

Who are you (today)?

Integrating Identity

Lifecycles

with Information Services

Joel Fletcher and Greg Lozeau

Western Michigan University

Office of Information Technology

Session Rules of Etiquette

- Please turn off your cell phone/pager
- If you must leave the session early, please do so as discreetly as possible
- Please avoid side conversations during the session

Copyright Western Michigan University 2007

This work is the intellectual property of the authors. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the authors. To disseminate otherwise or republish requires written permission from the authors.

Goals of this case study

- The IT Vision at WMU
- Initiatives, intentions and the resulting impact
- Time lines that drove the process
- Building the necessary infrastructure
- Business process management
- The collaborative challenge
- Life-cycle definition
- A new way of provisioning a user
- Lessons learned

Background on WMU

- Carnegie Comprehensive Doctoral Institution
- Seven Colleges
- Six Regional Campuses
- 26,000 Graduates and Undergraduates
- 3,500 Faculty and Staff
- Business Technology Research Park
- The Broncos!

The Vision

- Building the network infrastructure – President Haenicke
- Then came Wireless Western and strongly recommended laptop program – President Floyd
 - Anytime, anywhere access to resources
- A better e-communication infrastructure
 - Multi-platform, open source, end-of-life system
- A new Student Information System – a competitive advantage – President Bailey
- Take advantage of the built infrastructure
 - new applications to launch an over-arching solution for identity management

Initiatives

- Electronic Communications (ECI)
 - Various phases
 - Sun Center of Excellence
- Student Information System (SIS)
 - Banner – Luminis Portal – TracDat – iWebfolio – Cognos - TouchNet
- Identity Management (IdM)
 - Spin-off of ECI

Electronic Communication Initiative (ECI) - Intentions

- Phase I
 - Implement enterprise directory, messaging and calendar solution
- Phase II
 - Implement **Meta** directory, as well as web and portal services
- Phase III
 - Other Sun One (JES) applications – portal, IM, etc.
- Take advantage of **Wireless Western** to deliver e-communications to mobile devices

ECI - Intentions

- Phase I
 - Migrate existing UNIX e-mail users
 - Changing conventions
 - firstname.mi.lastname vs. username@ delivery
 - No forwarding off-campus
 - Requiring all mail host on campus to use one mail gateway

SIS Initiative

- Replace an aging mainframe student information system
- Eliminate Social Security numbers
- Budget challenges
- Capitalize on the opportunity to address data access and security
- Take advantage of a portal solution
- Integrate into a Course Management System

SIS - Intentions

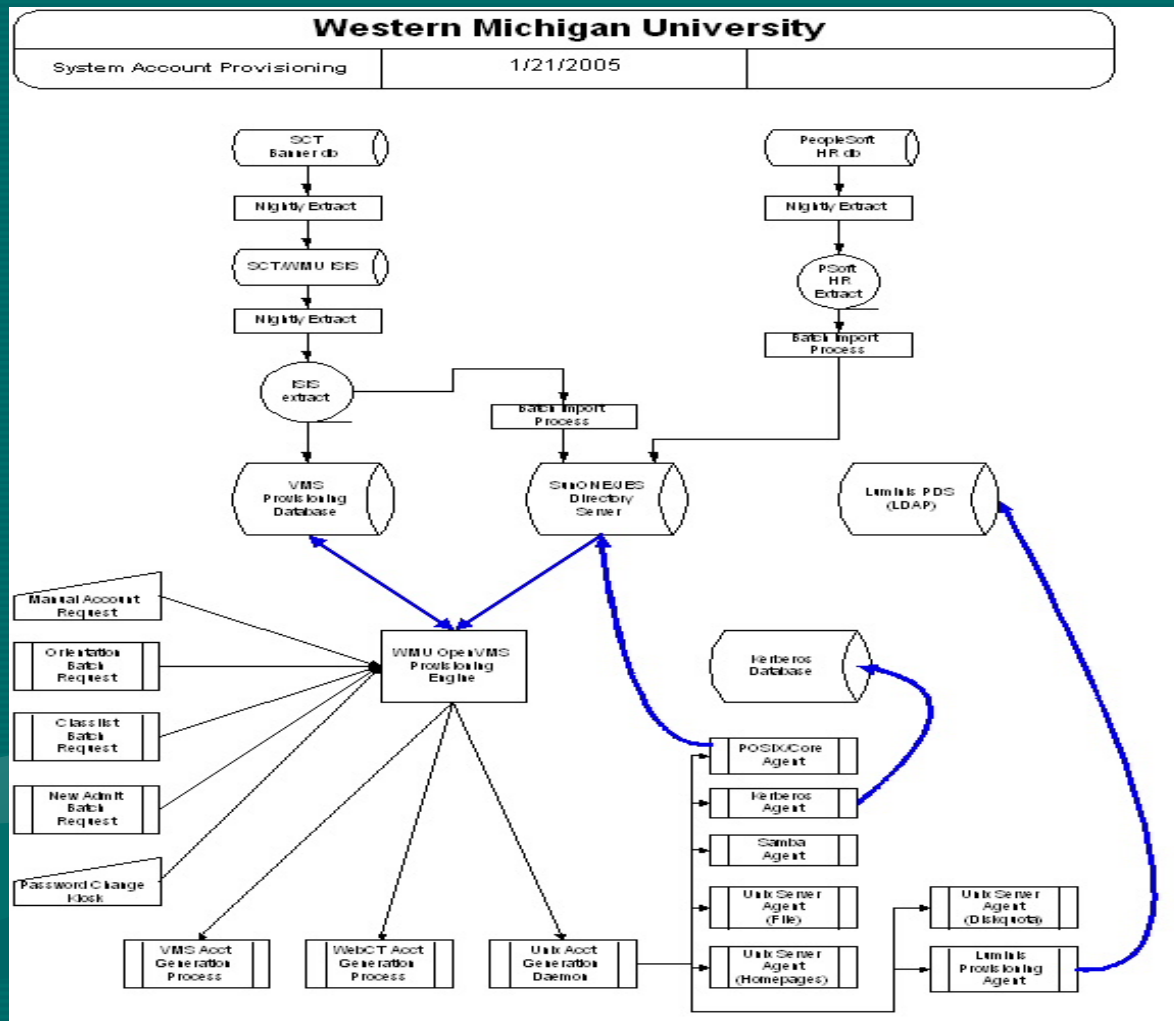
- GoWMU.wmich.edu – portal delivery
 - SSO (Single Sign-on) capabilities
 - Seamless access to Banner Self-Serve
 - Seamless access to WebCT
 - Seamless access to ECS
 - Seamless access to...
- Advancement of current portal capabilities
 - Beta test Parallel Deployment (multi-server)
 - Installed PD in February 2006

