

Groups, Roles, and Privileges

Tom Barton
University of Chicago

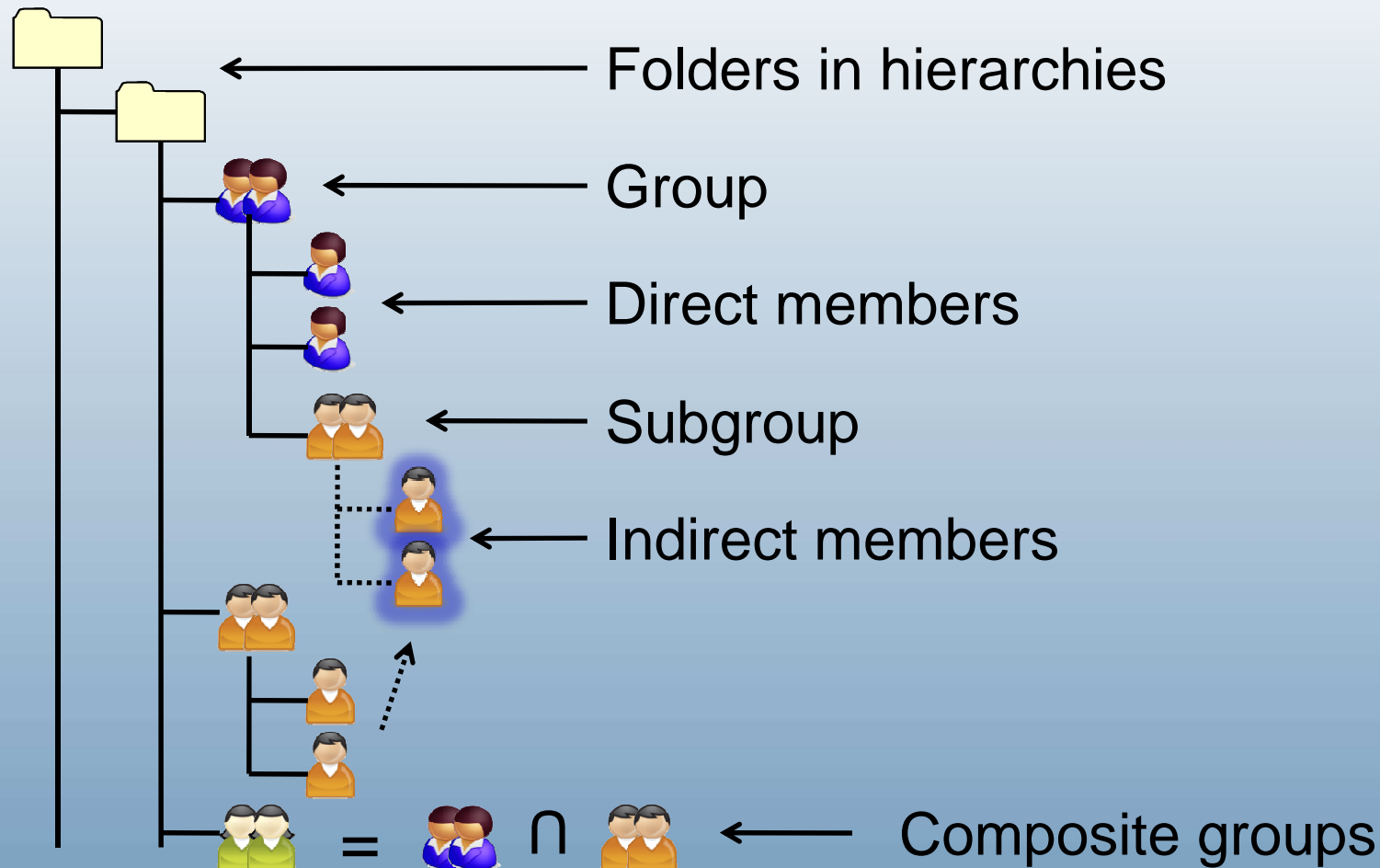
Outline

- Why use an access management tool?
- Essential concepts by way of Grouper
- Implementation examples

Why use an access management tool?

