nmi-edit

Network Identity Management Concepts and Standards: The Key Role of Middleware

Keith Hazelton, University of Wisconsin IT Architect
Internet2 Middleware Architecture Committee for Education
hazelton@doit.wisc.edu

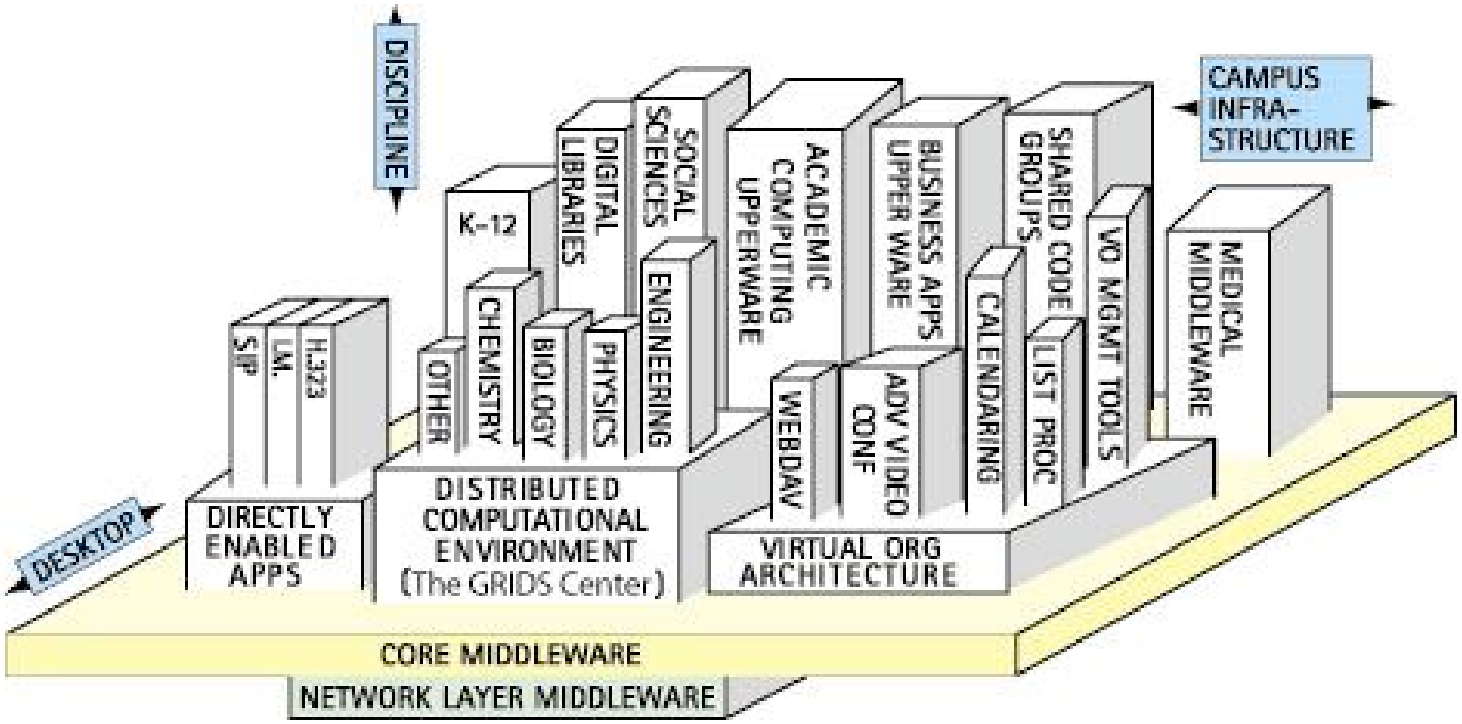
Please ask questions at any time!!!

