Access Management with Grouper

Tom Barton
University of Chicago

JA-SIG March 2, 2009

Outline

IAM = Identity & Access Management

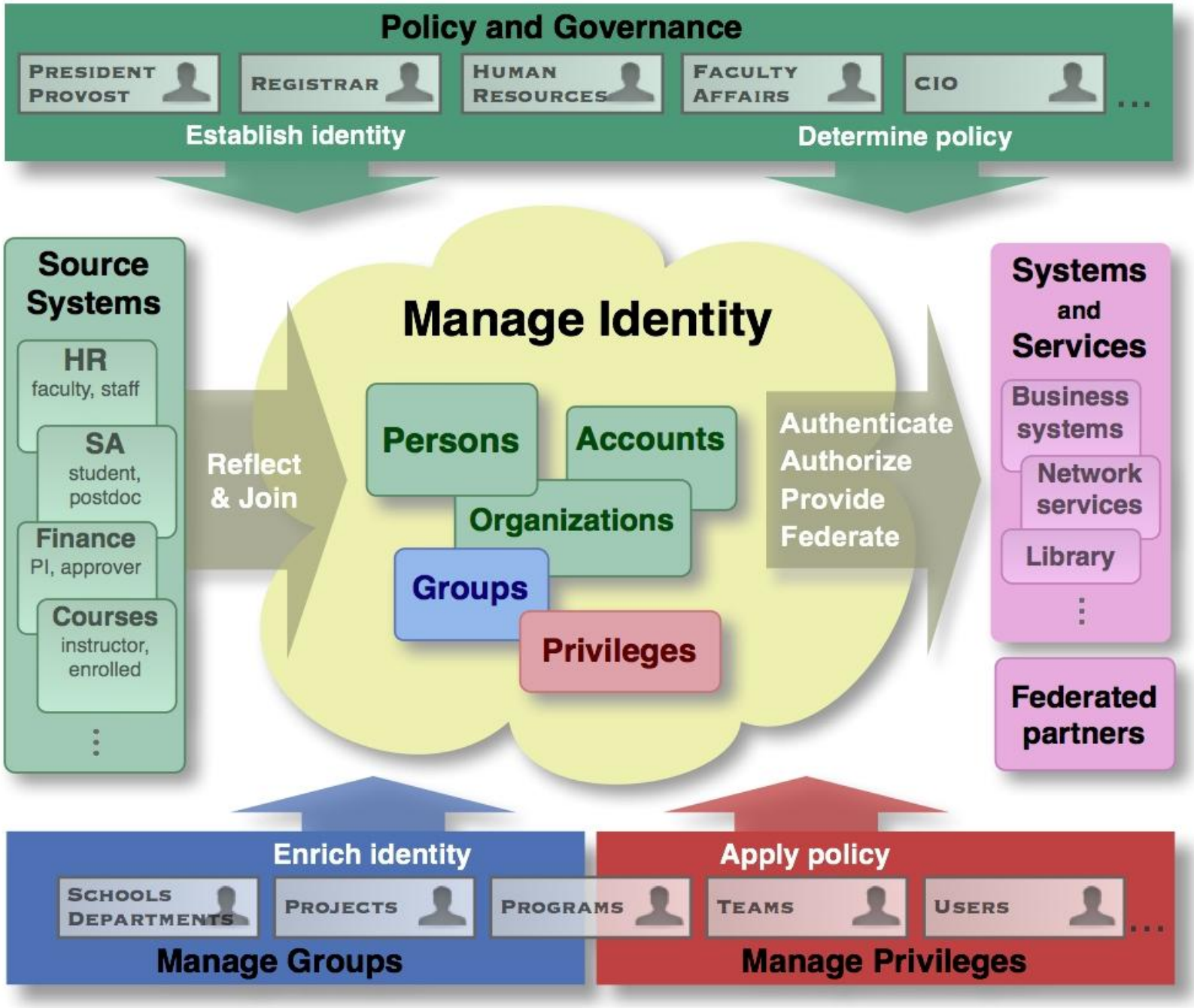
- Overview of IAM à la MACE/Internet2
- Grouper 101
- A few examples from the real world

Access management in Higher Ed

- Each person's online activities are shaped by many Sources of Authority
  - Institutional policy making bodies
  - Program/activity heads
  - Resource managers
  - Self
- All of those Authorities must be reflected in applications
- IAM is the layer of abstraction that allows that to happen in a scalable manner

IAM values

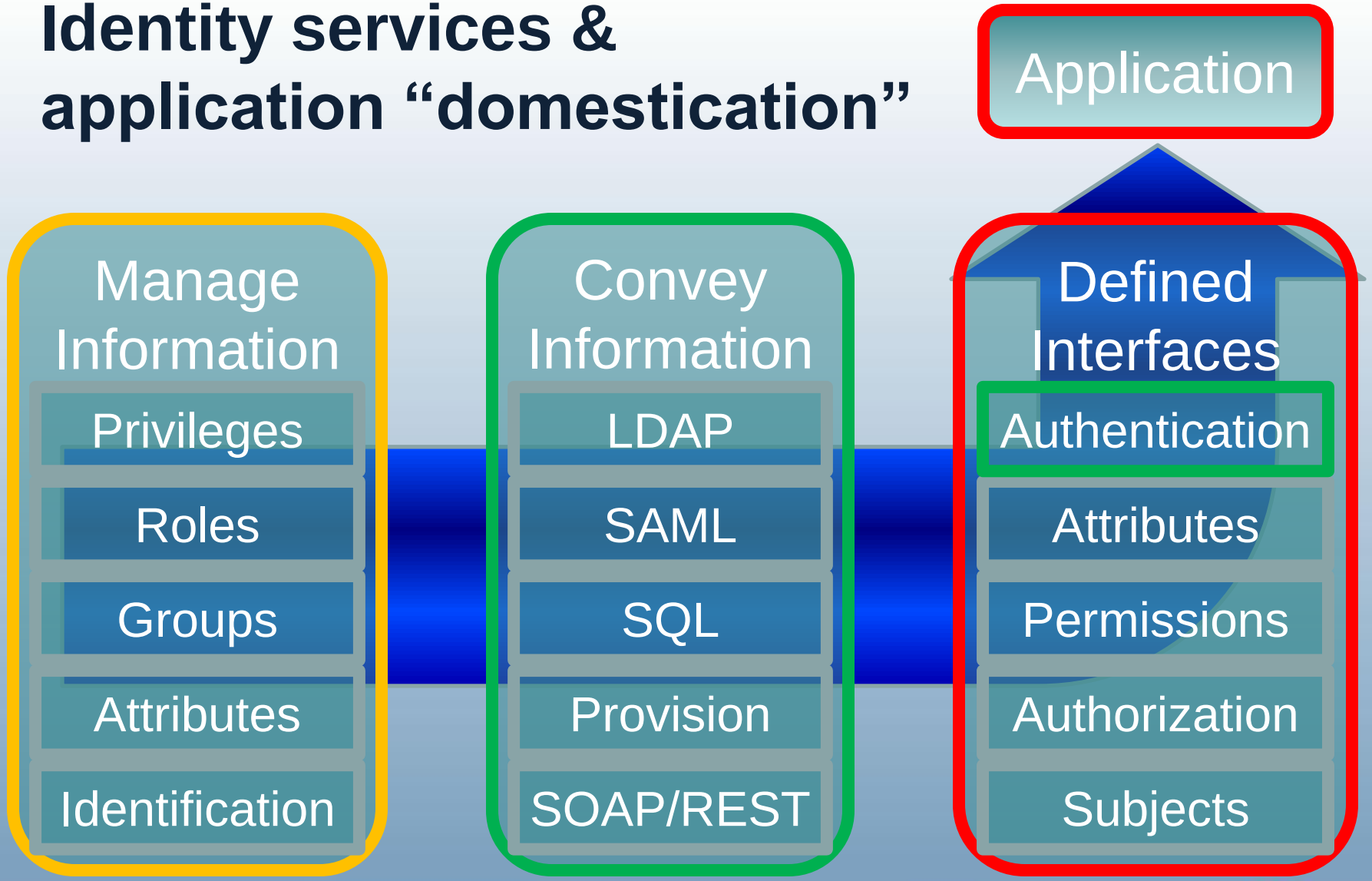
- Simplifies
  - Operations: highly leveraged
  - User perspective: FSO, SSO
  - Policy implementation
- Secures
  - Institutional authentication & access management services
  - Reduced exposure of PII
  - Increased auditability
- Connects distributed authorities


