Cal State University System
Identity Management in Education

July 20, 2006

dsimmons@burtongroup.com
www.burtongroup.com
Introduction

Overall Project Scope

• Develop an identity management architecture and migration strategy for CSU

• Architecture must provide flexibility to interface with multiple campuses and meet external facing requirements

Project Objectives

• Improve or enhance network, application, system and facilities security through a consistent set of identity life-cycle management and policy enforcement functions

• Improve the end-user experience through reduced sign-on capabilities, requiring fewer identities and passwords to remember to access systems throughout the infrastructure
Introduction

Project Objectives (cont.)

- Implement uniform authorization support policies to protect CSU information assets
- Enable more thorough and accurate audit capabilities of authorization rights to CSU information assets
- Enhance regulation compliance capabilities (FERPA, SB 1386, GLBA, HIPAA, and others)
- Streamline system user registration and identity life-cycle management processes by enabling self-update and delegated administration of specific identity data
Introduction

Presentation Objective: Describe the strategic context of Identity Management (IdM) in Higher Education and ‘beyond’

Agenda

• Discuss the business value of an IdM infrastructure
• Describe the core components of an IdM infrastructure
• Identify key best practices
What is identity management?

- A set of processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities
  - Involves both technology and process
  - Involves managing unique IDs, attributes, credentials, entitlements
  - Must enable organizations to create manageable life cycles
  - Must scale from internally facing systems to externally facing applications and processes

- The main objective: a general-purpose infrastructure utilizing authoritative identity data sources, with clean integration across people, process, and technology
Overview: The Business Value of IdM

Why is identity management important?

200,000 Ameritrade Client Files Lost
Tapes intercepted containing information on Ameritrade Clients
- Associated Press 4/20/05

Information was for people nationwide who may have been Ameritrade customers from 2000-2003. The data was different for each client and may have included their Social Security numbers, among other information

DSW Data Theft Much Larger Than Estimated
Database hacked containing 1.4 million credit card numbers and the names
- Associated Press 4/19/05

Thieves who accessed a DSW Shoe Warehouse database obtained 1.4 million credit card numbers and the names on those accounts—10 times more than investigators estimated… Besides the credit card numbers, the thieves obtained driver's license numbers and checking account numbers from 96,000 transactions involving checks….
52 million identities were stolen in 2005 according to the Privacy Rights Clearinghouse

This Year, there’s HP, U.S. Veterans’ Administration, and on and on

{Insert headline and CSU’s name here????}

Associated Press {future date}

Let’s hope not? Let’s plan!
Overview: The Business Value of IdM

Identity management isn’t just about technology

• It’s about reputation
• It’s about risk assessment
• It’s about legal responsibility
• It’s about protecting sensitive data
• It’s about dealing with outside organizations
• It’s about streamlining user lifecycle management
• It’s about audit reporting and regulation compliance
• It’s about business processes
Overview: The Business Value of IdM

Purpose of IdM

• We need to meet, exchange information, ideas, etc.
  • But we need to do so in spaces that are restrictive
  • Private domains, networks and systems

• From an IT perspective, we need to create online spaces that allow for collaboration
  • Taking into account security, privacy, affordability, and usability

Real space becomes virtual space
Overview: The Business Value of IdM

Why IdM? To improve confidence in virtual spaces

- IdM technology can improve security by
  - Restricting entry
  - Controlling access to resources
- Tool for achieving compliance with regulations
  - Establishing accountability
  - Respecting privacy
- IdM standards lay a foundation for trust
  - Promotes reusability of identity across multiple online spaces
- Increases usability
  - Accelerates discovery of services, personalizes services
- Lowers the cost of delivering online services
Overview: The Business Value of IdM

Privacy and regulatory laws are requiring more security and privacy

- **FERPA (Family Educational Rights Privacy Act)**
  - Protect student/family records while making them readily available to the institutions that need them

- **HIPAA (Health Information Portability & Accountability Act)**
  - Protect patient health care records while making them readily available to the institutions that need them

