



Introduction to Grouper

Tom Barton
University of Chicago

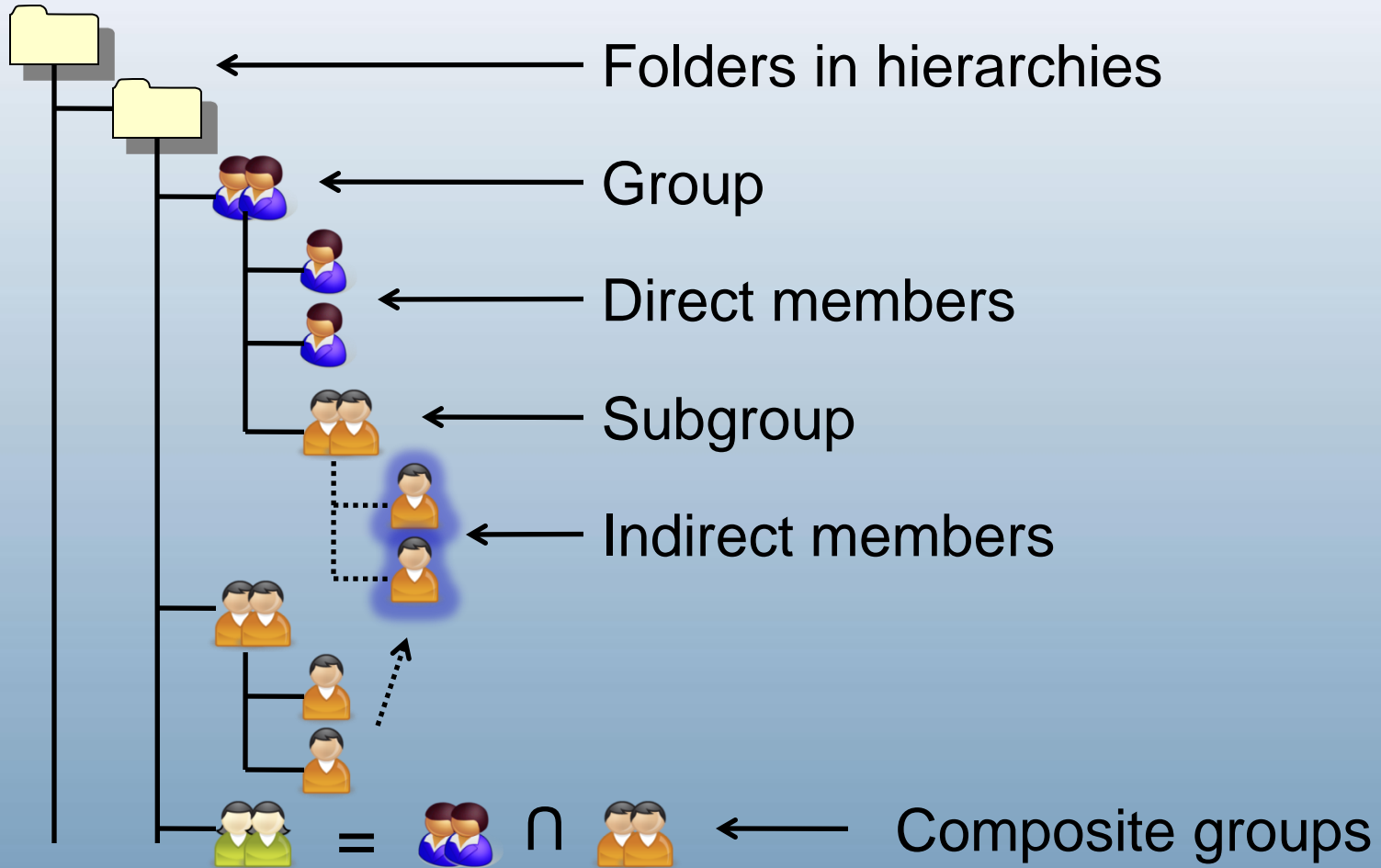
Outline

- Why use an access management tool?
- Grouper basics
- Implementation examples
- Grouper roadmap

Why?