Policy and Governance
President
Provost
Registrar
Human Resources
Faculty Affairs
CIO
...
Establish identity
Determine policy
Source Systems
HR
faculty, staff
SA
student, postdoc
Finance
PI, approver
Courses
instructor, enrolled
Reflect & Join
Manage Identity
Persons
Accounts
Organizations
Groups
Privileges
Authenticate
Authorize
Provide
Federate
Systems and Services
Business systems
Network services
Library
Federated partners
Enrich identity
Schools
Departments
Projects
Programs
Manage Groups
Apply policy
Teams
Users
...
Manage Privileges

MACE/Internet2 IAM work

- Shibboleth
- InCommon Federation
- Grouper
- Comanage
  - Identity services & application domestication
- Privilege & access management
  - MACE-paccman working group
  - !Signet
  - Grouper to add some privilege management capability
- MACE-directories working group
  - edu* schema, white papers, etc

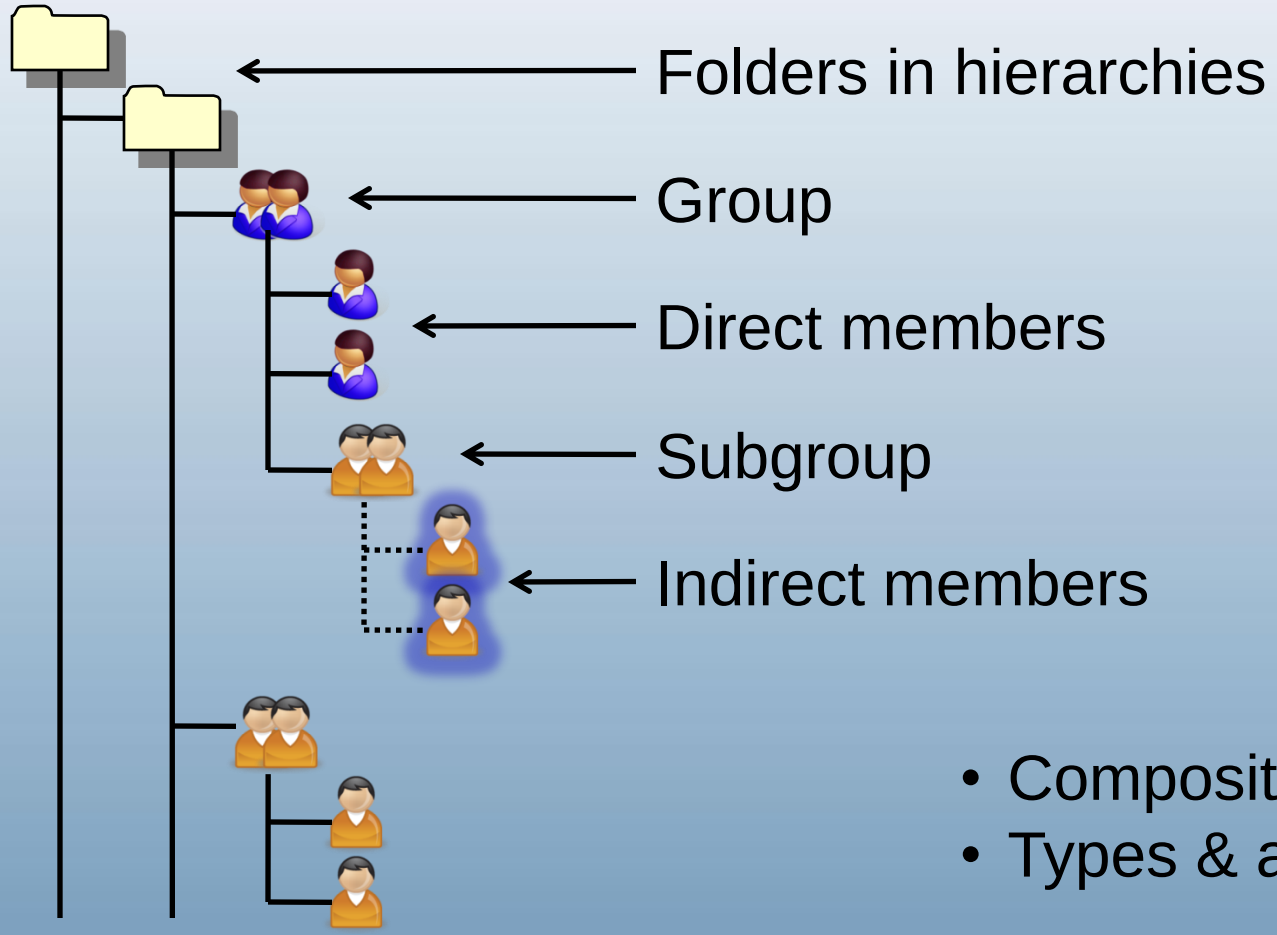
Identity services & application “domestication”



Identity services activities & Higher Ed

- MACE-paccman working group
- Kuali Rice
- OSS projects, some JA-SIG affiliated
- Liberty, Identity Gang, etc
- International efforts akin to MACE's
- Advanced CAMP June 2009 in Philly