Network Identity Management Concepts and Standards: The Key Role of Middleware

- Introductions
- Middleware: What and Why?
- Concepts and Architectures

Enterprise Middleware Definitions

Map of Middleware Land

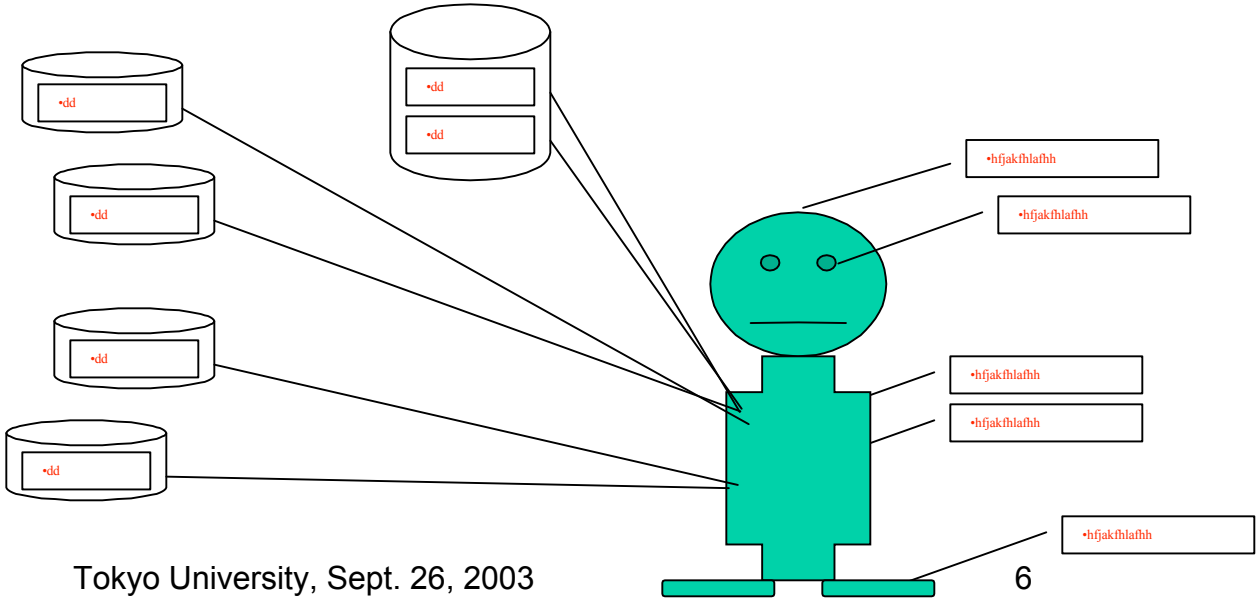


So what is Core Middleware?

- Suite of campus-wide security, access, and information services
  - Integrates data sources and manages information about people and their contact locations
  - Establishes electronic identity of users
  - Issues identity credentials
  - Uses administrative data and management tools to assign affiliation attributes
  - …and gives permission to use services based on those attributes

