



# University of Southern California Identity and Access Management (IAM)

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

# University of Southern California

- Private research university, founded 1880
- 33,500 students (16,500 undergraduate, 17,000 graduate and professional)
- 3,200 full-time faculty, 8,200 staff
- \$1.9 billion annual budget, \$432 million sponsored research
- Two major LA campuses; six additional US locations; four international offices

# Definition of Identity and Access Management

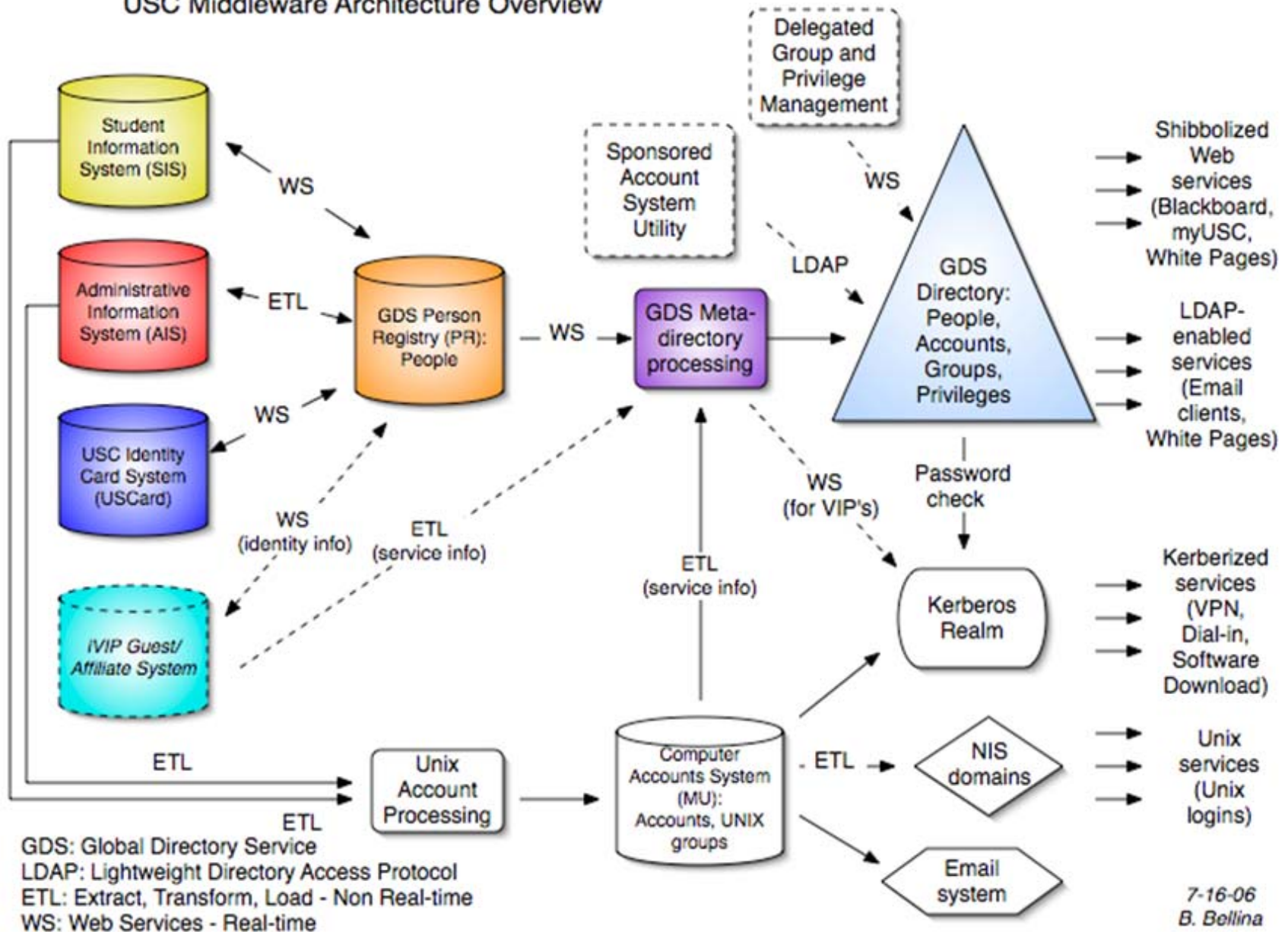
- Identity and Access management (IAM) is a broad administrative function that identifies individuals in a system (in this case, USC), and controls and facilitates their access to resources within that system by associating user rights and restrictions with the established identity.