Grouper: core concepts



- Composite groups
- Types & attributes

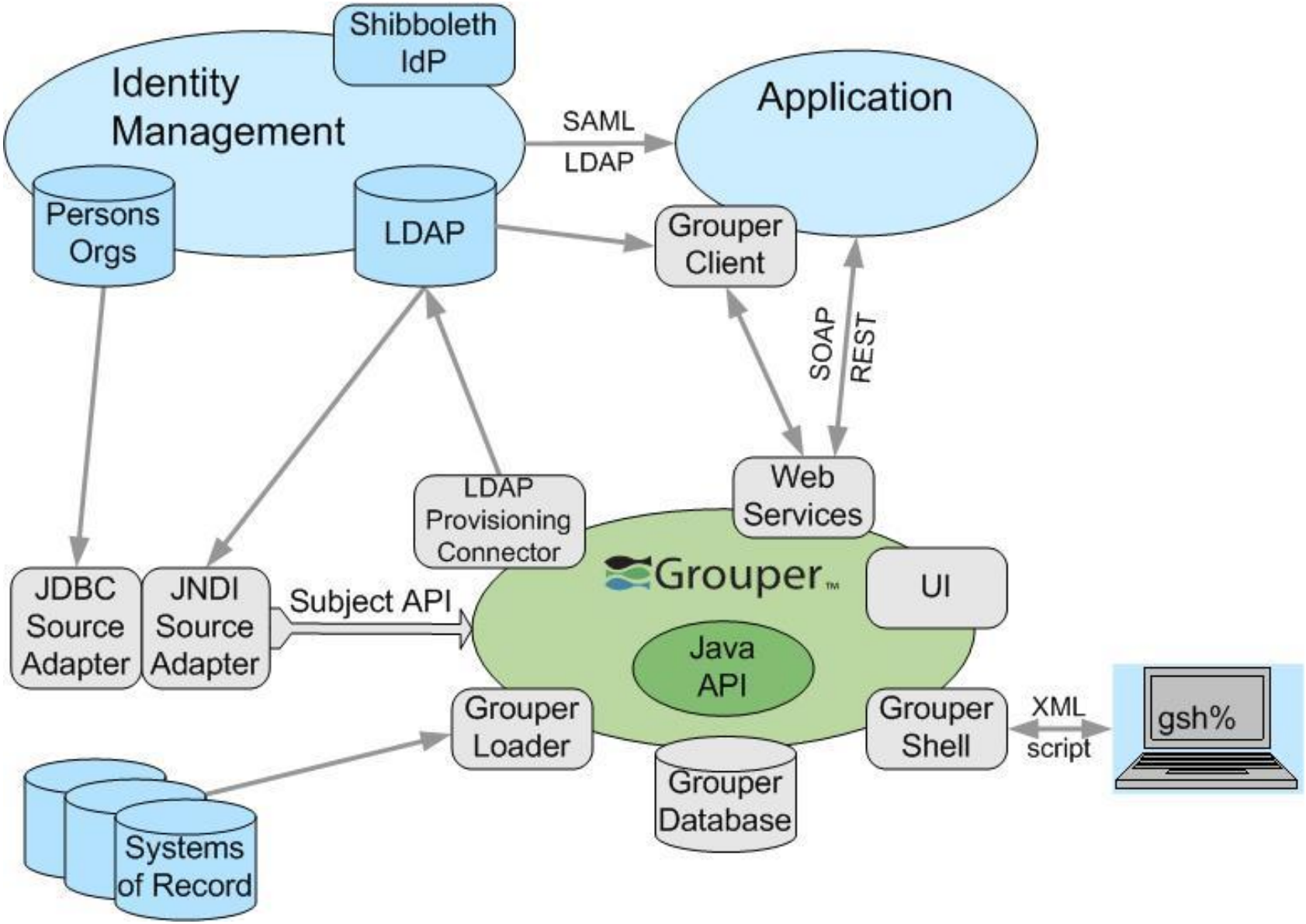
Grouper: security & delegation

- Create groups here
- Create subfolders

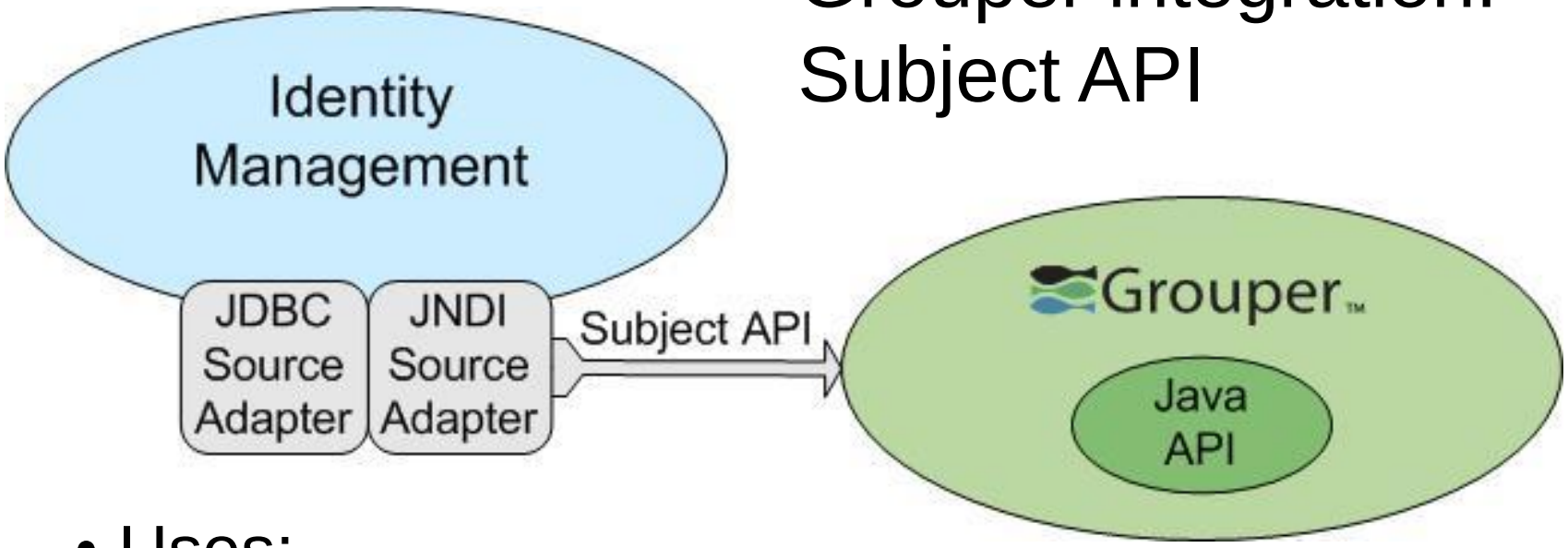
- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