- **Sarbanes-Oxley**
  - Protect investors by improving the accuracy and reliability of corporate disclosures - audit

- **Gramm-Leach-Bliley Act**
  - Protect access to sensitive ‘customer’ financial information

- **CA SB 1386**
  - Notification of private information breach

- **U.S. Patriot Act**

- **Digital signature legislation**
  - U.S. “E-Sign” legislature
  - E.U. electronically signed contracts December 2002

- **Real ID**
Overview: The Business Value of IdM

Justifications can be broken down into five overarching areas

1. Improved user experience
2. Cost savings
3. Security: Lifecycle identity administration
   - Audience: IT administrative, HR, Registrar
4. Security: Policy enforcement
   - Audience: Resource owners
5. Competitive advantage
Overview: The Business Value of IdM

Justification 1: “Improving end-user experience” provides

- Reduced Sign On (sometimes called “single sign on”)
- Improved quality of experience (QoE) for user communities
- Federation with other institutions, research partners, library systems, document archives and others
- Simplified, personalized access
- Automated password reset and other user grantable services
Overview: The Business Value of IdM

Justification 2: “cost savings” provide

• Hard dollar savings
  • Help desk password resets easily measured (specific number?)
  • Duplicate administration responsibilities
  • Eliminating redundant software and solutions
  • Canceling cell phone, other paid services after employee termination

• Soft dollar savings
  • User productivity
    • Training to use duplicate facilities
    • 15 minutes per user per day used for authentication
    • Bad addresses in directories waste time finding phone numbers, e-mail addresses
  • “Hidden administrative” costs
    • Many directories means many administrators usually taking time out of their real job
Overview: The Business Value of IdM

Justification 3: “Security – Life cycle identity management” provides

- Elimination of the potential for errors, omissions and redundancies in identity data across systems
- Accuracy and completeness of identity information
- Better management of identity lifecycle
- Dissemination of assets, services and accounts
- The right resources to the right people at the right time
- Connect ID access with application access
Overview: The Business Value of IdM

Justification 4: “Security – Policy enforcement” provides

- Response to heightened government oversight and regulations
- Logging and audit capabilities of University information assets and resources
- Minimization of security risks associated with dormant or orphaned accounts
- Cost avoidance in security administration
- More secure access to sensitive resources and applications both internal and external to the organization
- Centralized authorization framework across multiple applications
Overview: The Business Value of IdM

Justification 5: “competitive advantage” provides

- Framework for rapid deployment of internal and external applications
- Standards to minimize administrative overhead
- Reduction and consolidation of existing resources and personnel
- Support and protection of intellectual property
- Flexible infrastructure promoting quicker time to market for ‘service’ changes and enhancements
Overview: The Business Value of IdM

In summary, IdM enables many important functions

IdM Process
Portal/Personalization
Simplified Sign-On
Web SSO
Application Authorization
Audit
Others

IdM Infrastructure Technologies

And it requires architecture for long-term planning, deployment
Overview: The Business Value of IdM

IdM: a point of coordination for information
Overview: The Business Value of IdM

The challenge

- Today’s identity management systems are ad hocracies, built one application or system at a time
  - Apps, databases, OSes lack a scalable, holistic means of managing identity, credentials, policy across boundaries
  - Fragmented identity infrastructure: Overlapping repositories, inconsistent policy frameworks, process discontinuities
  - Error prone, creates security loopholes, expensive to manage
  - Cumbersome to cross security boundaries

- Infrastructure requirements: extend reach and range
  - Increased scalability, lower costs
  - Balance of centralized and distributed management
  - Infrastructure must become more general-purpose and re-usable
Identity Management 101
The ‘typical’ IdM infrastructure - a set of complementary, converging technologies:

- Identity data and directory services
- Provisioning services
- Identity policy and administration services
- Authentication services
- Authorization & access management services
- Federation services