# Evolution of IAM Program

- 2001 – Eliminate/Suppress US Government assigned Social Security Numbers from non-financial systems
- 2002 – Commit to unified identifier – USC ID number
- 2003 – Build data governance structure
- 2005 – Enable authentication and authorization
- 2007 – Support affiliates and visitors

# Technical Infrastructure and Components

# USC Middleware Architecture Overview



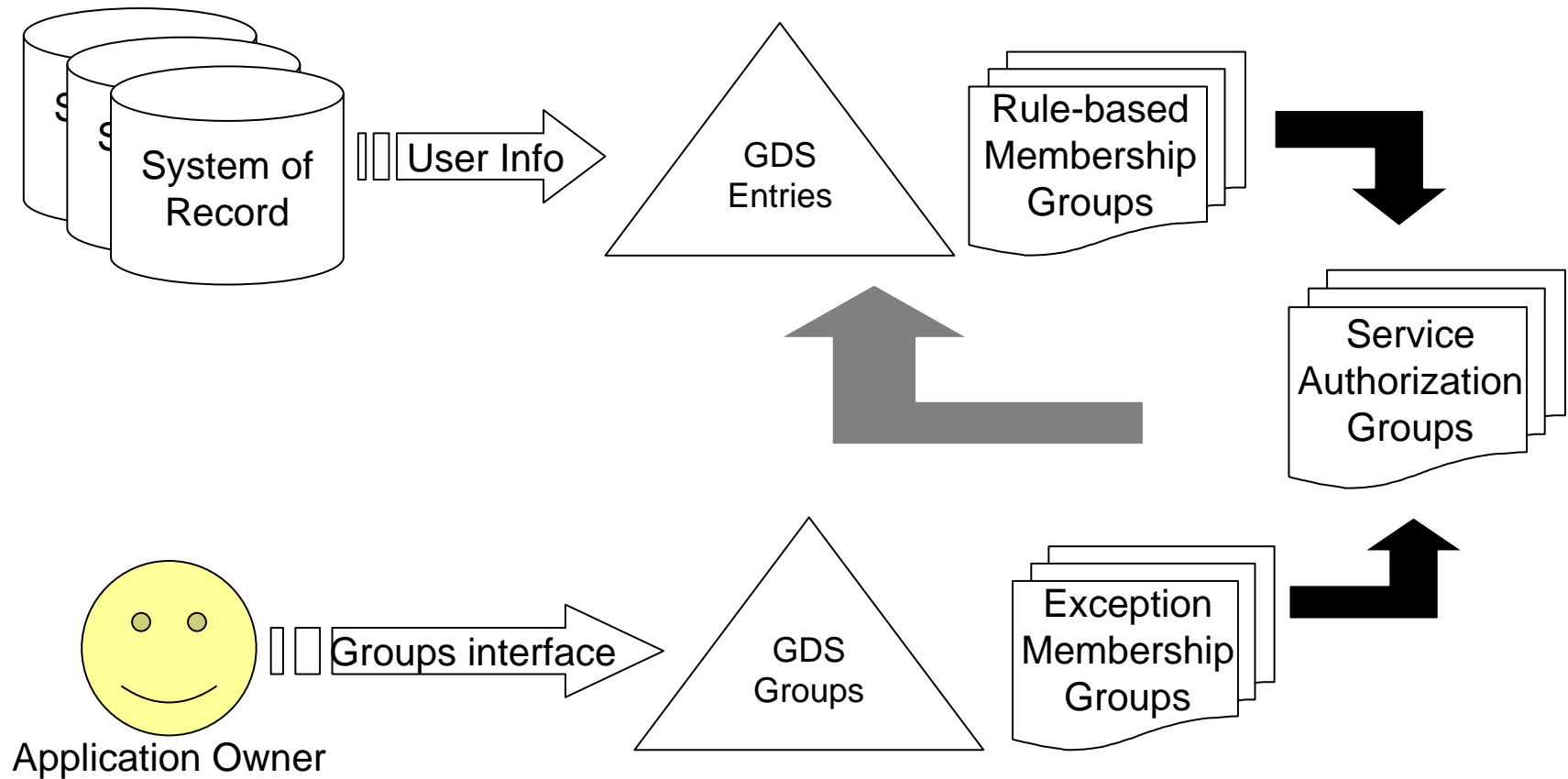
# Responsibilities of the Person Registry

