



Typical Directory Implementations at Institutions in Higher Education

Brendan Bellina
Identity Services Architect
Mgr, Enterprise Middleware Development
Information Technology Services
University of Southern California
Los Angeles, California, USA
bbellina@usc.edu



EuroCAMP Athens
How to build single sign on systems - Practical experiences

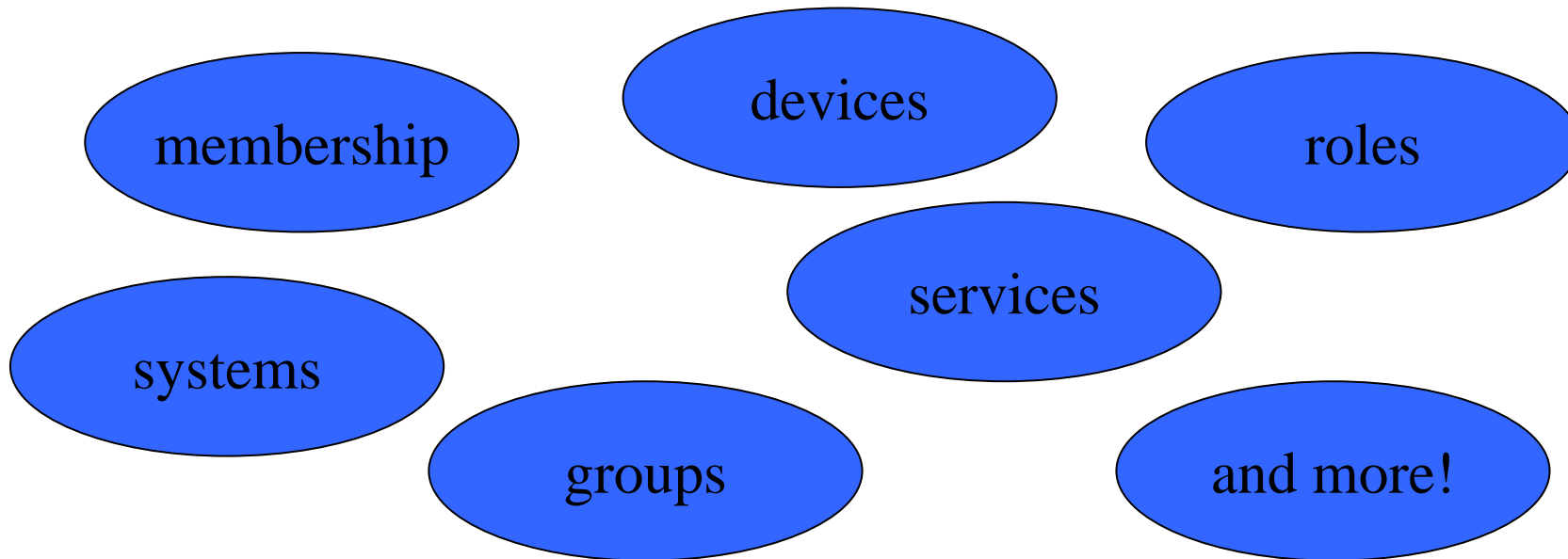
NTUA, Greece
5-6 November 2008

About the Author

- Background in Financial Software Development and Data Warehouse Design
- Active in Higher-Education Identity Management / Directory Services since 2001
- Designed and implemented the Enterprise Directory Service at the University of Notre Dame (2001-2004) <http://eds.nd.edu>
- Architect of USC Global Directory Service (2005-current) <http://www.usc.edu/gds>
- Chair of MACE-Dir Working Group (2008-current)
- Presentations and online materials available at <http://its.usc.edu/~bbellina>

What Are Directories Used For?

