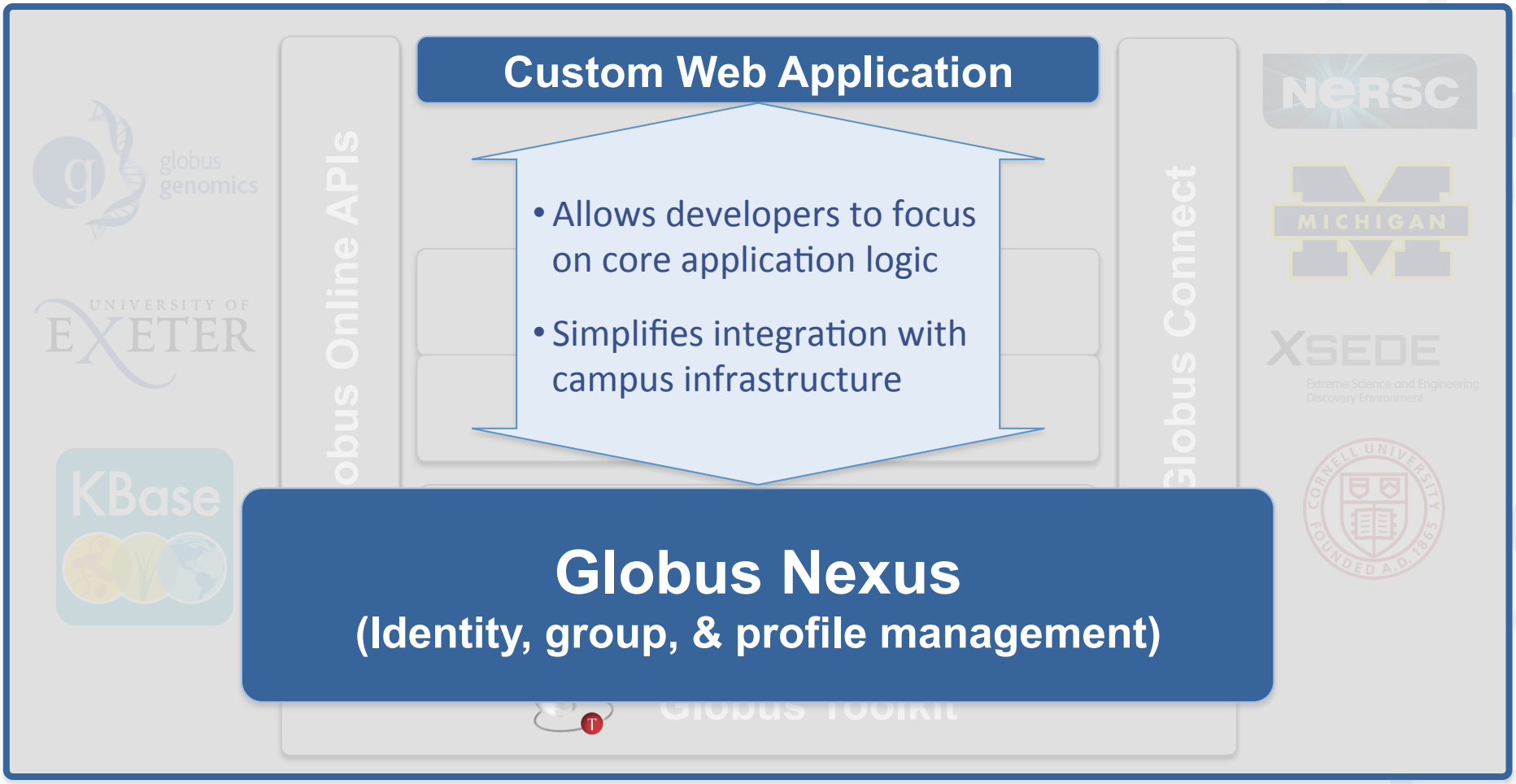
The identity challenge in science

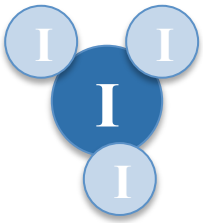
- Developers of collaborative science tools, applications, and cyberinfrastructures need to:
  - **Assign identities** to their users
  - Manage **user profiles**
  - Organize users into **groups** for authorization
- Providing **high-quality implementations** of such capabilities is challenging
  - Complexity of associated security protocols
  - Reliability, availability, scalability, security are all hard
- The result is **many identity 'islands'** across science domains and projects—often poorly implemented