…and the policies and processes that support them!
Roadmap of IdM Terms & Tech

Putting it together – Burton Group Reference Architecture Template for IdM

- **Subjects (Users, services)**
- **Subjects (Users, services)**
- **Access Policy Enforcement Infrastructure**
  - Proxy / Agent
  - Authorization service
  - Firewall
  - Other
  - Objects (Applications, services, resources)
  - Provisioning Services
  - Identity & Policy Admin
    - Delegated admin, self-service

- **Management and Audit**
- **Federation**
- **Identity Data Services**
- **Directory**
  - Proxy
  - Replication
  - Virtualization
  - Synchronization
  - Accounts, roles, groups
Core IdM components: Identity data & directory services

- The focus for the past several years has been a directory-enabled identity management infrastructure
- Authoritative identity repository
  - Contains people, organizational units, groups, roles, etc.
- Foundation for identity management
  - Authentication based on identity in directory
  - Authorization based on user attributes (roles, groups)
  - Personalization based on user attributes
- Virtual and meta-directories integrate disparate identity repositories
  - Meta = persistent synchronization; Virtual = non-persistent
- LDAP servers are commodities
Directory Services Support the IdM infrastructure

Authentication

Directory Services

Provisioning & User ID Management

Access Management, Authorization
Identity data services

Directory Services Concepts & Capabilities

Subjects (Users, services) → Access Gateway → Access Policy Enforcement Infrastructure
- Proxy / Agent
- Authorization service
- Firewall
- Other

Objects (Applications, services, resources) → Provisioning Services
- Identity & Policy Admin
- Delegated admin, self-service

Management and Audit

Federation
Identity Data Services
Directory
Virtualization
Proxy
Replication
Synchronization
Accounts, roles, groups
Core IdM components: Provisioning services

- Identity admin functions that span products and services
  - Creation, propagation, maintenance of user accounts, rights
  - Categorize users by roles, groups, for efficiency, accuracy
- Provisioning systems support workflows that automate process, reduce admin costs, enhance security
  - Create, modify, terminate users across multiple apps
  - Centralized admin: push roles, groups, policy
  - Centralized password management, reset/sync
  - Centralized, rapid termination of accounts
- Audit and compliance
  - Who has access to what?, who granted access?, for how long?, etc.
Provisioning Template

Source: Burton Group Reference Architecture
Provisioning Concepts and Capabilities

Identity management framework

- Subjects (Users, services)
- Authentication and reduced sign-on
- Access Gateway
- Access Policy Enforcement Infrastructure
  - Proxy / Agent
  - Authorization Service
  - Firewall
  - Other
- Objects (Applications, services, resources)
- Provisioning Services
- Identity & Policy Admin (Delegated admin, self-service)
- Federation
- Identity Data Services
- Directory
- Proxy
- Replication
- Virtualization
- Synchronization
- Accounts, roles, groups

Management and Audit
Core IdM components: Identity policy and administration

- Delegated admin tools distribute workload (and liability)
  - Assign subset authority to a designated user or group
  - Moves responsibility to campus, department, research partner or other constituent

- Self-service increases satisfaction, data integrity
  - Users can modify info
  - Self-service password reset a high priority for many companies
  - Self-service registration, subscription services can kick off workflow and provisioning process to speed revenue generation

- Often provided today as a subset of the provisioning services component
Provisioning Architectural Overview

Administrative Interfaces Template

<table>
<thead>
<tr>
<th>Users</th>
<th>IT administration</th>
<th>Identity data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Centralized admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delegated admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PKI admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automated admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Self-service admin</td>
<td></td>
</tr>
</tbody>
</table>

- Federated identity environments
- Internal identity environment
  - Identity and policy administration
    - User interface
    - Web services interface
    - Workflow
    - Audit
- Identity data services
  - Proxy
  - Virtualization
  - Synchronization
  - Directory
Provisioning Concepts and Capabilities

Identity management framework

- Subjects (Users, services)
- Internal Business Units
- Federated domains
- Public Identity Services
- Affiliate Enterprises

Access Policy Enforcement Infrastructure
- Proxy / Agent
- Authorization Service
- Firewall
- Other

Objects (Applications, services, resources)