- Prevent duplicate identities by matching
- Collect person attributes from SORs for matching and provisioning to GDS (Enterprise Directory Service)
- Generate University Identifier (USCID)
- Reject invalid data from SORs
- Merge functions
- Respond to queries for specific users from SORs to prevent duplicates
- Provide reports on partial identity matches for SORs

# Responsibilities of the Metadirectory

- Update GDS content based on:
  - Person information - Person Registry
  - Account information - Account System (“MU”)
  - Affiliate services - Guest/Affiliate System (“iVIP”)
- Generate Directory Identifiers “uscPvid”
- Maintain GDS groups based on attributes and discretionary group memberships
- Populate entitlements based on group memberships

# Groups Processing



# Responsibilities of the GDS LDAP

- Public LDAP interface for White Pages, Email clients, and other LDAP clients
- Master of groups
- Aggregates account information for use with Shibboleth SSO
- Attribute and Identity source for Shibboleth SSO
- Authentication services (via Kerberos plug-in)
- Authorization services (via service accounts and aci's)

# Shibboleth SSO

- Web-based community source Single Sign-on
- Developed by Internet2
- Privacy preserving
- Attribute and entitlement delivery
- SAML 2 compliant
- Unlike LDAP, the application does not need to handle the user password for authentication

# Policy and Governance

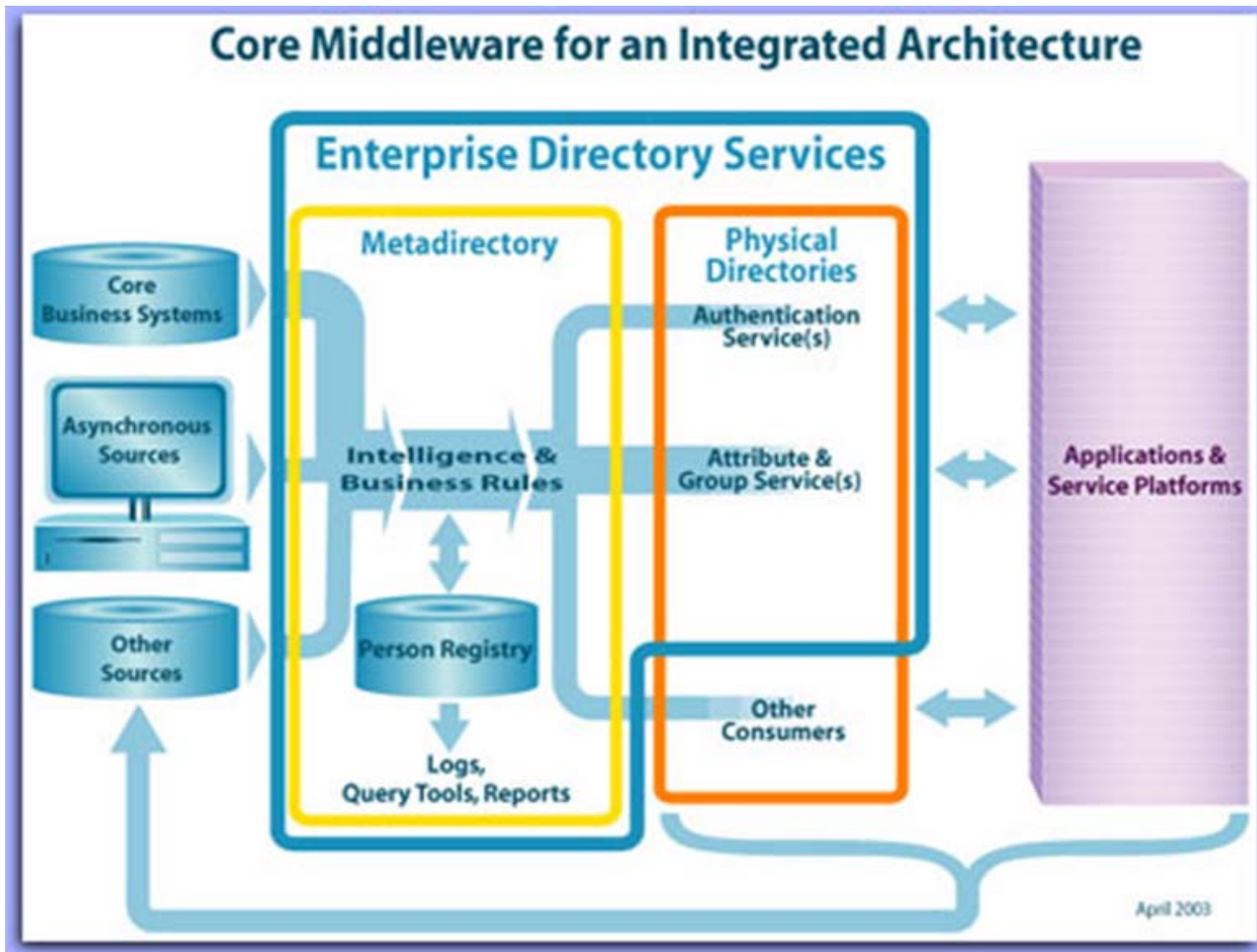
# Data Governance

- **Data Governance brings together cross-functional teams** to make interdependent rules or to resolve issues or to provide services to data stakeholders. These cross-functional teams - Data Stewards and/or Data Governors - generally come **from the Business side of operations. They set policy that IT and Data groups will follow** as they establish their architectures, implement their own best practices, and address requirements. Data Governance can be considered the overall process of making this work.

