Introduction to Grouper

Tom Barton
University of Chicago

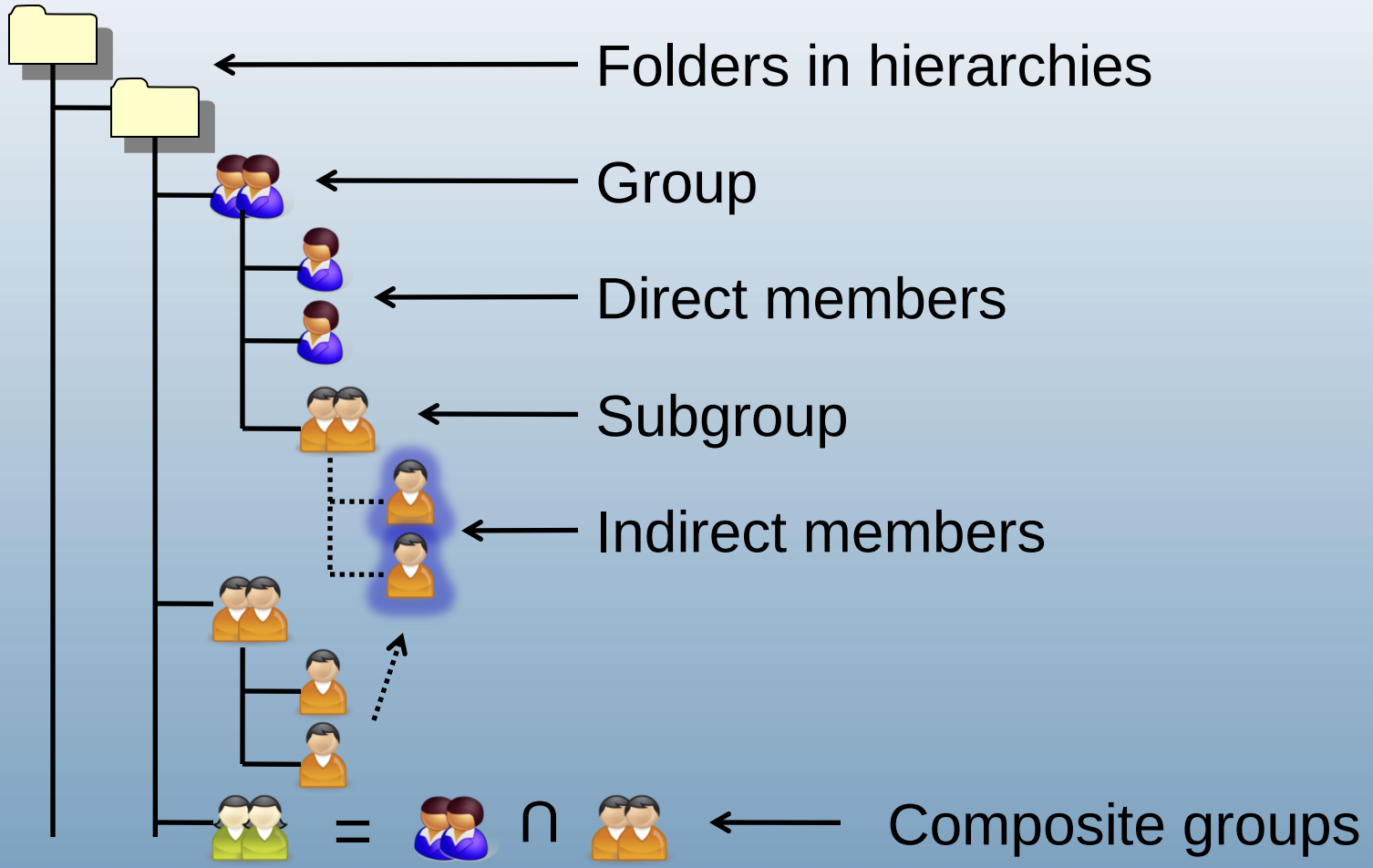
Outline

- 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

Grouper: core concepts



Security & delegation

- Create groups
- Create subfolders

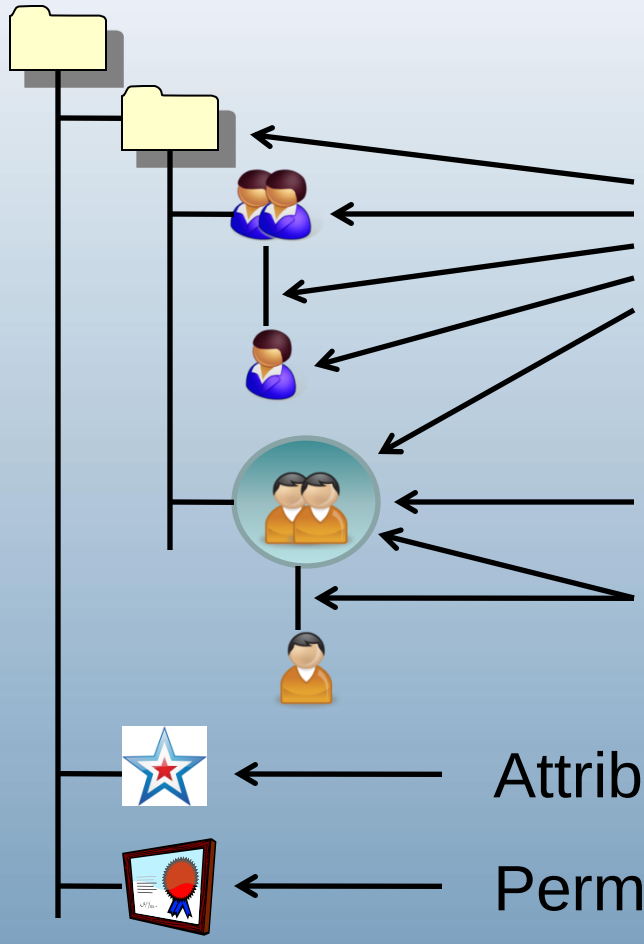
- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

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



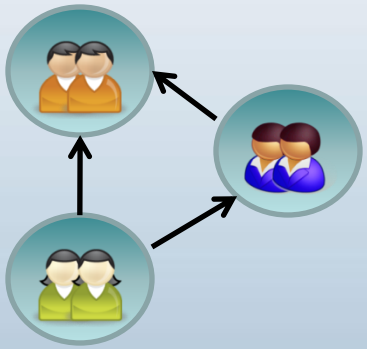
Attributes

Roles

Permissions

Attribute definition

Permission definition



Role inheritance

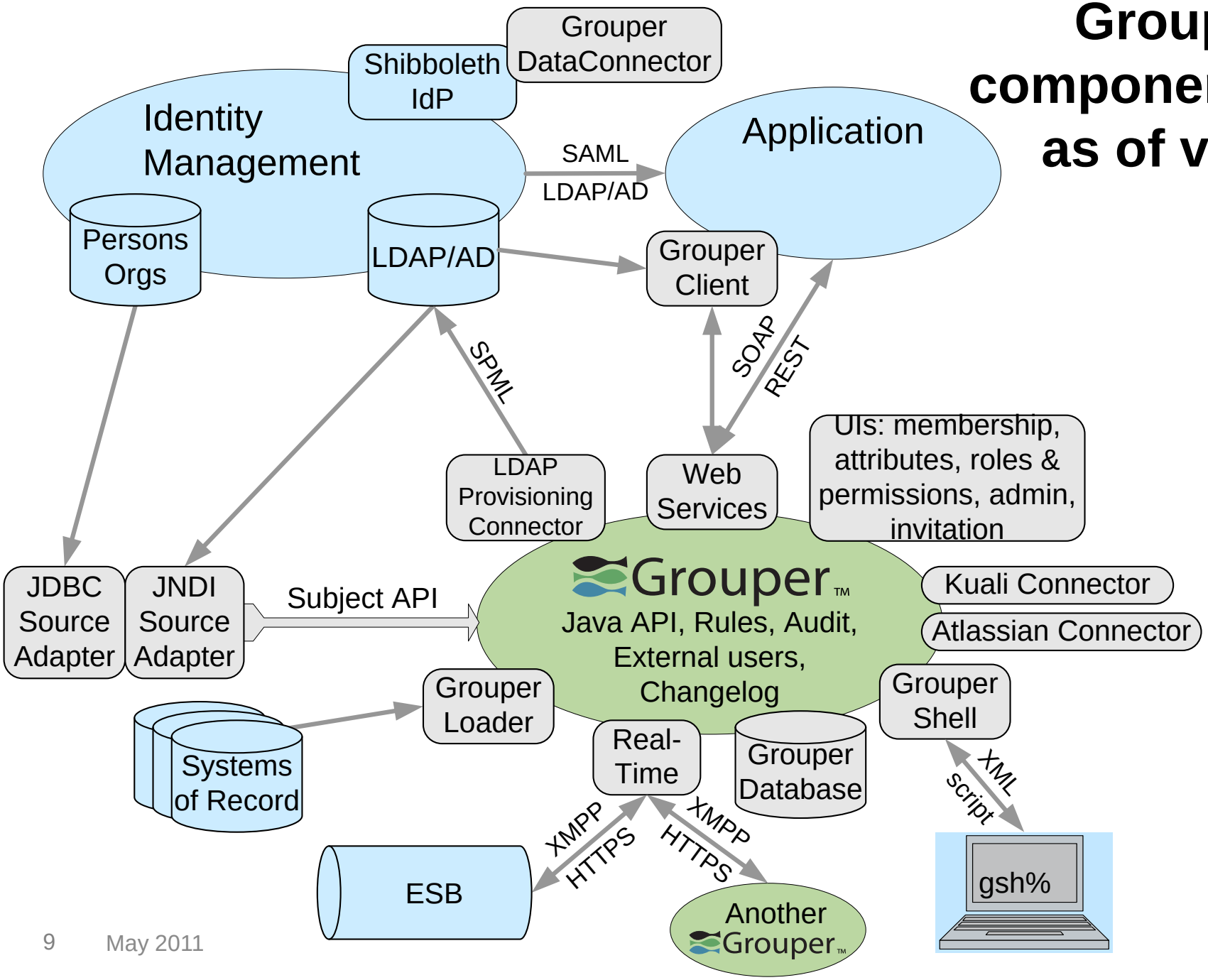
Delegation model extends that for Groups

