UC San Diego IDM Project

Respondent

Gabriel Lawrence, Director IT Security and IDM Project Manager

Goal/Problem Space

Create a common infrastructure that allows the campus community to easily access the resources they need when they need them and to assure that access is appropriate and correct for their role in the community.

Features

Web SSO

- Self Registration
- Self service password reset
- Pluggable authentication stores

Access Management

- Central point to provision and deprovision access to all systems
- Automated workflow for access assignments
- Reporting and history tracking for audit purposes

Enterprise Roles

- Job/task based access
- Building blocks that can be combined to match the real world business situation
- Give people the right access at the start rather then when discovered

Technology Stack

- Java
- Echo2
- Shibboleth
- Active Directory
- RACF
- LDAP
- DB2
- J2EE

Identity Services

Please indicate which of the following identity services you consume, produce, or broker/convey.

- **Consume**: Your project uses the services described. For example, you use identification information to determine which person you are dealing with, and you are a client to an authentication interface to confirm the person's identity.
- **Produce**: Your project provides the services described. For example, you provide facilities to manage groups and can write them out to LDAP.
- **Broker/Convey**: Your project serves as a middleman, taking data from a producer and providing it to a consumer. For example, you verify authentication information and then generate a SAML assertion.

Managed Information	**Consume?**	**Produce?**	**Broker /Convey?**
Privileges	X	X	X
Roles		X	
Groups	X	X	X
Attributes		X	X
Identification	X	X	X
Defined Interfaces	**Consume?**	**Produce?**	**Broker /Convey?**
Authentication	X	X	
Attributes		X	X
Permissions		X	X
Provisioning		X	
Authorization		X	

Subjects	X	X	X
Other	**Consume?**	**Produce?**	**Broker /Convey?**

Standards and Interfaces

Shibboleth/SAML

Custom web services

Issues and Challenges

Dependance on third party technologies

Legacy systems/poor integration points for centralized IDM

Enterprise view vs isolated system/business process view

More Information