowledge from implementing it
- Significant stride in the elimination of the use of Social Security Numbers as credentials
- Increased awareness and buy-in from institutions regarding middleware
- What else can we share? And How?

# The Great Plains Network (GPN)

## Region-Wide Collaboration Environment



# The Great Plains Network

## Region-Wide Collaboration Environment

### **Background:**

- 7 States in region (AR, KS, MO, ND, NE, OK, SD)
- GPN connected all states to Internet2/Abilene network as a gigapop. 3 states now connected and 4 are collaborating partners
- GPN has a history of network infrastructure collaboration - Midnet (1987) then GPN (1997)
- Can this history be turned into a collaborative research and education environment using middleware?

### **Project Basis:**

- Participation of 11 of 23 campuses in GPN consortium in the creation of a region-wide collaboration environment
- Initial thrust: To develop a plan and deploy Shibboleth at each institution to provide a means for inter-institutional authentication
- Determine issues with integrating Shibboleth at each home institution

### **Project Goals (Year 1):**

- Strategic planning on a regional basis to deploy Shibboleth authentication for collaborative activities
- Campus middleware assessment on campuses to determine impediments to moving forward
- Build a middleware testbed on two campuses to demonstrate interoperability for limited applications
- Attend and conduct workshops focused on middleware deployment (e.g., Shibboleth)

### **NMI Components at Work:**

- Shibboleth and Specifications
- NSF/NMI and NSF/NMI-Edit middleware software tools
- eduPerson Object Classification
- NMI Outreach and sponsored events
  - Shibboleth
  - Federations

### **Project Components:**

- Shibboleth installation and training occurred through install-fests
- Campus directory integration
- Support for federation
  - Initial deployment with Internet2 InQueue
  - Considering shifting GPN members to InCommon
  - Resource providers redirect access requests to the user's home institution for authentication
- MACE entitlements (`urn:mace:greatplains.net`)
  - Using eduPersonEntitlement for fine-grained authorization
  - Four entitlement-based resources at two institutions defined

### **Challenges:**

- Dealing with policy issues among multiple institutions
- Defining entitlements for coarse-grained and fine-grained authorizations
- Developing a strategy for authorizing and managing entitlements with standardized tools (e.g., Signet and Grouper) in a federation
- Moving a testbed environment toward a production level environment with a broader scope to support regional research and education activities

### Lessons Learned:

- A multi-institutional collaboration environment can be created using NMI middleware software tools
- Collaboration among individuals is essential
- Middleware projects will be limited by the level of support by the institutions in the region
- It is essential to remain aware of current events and changes within the broader NMI community
- Using NMI middleware: **We are light years ahead of our talking last year!**

## **NMI-EDIT is at work...**

- Helping campuses build their identity management infrastructure
- Solving research, academic, and administrative problems
- Enabling new functionality by building a national infrastructure

## For More on NMI...

- NSF Middleware Initiative
  - [www.nsf-middleware.org](http://www.nsf-middleware.org)
- NMI-EDIT
  - [www.nmi-edit.org](http://www.nmi-edit.org)
  - Authentication CAMP – Feb. 8-10

**Thank you!!**

**Q / A**

## Contact Information:

- The University of Alaska System
  - David Bantz, Chief Information Architect
    - [db@alaska.edu](mailto:db@alaska.edu)

## Contact Information:

- Stanislaus
  - Roland Johnson, Manager AITS
    - rjohnson@csustan.edu
  - Maithreyi Manoharan, Assoc.VP for IT
    - mmanoharan@csustan.edu
- San Luis Obispo
  - Dan Malone, Middleware Architect
    - dmalone@calpoly.edu
  - Theresa May, Information Management Coordinator
    - tmay@calpoly.edu
- Office of the Chancellor
  - Mark Crase, Sr. Dir., Tech Infrastructure Svcs
    - mcrase@calstate.edu

## Contact Information:

- The University of Texas System Administration
  - Paul Caskey, Technology Architect
    - [pcaskey@utsystem.edu](mailto:pcaskey@utsystem.edu)
  - Miguel Soldi, IT Policy and QA Coordinator
    - [msoldi@utsystem.edu](mailto:msoldi@utsystem.edu)

### Contact Information:

- The Great Plains Network (GPN)
  - Amy Apon, GPN ETR Project PI, University of Arkansas, [aapon@uark.edu](mailto:aapon@uark.edu)
  - Gordon Springer, GPN ETR Project Co-PI, University of Missouri, Columbia, [springer@missouri.edu](mailto:springer@missouri.edu)
  - Greg Monaco, GPN ETR Project Co-PI, Great Plains Network, [greg@greatplains.net](mailto:greg@greatplains.net)
- Visit the GPN ETR Website:  
<http://archie.csce.uark.edu/gpn>