- Lower cost by factoring access management out of individual applications
- Simplify & make consistent by using the same group or role in many places
- Let the right people manage access, directly, with no IT required
- See who can access what, in one place
- Reduce risk by automatically removing access

Grouper: core concepts



Security & delegation in Grouper

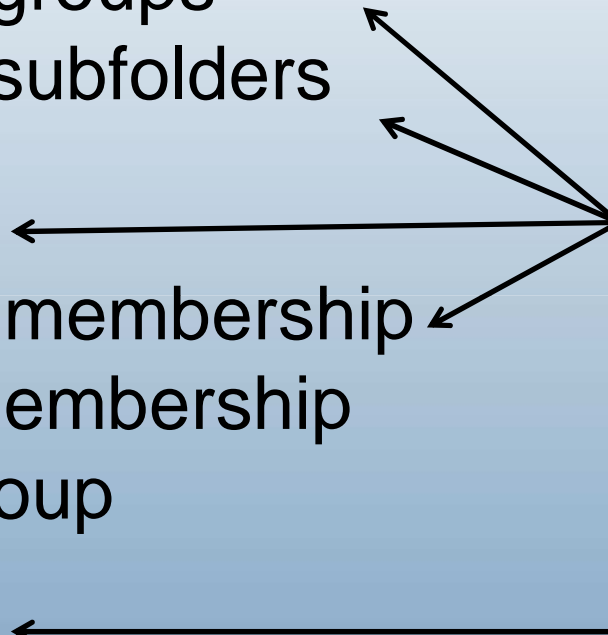


- Create groups
- Create subfolders



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

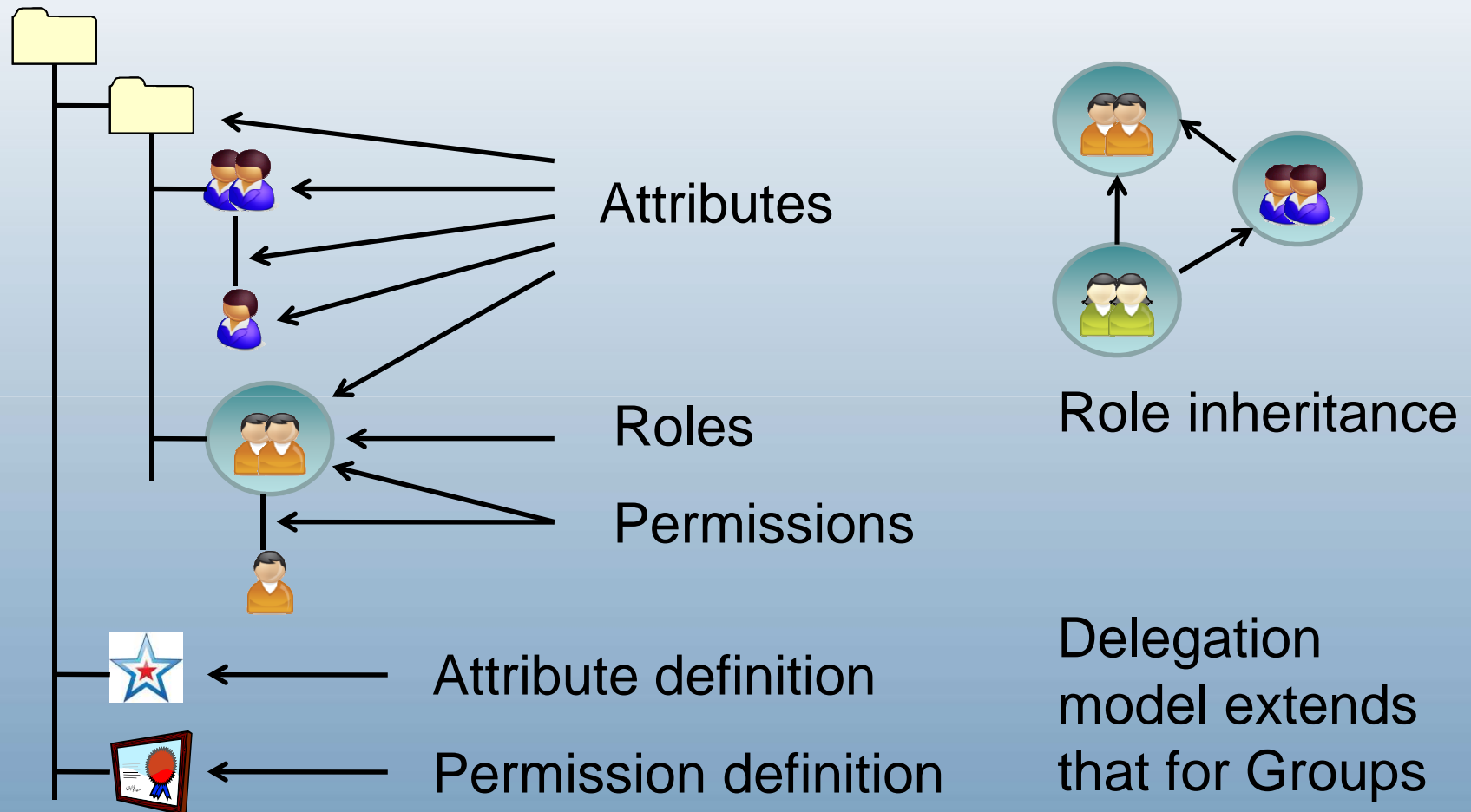
Delegation



What's in a Grouper group?

- Folder name
- Names – one short, one display
- GUID – globally unique identifier
- Description
- Members – opaque Subject references
- Privilegees – opaque Subject references
- Operational attributes
- Site-defined attributes