Streamline collaborative tool development

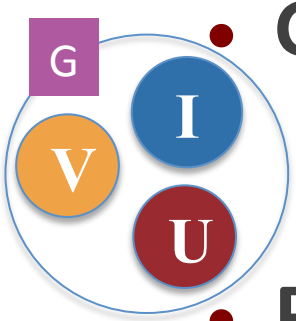


Nexus provides four key capabilities

- **Identity provisioning**
  - Create and manage Globus identities



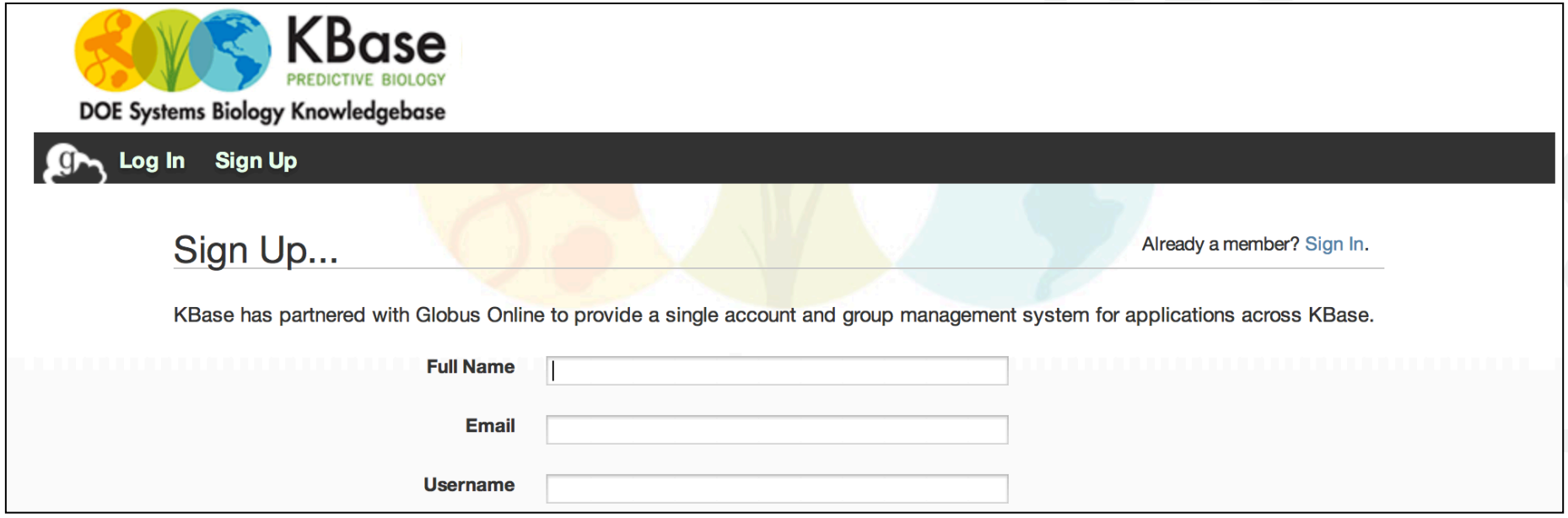
- **Identity hub**
  - Link with other identities; use to authenticate to Nexus and other services

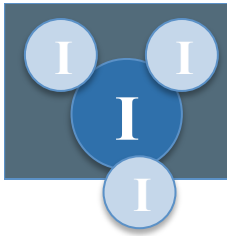


- **Group hub**
  - User-managed group creation, management; groups can be used for authorization
- **Profile management**
  - User-managed profile attributes and visibility; can be used in group admission

Identity provisioning

- Globus Nexus can act as an identity provider (IDP) for a project
  - User management, email validation…
- DOE Systems Biology Knowledge Base (kBase) is an example of such a project. ~400 identities to date

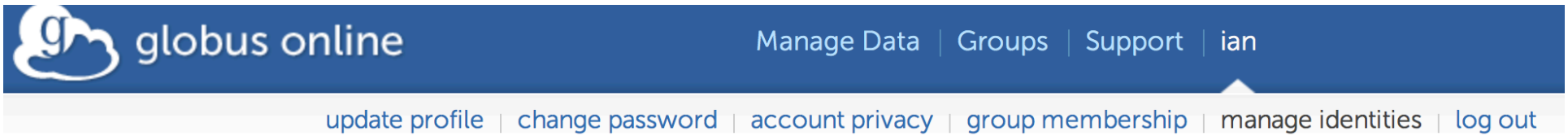




Identity hub

- **Link identities** from other federated IDP(s) with a Nexus identity
  - E.g., InCommon (SAML), Google (OpenID), XSEDE (OAuth MyProxy), IGTF-certified X.509 CA, SSH
- **Use linked identity** to authenticate to Nexus as the Nexus identity (e.g., use campus identity)
- **Leverage Nexus federated IDP** to 3rd-party services
  - Via Oauth or LDAP
  - E.g., to XSEDE, Jira, Zendesk, Drupal, Globus data management, Confluence
- Have Nexus **cache delegated credentials**
  - X.509, via CILogon, MyProxy