INTERNET2

Access management lifecycle support

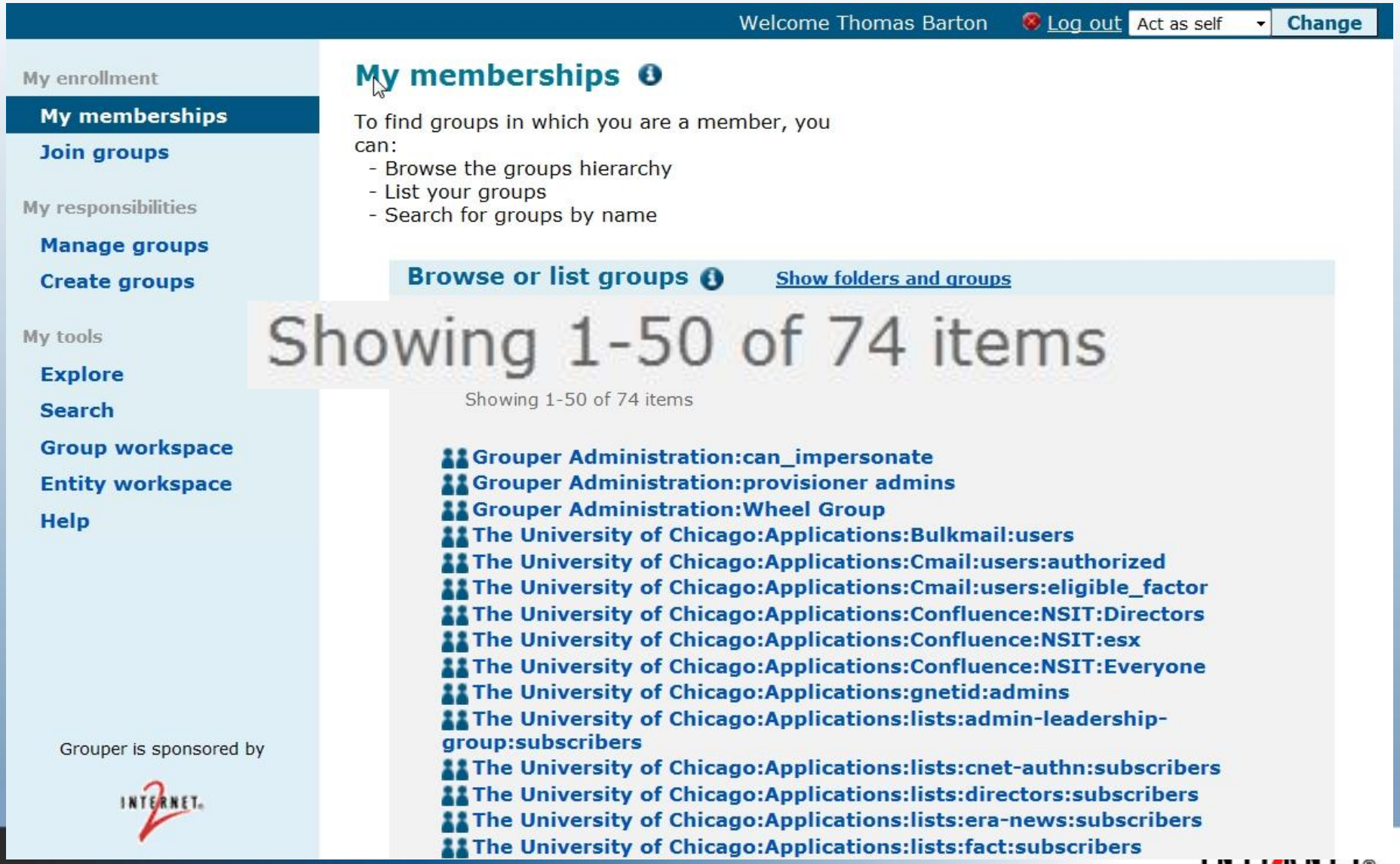
- Membership start & end times (optional)
- Move or copy folders, groups, etc
- User audit
- Point in time audit
- Rules