Delegation

Grouper integration

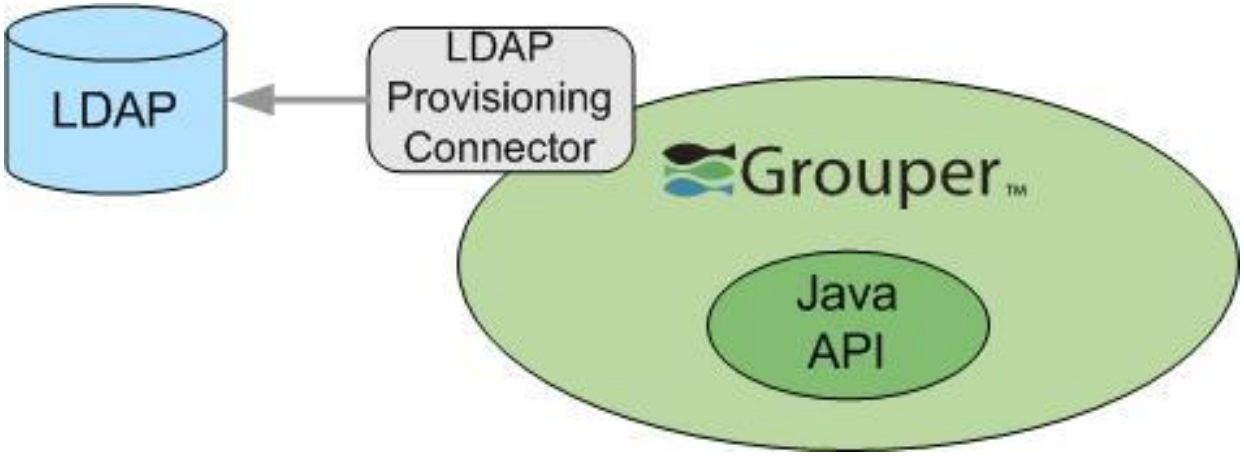


Grouper integration: Subject API



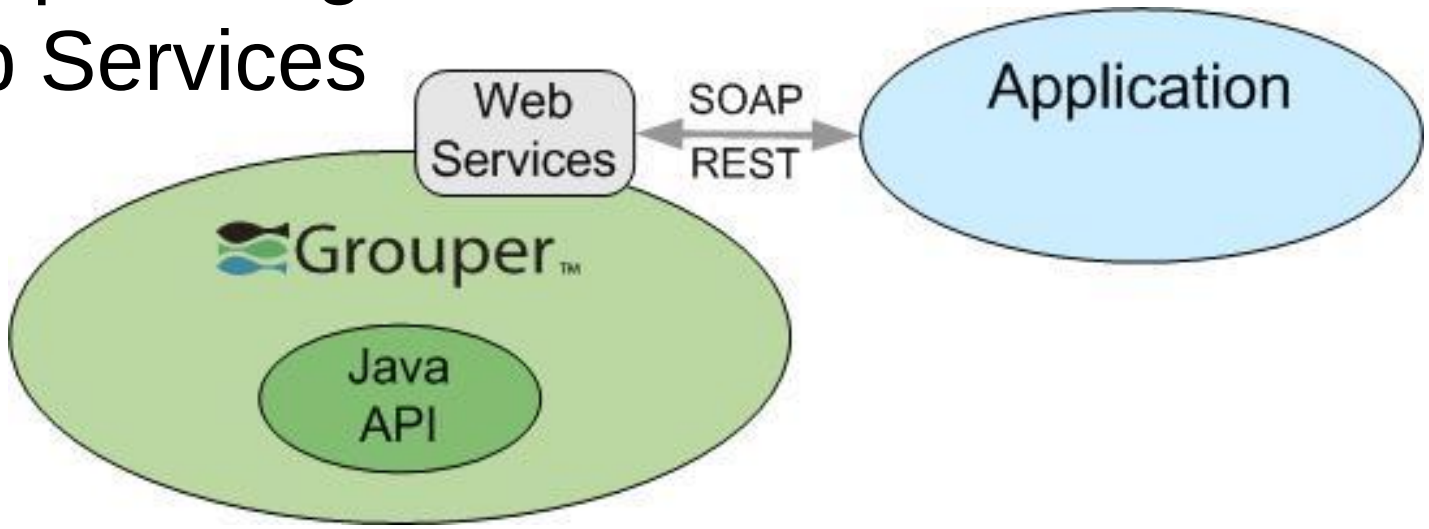
- Uses:
  - Grab Subject's attributes
  - Search for Subjects
  - Identifier crosswalk
- JNDI & JDBC adapters provided
- Plug-in interface for custom adapters

Grouper integration:
LDAP provisioning connector



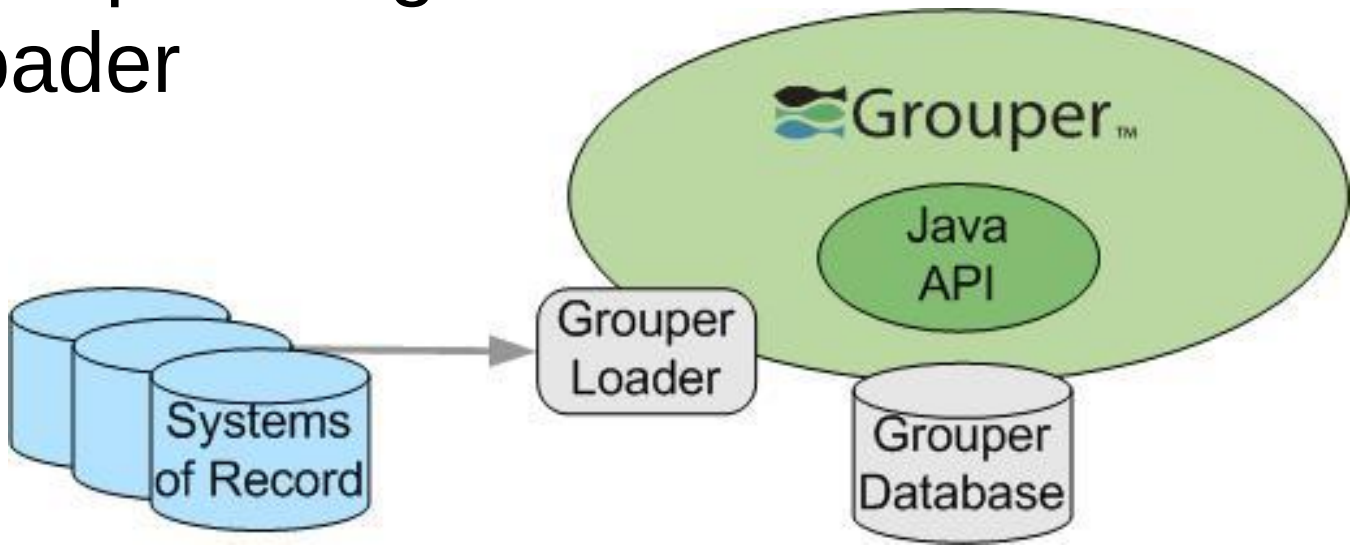
- Push groups and/or memberships to LDAP
- Variety of selection criteria
- Configurable appearance of LDAP entries
- Full & incremental provisioning modes now
- Asynchronous updating planned

Grouper integration: Web Services



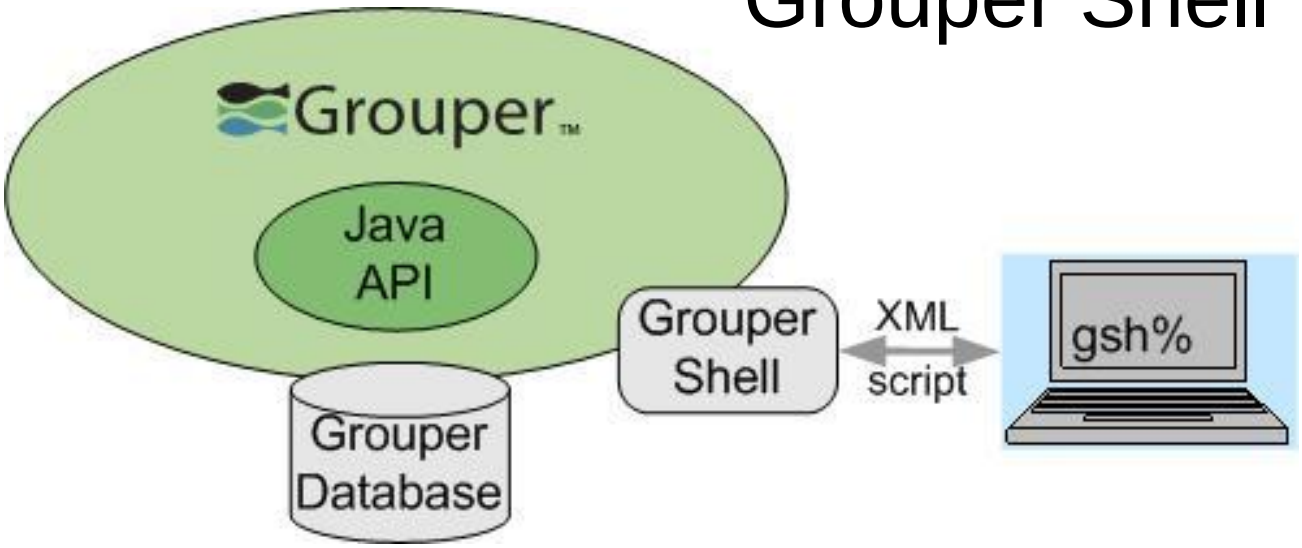
- (SOAP, REST) x (Lite, Heavy)
- Large fraction of java API is exposed
- Authentication by container or Rampart
  - Basic, kerberos, X.509, SAML
  - actAs
- .NET and PHP dev guides by U Newcastle

Grouper integration: Loader



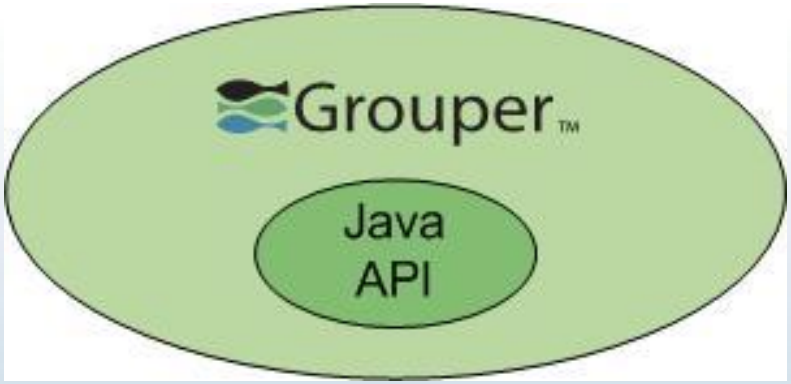
- Dynamically create and maintain groups by SQL query
- Quartz-based service/daemon launched by Grouper Shell