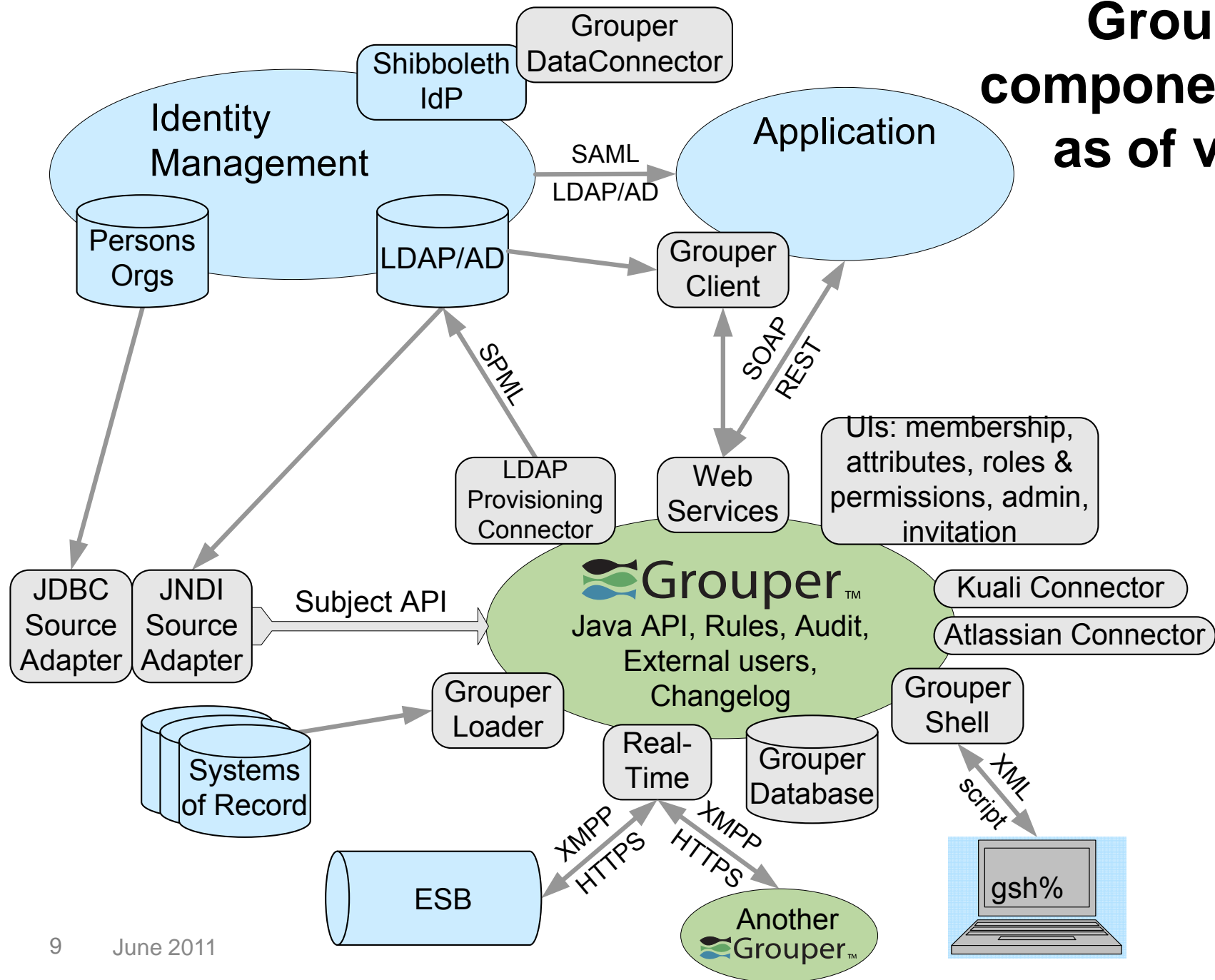
Beyond groups



Access management lifecycle support

- Membership start & end times (optional)
- Move or copy folders, groups, etc
- User audit
- Point in time audit
- Rules

Grouper components as of v2.0



Access management is a process: making authZ more than authN

- Start out with a single LDAP attribute
 - affiliation
- Get central IT out of the loop
 - distributed management
 - exceptions
 - departmental apps
- Increase integration of access management
 - Direct app integration with web services
 - ESB/SOA, REST/SOAP
 - Roles & privileges to support larger, deeper apps