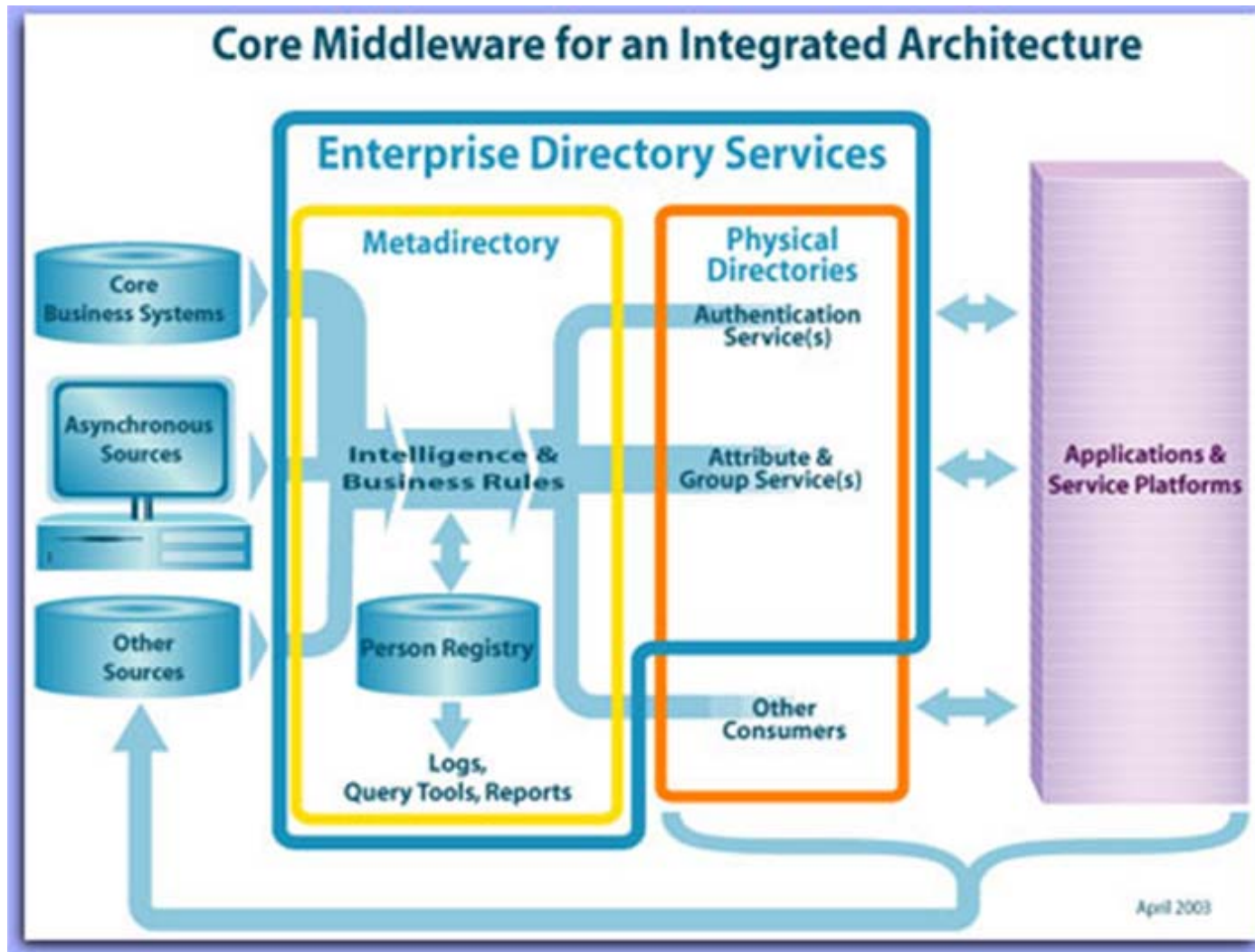
- A directory is ...
- a specialized database that contains information about an institution's



NMI Middleware Diagram

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.



Enterprise Directory Architectures

- Centralized EDS
 - Everything queries the central EDS
 - Central control
 - Performance bottleneck risk
- Replicated EDS
 - Replicate servers for performance
 - Small Risk of Data Latency
- Derivative directories
 - Distribute EDS data to stand-alone directories
 - Potential issues managing identities
 - Risk of data leakage and inconsistent access controls
 - Risk of Data Latency