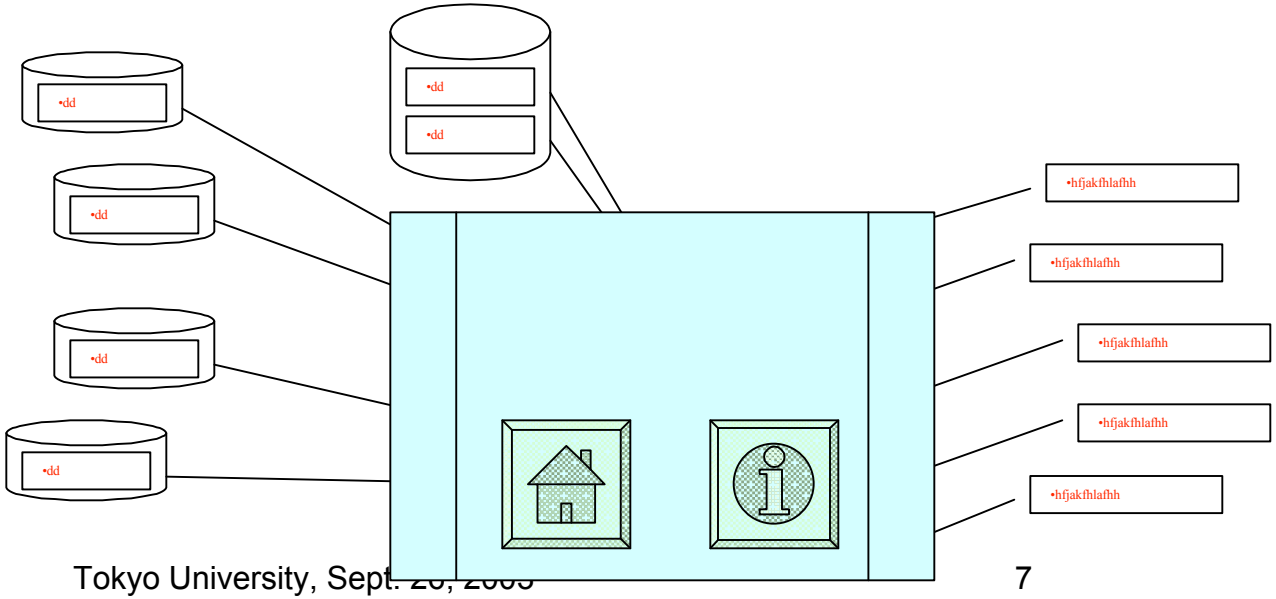
Some key terms

- Talk first about a person (you)
- **Attributes**: specific items of information about you or associated with you.
- **Identity**: the whole set of attributes about you



Some key terms

- Then remind you that these terms can apply as well to online resources, servers and services
- **Attributes**: specific items of information about **X** or associated with **X**.
- **Identity**: the whole set of attributes about **X**



Another key term

- **Identity credential**
  - Something issued to you (or to X) by an organization
  - It associates you with a specific identity known to the organization

More key terms

- **Authentication (AuthN)**
  - process of proving your identity by "presenting" an identity credential.
  - In IT systems, often done by a login process
- **Authorization (AuthZ)**
  - process of determining if policy permits a requested action to proceed
  - Often associated with an authenticated identity, *but not always and not necessarily*

Another key term: Identifiers

Identifiers– your electronic identification

- Multiple names and corresponding information in multiple places
- Single unique identifier for each authorized user
- Names and information in other systems can be cross-linked to it
  - Admin systems, library systems, building systems

Definition: Enterprise Directory Services

Enterprise Directory services - where your electronic identifiers are reconciled and your institutional identity is established and maintained

- Very quick lookup function
- Machine address, voice mail box, email box location, address, campus identifiers

Underlying Concepts & Architecture

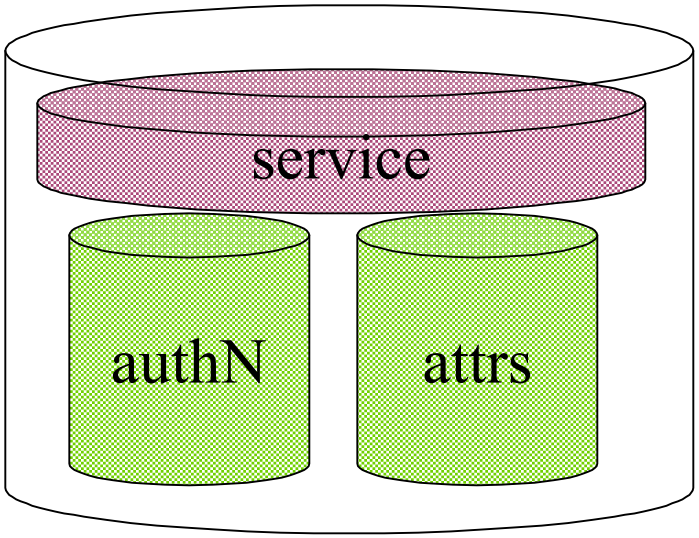
What IT needs to do

Determine who you are

Determine what resources you can use

Three service architectures: #1 Stovepipe (or Silo)

Service performs its own authentication. Consults own database for authorization and customization attributes (Traditional or legacy service architecture).