EXAMPLES

Tom Barton's UChicago group memberships

My enrollment

My memberships

Join groups

My responsibilities

Manage groups

Create groups

My tools

Explore

Search

Group workspace

Entity workspace

Help

Welcome Thomas Barton

Log out

Act as self

Change

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

Showing 1-50 of 74 items

Showing 1-50 of 74 items

Grouper Administration:can_impersonate

Grouper Administration:provisioner admins

Grouper Administration:Wheel Group

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

Grouper is sponsored by



12

June 2011



Memberships become LDAP 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

ucIsMemberOf :
uc:applications:vpn:authorized

ucismemberof: uc:org:library:gnet:admins

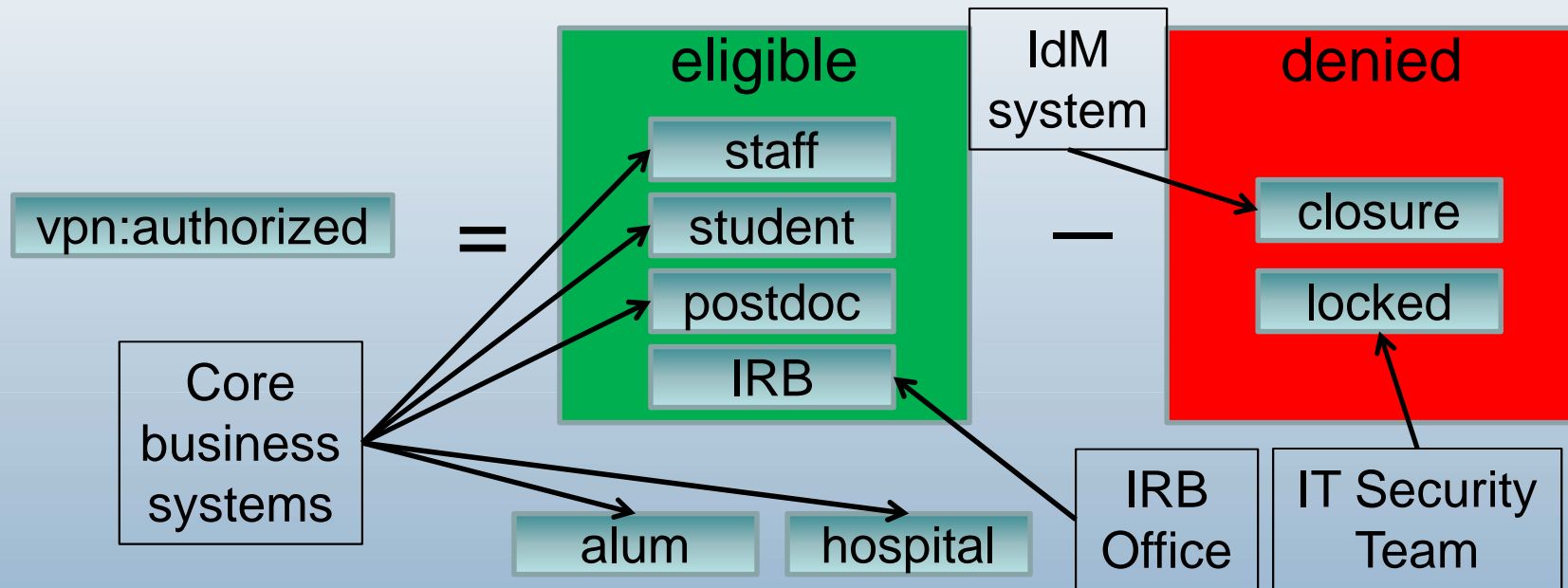
ucismemberof: uc:applications:gnetid:admins