- Lower cost by factoring access management out of individual applications
- Simplify & make consistent by using 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

Groupware: core concepts



Security & delegation

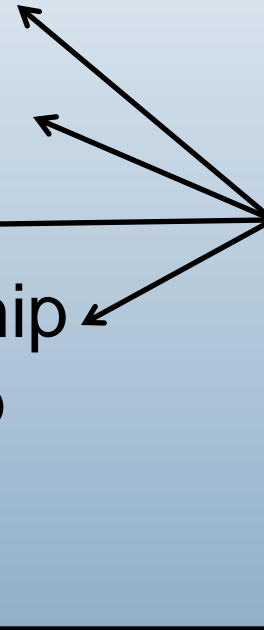


- Create groups
- Create subfolders



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

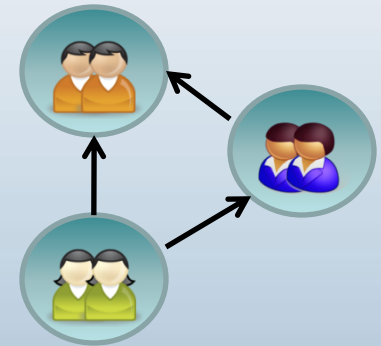
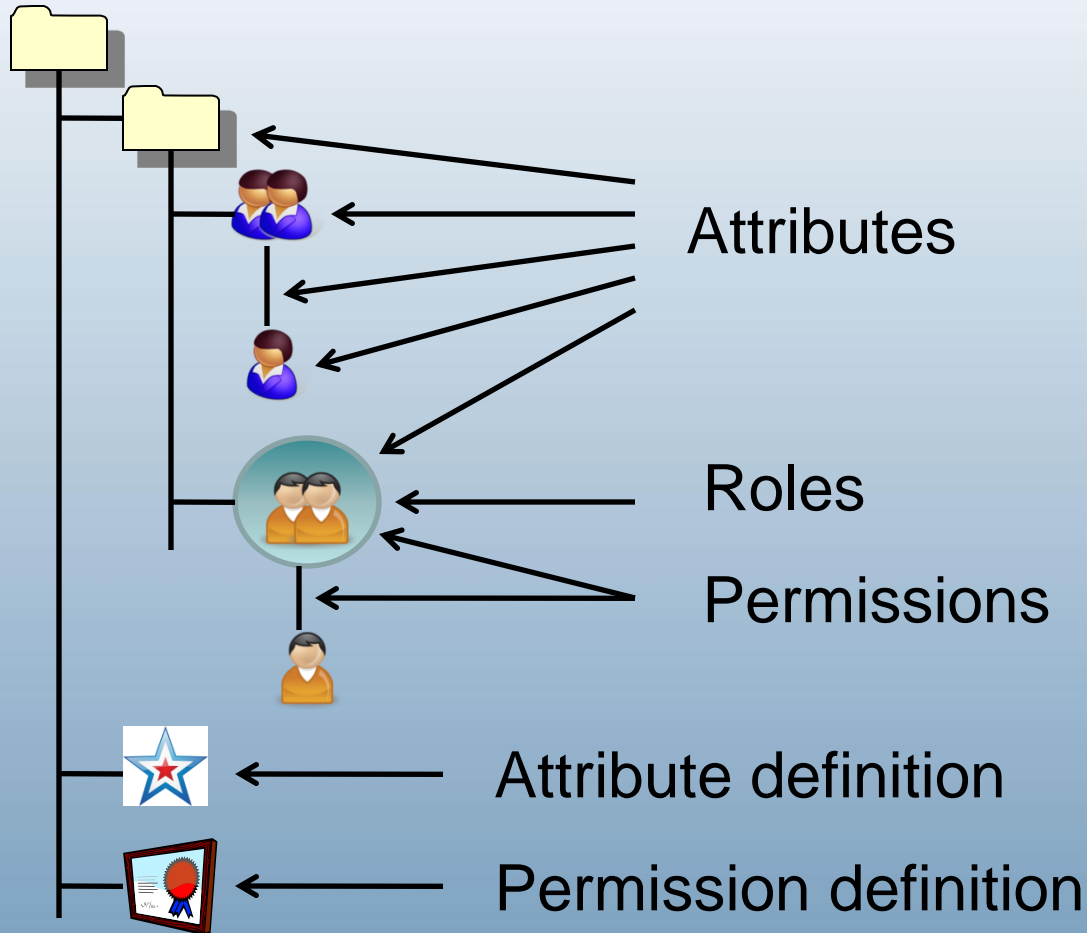
Delegation



