

Identity and Access Management Services

Jon Giltner
(jon.giltner@colorado.edu)

Melinda Jones
(melinda.jones@colorado.edu)

It's a Portal World

General Goals of a Portal

1. Provide information and services tailored to individuals. Meaningful information is private and therefore must be secured.
 - Must know who the user is
 - Must have information about user attributes
 - Must get this information from trusted/authoritative source

It's a Portal World

2. Consolidate information and services by delivering them through a common interface – regardless of where they originate or who has authority over them.
 - Must integrate campus and central business systems
 - Must be able to securely access data and functions – proxy, pass-through or re-authN

But...

...many services stand independent of a portal.

Q: How do we support both a consolidated, “portalized” user experience AND service autonomy?

A: By pulling user management and access management out of specific applications and making them network services themselves.

Defining the Terms

Identity Management (IdM) : Assigning roles to people and assigning people to groups. Role and group information is stored in the campus enterprise directory.

As a **Delegated Service:** Allow individual departmental administrators to manage roles and groups for users that are relevant to their services.

Access Management: Assigning access policies to resources using roles, groups, or other directory information.

As a **Delegated Service:** Allow individual departmental administrators to create and manage access policies for their services.

IdM and Access Management at CU-Boulder

SelectAccess

<http://www.managementsoftware.hp.com/products/select/index.html>

- ✧ Delegated administration of roles and groups
- ✧ Web authentication using IdentiKey
- ✧ Access control to on-line resources based on directory information
- ✧ Delegated administration of access policies

A Simple Example: ITS Internal Web Site

- Password protected
- Site restricted to all ITS employees
- Some applications within site restricted further (e.g. Secure Lookup)

BUT...

- Bobby Schnabel wants access
- Not all ITS employees should see Secure Lookup
- Mike needs to manage site access; Lisa needs to manage Secure Lookup access

With SelectAccess

SELECT ACCESS

ITS WEB SITE

Access Coordinator: Mike Matthies

Access Rule: Department = ITS-Administration

+ Bobby Schnabel

SECURE LOOKUP

Access Coordinator: Looker-Upper Role

Members of Looker-Upper Role:

Lisa Deutchman: Access Rule

CUPD: Access Rule

With SelectAccess

- ✧ Managing access is separate from managing content
- ✧ Uses readily-available data in the Enterprise Directory
- ✧ No authentication or authorization needed inside Secure Lookup
- ✧ Access decisions delegated to responsible party
- ✧ ITS internal site easily incorporated into portal

Example: Webfiles

- Web-based file services for students
- Standalone commercial application (Xythos Web File System)
- To be available to all students, plus some faculty
- Primarily accessed through CUConnect

With SelectAccess

- ✧ User authenticates to the portal and credentials are valid to Webfiles application
- ✧ Simple access policy: allow primaryAffiliation=Student
- ✧ Easily managed exceptions: allow certain professors by name

Limitation: Can not base access policy on data that is not in the directory such as “Instructor of XYZ Course.”

Example: Leeds School of Business

- Online resources for Leeds faculty and staff
- Requires granular, role-based control over who has access to what resources
- Files include both in-house developed applications and 3rd party applications

With SelectAccess

- ✧ Authentication and detailed authorization based on user roles and/or groups
- ✧ Managing access policies and role/group assignments delegated to administrators in Leeds
- ✧ Access to in-house and 3rd party applications managed in one location

Example: Libraries and PWR 1150

- On-line instruction and testing for PWR 1150
- Standalone application developed by Libraries
- User-dependent features (faculty vs. student)
- Want to store student progress data in local database ...but do not want to store authentication and authorization data locally
- Both students and instructors need to be associated with an appropriate course section

With SelectAccess

- ✧ Authentication provided
- ✧ Role information provided for controlled access to features
- ✧ PWR or Libraries administrator will manage access policies and roles

Limitation: the student's or instructor's section number is not in the directory.

That data must be provided separately... by CUConnect.

Project Status and Timeline

- Creating development environment
 - SelectAccess v6.0beta
 - SunONE directory v5.2
 - 2 Solaris 9 boxes
- Identifying customer requirements
- Configuring SelectAccess for Kerberos
- Timeline...