ucismemberof: uc:applications:wireless:authorized

ucismemberof: uc:applications:email:users:authorized

ucismemberof: uc:reference:affiliations:effective:staff

UChicago VPN simple delegation example

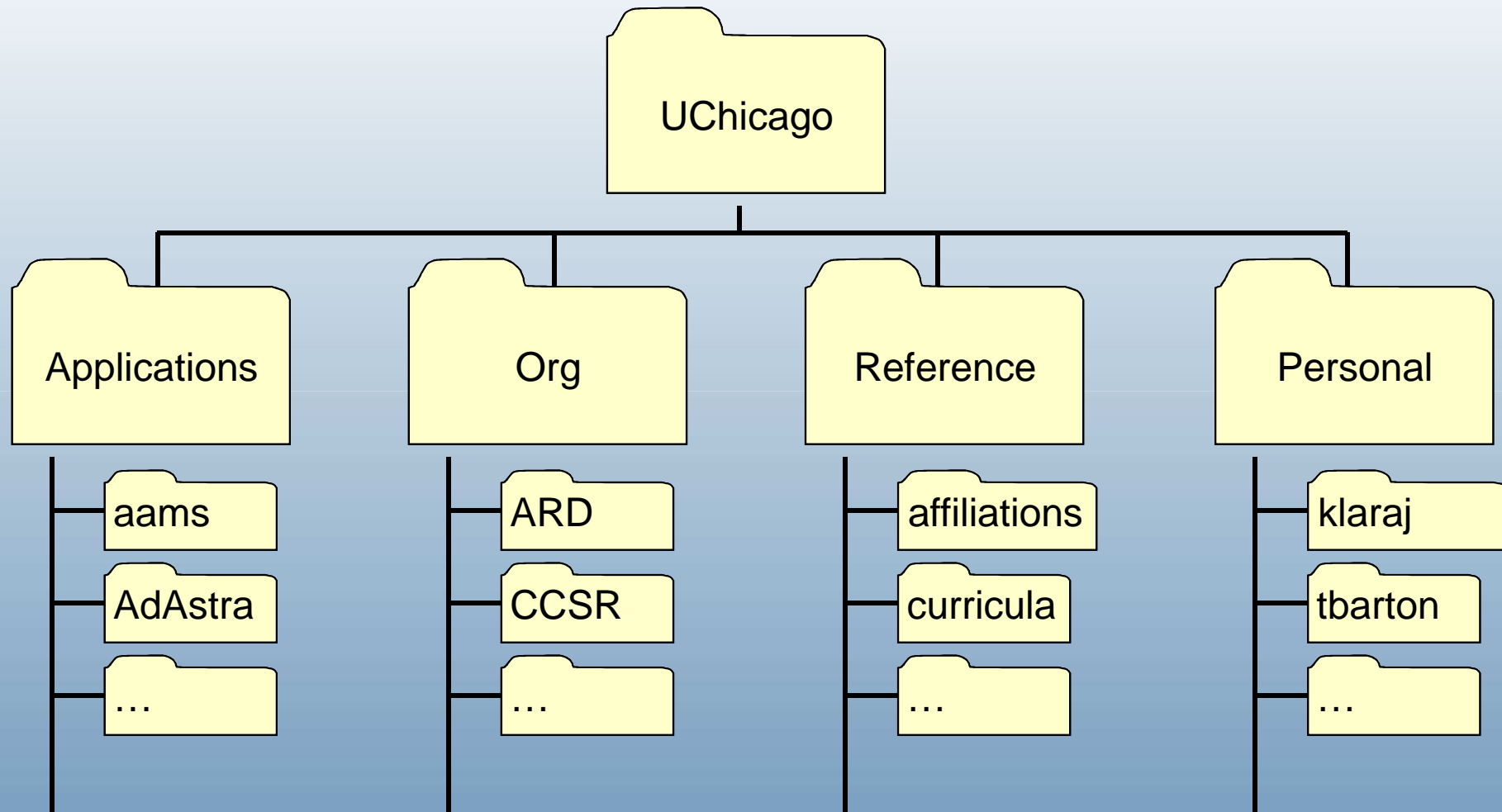


Different groups, different authorities.
VPN only uses “vpn:authorized”.

UChicago applications managed by Grouper, so far

aams	grouper	Service Now
Ad Astra	im	shibboleth
Bulkmail	isx	Statements portlet
Business Objects Enterprise	IT Ecosystem	SVN
Chalk	Lab School	tank
CityRyde	LDAP	UC Groups
Cmail	lists	unifiedcomm
cnet	Mail Forwarding	uPoV Monitor
Confluence	Microsoft Exchange	versions
Directory Administration	modem pool	voip
dmca	myUChicago	vpn
Facilities SIMS	online directory	web hosting
gnetid	password expiration	webproxy
	rt	Webshare
		webpace
		wireless

Distributed management: keep it straight



Northern Arizona's Add a Group Portlet

Add a Group

Step 1 - Name and describe your group. Give your group a name and description.

☒ Organizational Group ☐ Personal Group

Group Name: ITS - SIA - test group
(58 chars)

Organization ☒ Area or Team ☐ User-defined name
☐ No Area or Team

ITS-SIA-test group

Description: test
(100 chars)

Step 2 - Add owners. Enter the people or groups you want to be owners of your group.

Owner is System: ☐ NOTE: No other owners allowed.

Owners - People: Enter IDs... Search for People...

Owners - Groups: Enter Group Names... Search for Groups...

Step 3 - Add members. You may add people and other groups to your group.

Members Group Filter: ☐ Create special filter group

Members - People: Enter IDs... Search for People...

Members - Groups: Enter Group Names... Search for Groups...

Step 4 - Exclude members (optional). You may exclude selected people and sub-groups from the members you added in Step 3. They will not be members of your group.

Excluded People: Enter IDs... Search for People...

Excluded Groups: Enter Group Names... Search for Groups...

