Building a Distributed Access Management Infrastructure

CAMP: Denver, November 7, 2006

Session: A Look at Ourselves

Self-assessment questionnaire

Each entry below describes an aspect of distributed access management in three ways that that suggest a continuum from *basic* to *capable* to *advanced*, from *"just starting"* to *"battle scarred"* to *"been there, done that"*, from *clueless* to *clued-in* to *clue-full*, from *"I bought the book*" to *"I read the book"* to *"I wrote the book"*, from … well, you get the idea.

For each item, consider where your institution is today on a scale from 1 to 10. Observe that the 1 and 10 are sometimes extremes of the primitive past or dreams of a perfect future -- we expect everyone lives in the real world in between. Enter each score in the empty box to the right, subtotal each section, then compute your final total at the end.

Nota bene:

This is **not** a test. It's our first try at it, so relax and enjoy.

This is **not** a contest. Please, no wagering.

The scores? In the words of journalist Dan Eldon, "the journey is the destination". We'll do something fun with the scores.

1. Data Stewardship

Policies

Policies addressing data stewardship and custodianship either don't exist or don't provide a sound framework for making consistent access management decisions.	Policy addressing data stewardship and custodianship exists for core systems but not campuswide..	Policies addressing data stewardship and custodianship, access management decisions are in place covering both central systems, schools, departments, etc.

1	2	3	4	5	6	7	8	9	10	

Awareness

Awareness of data stewardship and custodianship issues is spotty.	Awareness of data steward and custodianship issues exists within central units responsible for the most sensitive data.	Awareness of policies governing access to services and information is high within all units across the institution.

1	2	3	4	5	6	7	8	9	10	

Commitment

Responsibility for centralized Identity Management services is scattered among different IT and business units.	Responsibility for most centralized Identity Management services is focused in one operational IT unit.	There is organizational commitment to overseeing IdM across the institution, e.g. an Identity Management program function with strong ties to the IT Security and Policy function or an Identity Management governance group with executive-level commitment.

1	2	3	4	5	6	7	8	9	10	

Results

We do the best we can interpreting source data to determine what a "student" is, who are regular employees, what constitute faculty. Other consumers of this data must make their own determinations.	Core affiliations are well understood enough to provide a common policy basis for privileges and service eligibility.	Strong, clearly articulated definitions from offices managing sources delineate regular students, faculty and staff, and variations as needed to implement policies.

1	2	3	4	5	6	7	8	9	10		

2. People in our Identity Management system

Coverage

Our identity management covers just the core community – faculty, staff and students as defined by source systems.	Our identity management includes faculty, staff and students, plus secondary sources like library patrons, conference attendees, hospital staff, etc..	We capture information about all people of interest to IT, schools, departments, central offices, libraries, etc.

1	2	3	4	5	6	7	8	9	10	

Matching and Uniqueness

We get information from many sources; it's possible someone can be represented multiple times. This is difficult for us to detect except in reaction to service issues.	We have good central identity matching processes, but need to work to resolve identity issues mostly as needed.	We have strong partners and practices across campus and multiple systems that participate in detecting, avoiding and resolving identity issues.

1	2	3	4	5	6	7	8	9	10	

People who aren't people

We seem to have a lot of people at our school named Test, Testing, Test1, Test2, Training, Fake, Bogus and J.Doe.	Policy is in place for managing people properly and keeping the data clean, but practice still lags behind in areas.	Every "person" in our Identity Management system is a bona fide unique sentient human being, no exceptions.

1	2	3	4	5	6	7	8	9	10		

3. Other entities in our Identity Management system

Accounts with privileges

We manage people; access rights for non-personal accounts are handled locally and vary across systems.	We manage functional accounts and program access consistent with person accounts, but not through the same infrastructure facilities.	Non-person entities have their own strong, policy backed identity management and infrastructure support.