Grouper Integration: Grouper Shell



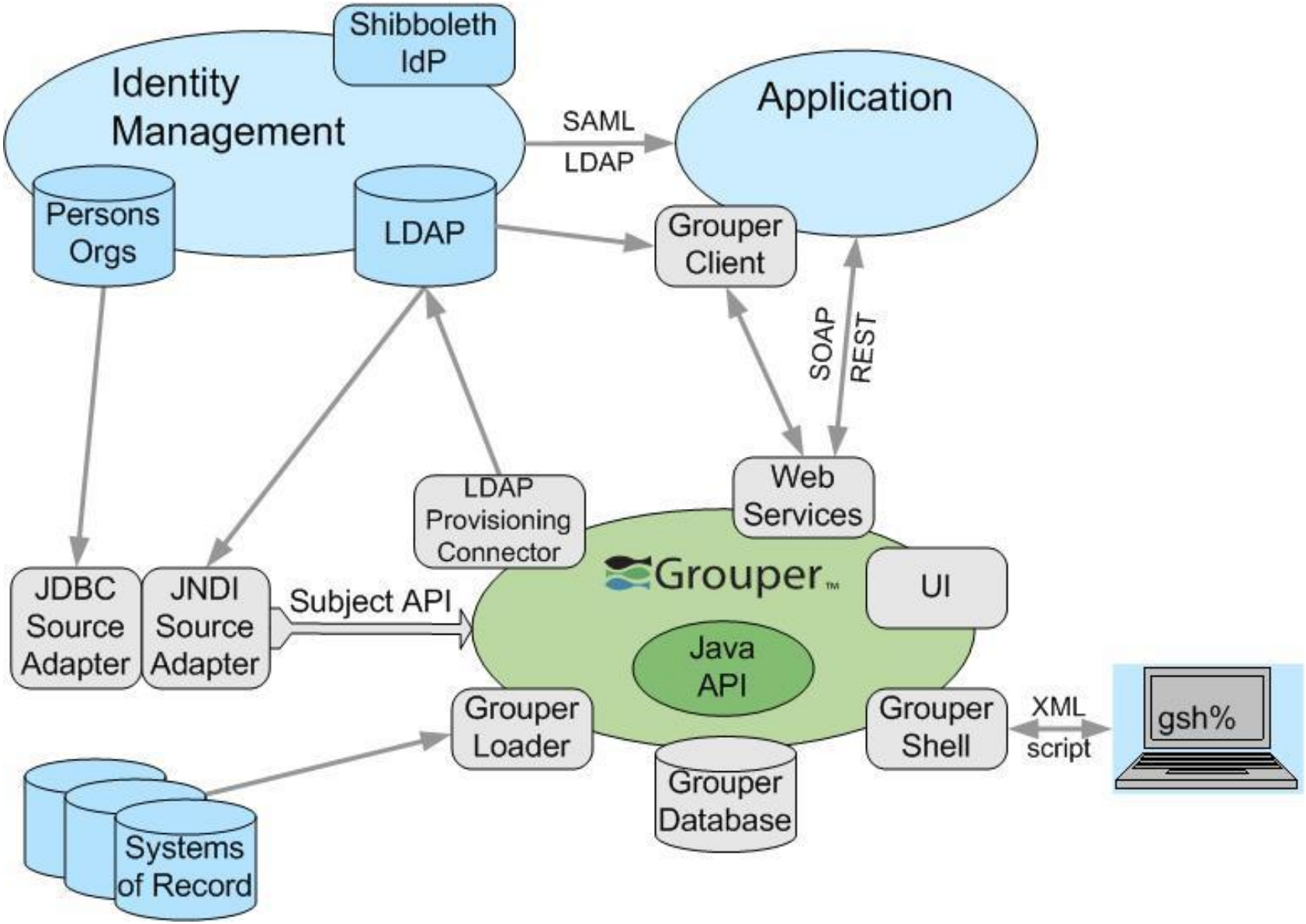
- Command line interface to java API & tools
- XML import/export
- Batch scripts
- Low-level grouper system administration

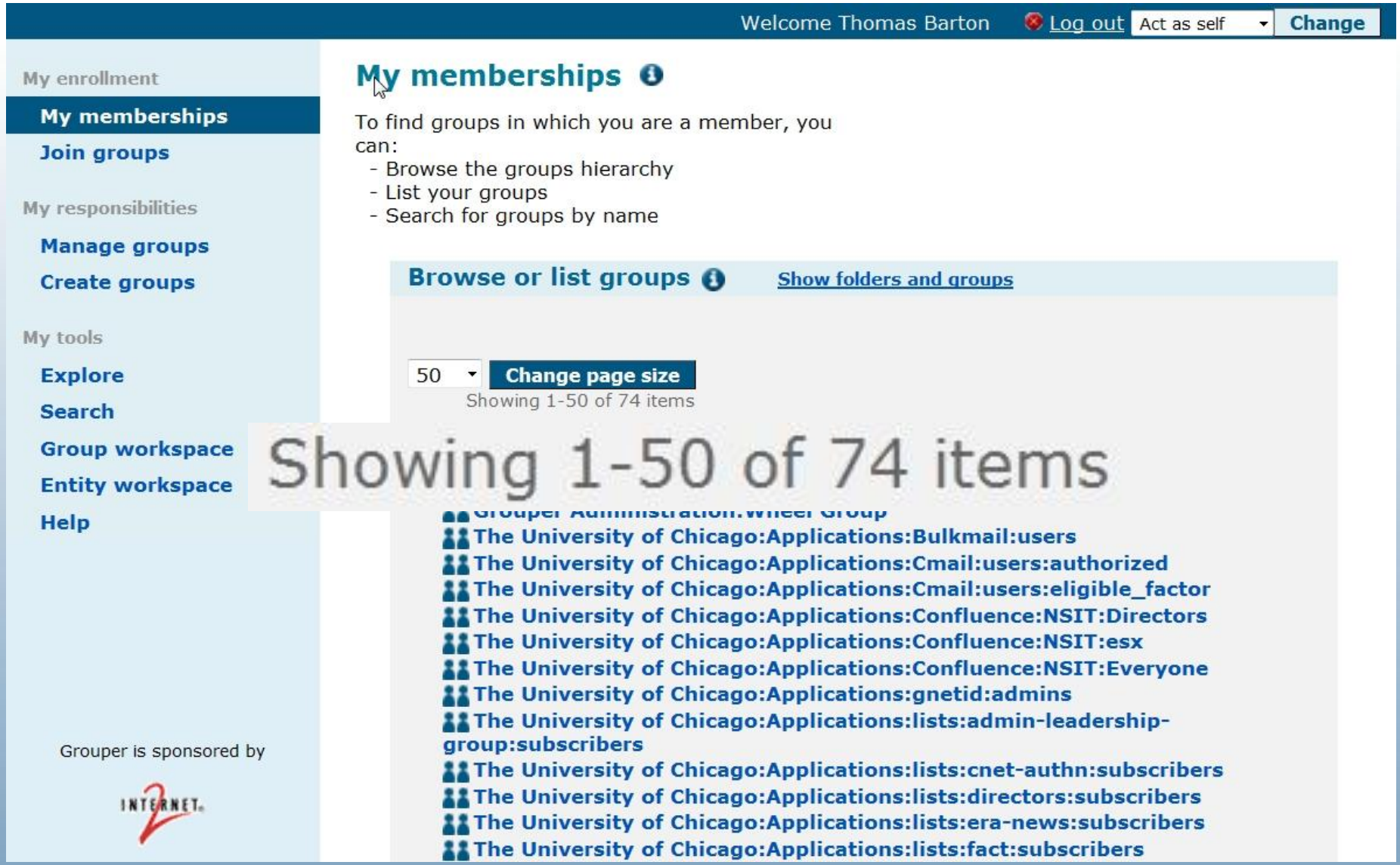
Grouper integration: Hooks



- 3rd party extension of key API events
- Veto & notify
- Group, Stem, Member, Membership, Composite, Field, GrouperSession, GroupType, GroupTypeTuple
  - preInsert, postInsert, postCommitInsert, preUpdate, postUpdate, postCommitUpdate, preDelete, postDelete, postCommitDelete
- addMember, removeMember
- LifecycleHooks

