Banner Enterprise Identity Services
Overview
Introduction

• Ted Schmidt
• Technology Strategist
• I have been using Oracle for 25+ years
• Ted.Schmidt@usg.edu
• http://www.usg.edu/information_technology_services/
What is Identity and Access Management?

• Identity Management
  – Identity management is a discipline which encompasses all of the tasks required to create, manage, and delete user identities in an electronic environment.

• Access Management
  – Ensures that the right services are available to the right people.

• Identity Access Management or (IAM)
Business and Identity

• Identification is the focal point of most business transaction.
• Most services are not available based on anonymous access.
• Service delivery necessitates a certain level of knowledge about the recipients.
• Identity matters!
So What is IAM - Really?

• Identity and Access Management
• Application Services Framework that will:
  – Improve Security
  – Reduce Cost
  – Enable new opportunities

• Via a common Framework for:
  – Provisioning
  – Deprovisioning
  – Authentication
  – Authorization
IAM Strategies and Challenges

• Complexity
  – Authoritative Identity Source(s)
• Cost
  – Development
  – Maintenance
Goals and Objectives

- Work from your prioritized drivers.
  - Re-state your challenges as opportunities for improvement.
- Know what success looks like before you begin.
  - Goals
    • Describe the desired outcomes and outputs by phase.
  - Scope
    • Describes the limits placed on phases.
  - Services
    • Describes the services that will be delivered by phase.
  - Timing
    • Describes the timelines associated with the implementation of phase.
  - Activities
    • Describes the activities that will be undertaken to implement the phase.
  - Infrastructure
    • Describes the newly introduced and retired components relative to the phase.
Banner Identity Management Goals

• Allow Ellucian Applications to work with 3rd Party Enterprise Identity Management Systems.
• Adopt a single/unified Campus Identity definition.
• Support user provisioning to Ellucian applications.
• Support user provisioning from Banner.
• Support user provisioning to Banner.
• Standards based authentication support.
• Support SSO protocols.
Banner Enterprise Identity Services (BEIS)

• Standards based architecture
  – LDAP
  – CAS
  – SPML

• Allow Banner to participate in an Enterprise Identity Managed environment.
  – Identity Producer
  – Identity Consumer
Banner Enterprise Identity Services

• IAM Services supported via BEIS:
  – Automated Services
    • Provisioning
    • Deprovisioning
    • Service Provisioning Markup Language (SPML)
  – Identity Data Export Utility
    • Batch interface for Identity Data Processing
  – Single Sign On
    • Central Authentication Service (CAS) for BANNER Internet Native BANNER (INB) and Self-Service BANNER (SSB) applications
Banner Enterprise Identity Services - Provisioning

• Service Provisioning Markup Language – SPML 2.0

• Outbound Provisioning
  – Banner is the Authoritative Source of Identity.
  – Target Systems Identity lifecycle management.

• Inbound Provisioning
  – Banner is Non-Authoritative for Identity.

• Can I do both Inbound and Outbound?
  – Yes!
Identity Provisioning with Enterprise IdM - with Banner Authoritative

Luminis

Create User

Banner Identity XML

Banner

Identity Gateway

Identity Topic

Identity Proxy

SPML 2.0

UDC Identity XML

UDC Identity XML in SPML

Identity Proxy

Identity Store

Rules

Provision User

Provisioning

Vendor Enterprise Identity Manager

Provision User

UDC Identity XML in SPML

Provisioning
Identity Provisioning with Enterprise IdM - Banner as Consumer

- Banner as Consumer
- Banner
- Luminis
- Create User
- Banner Identity Gateway
- UDC Identity XML in SPML
- Provision User
- Identity Store
- Provisioning Rules
- Provision User
- Provision User
- UDC Identity XML in SPML
- Vendor Enterprise Identity Manager
- Other Authoritative Source
- Workflow
BEIS Components

Batch Utilities
- Identity Data Export Utilities (IDEU)

Provisioning Components
- Banner Identity Gateway (BNIG)
- Identity Proxy Services (IdProxy)
- SPML LDAP Adapter

Single Sign-on Components
- CAS validation service
- SSO Manager

WebLogic 11g Basic Domain

Oracle Database
Identity Data Export Utilities

- UDC Identifier Assigner – generates GUIDs for all living persons in the Banner database.
- UDCIdentity Extractor – creates a UDCIdentityList structure.
- LDIF Generator – generates an LDIF files from a UDCIdentityList XML document.
- SPML Publisher – publishes SPML messages from a UDCIdentityList XML document.
- File Operations – download and delete files created by IDEU.
BEIS Components (batch utility runtime)
Banner Identity Gateway

Transforms Banner Identity XML messages to UDCIdentity XML messages.

- It is both a Consumer and a Producer.
  - Consumes Banner Identity XML messages from the Banner Identity Topic.
  - Publishes UDCIdentity XML messages to the UDC Identity Topic.
- Deployed to the Weblogic Server.
- Provides a host of functional and administrative services.
  - i.e. A GUID service for the creation of globally-unique identifiers.
- Administrative management console.
- For Inbound Configuration Scenarios
  - Banner Identity Gateway serves SPML Provisioning Service Target (PST) for inbound provisioning.
  - Banner Identity Proxy Service bypassed.
Banner Identity Proxy Service

Consumes UDCIdentity XML messages from the UDC Identity Topic.

- As the RA will POST SPML messages to defined PSPs
  - SPML Request Authority (RA) – Registered agent for creation of well form SPML provisioning Request.
  - Provisioning Service Provider (PSP) – Service which satisfies provisioning service request from an RA (consumes SPML message).
  - Provisioning Service Targets (PST) – Actual end points for the identity data.
Support three ways to allow applications to authenticate users.

- **Local Native Authentication**
  - We continue to support the current authentication methods for SSB and INB.

- **LDAP Authentication**
  - Applications can authenticate with a configured LDAP directory server.
  - Allows a common login identifier and credential to be shared by all applications.

- **Token-based Authentication**
  - Applications support a pre-authenticated token used to establish user identity.
  - Supports Identity Management controlled environments and provides support for SSO protocols (CAS).
Single Sign On

1. **Web Browser**
   - User goes to access Digital Campus Applications through a browser.

2. If no SSO Token, Web Gate will redirect browser to Auth Server.

3. **Digital Campus Application Web Tier**
   - **Web Gate**
     - SSOManager
     - Provides http token with UDC ID
   - **Banner**
     - Self Service (or Workflow, Luminis, etc...)

**Authentication Server**
- Sun, Oracle, Novell, CAS / Other Web ISO...
BANNER Configuration

- **GUBUMAP**
  - Maps entity PIDM to UDC_ID

- **GOBTPAC**
  - Trigger to generate BEIS event
  - External User by default maps to LDAP login
  - PIN can be extracted to default LDAP password

- **GOBEACC**
  - Maps entity PIDM to Oracle login
  - Required for INB and BANNER XE Administrative that use Oracle login access controls
BANNER Configuration

• Possible New Administrative Tasks
  – Create BANNER entity accounts for all INB and BANNER XE administrative accounts
    • All Oracle BANNER application users must be mapped in GOBEACC
  – Map BANNER Entity to Oracle Login
    • (see above)
LDAP Configuration

- **GUBUMAP**
  - CAS asserted UDC ID must be populated in this table

- **GOBEACC**
  - BEIS SSO Manager and Adm9inistrative XE applications must be able to look Oracle login via the entity PIDM from this table
Questions