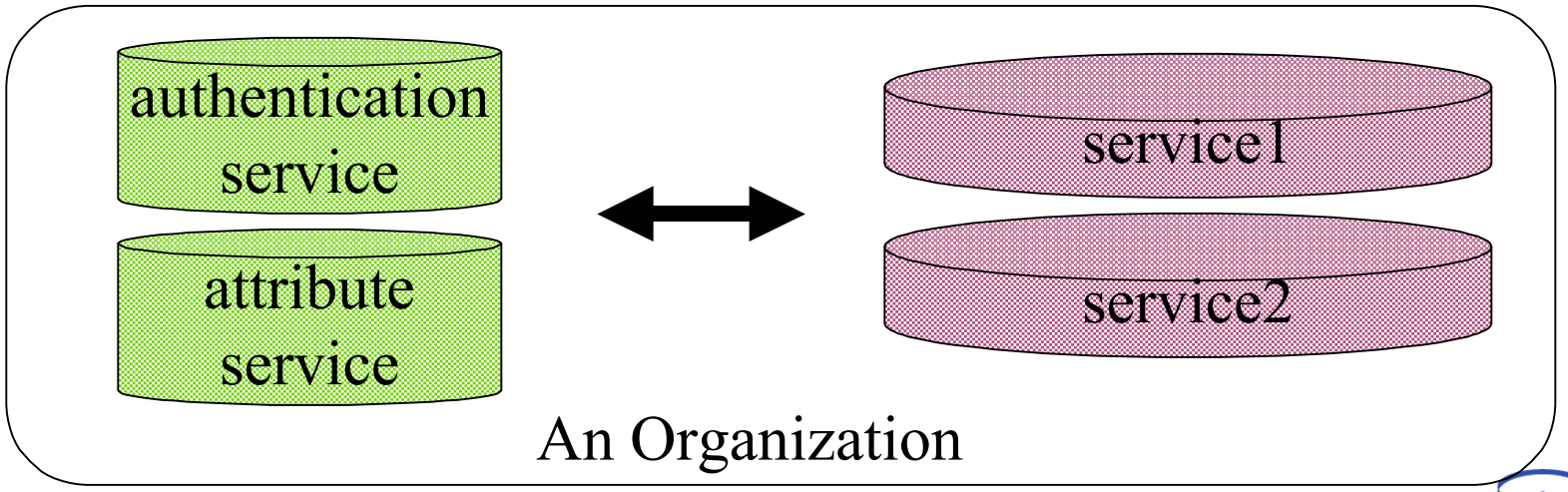
#1 Stovepipe (or Silo) Architecture Characteristics

Stovepipes authentication and attribute services are run by separate offices.

- Environment is more challenging to users, who may need to contact each office to arrange for service.
- No automated life cycle management of resources.
- Per-service identifiers and security practices make it more difficult to achieve a given level of security across the enterprise.

Three service architectures: #2 Integrated

Service refers authentication to and obtains attributes for authorization and customization from enterprise infrastructure services (modern service architecture).