Identity Management (ECI – Phase II) - Intentions

- The provisioning/de-provisioning challenge
 - More granular control of access to services
- Provide a new identifier on the campus ID card
 - Elimination of SSN on magnetic stripe
- Take advantage of the capabilities to better integrate SIS with Course Management with Luminis portal with...

The Impact!

Old Provisioning Model from the 50,000 foot view



Initiative Timelines

- ECI Kickoff Summer 2003
- SIS Kickoff Winter 2004
- ECI implementation Spring 2004 with phased in services throughout the year
- Portal – Summer 2004 with SSO to self-serve applications Winter 2005 and content management (LCMS) starting March 2006
- IdM Kickoff Winter 2005 – implementation in progress
- The initiative rollout determined the order and urgency with the collaborative dialog of the various stakeholders

Project Planning

- Professional Services
 - Sun and SCT
 - Meeting the project time lines **and** the day-to-day tasks/responsibilities
- Altering the time line to accommodate the university's bureaucracy
 - “Stops” between the design and implementation phase
- Running parallel paths

Infrastructure building blocks

- Single enterprise UserID – “Bronco NetID”
- Kerberos
- LDAP – Sun JES Directory Server
- “Legacy” provisioning services
- Multiple web-authentication schemes
- ID Card-driven authentication services + self-serve kiosks

Services built on that infrastructure

- E-mail – (imap, smtp, webmail)
- Student/faculty web pages (homepages.wmich.edu)
- WebCT e-learning system
- Interactive systems (OpenVMS, UNIX)
- Departmental systems – Parking, Residence Halls, etc.

Services not built on that infrastructure

- Netware file and print (to be added)
- Windows Active Directory services (to be added)
- Institutional database services

Secure infrastructure

- Three(plus)-tier network
 - Tier 0 – Internet and Residence Hall Network
 - ----- Cisco PIX Firewalls -----
 - Tier 1 – User Tier (Untrusted Clients)
 - ----- Cisco CSS Load-Balancer -----
 - Tier 2 – Application Services (DMZ)
 - User Services – imap, portal, etc.
 - Proxy Services
 - Application Services
 - ----- Cisco CSS Load-Balancer -----
 - Tier 3 – Secure Network Services
 - Secure back-end (core LDAP, message store, Kerberos)
 - Secure Databases
- Cisco VPN (External access to secure services)

The new building blocks

- Sun JES (Communications Suite) Messaging and Calendar
- Sun JES Identity Manager (formerly Waveset Lighthouse)
- Sungard Higher Ed Banner Self Service
- SHE Luminis Data Integration (LDI)
- SHE Luminis Portal
- Blackboard Vista - Banner Integration
- New Student/Employee ID (no SSN)

