



# **Practical Applications of Identity Management**

An overview and discussion of the  
Medical College of Georgia  
identity management  
implementation

# Introduction

- Identities
- Account Management
- Authentication
- Access Controls
- Novell Identity Manager 3.6

# Challenges

- Many systems of authority
- Many applications and services
- Overlapping user roles
- Disparate account management
- Many different user ID's and Passwords
- User start delayed until account is created
- Disabling access in a timely manner

# Goals

- Common Authentication (not SSO)
- One system with superset of identity data
- Eliminate manual exchange of ID data to systems
- Account management for applications
- Automatic provisioning of IT “birthrights”
- Zero-day-start for students & employees
- Deprovision instantly upon termination

# Planning

- Kickoff and Discovery
- Established Authoritative Sources
- Identified data consumers
- Defined data elements

# Kickoff & Discovery

- Business Unit participation very important
- Defined user roles and permutations
- Discovered the business processes
  - Documented and undocumented
- Consultants were helpful during this phase

# Established Authoritative Sources

- Determined user entry points
- Noted exceptions
- Identified & documented current vetting practices and requirements
- Established data ownership

# Identified data consumers

- Identified all systems that could potentially benefit from IDM
- Decided which systems to include in initial implementation based on:
  - Extent of benefit
  - Impact to system & business process
  - Difficulty of integration
- Established business unit and technical contacts for each system

# Defined data elements

- Classes (object or record type)
- Attributes
- Created data mapping
- Established the direction of the flow for each data element

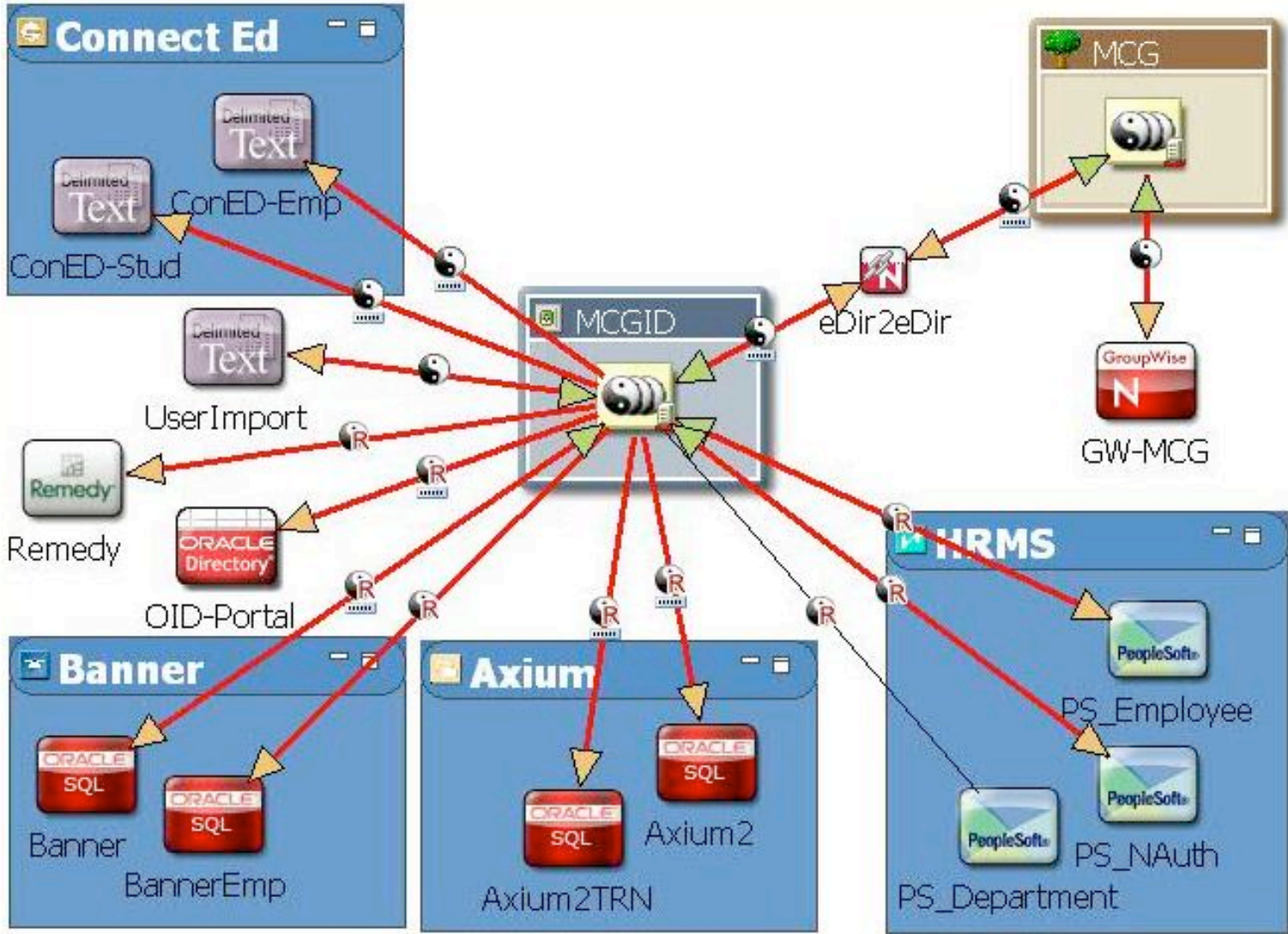
# Connected Systems

- Authoritative (providers)
  - PeopleSoft HRMS
  - Banner
  - Enterprise directory (eDirectory)