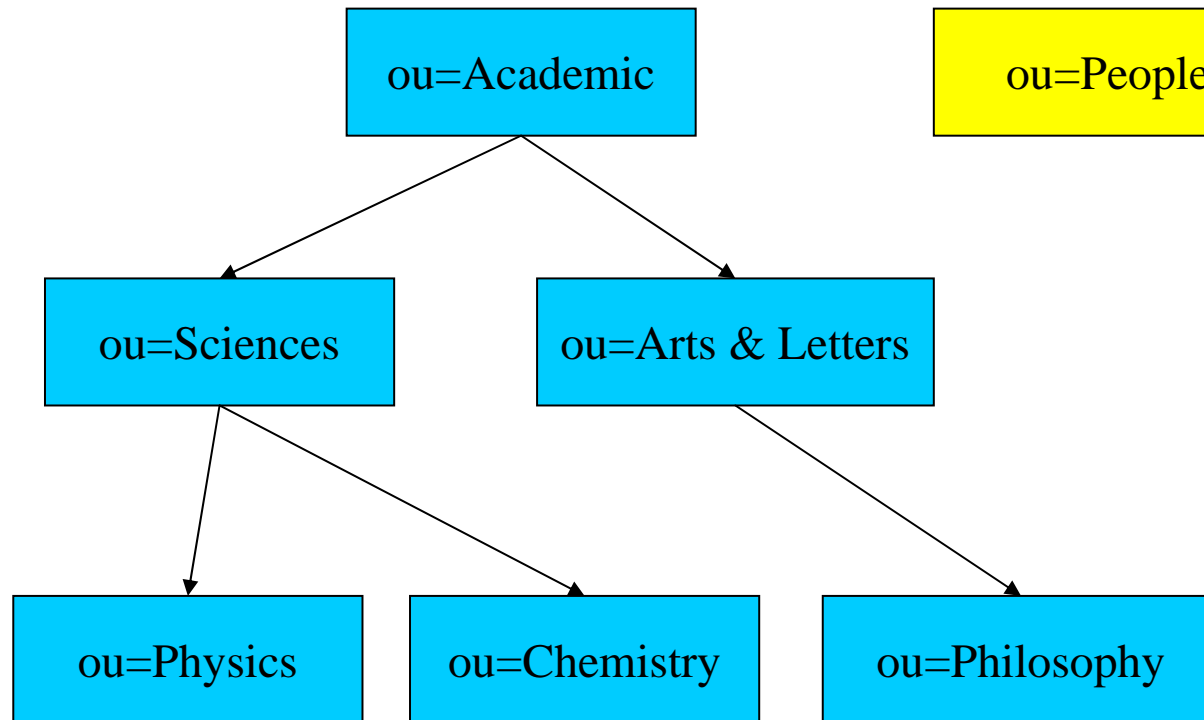
Directory Products

- Sun SJES Directory Server
- Novell eDirectory
- OpenLDAP Directory
- Fedora Directory
- Oracle Internet Directory
- Microsoft Active Directory

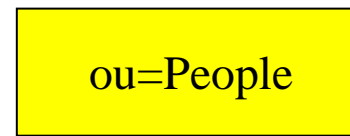
Directory Schema

Directory Information Tree (DIT)

- Tall & Spiky



Flat



Why not Tall and Spiky?

- Not amenable to people being in multiple organizational units simultaneously
- Not efficient when people move between organizational units frequently
- Not efficient when organizational hierarchy changes occur

Distinguished Name Structure (dn)

- Issues

- Useful for LDAP enabled apps
- Visible if any attribute in the entry is visible
- Must be unique within scope
- Benefits in being persistent, non-reassignable, and opaque

- Standards

- X.500 naming (based on geographical location)
 - ❖ cn=Bullwinkle Moose, ou=people, o=Wossamotta U, st=Confusion, c=US
- Domain Component naming (most commonly used)
 - ❖ cn=Bullwinkle Moose, ou=people, dc=Wossamotta, dc=edu

Choosing Relative Distinguished Name

- Initial part of dn, guarantees uniqueness
- Why not name-based, like cn or uid?
 - Names change - not really owned by directory
 - Facilitates binding directly to entry
 - ❖ Possible attack vector
 - ❖ Means of authentication without approval or authorization
 - ❖ Releases identity if any other attribute is releasable
- Consider use of opaque identifier owned by directory
 - Exp. **uscrdn=usc.edu.scbs5rm6**,ou=people,dc=usc,dc=edu