Business process changes

- Official university email delivery – no forwards, etc.
- ALL students admitted to University get a Bronco NetID
- Role-based identity
- “Life-cycle” of the identity
- Need a Bronco NetID **now** to register

The collaborative effort

- Collaboration brings IT all together
 - Internal to the IT unit
 - Internal to the organization
 - External to the organization
 - IT and the vendor

The collaborative initiatives

- Services targeted to stakeholders
- Electronic Communication
 - Directory, Messaging and Calendaring
- Student Information System
 - GoWMU, iWebfolio, TouchNet, Cognos
- Identity Management
 - ID cards, provisioning, roles-based access

The collaborative challenge – lessons learned

- Educational process
 - Salesmanship and marketing
- Take advantage of existing governing groups
- Formulation of new governing groups
- When contracting with professional services, allow time for acceptance/buy-in
- Can never start the dialog too early

Life-cycle definition

- Student life-cycle
 - When is a student a student?
 - How long to keep a student “around”?
 - What services are they entitled to at various stages of their life-cycle?
- Who needs to answer these questions? Not IT!
 - Registrar – Admission – International student services

Life-cycle definition

- Faculty and staff life-cycle questions
 - When is a new faculty member issued a Bronco NetID?
 - When does a faculty/staff lose access to resources when they retire, terminate employment, move to another position,...
 - What about those individuals “loosely” associated with the university?
 - Contractors, rec center users,...= affiliates

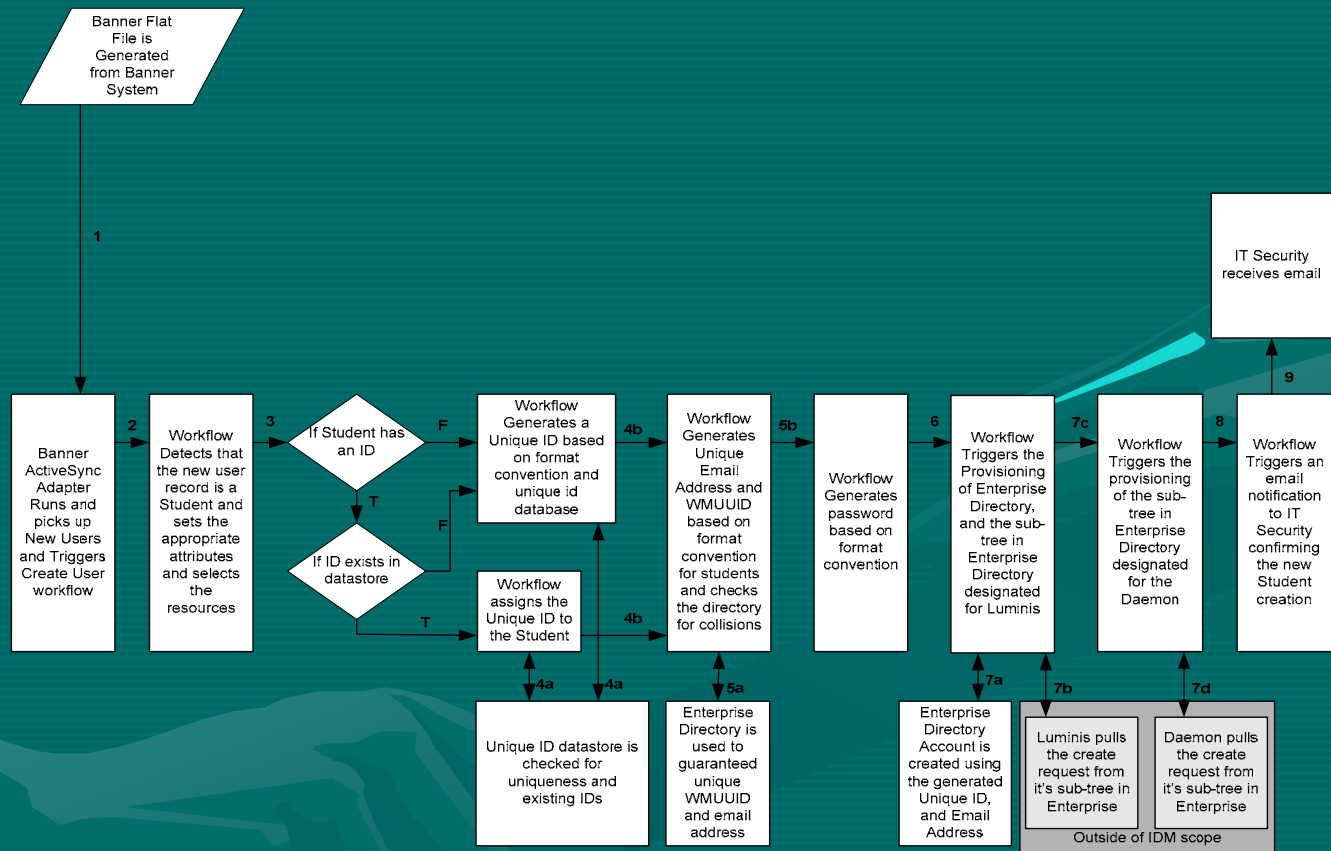
Life-cycle definition

- What about student employees? What services are they entitled to?
- What about “guest” to the University?
- Who needs to answer these questions? Not IT!
 - Human Resources – Provost