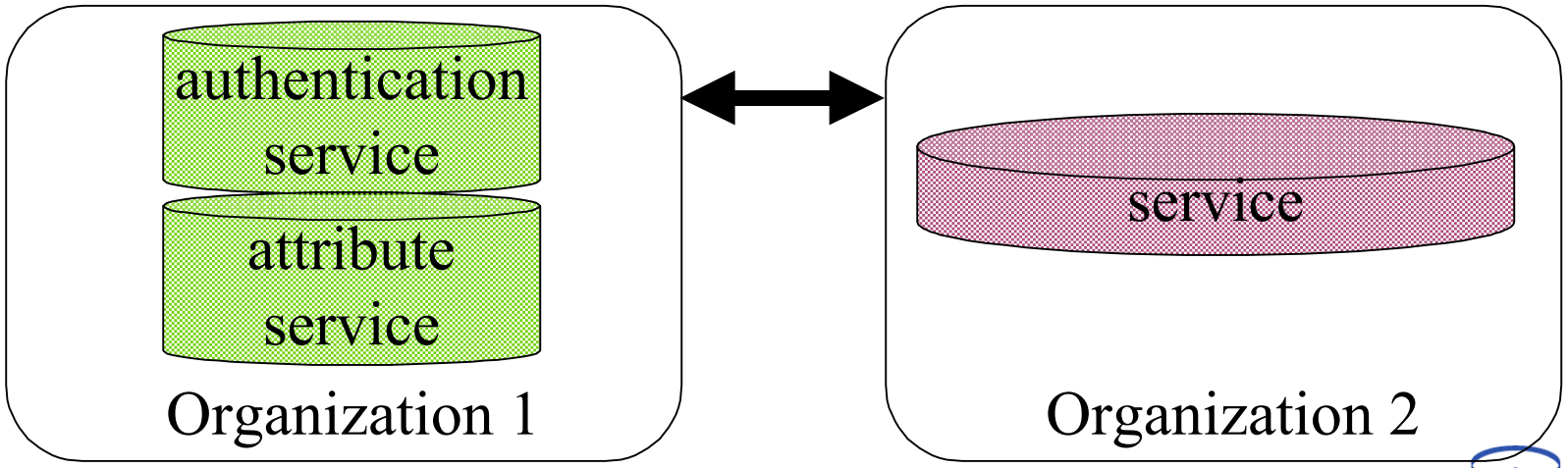
#2 Integrated Architecture Characteristics

Enterprise authentication and attribute services are run by a central office.

- All attributes known by the organization about a member can be integrated and made available to services.
- Automated life cycle resource management is possible across the enterprise.
- Common identifiers across integrated services make an easier and more secure user environment.

Three service architectures: #3 Federated

Service refers authentication to and obtains attributes for authorization and customization from possibly external infrastructure services (emerging service architecture).