Identity hub management



Manage Identities

Add External Identity ⓘ Add X.509 Certificate ⓘ Add SSH Public Key ⓘ

Alias	Type	Authentication Provider			
system-generated openid alias	openid	google.com	View Details	Update	Delete
CI	myproxy	grid.ci.uchicago.edu	View Details	Update	Delete
	myproxy	dev.esg.anl.gov:7512	View Details	Update	Delete
MBook	ssh2	SSH Public Key	View Details	Update	Delete
galaxy-climate	x509	/O=Grid/OU=DemoG...			Delete
Ian Laptop	x509	/C=US/O=Globus C...			Delete
InCommon / CILogon Sign In	oauth	cilogon.org			Delete

Add External Identity ⓘ Add X.509

Add External Identity

Alias

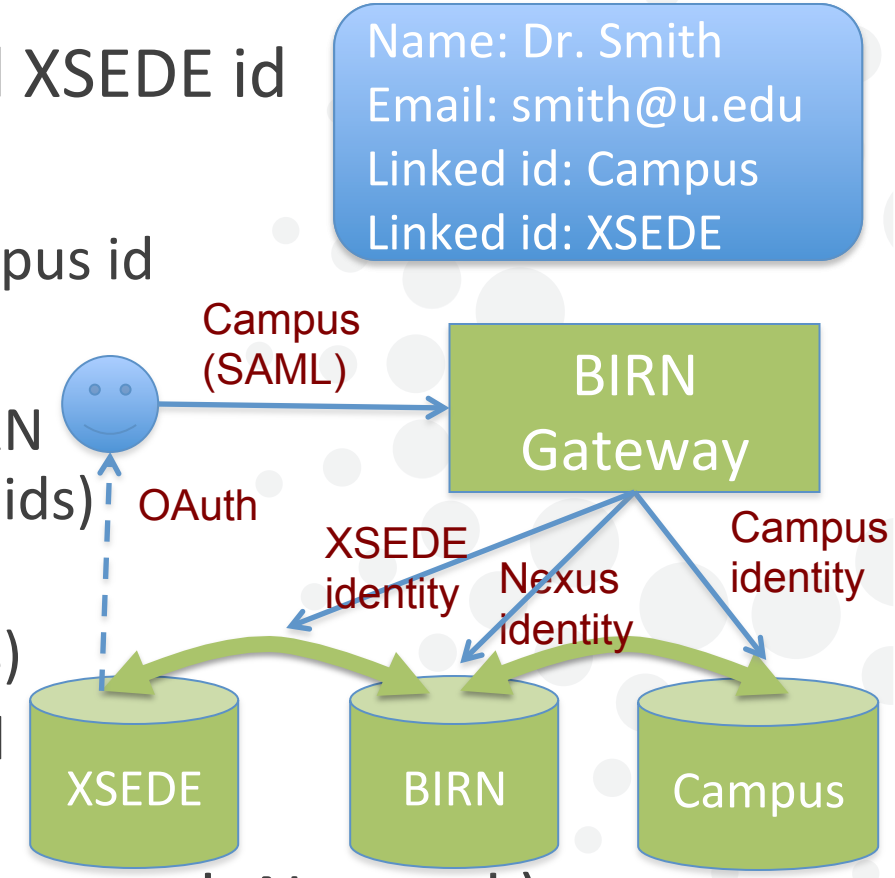
Account Provider