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



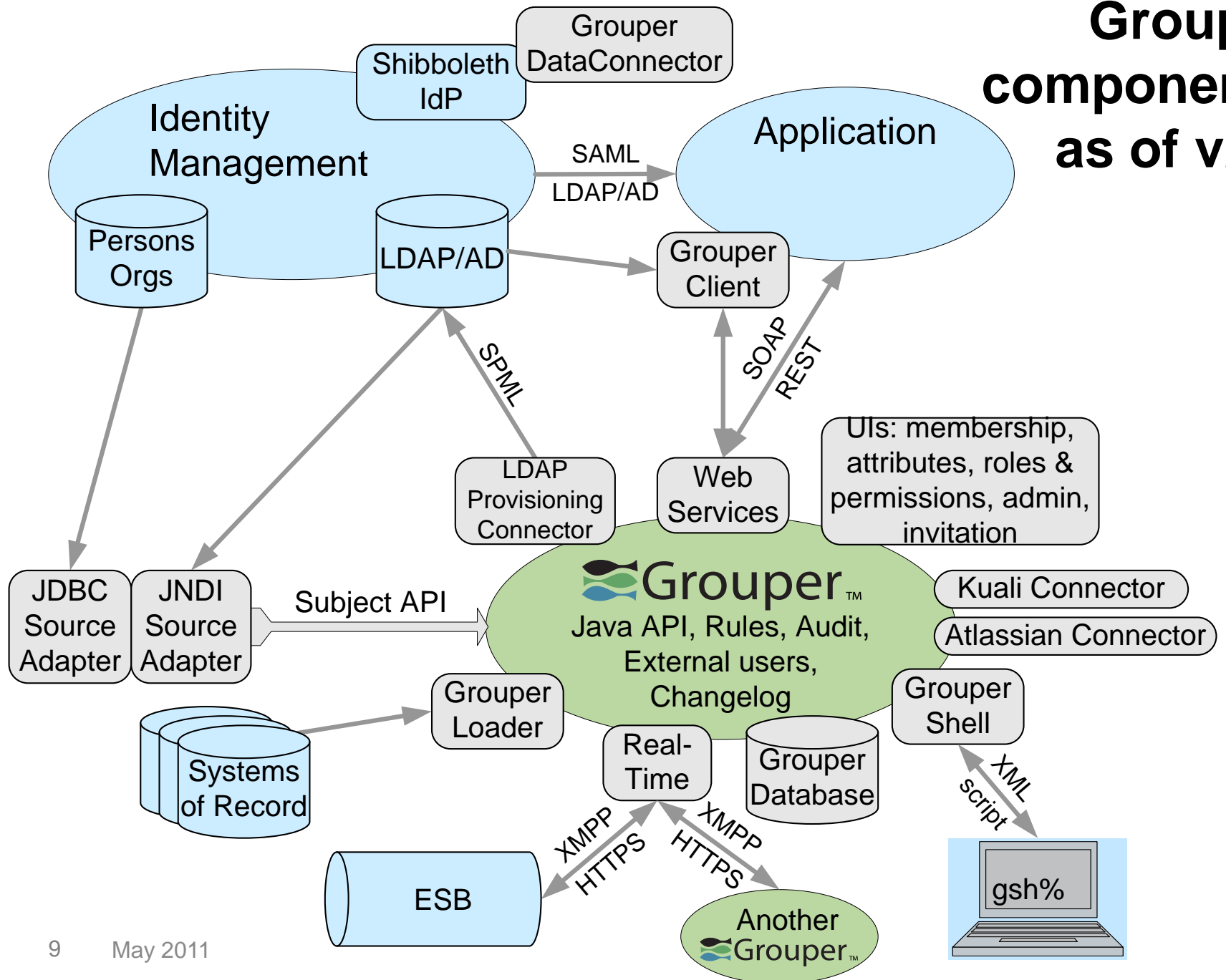
Role inheritance

Delegation model extends that for 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



EXAMPLES

Tom Barton's UChicago group memberships

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](#)