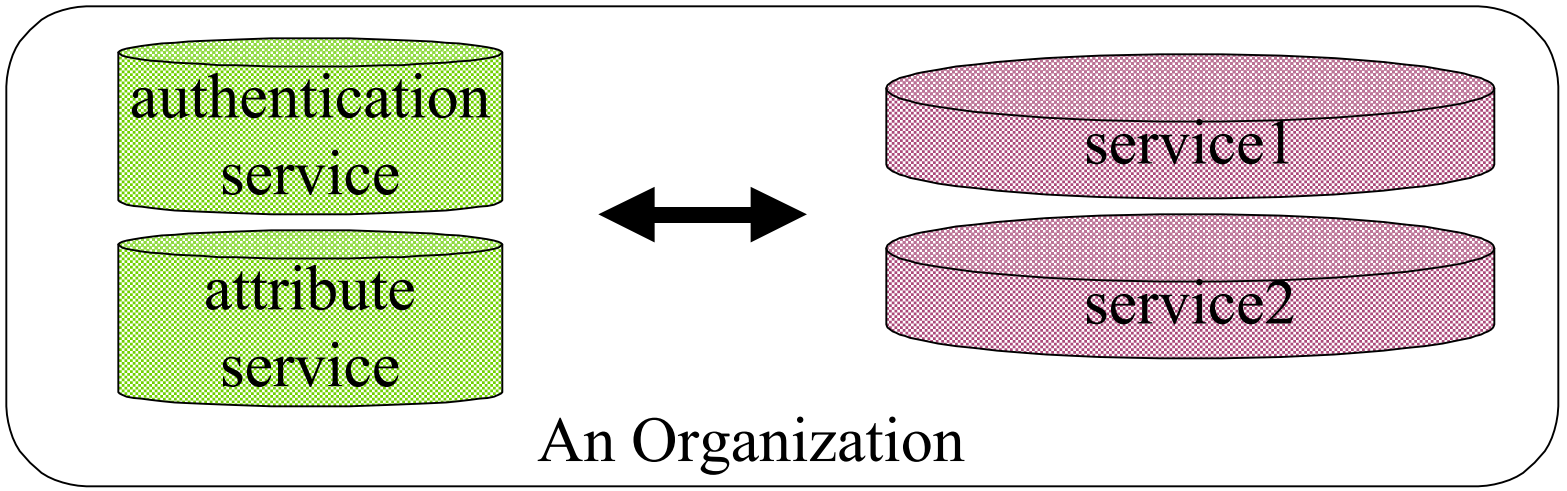


#3 Federated Architecture Characteristics

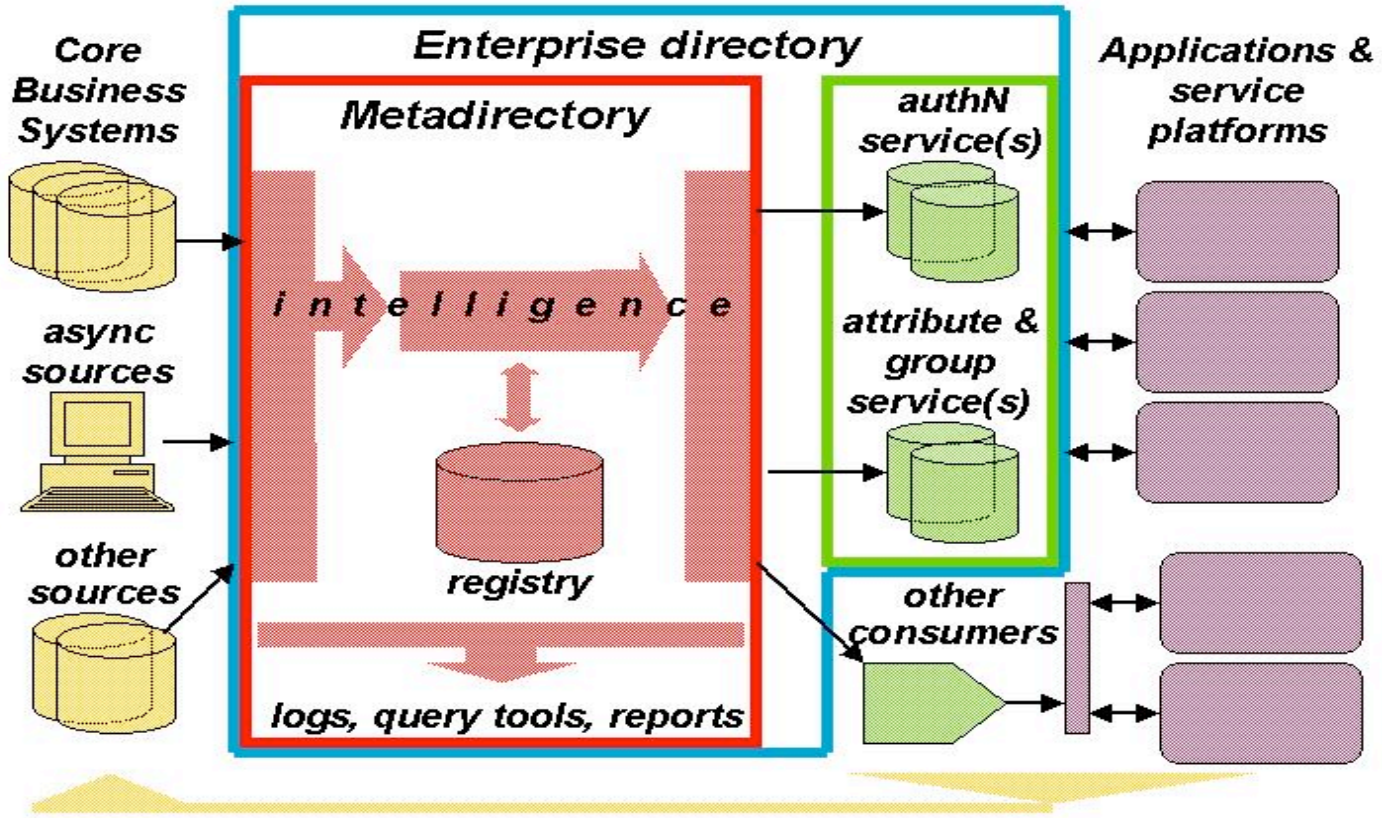
- Federated authentication and attribute services rely on participating organization's enterprise services.
- Inter-organizational applications such as Grids and digital-library content provision are integrated with and facilitated by enterprise services.