Provisioning Services

Identity & Policy Admin
- Delegated admin, self-service

Authentication and reduced sign-on

Management and Audit

- Federation
- Identity Data Services
- Directory
- Proxy
- Replication
- Virtualization
- Synchronization
- Accounts, roles, groups
Core IdM components: Authentication

• Principal provides sufficient credentials to satisfy challenge, gaining access to a service, application, or system

• Variety of authentication mechanisms
  • Strength necessary depends on the needs of the application
  • User name/password, personal identification numbers (PINs)
  • One-time password tokens (SecurID), digital certificates (PKI)
  • Biometrics (finger print scans, retinal scans)

• User name/password most common, will remain so until the cost and complexity of stronger authentication subsides
Core IdM components: Authorization and access management

- Determining rights, privileges using policy-based systems
- Web-based access management products combine authentication, authorization => Single Sign On (SSO)
  - Use roles-, group-, rules- based systems for scalability
  - Integrate with applications/application servers
  - Identify objects by URL, operate at page, button, field level
  - Integrate with identity repositories: directory, database
  - Support multiple authentication systems
  - Include user management functions
  - Dynamic enforcement w/variables (location, time)
- Session management after authentication
Authentication and Authorization Mechanisms

Identity management framework

- Subjects (Users, services)
- Internal Business Units
- Federated domains
- Public Identity Services
- Affiliate Enterprises

- Access Gateway
- Access Policy Enforcement Infrastructure
  - Proxy / Agent
  - Authorization service
  - Firewall
  - Other

- Objects (Applications, services, resources)

- Provisioning Services

- Identity & Policy Admin
  - Delegated admin, self-service

- Management and Audit

- Federation
- Proxy
- Virtualization

- Identity Data Services
- Directory
- Replication
- Synchronization

- Accounts, roles, groups
Authentication and Authorization Mechanisms

Single Sign On: Web access management systems
Physical and Logical Integration

Common authenticator

- Web Server
- Client/Server Application
- eSSO
- JAVA Card Apps
- Windows
- Client Authenticated SSL
- Digital Signature
- PKI
- ePurse
- Facility Access
- OTP or PKI
- Contactless
- NOS Authentication
- eSSO
- PKI
- Digital Signature With Workflow

VPN
Role Based Access Control (RBAC) basic element relationships

- Users are assigned to roles
- Resources have associated permissions
- Permissions are granted to roles for resources
- Roles provide abstraction, which results in efficiency, flexibility, scalability
Why Role-Based Access Control (RBAC)?

- Administration is easier, faster, more effective
  - Less work – making administrator and user more productive
    - Users + permissions, instead of users x permissions
  - Add and remove roles without modifying access
  - Requires less skilled day-to-day administration
  - User administrator doesn’t need to know details of business process
  - Fewer assignments yield fewer errors
  - Persistence of roles reduces permission changes

- Simplification reduces cost
  - Enables automation, which reuses other work
  - Lower training and operational costs

- Scales with growth
Role Based Access Control

Brief history

• First standard model not proposed until 2000
  • National Institute of Standards and Technology (NIST) model
    • Components include
      • Core
      • Hierarchical
      • Static separation of duty
      • Dynamic separation of duty
    • Provides good reference; not used by [many] vendors
    • Approved by ANSI in February 2004

• RBAC implementations today focus on single domains
  • Database management systems, network operating systems, enterprise resource planning
  • Role implementation defined by technology resource owner
Core IdM components: federation services

- Manage identity and access rights (entitlements) across domain boundaries
- Agreements, standards, technologies that make identity and entitlements portable across autonomous domains
  - Relying parties don’t need prior knowledge of complex system internals or pair-wise mappings between systems
- Eliminates/reduces cross-domain account management or synchronization
Federated IdM

The challenge: Managing Many Identities

Loosely or tightly-coupled, Integrated or federated interior systems

Loosely-coupled, Federated exterior systems

Internal Systems & Data

Extranets

Students, Faculty, Staff

Partner or xSP

Other Institutions

Less-known

Unknown
**Federated identity**: Agreements, standards, and technologies that make identity and entitlements portable across autonomous domains