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



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

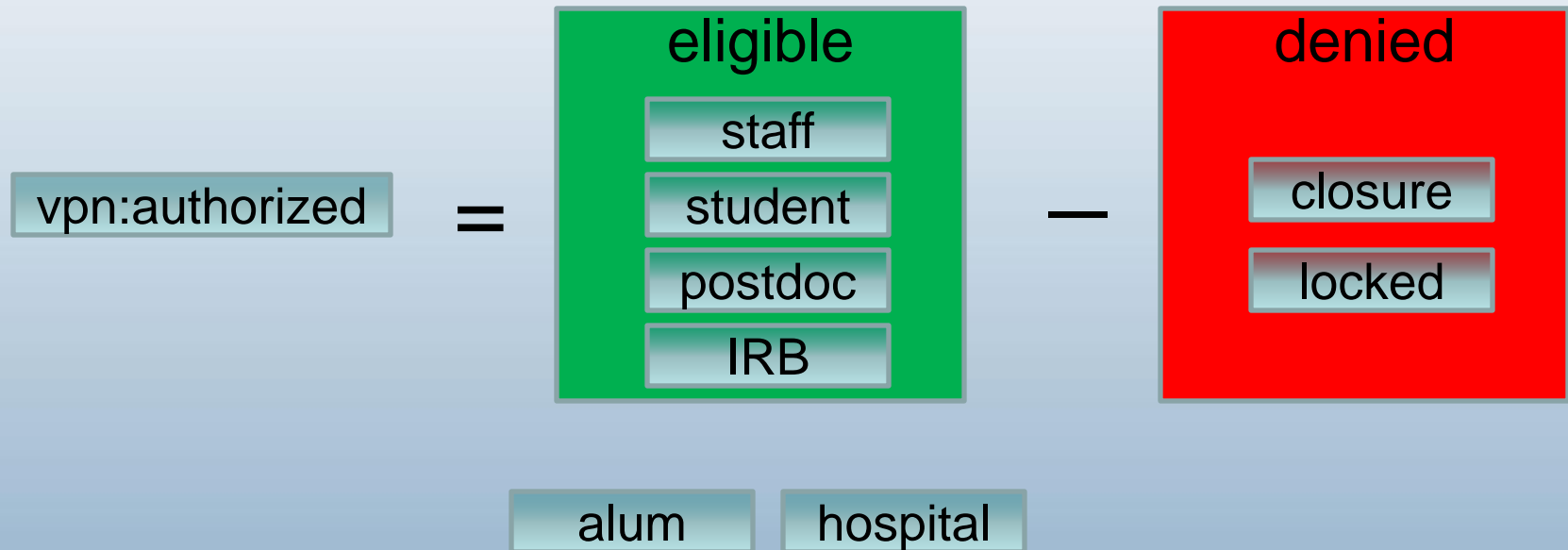
ucismemberof: uc:applications:gnetid:admins

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

Ad Astra

Bulkmail

Business Objects Enterprise

Chalk

CityRyde

Cmail

cnet

Confluence

Directory Administration

dmca

Facilities SIMS

gnetid

grouper

im

isx

IT Ecosystem

Lab School

LDAP

lists

Mail Forwarding

Microsoft Exchange

modem pool

myUChicago

online directory

password expiration

rt

Service Now

shibboleth

Statements portlet

SVN

tank

UC Groups

unifiedcomm

uPoV Monitor

versions

voip

vpn

web hosting

webproxy

Webshare

webspace

wireless

Add a Group

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

Organizational Group Personal Group

Group Name: - -
(58 chars)

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

ITS-SIA-test group

Description:
(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:

Owners - Groups:

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

Members Group Filter: Create special filter group

Members - People:

Members - 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:

Excluded Groups:

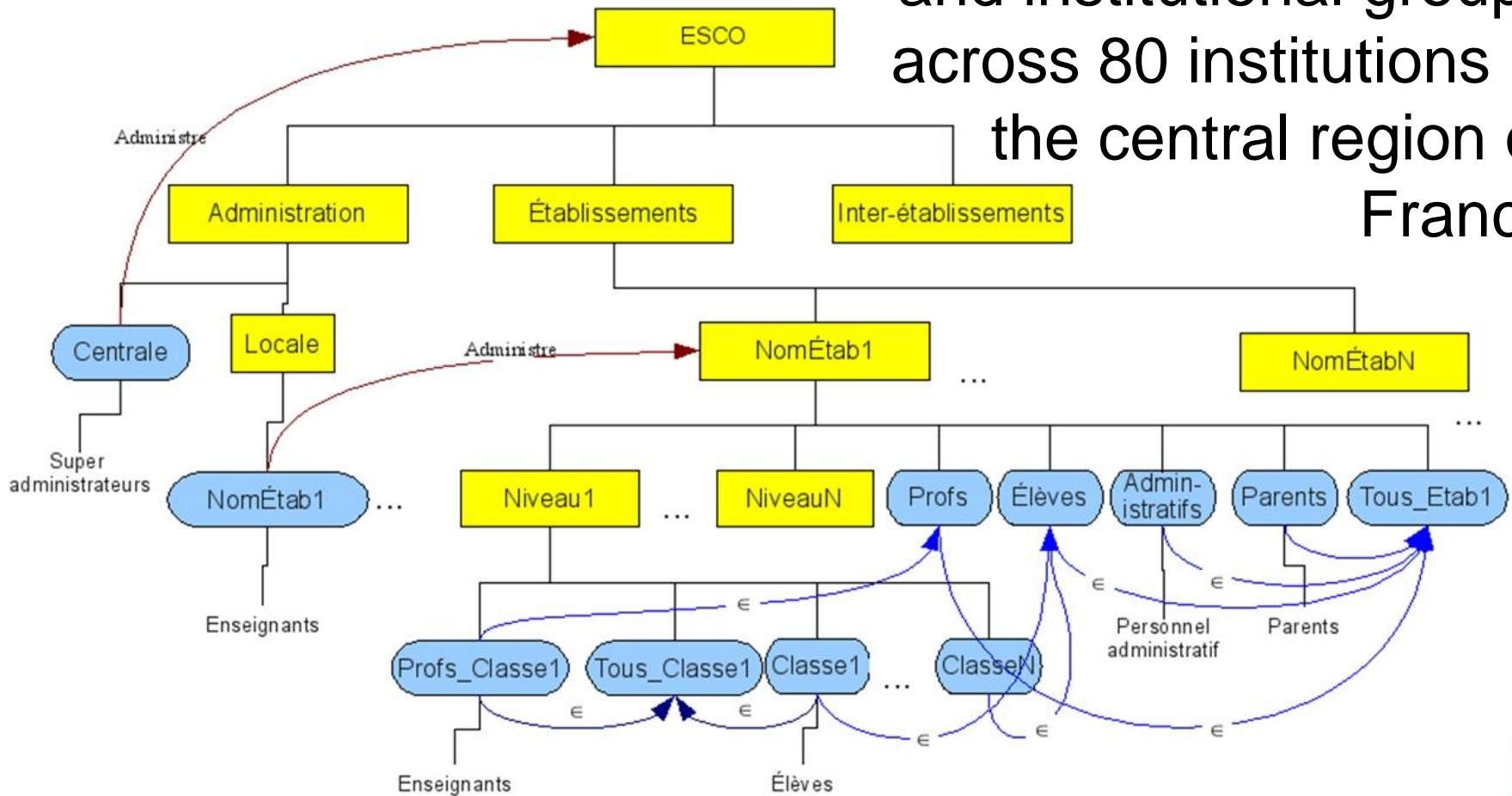
Step 5 - Add your group. Review the information you have entered, especially the group name, since it cannot be changed once the group is added. Then click the *Add Group* button to add this group.

Northern Arizona's Add a Group Portlet

Grouper : Extrait de l'arborescence à créer

- Dossiers
- Groupes

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



May 2011

ESUP Days - 03 février 2009



① SURFfederatie SAML

+



① SURFteams (grouper)