Grouper components as of v2.0



EXAMPLES

Tom Barton's UChicago group memberships



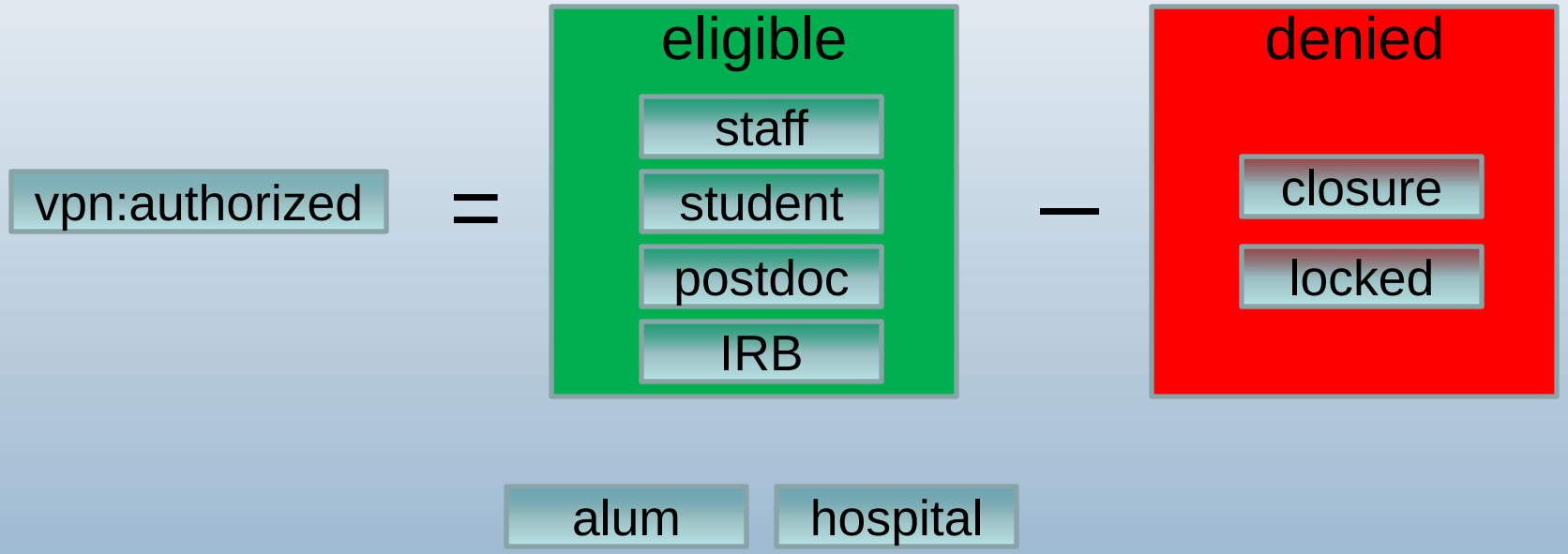
Memberships become LDAP attributes

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:cmail:users:authorized
ucismemberof: uc:reference:affiliations:effective:staff