An Identity Management (IdM) solution

- Components of Sun IdM product
 - IdM Database (Oracle)
 - Interfaces to LDAP and enterprise databases
 - Rules Engine
 - Scheduler
 - Provisioning Agents/Listeners

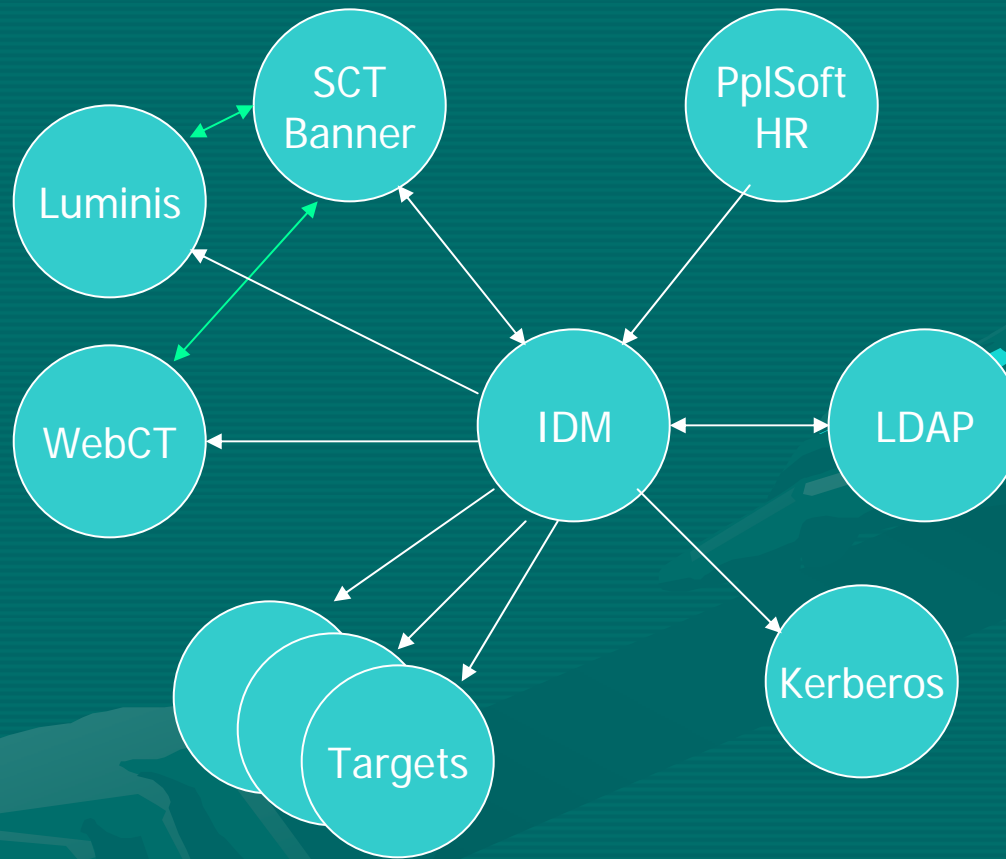
Process flow



Still needed a better way of provisioning a user

- Does Banner need to start the process of a new user?
 - Ultimately, yes
- Change in Bronco NetID format
 - License plate design
- Need to accommodate faculty/staff account creations
 - PeopleSoft HR integration
 - Banner faculty assignments (SIBINST)

After IdM – from 50,000 feet



Next Steps

- Real-time provisioning – no feeds
- Federated Identity support
- Two-factor authentication
- Integration of multiple SSO technologies into common SSO platform
 - WMU WebLogin (NormCookie) – Sun Access Manager
 - Luminis CPIP use

Critical Success Factors

- Top-level support
- Vendor involvement and guidance
- Flexible product and project plan
- Solid infrastructure
- Being “big picture” but still attend to details
- Relationships

Questions & Answers

Thank You!

- Joel Fletcher
 - Systems and Operations
 - joel.fletcher@wmich.edu
- Greg Lozeau
 - Planning and Middleware Services
 - greg.lozeau@wmich.edu