1	2	3	4	5	6	7	8	9	10	

Organizations

Our institution has many definitions of the organization's structure, depending on the history and needs of each system.	Organizational identity is pretty well understood and share enterprise names and identifiers, but organizational structure is still not well-understood.	There are one or more well-articulated organizational hierarchies that can be leveraged across systems for scoping access rights and defining chains of delegation.

1	2	3	4	5	6	7	8	9	10	

Enterprise reference data and definitions

Unfortunately we must deal with a variety of ways systems handles common data like phones, addresses, buildings and locations, etc.	We achieved a fairly high degree of uniformity of data of like type, through cooperation and multiple data mappings.	All descriptive data where applicable is governed by local, national and international standards and data definitions are shared across campus systems..

1	2	3	4	5	6	7	8	9	10	

Guests or weakly identified entities

We do not have a centrally supported guest login. This brings weakly identified people into our identity management system that are poorly tracked and managed over time.	We have policies to prevent the abuse of our identity infrastructure, and some infrastructure support for alternatives.	We have a centrally supported guest account infrastructure with policies that do not compromise core identity management.

1	2	3	4	5	6	7	8	9	10		

4. IT infrastructure

Identity Management Roadmap

Identity Management Roadmap? We don't need no Identity Management Roadmap.	An Identity Management roadmap is under development.	An Identity Management roadmap is in place and being actively maintained.

1	2	3	4	5	6	7	8	9	10	

Integration technologies

We gather information from sources with a mix of flat file transfer, reports, direct SQL access, even email.	We rely on batch processes but use consistent techniques with our clients and a common secured infrastructure.	We have realtime access to data, e.g., through LDAP, as well as an enterprise, message-based integration infrastructure.

1 2 3 4 5 6 7 8 9 10 ☐

How fresh is your data?

We periodically gather information from sources on cycles that can vary from daily, to weekly or longer.	We regularly gather information from sources, generally no less than daily.	We have realtime or near realtime connections to source and client systems that allow service and access changes to take effect in minutes -- on or off -- when data changes.

1 2 3 4 5 6 7 8 9 10 ☐

Cohesiveness of effort

We have little connection or control over changes in external systems, so we mostly react to changing business rules or data definitions about faculty, staff and students.	We have development, test and user-acceptance environments, but inconsistent source system involvement, and problems with authentication/SSO.	We have end-to-end test, development, and user-acceptance environments with all sources and consumers, and cooperative processes for planning change.

1 2 3 4 5 6 7 8 9 10 ☐ ☐

5. Data sharing and re-use

Support for contributed data

We rely on “official” data from central systems and have little additional descriptive data from other sources.	Our business systems provide some options for offices to extend identity information to enhance business processes.	We provide independent means, e.g., groups support, for units and users to extend identity information to enhance privilege control.

1 2 3 4 5 6 7 8 9 10 ☐

Breadth of campus focus

There is little connection between central IT support for core infrastructure and business systems, and distributed school or departments system. There means many independently maintained shadow systems with poor data sharing and little automated updates from common sources.	We can make data available, through reports or directory lookups to more directly enable local systems, but actual reuse is inconsistent across campus.	We support collaborative work in schools and departments by enabling them to define and share information and privileges on their own. It is easy to access common enterprise data, either for realtime reference or for ongoing synchronization.

1 2 3 4 5 6 7 8 9 10 ☐

Federated identities

We look forward to the day we can start to think about federated identities. Meanwhile we give out local login Ids to external colleagues as needed.	We have local solutions or work-in-progress to recognize and share services based on external sources of authorization.	Our infrastructure supports the ability for applications to respond to federated identities for both authentication and authorization as easily as they do for our people.

1 2 3 4 5 6 7 8 9 10 ☐ ☐

6. Enriching identity through Groups

Level of Groups investment

We currently do not have any "groups" management strategy or system beyond, perhaps, system-specific "roles" as defined by local application security.	We have groups and a model for distributed maintenance of membership, but limited integration with or leveraging of this information across the infrastructure.	We support groups at a high level, integrating institutional roles (e.g., faculty, student) with ad-hoc groups, easily leveraged across campuswide systems.