UChicago VPN simple delegation example



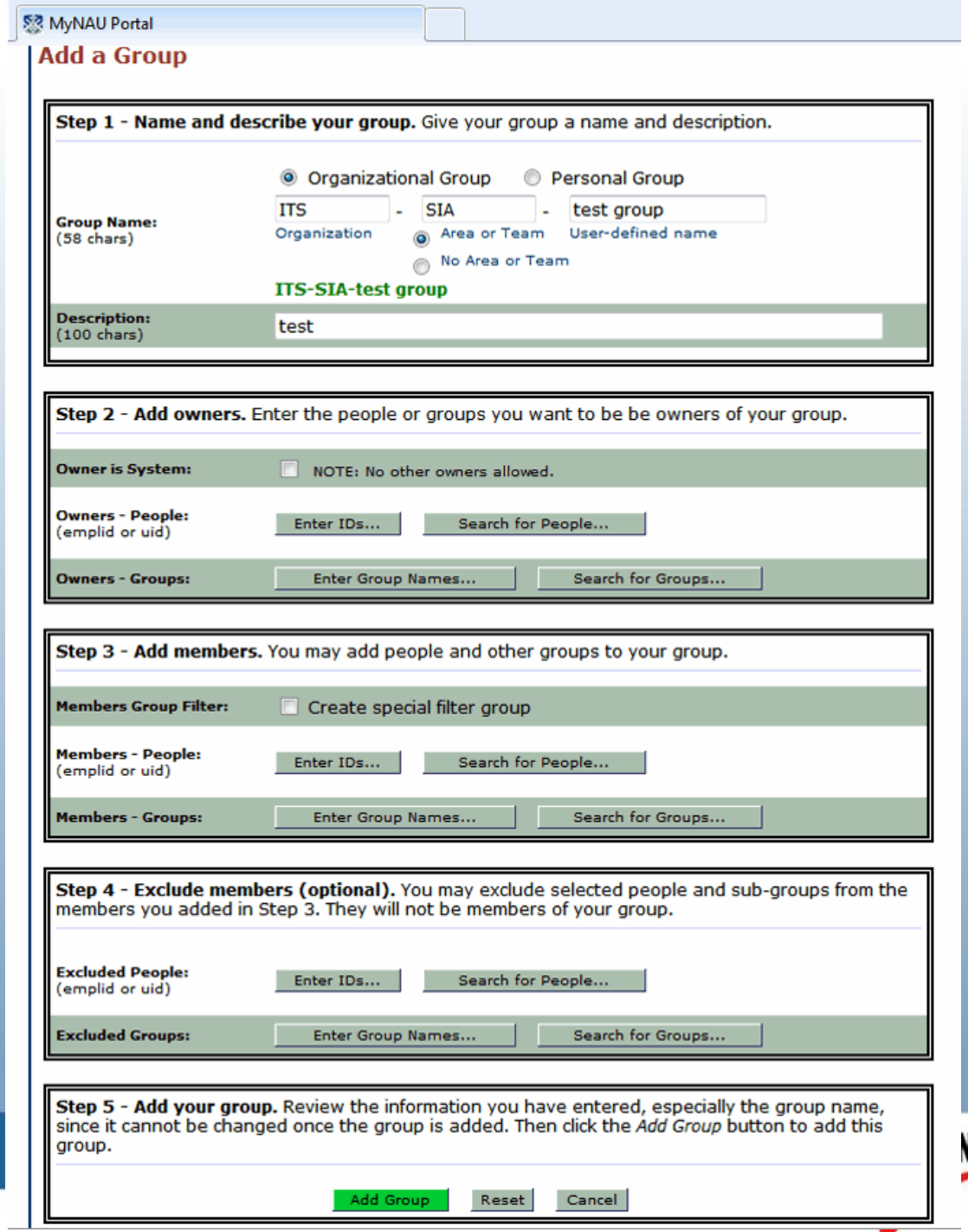
Different groups, different authorities.

