Enterprise Directory Services

July 13, 2006

http://www.itd.umich.edu/enterprisedir/
Today’s Agenda

- Project Overview and Status
- Data and Governance
- Architecture
- Deliverables and Timeline
Project Overview and Status
Project Overview

- The Enterprise Directory will bring together data from multiple institutional sources and will organize, present, and secure the data in a way that is particularly well suited to managing access to University resources.
- Provides units and end users with a "one stop directory shop" for provisioning of services, access control, and directory enabled applications.
- A robust set of tools that include/enable:
  - Identity and life-cycle management
  - Real time provisioning of central IT resources
  - Real time provisioning of local IT resources
  - Clearly defined and documented programming interfaces
  - Auditing system
  - Integrated workflow
Phase II Teams formed in September

Charge to teams
- Data and Governance
  - Establish Governance Board
  - Establish guidelines for data use and access
- Solution Architecture
  - Make a software selection
  - Refine design
- Produce cost estimate of higher confidence
Governance Board Members

- Ed Adams, Ross School of Business
- Karen Arnold, Registrar, Flint
- Linda Brown, Assistant Vice Chancellor, Dearborn
- Bob Korniski, Development Office
- Justin Laby, College of Engineering
- Sue MacDavitt, Director, HRAA
- Phil Ray, School of Natural Resources & Environment
- Paul Robinson, Registrar, Ann Arbor
- Liz Salley, MAIS
- Cory Snavely, University Libraries
- Luke Tracy, ITCS
- Mark Weishan, College of LSA
Project Overview (continued)

- Design Team
  - Gray Carper, Medical School
  - John Herlocher, Life Sciences Institute
  - Seth Meyer, MAIS
  - Vasilios Pliakas, Development Office
  - Liz Salley, MAIS
  - Barry Starrfield, University Housing
  - Luke Tracy, ITCS
  - Paul Turgyan, ITCS
  - Jeff Wixon, MAIS
  - Howard Young, ITCS
Project Status

- Governance Board recommendations being prepared for review
  - Populations and Data Sources
  - Person Attributes
  - Institutional Roles Proposal
- Produced Request For Proposal (RFP) and software recommendation
- Developed Detailed Solution Architecture
Project Status – What’s left?

- Presentations to Campus IT Communities
- Complete Phase III Project Plan
- Complete Cost Estimates
- Detailed Solution Description Document
- Solution Branding
Data and Governance
Data and Governance (cont.)

- Populations
  - Employee
  - Student (Ann Arbor, Dearborn, Flint)
  - Alumni
  - Sponsored

- Data Sources
  - Institutional
  - Sponsor System
Data and Governance (cont.)

- Sponsor System
  - Web-based UI and Programmatic Interface
  - Documenting institutional processes
  - Minimum data standards
  - Life-cycle management
  - Distributed creation
  - Will not require physical presence
  - User self registration
Data and Governance (cont.)

- Person Attributes - Recommendations
  - More attributes will be hidden from public view by default, unless the individual chooses otherwise.
  - Some employment related attributes will not be concealable.
  - Attributes hidden from public view, would still be available, as needed, for provisioning and access control.
Data and Governance (cont.)

- **Roles**
  - Institutionally Managed
    - describe a person’s associations with the University for the purpose of granting access to services.

- **Roles Management System**
  - Departmentally Managed
    - Elevated access to fine-grained directory data
    - Provisioning of local IT resources
    - Technical and compliance training for Admins
Future Governance Board Activities
- Wrap up current phase of work on June 19th
- Participate in detailed design during Phase III
- Participate in creation of training guidelines and materials
- Define access procedures and guidelines
- Be available to field requests for additional data
Architecture
Design Team Recommendation

- Based on the results of the RFP process, Novell is the preferred vendor.
- The final decision on vendor selection will be made by the project sponsors.
- Following further work on the next phase project plan and cost estimates, a proposal will come forward to the IT Capital Projects Team.
Architecture – Future

- Key requirements of software solution
  - Workflow engine
  - Audit system
  - Customizable interfaces
  - Re-usable business logic
  - Scalable and flexible directory
  - Native connectivity to key systems
  - Life-cycle management
Architecture - Future

- Workflow
  - Integration Points
    - Connector Integration
    - Web-based User Interface Integration
    - Directory Integration
  - Capabilities
    - User Self Service
    - Series of automated tasks
    - Manual intervention
    - Custom routing patterns
Architecture - Future

- Audit System
  - Integration Points
    - Directory
    - Connectors
    - User Interfaces
  - API for extending functionality
    - Custom actions
    - Custom data stores
    - Instrument local apps
  - Granular definition of data to be audited
  - Secure logging with non-repudiation
Customizable interfaces