# Connected Systems (cont.)

- Non-Authoritative (consumers)
  - PeopleSoft HRMS
  - Banner
  - Enterprise Directory
  - Enterprise Email (GroupWise)
  - Dental School Mgt. System (Axiom)
  - Enterprise Portal (Oracle portal)
  - Remedy Helpdesk Request System
  - Connect Ed (emergency notification system)

# User data flow



# PeopleSoft HRMS

- Authoritative source for Employee roles, HR specific attributes and Department objects
- Split into three interfaces (drivers)
  - All data for Employee roles
  - HR specific data for non-employee roles
  - Department objects and data
- Interfaces utilize driver, Peoplesoft Component Interface and staging table

# Banner

- Authoritative source for Student roles and Registrar specific attributes
- Split into two interfaces:
  - All data for Student only roles
  - Registrar specific data for student-employees
- Interfaces utilize JDBC driver, staging table and event log

# Enterprise Directory

- eDirectory-to-eDirectory
- Synchronizes Users and Groups
- Consumes Identity data
- Provides auth./access control attributes
  - Group Memberships
  - Passwords
  - Account expirations/Login disabled
- Pass-through for Email attributes
- Placement based on department number
- All birthrights for dept. are granted upon creation.

# Enterprise Directory (cont.)

- Pass-through for Email attributes
- Placement based on department number
- All birthrights for dept. are granted upon creation.
- Accounts Automatically Deprovisioned:
  - moved to “Inactive” context
  - Expiration date set to 1 yr.
  - Group Memberships are stripped

# Enterprise Email

- Accounts created upon hire/acceptance
- Accounts expired upon termination/graduation
- Name change automatically generate alias for original name.

# Others

- Dental school Mgt. System (Axium)
  - Oracle DB user table
  - Password sync to staging table (encryption trigger)
- Enterprise portal (Oracle portal)
  - Oracle Internet Directory
- Remedy Helpdesk Request System
- Connect Ed (emergency notification system)
  - Text based export of Identity information changes
  - Perl script transfers delimited txt file to Vendor nightly

# Building

- Lab Environment
- Identity Vault & Drivers
- Test Plan

# Building: Lab Environment

- Utilized existing development or test environments for connected systems
- Virtual hardware
- Exported production directory schema and objects with LDIF utilities

# Building: Identity Vault & Drivers

- Vault
  - Flat tree with schema extended to accommodate all attributes
- Drivers
  - Driver teams – one connected system expert & one IDM system expert
    - IDM expert was responsible for driver logic (rules, policies, mappings, etc.)
    - Connected system expert was responsible for the system API (component interface, staging table, DB triggers, etc.)
  - Constant communication with and feed back from the business unit contacts
  - Remotely loaded driver shims for performance

# Building: Test Plan

- Unit Testing
- End to end testing
- Business Unit Sign off

# Implementation

- Started with Pilot
  - Automated an existing manual process
  - Unidirectional flow of Identity data
  - Relatively few access controls to provision
- Migrated drivers
- Normalized Data in vault and systems
- Documented changes in business process
- Activated drivers individually

# Lessons Learned

- Business unit impact on other systems
  - Changes in process must be communicated
  - Data in authoritative sources affects much more than the dept. where data is entered
- Do not under estimate the complexities of the API's.
- XSLT stylesheet, XPATH and regular expression is extremely helpful
- Avoid using object name as key field for association

# Lessons Learned (cont.)

- Become very familiar with the **entire** account management life cycle for each connected system (provisioning is only the beginning)
- Make sure your business units completely understand the overall affect of the IDM system.
  - Don't be surprised to find areas that are dependent on the delays caused by manual processing
- Be careful with your time formats
- Utilize auxiliary classes in eDirectory for added attributes when possible

# What's in the Future?

- We will continue to integrate existing and new systems
- Role-based provisioning
- Entitlements
- Workflow
- Access Management
- Federated Identity

# Contact Info

- Ron Long
  - [flong@mcg.edu](mailto:flong@mcg.edu)
  - 706-721-1068
- Morgan Whaley
  - [mwhaley@mcg.edu](mailto:mwhaley@mcg.edu)
  - 706-721-7291