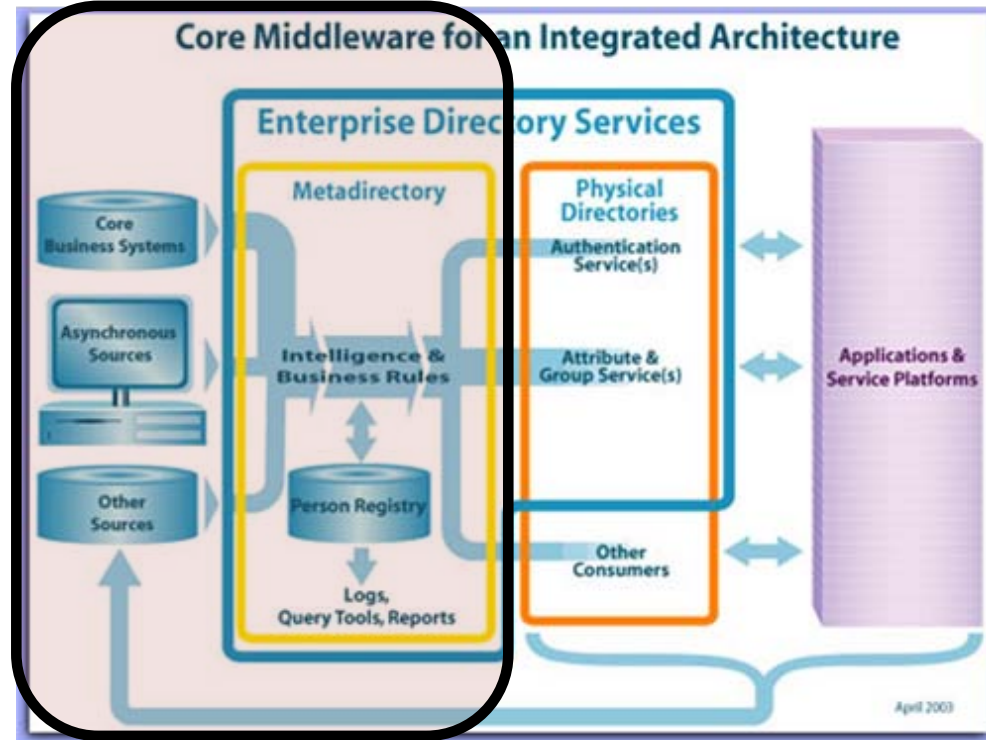
- [http://www.datagovernance.com/adg\\_data\\_governance\\_governance\\_and\\_stewardship.html](http://www.datagovernance.com/adg_data_governance_governance_and_stewardship.html)

# Data Governance Committees

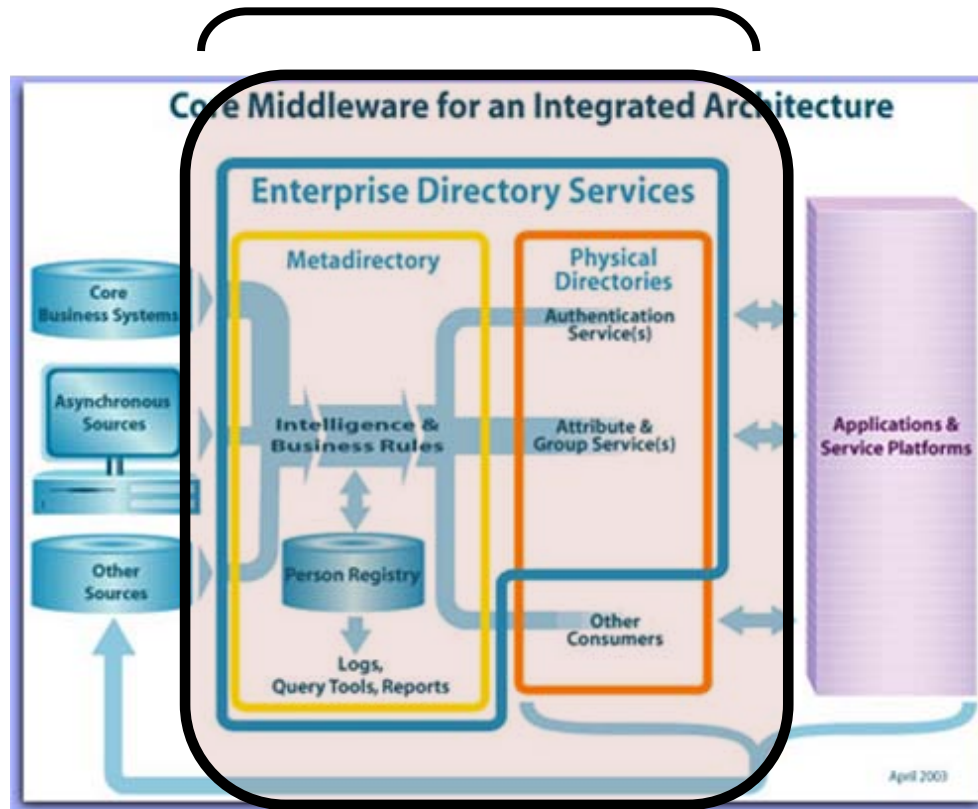
- **Directory Services Steering Committee** – policy development committee meets every 3 weeks
  - focuses on policy regarding data acquisition and release, integration, and communication
  - attendees include senior management representatives from academic schools, administrative departments, major IT units, General Counsel
- **GDS Executive Committee** - management committee every other week
  - focuses on technical and staffing issues affecting direction and prioritizations
  - attendees include management representatives from SOR's and GDS team
- **Data Team** - technical committee meets monthly
  - focuses on operational issues affecting SOR's and PR/GDS
  - attendees include representatives from SOR's and GDS team
- **Working Groups**