- Customizable layout and color scheme.
- Web-based User Interfaces use Java Portlets which can be customized.
- Ability to add our own Java Portlets to provide UM specific content and integrate existing content.
Re-usable business Logic

- Business logic defined using XML and XSLT and stored in the Directory.
- Existing business logic can be used multiple times by referencing their directory objects.
- Integrated development environment for building and testing business logic off-line, and then easily deploying to test and production systems.
Scalable and Flexible Directory
- Mature multi-master replication model
- Dynamic Access Control Lists and schema
- Cross platform support
  - Windows, Linux, NetWare, AIX, HP-UX, more...
- Fully Instrumented for Auditing
- Standards compliant
- Referential Integrity
Native Connectivity to Key Systems

Connectors that speak to the directory on one side, the application or system on the other side, and XML & XSLT business logic in the middle.

Some of the connectors provided by the vendor:

- Peoplesoft, Active Directory and Exchange, eDirectory, LDAP, JDBC, DB2, SOAP, JMS

SDK and APIs for custom connectors to other key systems, such as MIT Kerberos and AFS.

Collaborative development opportunities exist with other units on campus and other Universities.
Architecture - Future

- **Life-cycle Management**
  - Unique Loopback connectors allow for continuous evaluation of directory data using the same techniques and logic as connectors to other systems.
  - Provides the same integrated workflow and auditing capabilities.
Vendor software solution provides the foundation elements of an Enterprise Directory Service for the University of Michigan, allowing us to focus on the functionality that is unique to our institution.

- Sponsor System
- Roles Management System
- Business Logic
Most "People" entries are created initially by UNS when the uniqname is assigned. Data for which other systems are authoritative are updated through "feeds."

The update process runs weekly. The feeds come at various frequencies. MAIS data comes daily, but needs frequent manual resolution, hence the weekly update process. Other feeds are delivered less frequently: Flint once per term, UMOL as requested, etc. Feeds are converted to an internal format (.LDIF) before input to YAM. YAM is able to communicate either with a live directory or a text representation of a directory. In pass 1, text is used to reduce load on the directory servers. In pass 2, the live directory is used.

Changes are propagated to AD and eDir in realtime.
Architecture - Future

Simplified

- Includes all IDs, regardless of source or status
- Protected data, limited access, includes more sensitive data
- Performs real-time queries of source data as needed
- Includes attributes for a person

Sponsor System
- Create Ad Hoc IDs
- Require minimum data
- Find/Assign UMID
- Assign unique ID
- Assign Departmental Roles
- Manage Lifecycle

Departmental Sources
- Department-specific attributes
- Create Entries
- Assign Departmental Roles
- Manage Lifecycle

Directory
- Outward-facing directory
- Contains "active" IDs
- Groups and Roles
- Performs real-time queries of Registry as needed
- May include support for unit-specific views

UMOD
- White Pages application
- Mail forwarding service

MAIS

Dearborn

Logic

Central Systems
- Card Key Access
- ITCS services
- 2-factor authentication

Departmental Systems
- Apply local business rules
- Provision and De-provision departmental services

http://www.itd.umich.edu/enterprisedir/
Architecture - Future

http://www.itd.umich.edu/enterprisedir/
Deliverables and Timeline
Deliverables and Timeline

EDS Phase III Timeline

- Funding approved
- Stated
- Dev Registry and Directory
- LDAP Proxy Method built
- User and Roles Admin Interface built
- Kerberos
- Elevation of Directory and Directory
- Initial Release of User Interface
- UMDD UI decommissioned
- LANKOS services provisioned from ED
- UMCE services provisioned from ED
- CAEN services provisioned from ED
- Six additional units’ services provisioned from ED

+6 months
+12 months
+18 months
+24 months
+30 months

Project startup and initial install
Development and testing
Define data access policies and training
Training materials & documentation
Services Integration
Role Admin Training
Sponsor Training

http://www.itd.umich.edu/enterprisedir/
Deliverables and Timeline

- 6-12 months after funding approved
  - Development Registry and Directory
  - Sources Connected
  - v0.5 release of User and Roles Admin Interfaces
  - Elevated directory access training materials

- 12-18 months after funding approved
  - Production Registry and Directory
  - Initial release v1.0 of User and Roles Admin Interfaces
  - UMOD UI decommissioned
  - LANNOS services provisioned from ED
To Stay Informed

Project updates at
http://www.itd.umich.edu/enterprisedir/
Email updates at ED.Project@umich.edu