VPN only uses “vpn:authorized”.

UChicago applications managed by Grouper, so far

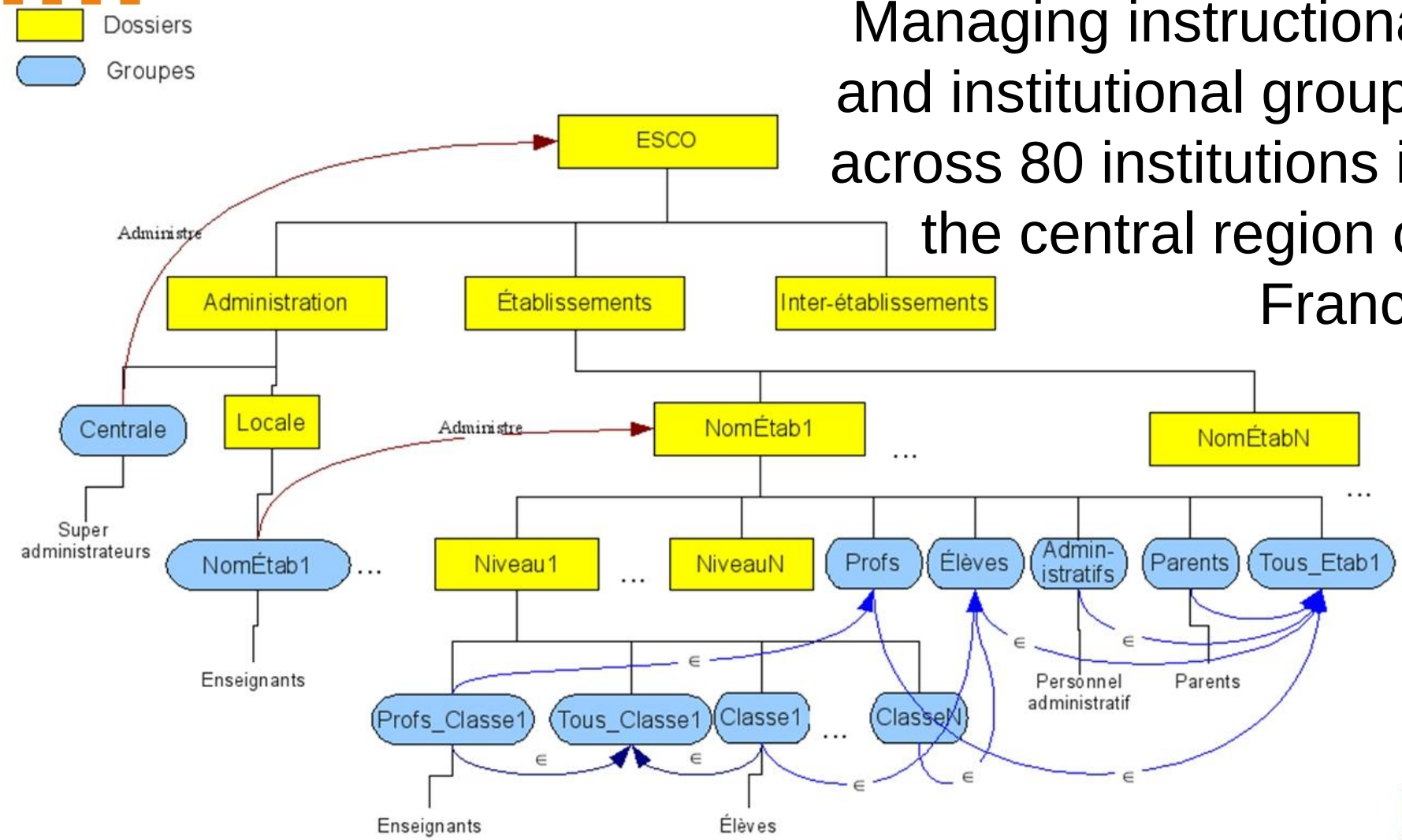
aams
Ad Astra
Bulkmail
Business Objects Enterprise
Chalk
CityRyde
Cmail
cnet
Confluence
Directory Administration
dmca
Facilities SIMS
gnetid
grouper
im
isx
IT Ecosystem
Lab School
LDAP
lists
Mail Forwarding
Microsoft Exchange
modem pool
myUChicago
online directory
password expiration
rt
Service Now
shibboleth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