Middleware Initiative Objective

Help prepare campuses to implement core middleware for an integrated and ultimately a federated architecture.



Core middleware for an integrated architecture



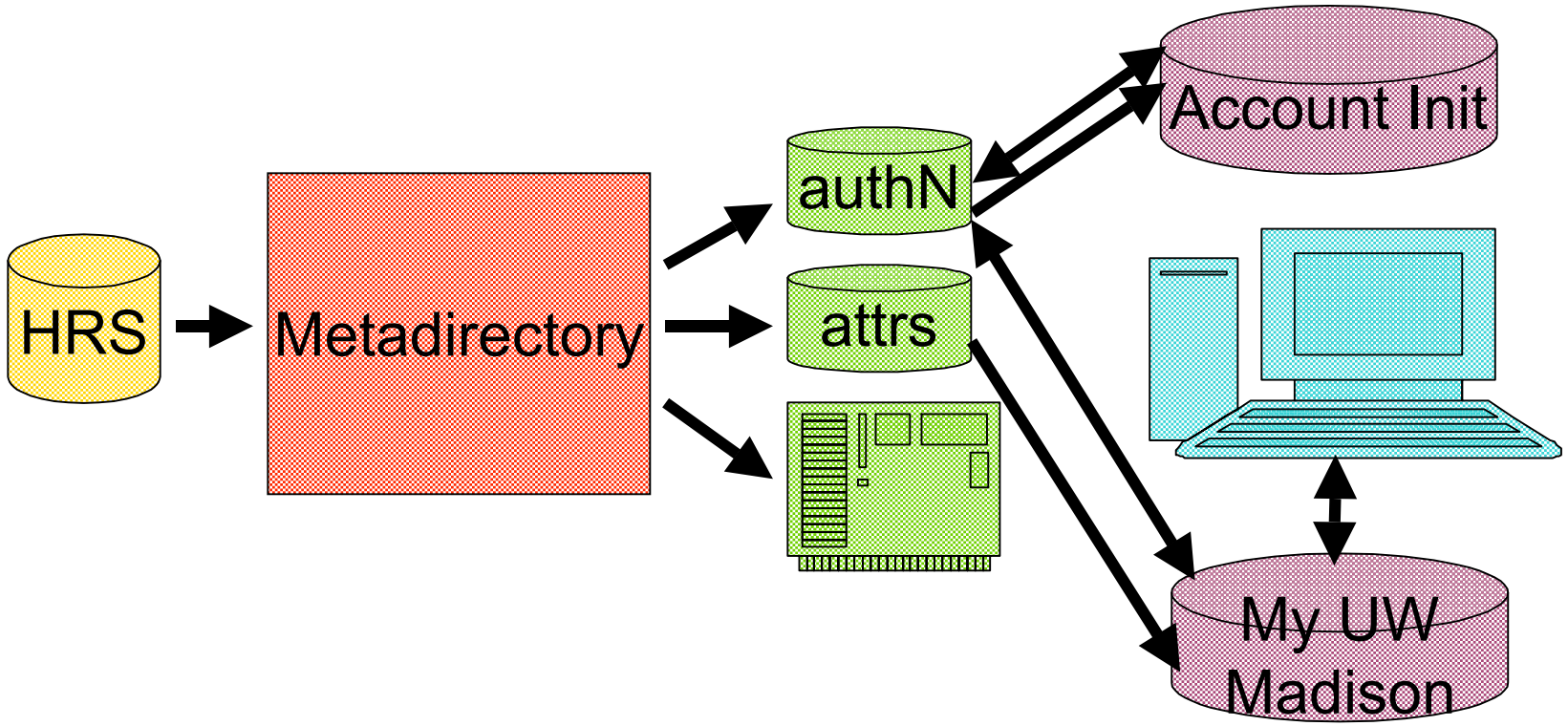
Demo analysis

Set of demos portray:

- Seamlessness of transitions between services
- Independence of location of service or user
- Suites of services designed to support activities of different constituencies
- Absence of need to make prior arrangement for resources required to enable services

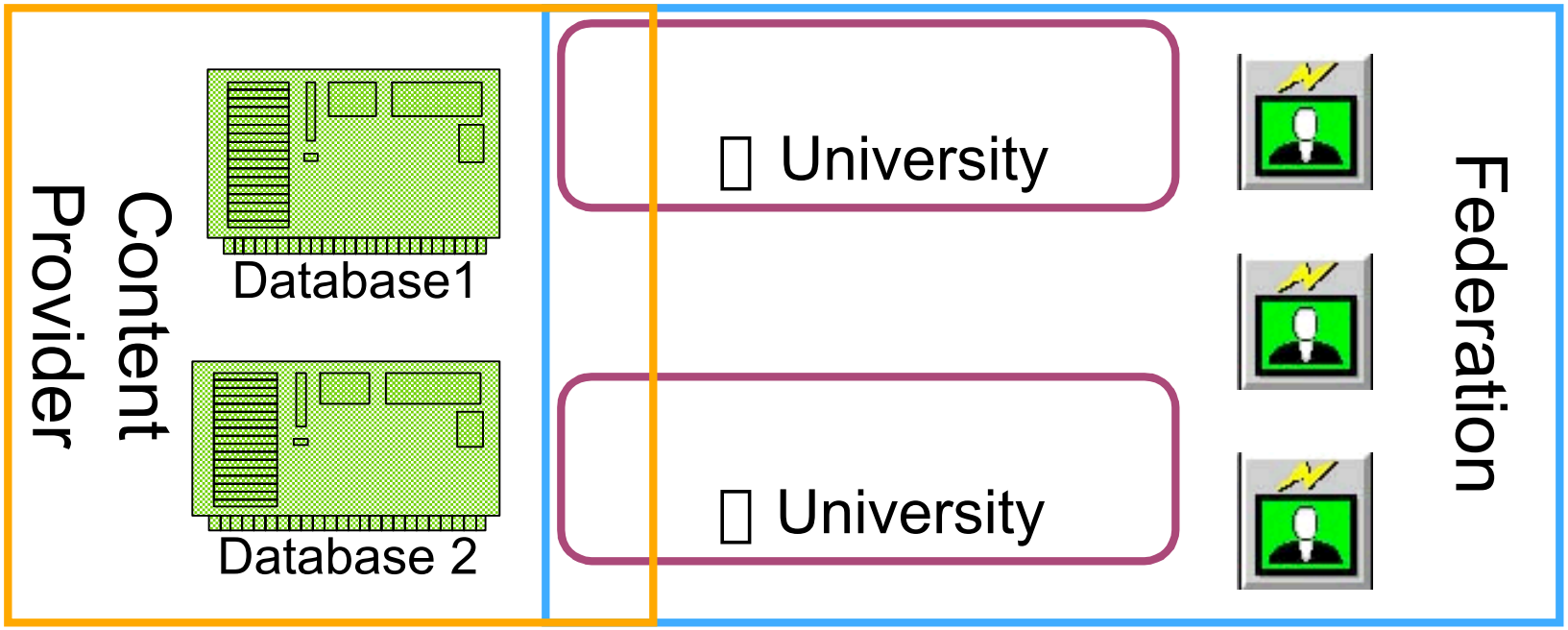
Provisioning Vignette:

New staff member accessing campus portal <to model>



Federated/Restricted Resources Vignette:
Sam using remote, online database

<to architectures>



Integrated Services Architecture: University of Wisconsin Portal Demo

http://my.wisc.edu

Federated Services Architecture: Blackboard, Inc. Shibboleth Demo

http://bbcommerce.blackboard.com/webapps/portal/frameset.jsp

Websites and Discussion Lists

- Websites

  http://middleware.internet2.edu

  http://www.nmi-edit.org

- Middleware information and discussion lists

  http://middleware.internet2.edu/lists.html

Questions and Comments?

– Keith Hazelton

University of Wisconsin/Internet2
hazelton@doit.wisc.edu