1 2 3 4 5 6 7 8 9 10

Managing groups

Group membership is maintained manually, ad-hoc groups only.	Automated processes update membership for a limited set of groups.	We have robust mechanisms for automated population of groups based on identity data of record.

1 2 3 4 5 6 7 8 9 10

Integration of groups with infrastructure services

Group membership is an attribute for a person to be leveraged by downstream systems for authorization as desired.	We are beginning to leverage groups internally to tie together infrastructure services like groups and lists. Groups can be referenced in .htaccess rules.	Group membership are fully leveraged across our IT infrastructure services, such as directory and file system ACLs, mailing lists, calendar groups, etc

1 2 3 4 5 6 7 8 9 10

7. Basic Access Management

Access rule consistency

IT staff may find themselves making access management decisions where business rules don't exist and no decision-making body exists.	Policies providing a framework for consistent access management decisions are in development or in place.	Business units base access management decisions on policies and the classification of the data being protected.

1 2 3 4 5 6 7 8 9 10

Leveraging roles and groups

We can barely get people to depend on the institutional roles available to them, which you'd think would be a no-brainer.	Or culture is ready to take advantage of roles, but practically speaking we are only leveraging institutional roles and definitions.	Groups, whether institutional, client contributed, or ad-hoc, are central to our campuswide access management strategy.

1 2 3 4 5 6 7 8 9 10

Who gets to say who gets to say?

We don't have firm policies or guidelines governing who can manage privileges or groups. People are enabled "as needed".	We have general workplace guidelines that designate who can manage privileges and groups controlling access to services.	We have policies that establish responsibilities and a chain of authority for group and privilege management.

1 2 3 4 5 6 7 8 9 10

8. Policy control through Privilege Management

Interfaces

Privileges are generally managed internally by individual service providers through a variety of online methods, including email or help ticket requests.	Departments and users have direct access to manage privileges, but across multiple systems in a variety of interfaces	Users have a common interface to manage privileges, for both assigning and review.

1	2	3	4	5	6	7	8	9	10	

System-centric vs function-centric

Privileges are managed on a system-by-system basis; associated privileges must be manually coordinated across services.	Some services have moved to more role-based authorization, accessing common identify data, e.g. through LDAP, to based authorization decisions on.	Privileges are managed according to a job or task, and entitlements based on policy. The details of how access is managed in individual systems is hidden from users.

1	2	3	4	5	6	7	8	9	10	

Leveraging policy and roles

Each new faculty or staff position must be incrementally enabled for privileges as needed. This can take days, weeks, or months to get it all set up.	Good processes are in place to identify and to facilitate the many steps in establishing privileges.	Privileges for new individuals can be quickly established based on role or transferred from the last holder of that position.

1	2	3	4	5	6	7	8	9	10	

9. Managing Access Management data

Provisioning and Lifecycle

Privileges need to be granted and revoked manually by the responsible managers or administrators. Too often we rely on one's login being turned off to cut off services.	Basic computing services – login, email, web – are automatically tied to affiliation and status, but other forms of authorization require manual control.	Privileges of all kinds – infrastructure services, business systems authority, resource access – are subject to common date and status controls for automated life-cycle management.

1	2	3	4	5	6	7	8	9	10	

Reporting, review

No good way to determine all the privileges a person has or all the holders of a certain privilege; this information is scattered across many systems and accessible only to the maintainers of those systems.	Processes are in place to answer questions about privileges and privilege holders to central offices and auditing.	Privilege information is available on demand to individuals in offices or departments who are responsible for managing them.

1	2	3	4	5	6	7	8	9	10	

Capturing the past

Answering the question "who had the ability to …" at any point in the past is extremely difficult.	Answering this question is possible but requires reconstruction of information from available logs, reports, etc., or is only available to a few as needed.	Accessing a historical perspective on privileges is not a problem, and is accessible to those who need it.

1	2	3	4	5	6	7	8	9	10	