**Identity provider (IDP) domain**: Domain that generates authentication assertions or other assertions that vouch for a subject's identity

**Service provider (SP) domain**: A domain that relies on assertions from an IDP to authenticate or authorize subjects' actions on its resources

**Definitions**

**Scenarios**

- Federated identity: Agreements, standards, and technologies that make identity and entitlements portable across autonomous domains
- Identity provider (IDP) domain: Domain that generates authentication assertions or other assertions that vouch for a subject's identity
- Service provider (SP) domain: A domain that relies on assertions from an IDP to authenticate or authorize subjects' actions on its resources
Federated IdM

Shibboleth – Internet2/MACE

• Architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls.

• Policy framework that will allow inter-operation within the higher education community.

• Key concepts within Shibboleth include:

  • Federated Administration. The origin campus (home to the browser user) provides attribute assertions about that user to the target site. A trust fabric exists between campuses, allowing each site to identify the other speaker, and assign a trust level. Origin sites are responsible for authenticating their users, but can use any reliable means to do this.
Federated IdM

Shibboleth (cont.)

• Access Control Based On Attributes
  - Access control decisions are made using those assertions. The collection of assertions might include identity, but many situations will not require this (e.g., accessing a resource licensed for use by all active members of the campus community, accessing a resource available to students in a particular course).

• Active Management of Privacy
  - The origin site and the browser user control what information is released to the target. A typical default is merely "member of community". Individuals can manage attribute release via a web-based user interface. Users are no longer at the mercy of the target's privacy policy.

• Standards Based
  - Shibboleth uses SAML for the message and assertion formats and protocol bindings.
Federated IdM

Shibboleth (cont.)

• InCommon - a Framework for Multiple, Scaleable Trust and Policy Sets.
  • InCommon establishes a federation of higher education institutions, content providers, CBT’s, etc. who have agreed to a common set of policies. This moves the trust framework beyond bi-lateral agreements, while providing flexibility when different situations require different policy sets.
  • A Standard (yet extensible) AttributeValue Vocabulary. Shibboleth has defined a standard set of attributes; the first set is based on the `eduPerson` object class that includes widely-used person attributes in higher education.
eduPerson Object Class

**eduPersonAffiliation** - contains values that describe the person’s relationship to the institution, such as student, faculty, staff, alumni – strict values.

**eduPersonNickname** – contains the person’s self-selected personal nickname, such as ‘Bob’.

**eduPersonOrgDN** – contains the distinguished name (LDAP name) of the institution the person is a member of.

**eduPersonOrgUnitDN** – contains the distinguished name(s) of one or more departments or divisions the person is a member of.

**eduPersonPrimaryAffiliation** – defines what the person’s primary relationship is to the institution, in cases where an employee may also be a student, for example. In such a case, the primary affiliation may be ‘employee’, or vice versa depending on the specific circumstances.

**eduPersonPrincipalName** – contains the person’s ‘network name’, which in many cases may be the person’s email address.
**Federated IdM**

**eduPersonPrimaryOrgUnitDN** – contains the distinguished name of the person’s ‘home department’.

**eduPersonEntitlement** – this attribute contains a URI pointing to specific resources to which the person has rights or privileges assigned. This attribute definition is directly driven from the Shibboleth architecture as a means of maintaining lists of resources a person is entitled to access across federated sites.

**eduPersonScopedAffiliation** – defines a person’s affiliation within a specific security domain. This value will contain a domain on the right of an @ symbol, with an example being ‘faculty@ucsc.edu’.

- Internet2 also recommends the institution implement the X.521 person and organizationalPerson object classes, as well as the IETF inetOrgPerson object class (RFC 2798).