+



② OpenSocial

+



① Collaboration tools

SURF

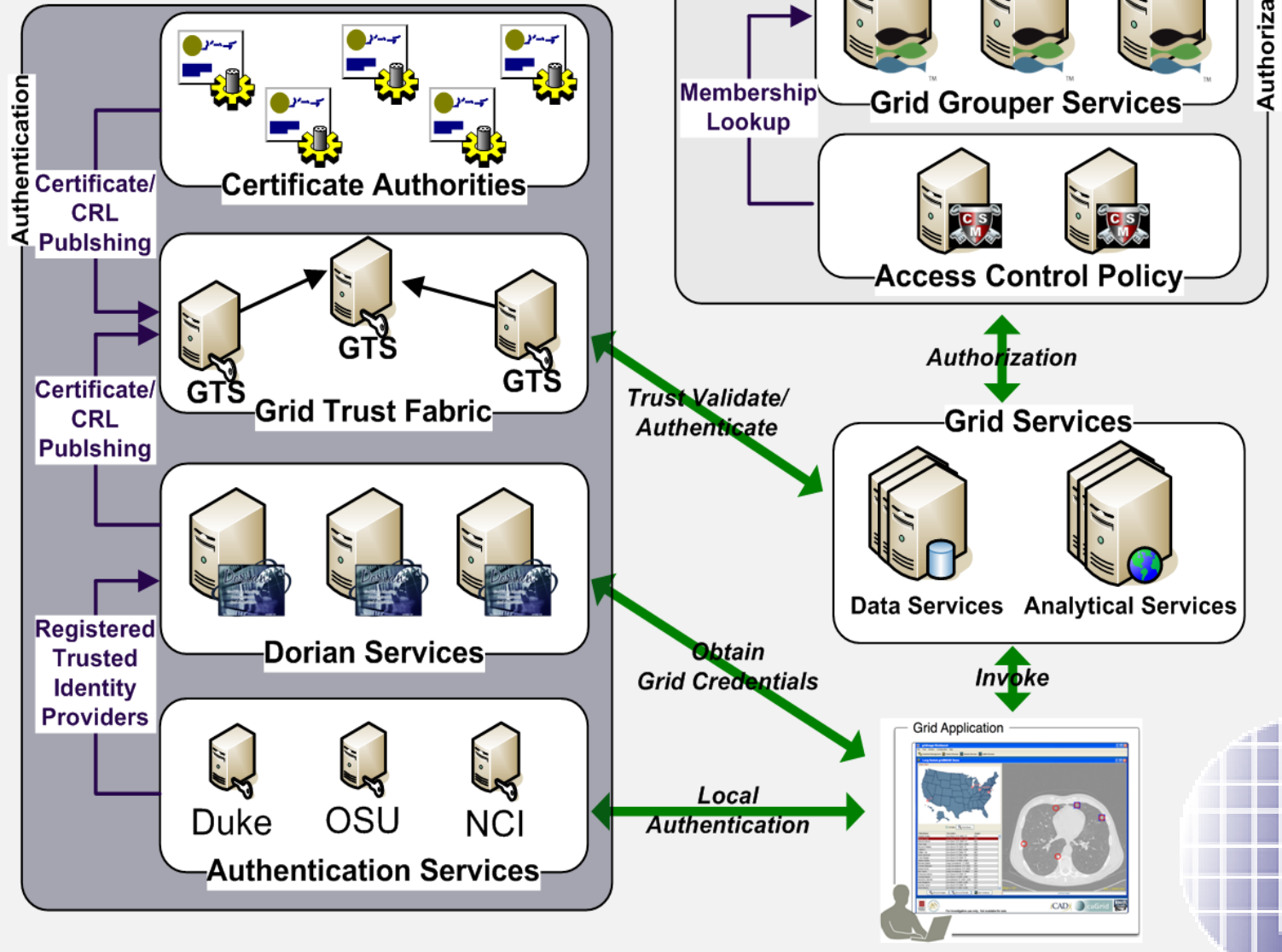
=

CONEXT



SURFnet's
national scale
collaboration
platform

GAARDS Security Infrastructure



Coming soon: managing access to research data sets



globus online
Reliable File Transfer. No IT Required.

Sign Up

Sign In

Reliable, high-performance, secure file transfer.
Move files fast. No IT required.

+ WATCH A VIDEO

Globus Online in a nutshell

> GET STARTED

Sign up and get moving

Globus Online makes robust file transfer capabilities, traditionally available only on expensive, special-purpose software systems, accessible to everyone.

Learn more

Contributing organizations, so far

- Brown University
- California Polytech
- Cardiff University
- Cornell University
- Duke University
- Freie Universität Berlin
- GIP RECIA
- LIGO
- Newcastle University
- Northern Arizona University
- Ohio State University
- SURFnet
- University of Bristol
- University of Chicago
- University of Kansas
- University of Memphis
- University of Pennsylvania
- University of Washington
- University of West Bohemia

Grouper roadmap

Current: v1.6.3	v2.0: August 2011	v2.1: 1Q2012
2.0	Point-in-time audit	
	Attribute, Role & Permissions UI	
	Rules	
	Atlassian connector	
	Real-time & incremental LDAP provisioning	
	Member search & sort	
	External Subjects	
	Federated Groupers	
2.1	uPortal integration	
	Grouper Web Service high availability	
	Dynamic groups from LDAP	
	Unix GID management	

Thanks!

Further questions?

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

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