Standard Object Classes for People

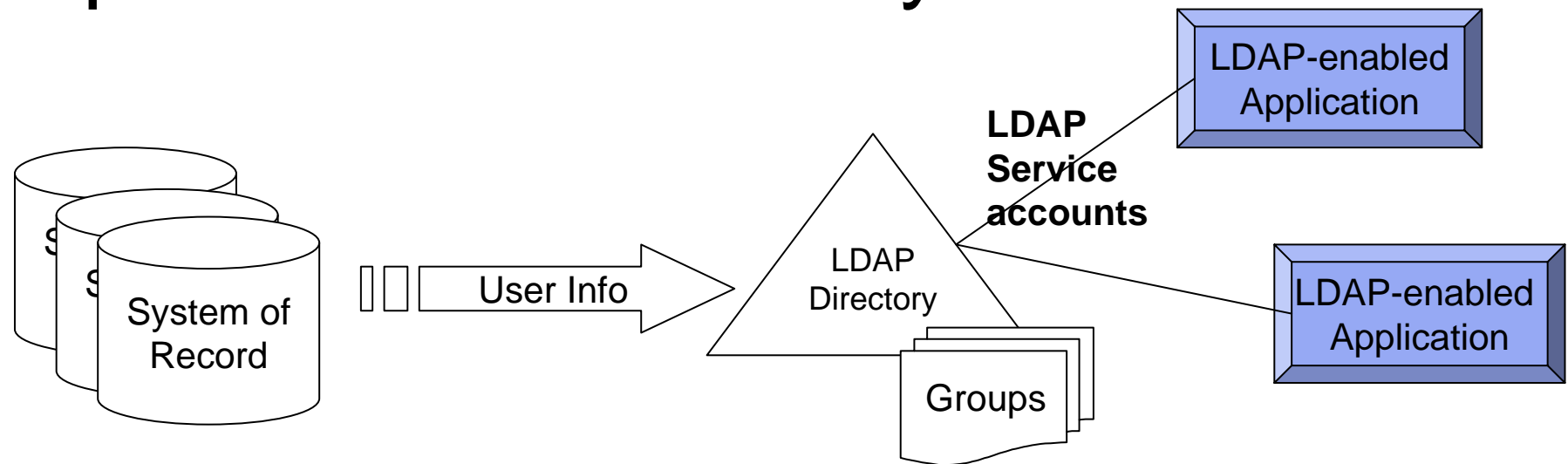
- person
- organizationalPerson
- inetOrgPerson
- eduPerson
- SCHAC - SCHema for ACademia
- eduCourse
- National object classes - norEdu, plEduPerson, swissEduPerson, etc.
 - See <http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-higher-ed-person-analysis-latest.htm> (last updated 2005)

Schema Extensions

- Step One: Get an OID assignment for your institution from IANA
- Step Two: Create new objectclasses for new attributes
- DO NOT make up or reuse an OID
- DO NOT modify a standard objectclass
- DO NOT populate standard attributes in non-standard ways

Controlling Access

Enterprise LDAP Directory Model



Because an Enterprise Directory contains all people who use all applications and all their attributes, population and attribute filtering must be done between the application and the directory.

LDAP-enabled applications should use assigned LDAP Service accounts to filter based on directory ACL's.

Access Control Instructions/Lists

- Direct access via LDAP/LDAPS

- Sun SJES ACI (example @ USC)

- ❖ # Allow all access to the Directory Administrators Group

- ❖ aci: (targetattr = "*")

- ❖ (version 3.0;aci "Directory Administrators Group";

- ❖ allow (all)

- ❖ (groupdn = "ldap:///cn=Directory Administrators, dc=usc,dc=edu")

- ❖ ;

- ❖)

- ❖ #

- Access to an entry is based on attributes of the entry or group membership of the querying entity. Group membership of the target is not an attribute unless you create one like isMemberOf and populate it.

Populations

- Students
- Faculty
- Employees
- Instructors
- Affiliates / Guests
- Alumni
- Retirees
- Emeriti

Typical Attribute Categories

- Identifiers
- Name
- Contact Information
- Academic Information
- Employee Information
- Affiliation Information
- Attribute Release Policies
- Entitlements

An Enterprise Directory Service...

- is a transactional system, read frequently, updated infrequently
- **is not** designed to provide reporting or analysis
- **is not** a data warehouse
- **is not** an alternative to bypass Data Steward oversight
- **is not** a source for data to populate local databases and networks

Common Services of an EDS

- White Pages
- Email client lookup
- Authentication service
- Data source for attribute release products such as Shibboleth

- And sometimes:
 - Authorization / Privileges
 - Group services

Links

- USC: <http://www.usc.edu>
- Brendan Bellina, bbellina@usc.edu