  There is also an eduOrg object class for describing organizations, departments, locations, etc. in a standard syntax.
Federated IdM

Shibboleth High Level Architecture

1. I want to access your protected resource
2. Where are you from?
3. Crimson College
4. Tell me if this person is a legitimate student
5. This person is a legitimate student
Federated IdM

Shibboleth Architecture
Federated IdM

Current Shibboleth Deployments

• NC State Physics Department
• UC Office of the President Employee Benefits Management
• JSTOR, EBSCO content to numerous universities
• WebCT on line courses to numerous universities
• Penn State and Napster
• And many, many more…the list is growing
The IdM process: managing the identity life cycle

- Extend reach and range
- Increase scalability, lower costs
- Balance centralized, distributed management via loose coupling
And Then There’s Audit

Beyond IT: IdM requires integrated infrastructure
Audit and Reporting

What auditors expect from IdM systems

- IdM Audit tools show systematic, repeatable management and monitoring
  - Management access approval
  - Excessive privilege
  - Segregation of duties
Roadmap of IdM Terms & Tech

IdM: a ‘top-down’ perspective

Identity-based company access

Advanced business infrastructure

Meta Directory services

Advanced business infrastructure

Identity management
Access/Authorization
Authentication
Resource provisioning

business process integration

business applications

Enabling technology network/basic network infrastructure (network, servers, routers, OS, transport services)

Basic business infrastructure

Data bases
LDAP directories
Messaging
PBX / CTI VoIP
Security /PKI
Management
Object services
Web services

Employees
Suppliers
Partners
Customers
Remote employees
Legal/public authorities

Employees
Suppliers
Partners
Customers
Remote employees
Legal/public authorities
The Identity Management Vendor Landscape
Overview of Vendors and Products

Market Trends

• Many of the technologies may come from different vendors
  • Overlap between products and approaches
  • Burden of full integration is ‘still’ on the customer

• Consolidation across these functional categories has already begun, and the market will drive further consolidation over the next year to 18 months
  • ‘Name’ vendors have succumbed to “platformania”
  • IBM, Sun, Oracle, BMC, Novell, CA, HP…

• But the need is clear and the market is driving solutions
  • Hence the focus on interoperability and federation
The Ever-Changing Vendor Landscape

Vendor consolidation: IdM feeding frenzy
Overview of Vendors and Products

Standards relevant to the IdM market

- Identity portability through federation standards
  - SAML, Liberty Alliance, WS-Federation
  - Reuse credentials and authentication events across virtual spaces

- Policy portability through languages and specifications
  - SPML, XACML, WS-Security
  - Enterprise rights management
  - RBAC

- Directory server independence
  - LDAP, DSML
## Overview of Vendors & Products

### How they stack up

- **Comparative features of IdM generalists**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BMC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidian</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Novell</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Protocom</td>
</tr>
<tr>
<td>Oracle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Siemens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sun</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Microsoft)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Component rating:**
- **Strong**
- **Average**
- **Afterthought**
## Overview of Vendors & Products

### IdM specialists with multi-function products and suites

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockade</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Courion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entrust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>Siemens Critical Path</td>
<td></td>
</tr>
<tr>
<td>MaXware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M-Tech</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radiant Logic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>Oracle (Thor)</td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Blue: Available
- Yellow: Not Available
- Grey: Not applicable
Overview of Vendors & Products

It’s not just about the products: other factors in vendor selection

• Longevity in the IdM market
  • Many of these companies have in the market for a decade

• Momentum
  • The forward kind is what you’re looking for

• Support, maintenance, and customer relations

• Strength of Systems Integrator

• Dedication to standards

• Inclination
  • Preferred vendor, philosophical alignment
Open Source Alternatives

“The best things in life are free...”

- Shibboleth
- OpenSAML
- OpenLDAP
- Pubcookie
- Common Authentication Service (CAS)
- Signet
Open Source Alternatives

OpenSAML

• OpenSAML 1.1 is a set of open source Java and C++ libraries that implement the SAML 1.0 and 1.1 specifications

• Shibboleth is deployed on top of OpenSAML services

http://www.opensaml.org
Open Source Alternatives

OpenLDAP

• Open source implementation of the Lightweight Directory Access Protocol, distributed with:
  • slapd - stand-alone LDAP daemon (server)
  • slurpd - stand-alone LDAP update replication daemon
  • libraries implementing the LDAP protocol
    • C and Java libraries
  • utilities, tools, and sample clients

http://www.openldap.org
Open Source Alternatives

Pubcookie – Web SSO

• Pubcookie consists of a standalone login server and modules for common web server platforms like Apache and Microsoft IIS