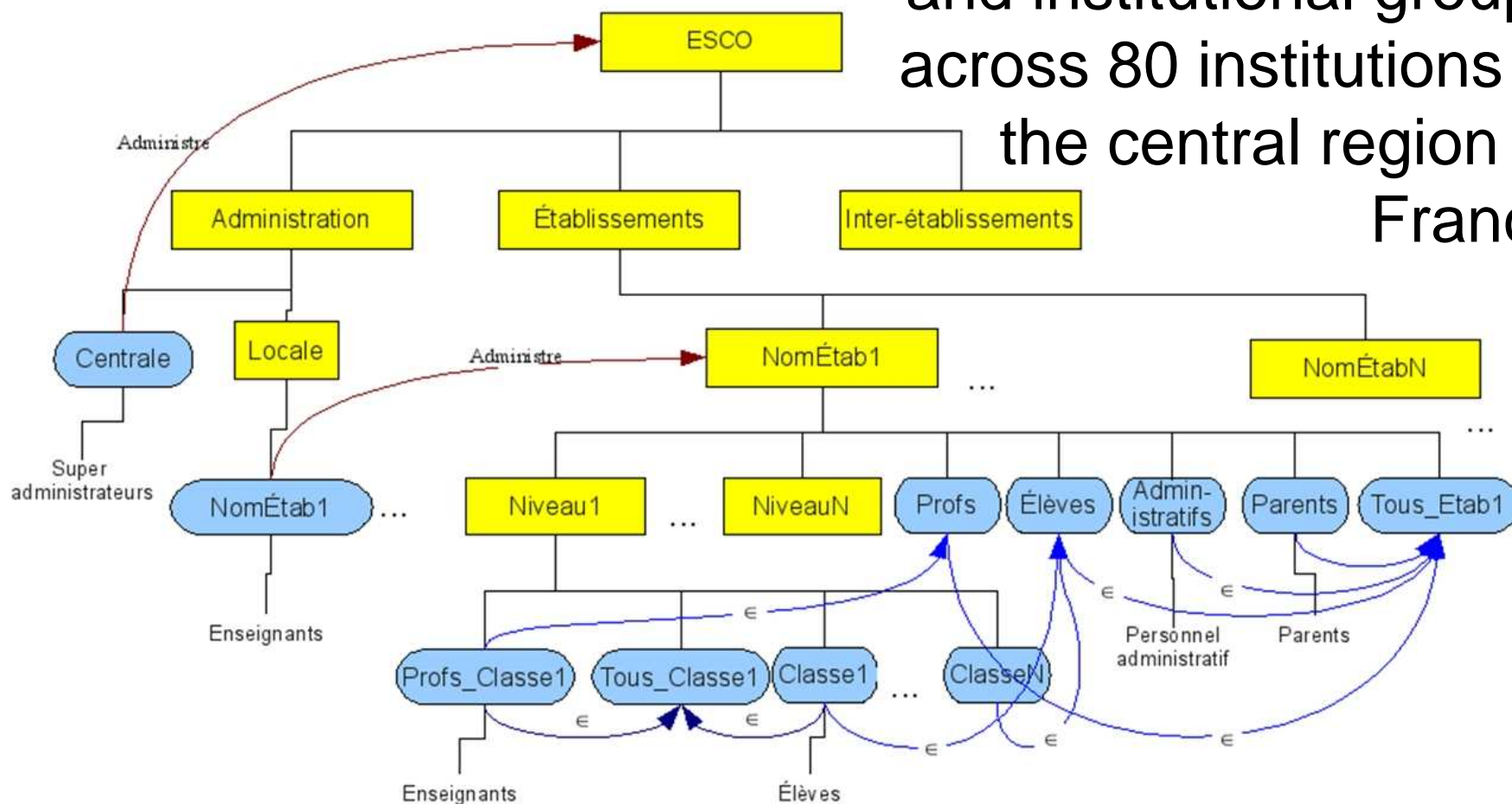
Step 5 - Add your group. Review the information you have entered, especially the group name, since it cannot be changed once the group is added. Then click the *Add Group* button to add this group.

Add Group Reset Cancel

Grouper : Extrait de l'arborescence à créer



Managing instructional and institutional groups across 80 institutions in the central region of France





① SURFfederatie SAML

+



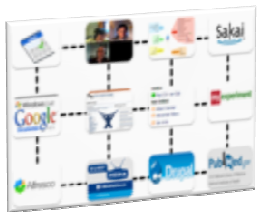
① SURFteams (grouper)

+



② OpenSocial

+



① Collaboration tools

SURF

=

CONEXT



SURFnet's
national scale
collaboration
platform

Thanks!

Further questions?

Infosheets, mail lists, wiki, downloads, etc:
www.internet2.edu/grouper

Grouper demo server:
<https://grouperdemo.internet2.edu/>