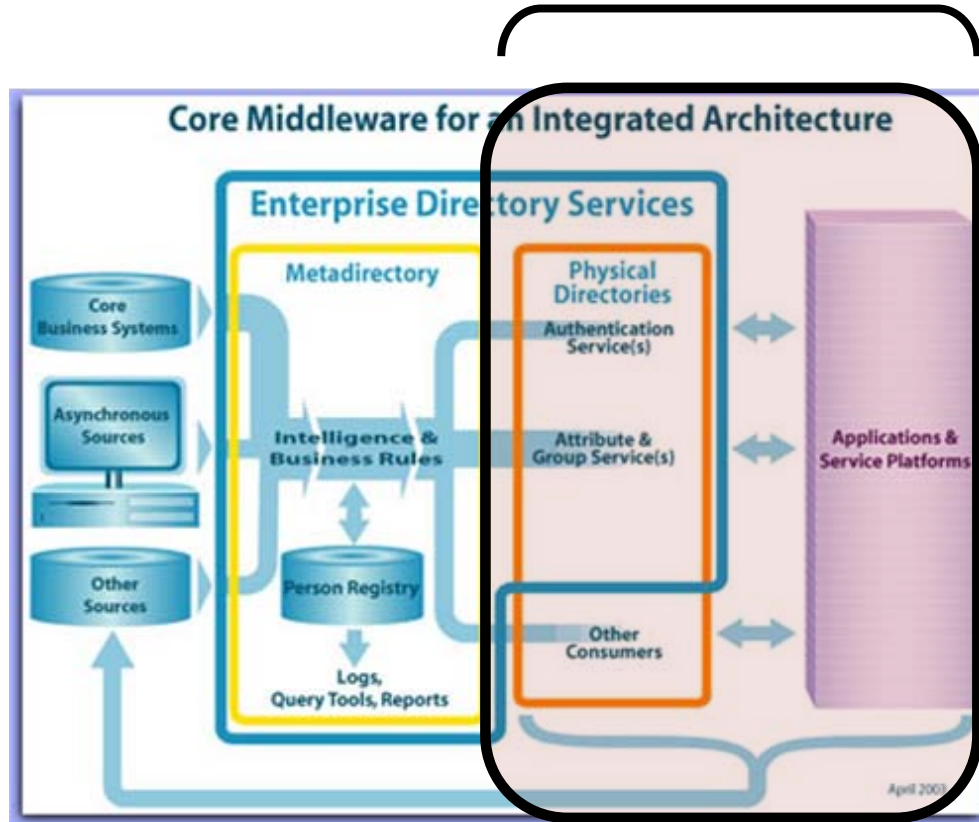
# Data Team



# GDS Executive Committee



# Directory Services Steering Committee



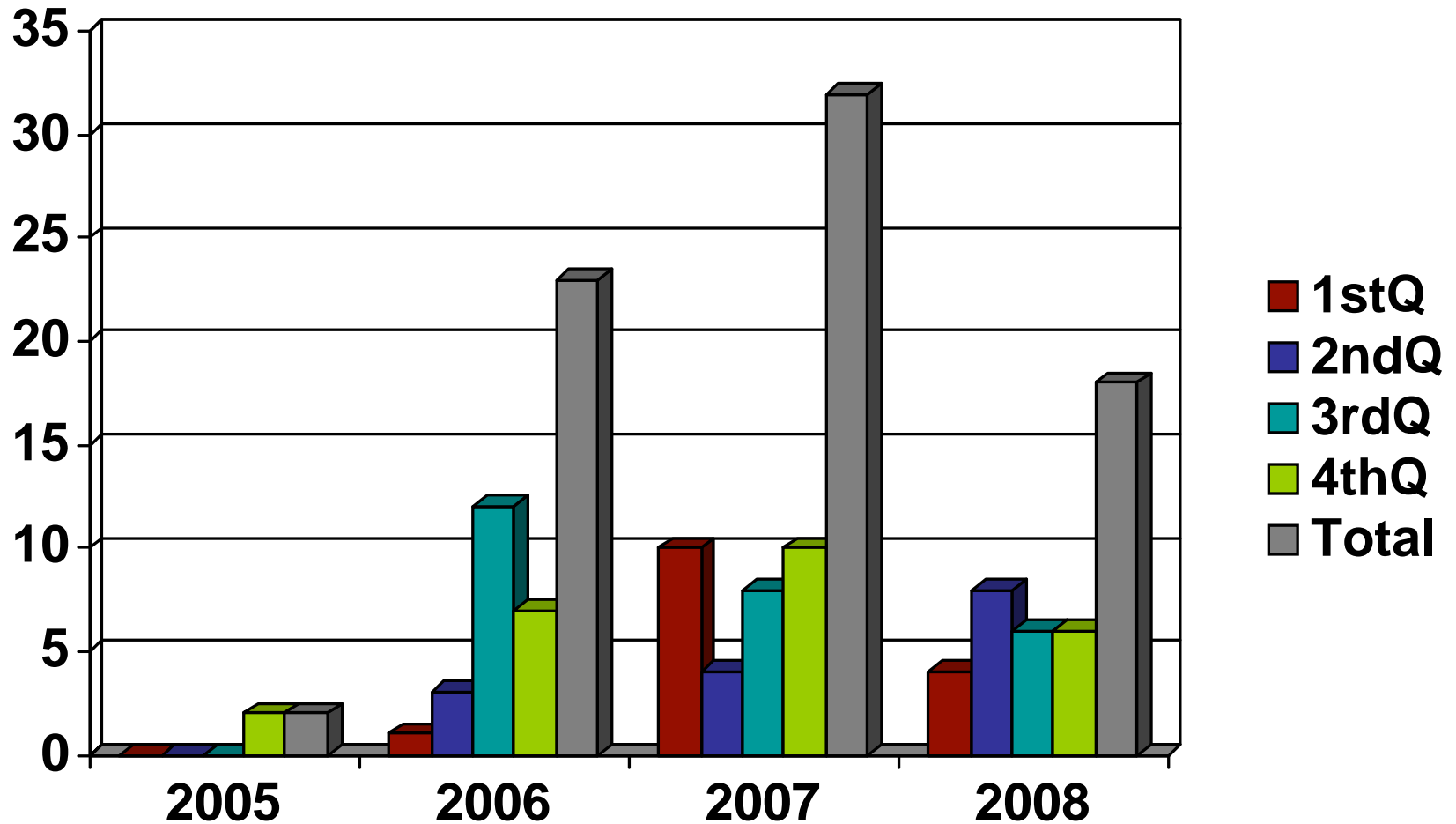
# Attribute Access Request Process

- Required for all data requests to GDS content
- Directory Steering Committee reviews all new AAR submissions
- Data Stewards must also approve requests
- Requests must be reauthorized every 2 years
- Changes in data requirements require submission of a new AAR

# Typical AAR Questions

- What information is needed?
- For what purpose?
- For what population?
- For what service?
- Is data for confidential students or employees required?
- Are there user exceptions?

# Number of AARs Processed



# Links

- USC: <http://www.usc.edu>
- GDS Website: <http://www.usc.edu/gds>
- Brendan Bellina, [bbellina@usc.edu](mailto:bbellina@usc.edu)