• Together, these components can turn existing authentication services (like Kerberos, LDAP, or NIS) into a solution for single sign-on authentication to websites throughout an institution

http://www.pubcookie.org/
Open Source Alternatives

Common Authentication Service (CAS)

• CAS is an authentication system originally created by Yale University to provide a trusted way for an application to authenticate a user
  • An open-source Java server component
  • A library of clients for Java, .Net, PHP, Perl, Apache, uPortal, and others
  • Integrates with uPortal, TikiWiki, and others

http://www.ja-sig.org/products/cas/index.html
Signet

• A centrally administered system that supports distributed privileges management

• Administrators and business analysts first model the privilege requirements, from the business practices of an organization to the simpler requirements of a single application or service, in a set of distinct rules

• Includes a Java-based program toolkit, and its user interface runs in a standard Servlet Container, such as Tomcat

http://middleware.internet2.edu/signet/
Some Best Practices
‘Best’ Practices

Things to Focus On:

• Planning and strategy
• Executive sponsorship
• Getting your data in order
• Ongoing system governance
• Interoperability vs. interchangeability
• Extending and customizing schema
• Politics and data ownership
• Data replication topology
• Access control policies
• Measuring and demonstrating success
• Don’t try to do too much, too soon
Best Practices

Business strategy and planning lead to success

• Understand the detailed requirements of affected business units
• Manage the project
  • Politics, expectations, involvement
  • Establish a project plan
  • Requires a strong leader
• Document the project
  • Build awareness throughout the enterprise
  • Comply with convention
  • Gain recognition and approval
  • Disseminate information
The Design and Deployment Process

Who MUST participate?

- Senior executives
- HR and Student Administration/Registrar
- College/school IT stakeholders
- Data and network security services
- Library services
- Learning Management Systems
- ‘Enterprise’ Architecture team(s)
- Application development
- Change control – governance group(s)
- Desktop services groups
  - Networks
  - Email, calendaring, web file share, ‘collaborative’ applications
Best Practices

Executive Sponsorship

• Financial capital
• Political capital
• Multi-departmental sponsorship:
  • Official Executive Committee
  • Security, Architecture, HR, CIO, Finance, Registrar…
Define the strategy

• What needs to be addressed?
  • Key business drivers
  • Any ‘low hanging fruit’?
  • May be the demand to satisfy audit requirements
  • How do these translate to technical and functional requirements?

• When does it need to be addressed?
  • What are the possible deployment phases?
  • What other identity management components are part of the strategy?

• How should it be addressed?
  • Key technical and functional requirements

• Who is responsible?
...
Establish Guiding Principles

Guiding principles facilitate the decision-making process throughout the project. For example:

- Infrastructure will be standards-based
- Only mature products will be used
- We prefer open source alternatives
- We prefer to work with Vendor X and its alliance partners
- Data in the directory must be used by more than one application
- A process must be defined to maintain data integrity…
Best Practices

Evaluate Requirements

- Identify and survey key stakeholders for business application requirements
- Determine application requirements for
  - Schema, authoritative sources of all data, data ownership
  - Access controls, authentication, federation
  - Performance, reliability, scalability
  - Accessibility
  - Manageability and support
- Identify the key business process requirements
Best Practices

Develop the Detailed Architecture

- Data sources, flows and mappings that make an identity ‘usable’ as an entitlement determinant
- Delegated administration
- Self-administration
- Account provisioning
- Business process flows
- Security controls to protect the data
- Federation
- Audit capabilities
- Establish governance policies
Best Practices

Use Outside Help

• Consultants, if chosen correctly, can help you avoid pitfalls through experience and knowledge of best practices. Help with:
  • Requirements gathering
  • Architecture planning
  • RFI/RFP, vendor selection