Northern Arizona's Add a Group Portlet



Grouper : Extrait de l'arborescence à créer

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



① SURFfederatie SAML

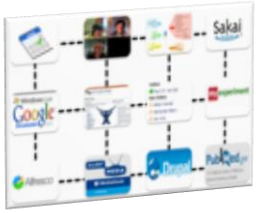
+

① SURFteams (grouper)

+

② OpenSocial

+

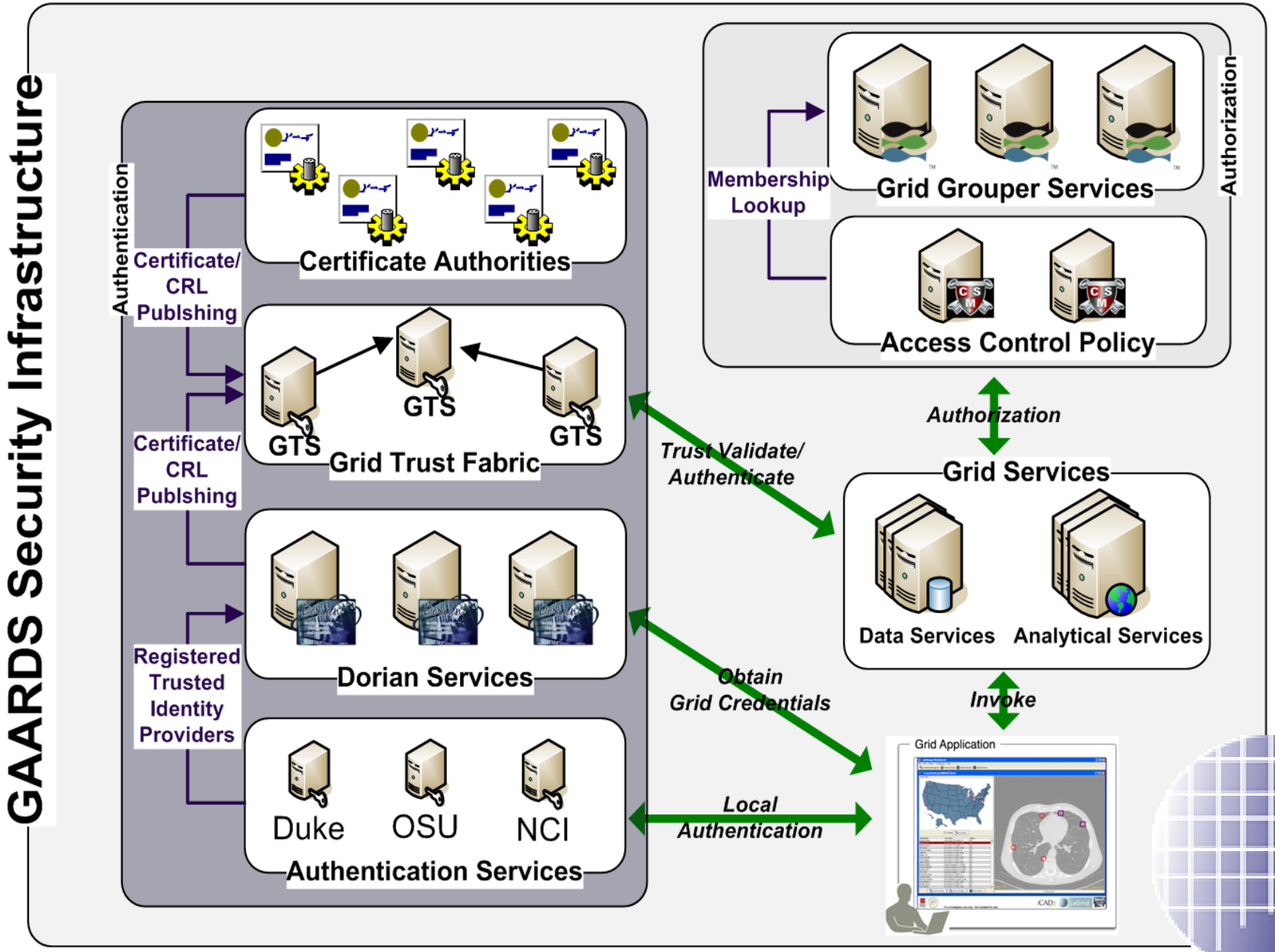


① Collaboration tools

SURF CONEXT

=

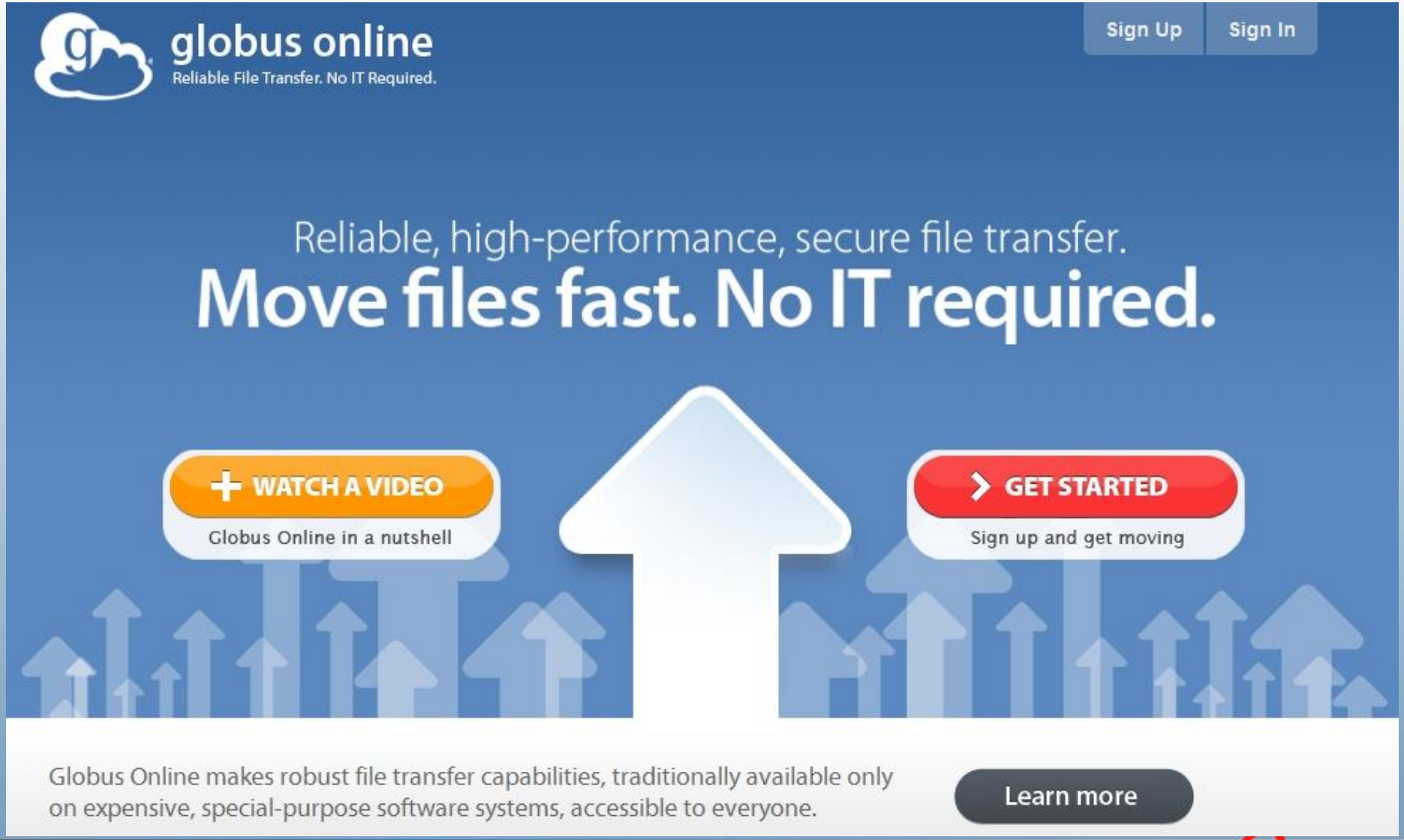
SURFnet's national scale collaboration platform



Cancer BioInformatics Grid

caGrid

Coming soon: managing access to research data sets



INTERNET2®

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	

INTERNET2

Thanks!

Further questions?

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

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