Grouper integration




Welcome Thomas Barton
Log out
Act as self
Change
My enrollment
My memberships
Join groups
My responsibilities
Manage groups
Create groups
My tools
Explore
Search
Group workspace
Entity workspace
Help
Grouper is sponsored by
My memberships
To find groups in which you are a member, you can:
- Browse the groups hierarchy
- List your groups
- Search for groups by name
Browse or list groups
Show folders and groups
50
Change page size
Showing 1-50 of 74 items
Showing 1-50 of 74 items
The University of Chicago:Applications:Bulkmail:users
The University of Chicago:Applications:Cmail:users:authorized
The University of Chicago:Applications:Cmail:users:eligible_factor
The University of Chicago:Applications:Confluence:NSIT:Directors
The University of Chicago:Applications:Confluence:NSIT:esx
The University of Chicago:Applications:Confluence:NSIT:Everyone
The University of Chicago:Applications:gnetid:admins
The University of Chicago:Applications:lists:admin-leadership-group:subscribers
The University of Chicago:Applications:lists:cnet-authn:subscribers
The University of Chicago:Applications:lists:directors:subscribers
The University of Chicago:Applications:lists:era-news:subscribers
The University of Chicago:Applications:lists:fact:subscribers

Memberships are attributes

dn: uid=tbarton,ou=people,dc=uchicago,dc=edu
ucismemberof: uc:org:nsit:integration:techag
ucismemberof: uc:org:nsit:srdirs
ucismemberof: uc:org:nsit:integration:iteco:wr
ucismemberof: uc:applications:confluence:NSIT:esx
ucismemberof: uc:org:nsit:integration:iteco:rd

uc:reference:affiliations:effective:staff

ucismemberof: uc:org:library:gnet:admins
ucismemberof: uc:applications:gnetid:admins
ucismemberof: uc:applications:wireless:authorized
ucismemberof: uc:applications:cmail:users:authorized
ucismemberof: uc:reference:affiliations:effective:staff

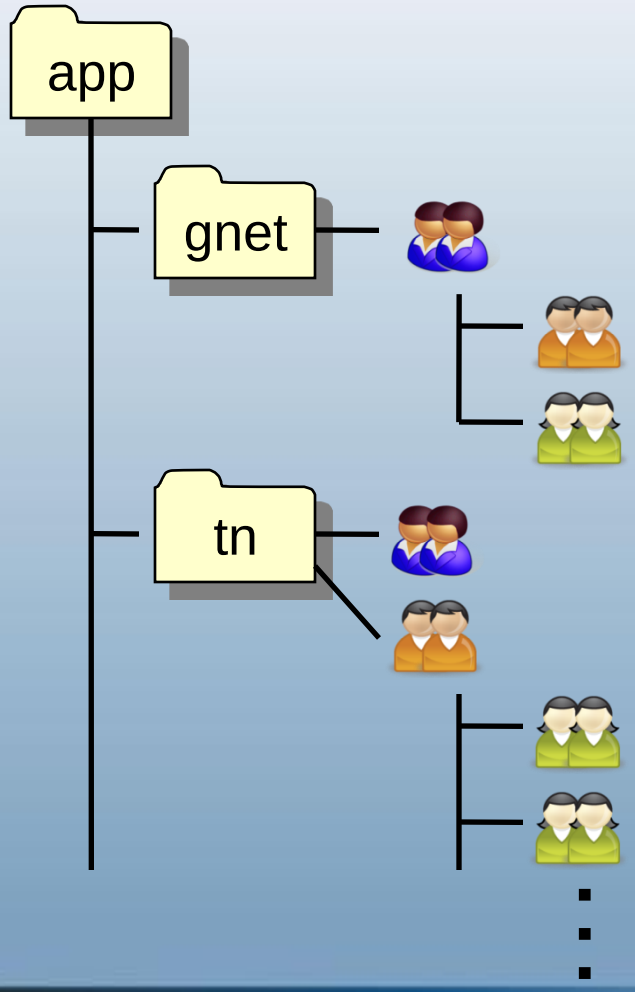
Examples

- U Chicago's simple delegation examples
- Brown University & course groups
- French national portal for HE & SE
- SURFnet's "services-spanning group management"
- NIH's Cancer BioInformatics Grid

Application-specific delegation: U Chicago

- Different people must manage different groups that have the same access
- Examples:
  - Guest network ID management
  - Termination notifications

Application-specific delegation: U Chicago



GNet Admin role

- Faculty Club GNet Admins
- Library GNet Admins

TN writers

TN read role

- Financials TN readers
- SIS TN readers

Brown's Course Group Schema

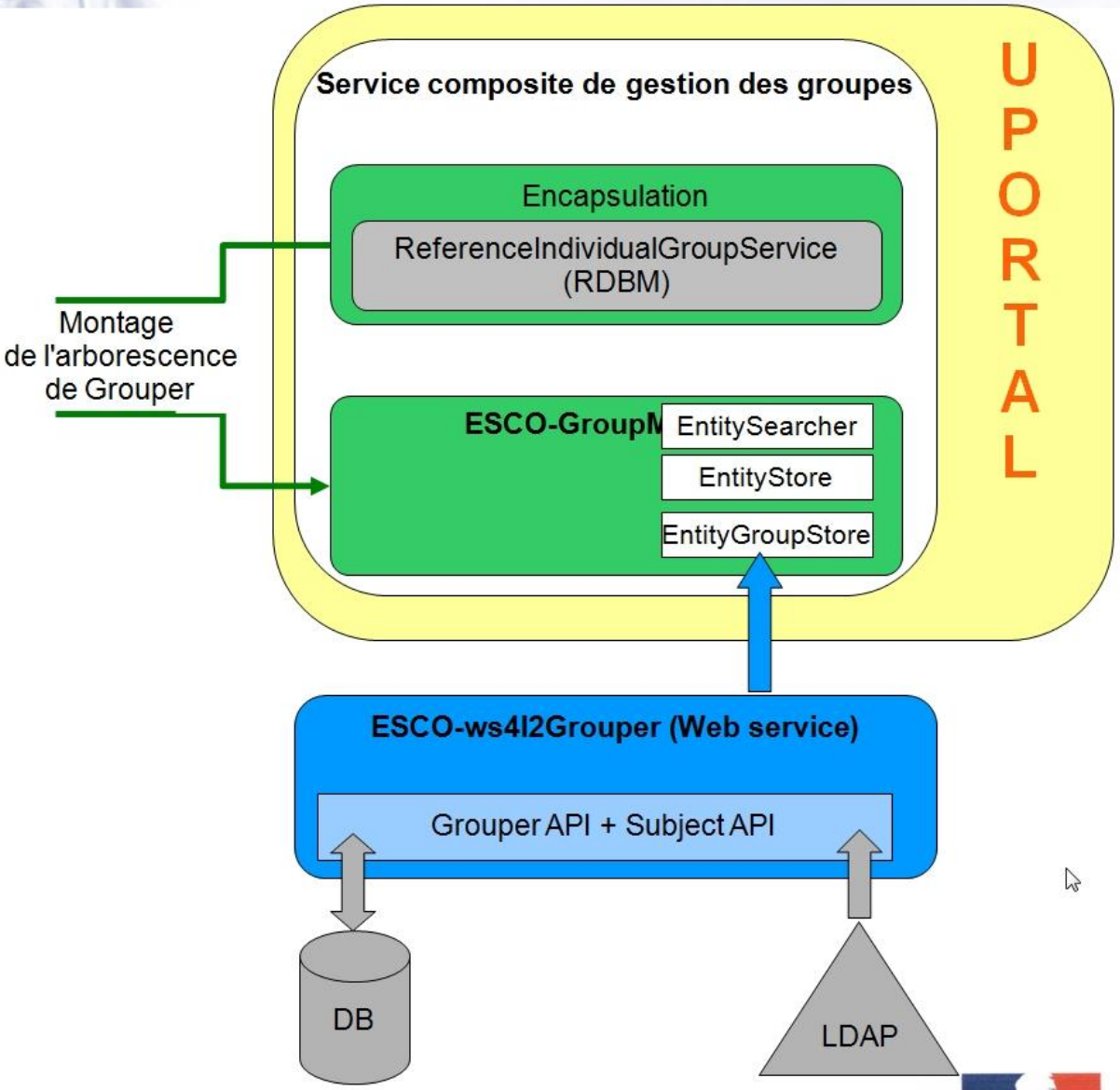
- Course : [Subject] : [Number] : [Term] : [Section]
  - All
  - Administrator
    - Instructor (Provisioned)
    - TeachingAssistant
    - Manager
  - Contributor
    - ContentDeveloper
    - Mentor
  - Learner
    - Student (Provisioned)
    - Auditor
    - Vagabond
- Schema is flattened to provision LDAP
  - 12 groups per course provision hasMember attribute in Groups OU
  - Person objects get isMemberOf pointers to groups