• Professional services are often invaluable and necessary for integrating the complex environment. Help with:
  • Build agents or connectors
  • Configure replication
  • Recommend appropriate hardware
  • Application integration and deployment
  • Training

• You should be able to reduce your dependency on both as the project matures
Politics and data ownership

• Political issues are often overlooked, but can kill the project
• Who owns the data?
• Are they a stakeholder in the project?
• Targeting the data you want, and getting buy-in before you start, will speed things up considerably
• Cross-organizational teams are good from this perspective
Politics and data ownership

- Determine what data you will need to establish access rights
- What state is the data in?
- What constants can you rely on?
  - IDs: Are they organizationally-unique?
  - IDs: Are they generated and applied consistently
  - Is the data accurate?
- Is HR or Student Records a suitable source? Don’t assume so
- Many identity projects become data-scrubbing operations
Defining the Schema - Get your data in order

- Garbage in = Garbage out
- Integrated identity infrastructures highlight the level of inconsistency in data administration
- Most of the effort in an IdM deployment is standardization of the data content and data modeling
- Expect to find bad data
- Good news – with an integrated IdM infrastructure it is easy to find the source
Best Practices

Sample attributes used for access rights, entitlements

- Role
  - student, faculty, employee, library patron, etc.
  - roles can be defined within each of the above
- Major
- Classes taught
- Job code
- Department
- Cost center
- Location, primary campus
- Grade level
- Alumni
- Donor
The Need for IdM governance

- Independent teams with little coordination
- Informal collaboration because of individual initiatives
- No authoritative owners
- Cross-organizational decisions are difficult to make
- Growing demand for more structured governance
- Regulatory demands driving strategic decisions
Best Practices

Governance - How to begin

• For a given initiative, there will be multiple influencers that represent the steering community for that initiative
• Individual initiatives will have priorities and objectives that don’t align directly to others
• The governance body should
  • Establish the organizational principles surrounding IdM
  • Rationalize common requirements and capabilities
  • Arbitrate the needs of different initiatives
  • Acknowledge and accommodate the current state
  • Establish the point of convergence
  • Foster and manage the migration
• Business initiative liaisons should align initiatives to governance recommendations
**Levels of Governance**

**Level 1 – Initial**
Few processes are defined, and success depends on individual effort, talent, and heroic effort.

**Level 2 – Repeatable**
The necessary process discipline is in place to repeat earlier successes on projects with similar applications.

**Level 3 – Defined**
The process for both management and engineering activities is documented, standardized, and integrated into an organization-wide process and used by all projects.

**Level 4 – Managed**
Both the process and end-products are quantitatively understood and controlled using detailed measures.

**Level 5 – Optimizing**
Continuous process improvement is enabled by quantitative feedback from the process and from testing innovative ideas and technologies.
Best Practices

Governance Process

Entitlement Classification → Analysis

Constituent Classification → Change Management

Data Classification → IdM Plan Development

Analysis → Strategy Identification

IdM Technology Architecture

Education

Metrics

Audit Point
More architecture issues:

- Replication topology
  - Multi master? Single master?
  - Server locations
  - Fail over strategy for read and write operations
  - Load balancing
  - Can affect costs and performance

- Access control policies
  - Enable delegated administrators to assist in granting access rights
  - Fine grained vs. coarse grained
  - Can CSU roles be established?
  - Give control up where it makes sense
  - Always log changes to access rights, entitlements
More architecture issues:

- Reporting
  - Events written to logs must be accessible to reporting systems
- Assess your audit requirements and determine the logging and reporting functionality needed
  - Log archiving
  - Reporting from archived logs
  - Factor in data storage capabilities
Conclusion

Setting expectations

• There isn’t a one-size-fits-all solution for IdM
• Solid business justification is there for most large organizations
• Plan carefully, but be flexible
  • Develop an *Identity Management Architecture and Migration Strategy*
  • Begin deployment, measure and demonstrate success
• Use the resulting infrastructure to gain a strategic competitive advantage
Let’s Go!

Open Discussion