Brown's Application Role Mapping

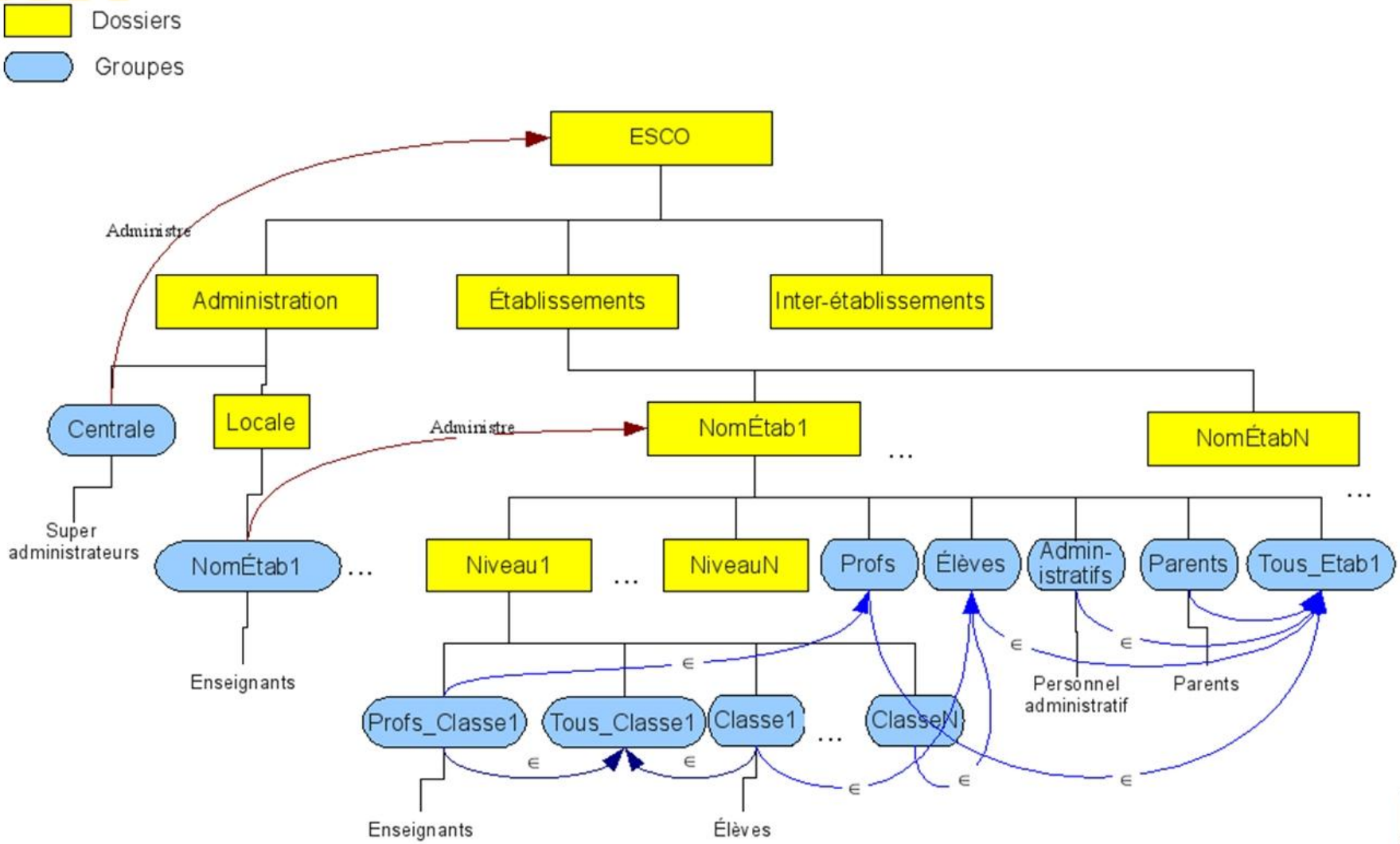
MACE Grouper Course Groups	iTunes	Majordomo	Confluence	WebCT
All		Recipient list, Discussion Sender	Can Use	
Administrator	Instructor	Broadcast Sender	Space Admin	
Instructors (provisioned)				Instructor
Managers				
TAs				TA and Designer
Contributor	Instructor		Space Admin	
Content Developers				Designer
Mentors				
Learner	Student			
Auditors				Auditor
Students (provisioned, read only)				Student
Vagabonds				Auditor
Other, outside MACE Grouper	Super Admin			Super Admin(s)

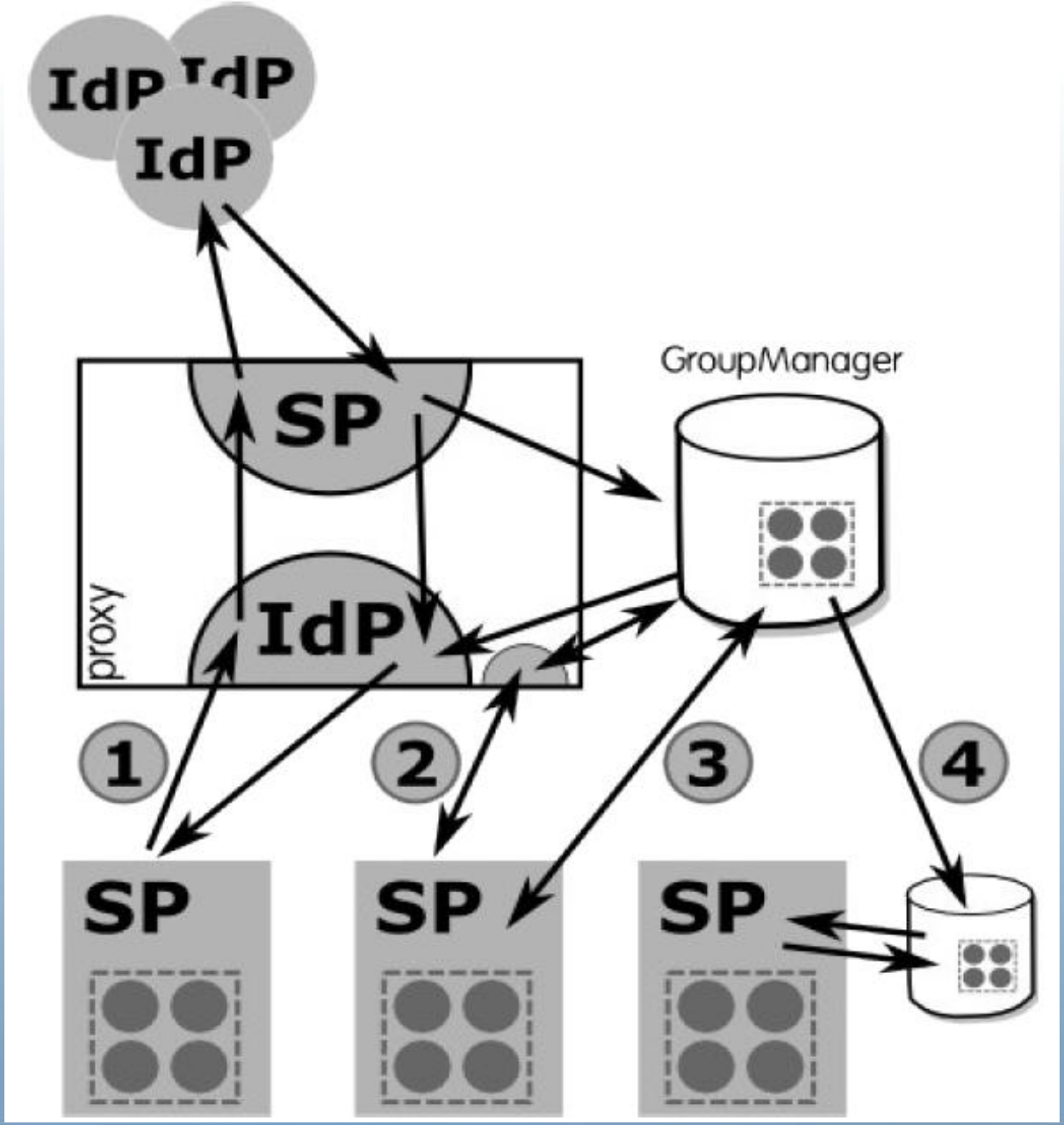
INTERNET2

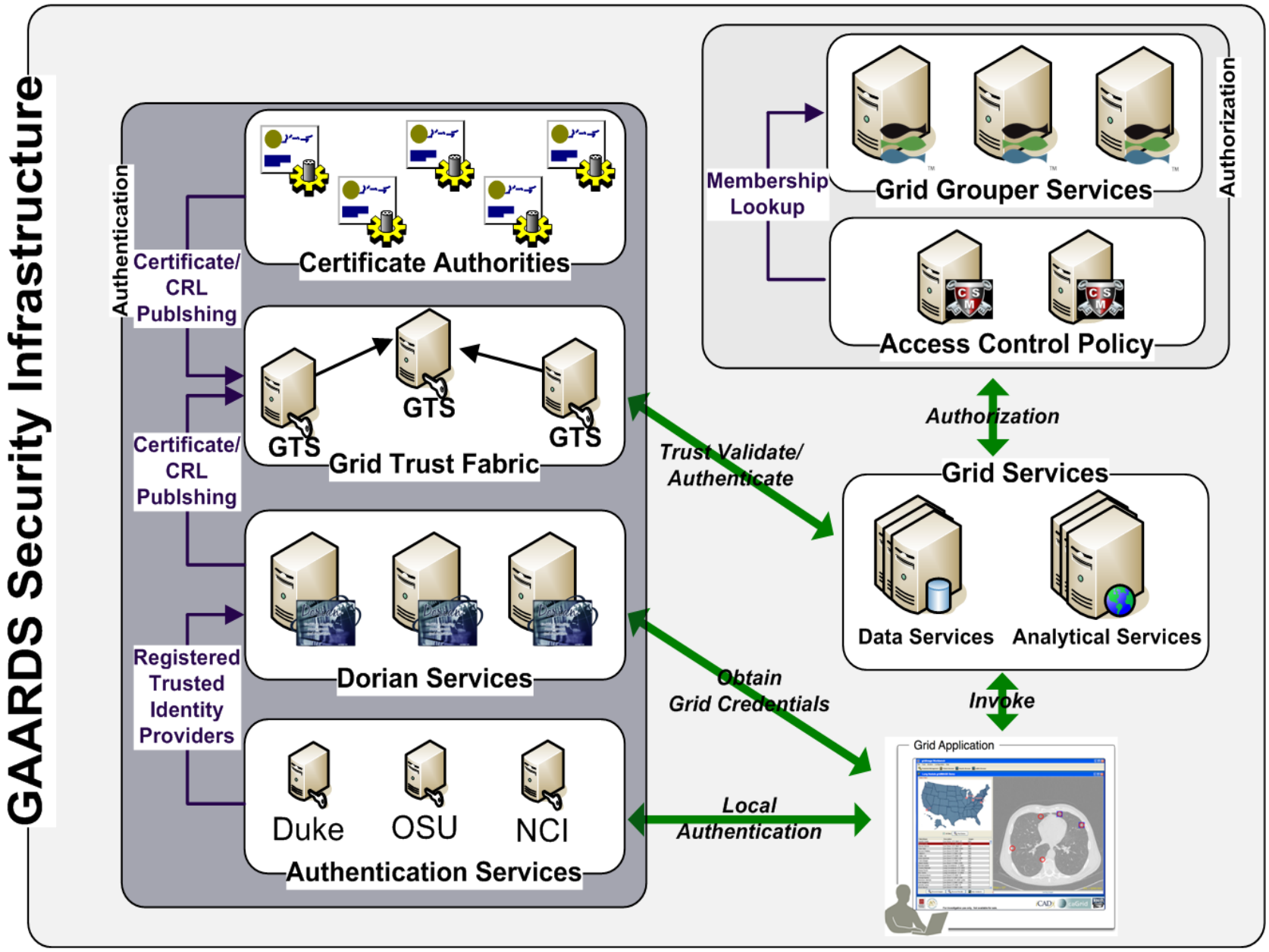
Grouper : accès aux groupes pour uPortal



Grouper : Extrait de l'arborescence à créer




IdP
IdP
IdP
SP
GroupManager
proxy
IdP
1
2
3
4
SP
SP
SP


GAARDS Security Infrastructure
Authentication
Certificate/
CRL
Publshing
Certificate Authorities
Certificate/
CRL
Publshing
GTS
GTS
GTS
Grid Trust Fabric
Registered
Trusted
Identity
Providers
Dorian Services
Duke
OSU
NCI
Authentication Services
Trust Validate/
Authenticate
Obtain
Grid Credentials
Local
Authentication
Membership
Lookup
Grid Grouper Services
Access Control Policy
Authorization
Authorization
Grid Services
Data Services
Analytical Services
Invoke
Grid Application
caGrid

Grouper roadmap

- Current version is 1.4.1
- v1.5.0
  - Attribute framework
  - Namespace transition support
  - Audit & notification: phase I
  - Ldappc enhancements
- To come
  - Completion of audit & notification
  - Access management interfaces & tools

www.internet2.edu

grouper.internet2.edu