InCommon / CILogon

Add Account Close

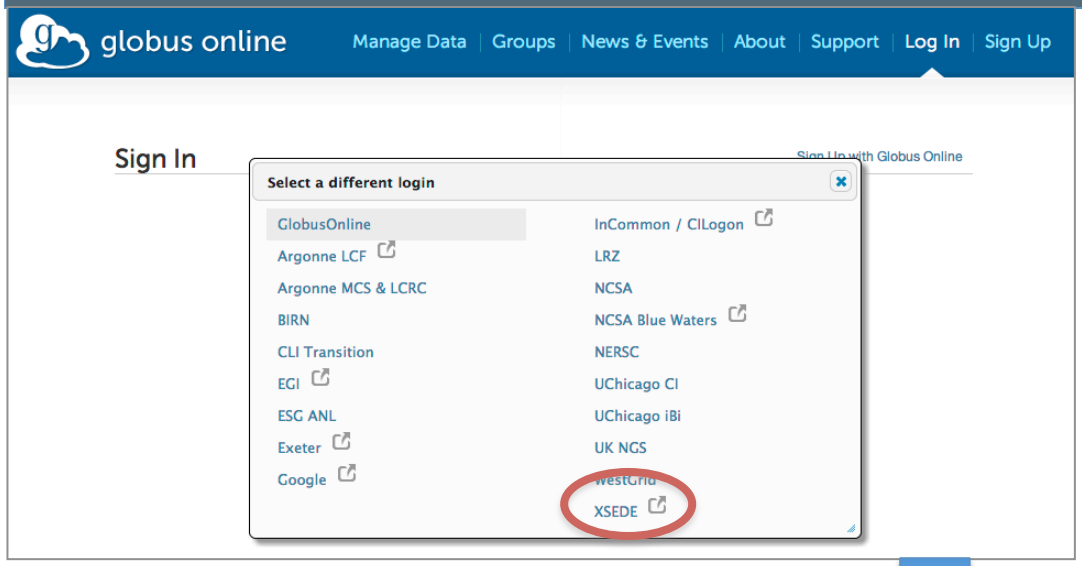
Identity hub: Biomedical science

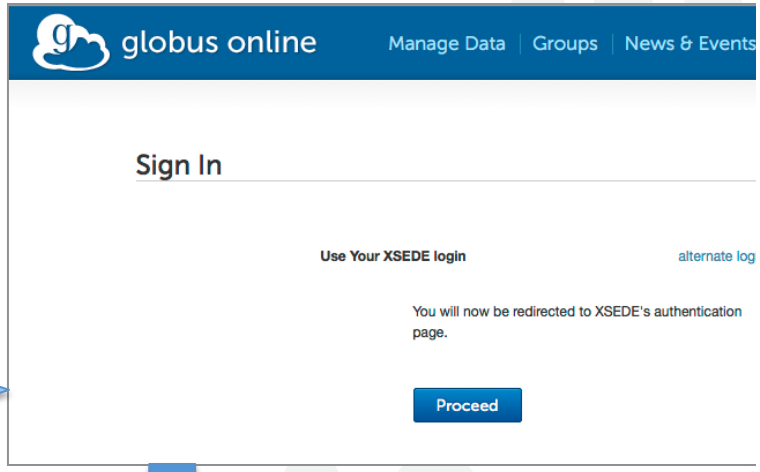
- Dr. Smith creates a BIRN id (Nexus id via BIRN-tailored interface)
- Dr. Smith links campus id and XSEDE id
- Dr. Smith can then:
  - Authenticate to BIRN with campus id
  - Query catalog (Nexus/BIRN id)
  - Request data transfer from BIRN to campus (Nexus and campus ids)
  - Request transfer from BIRN to XSEDE (Nexus and XSEDE ids)
  - Repeat these tasks: use cached credentials

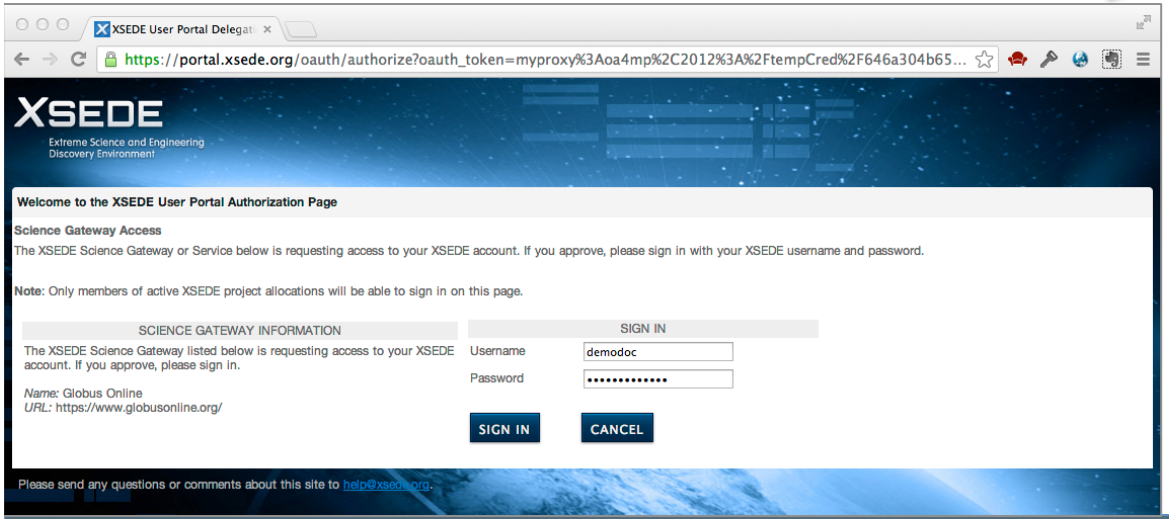


(BIRN=Biomedical Informatics Research Network)

Use linked identity





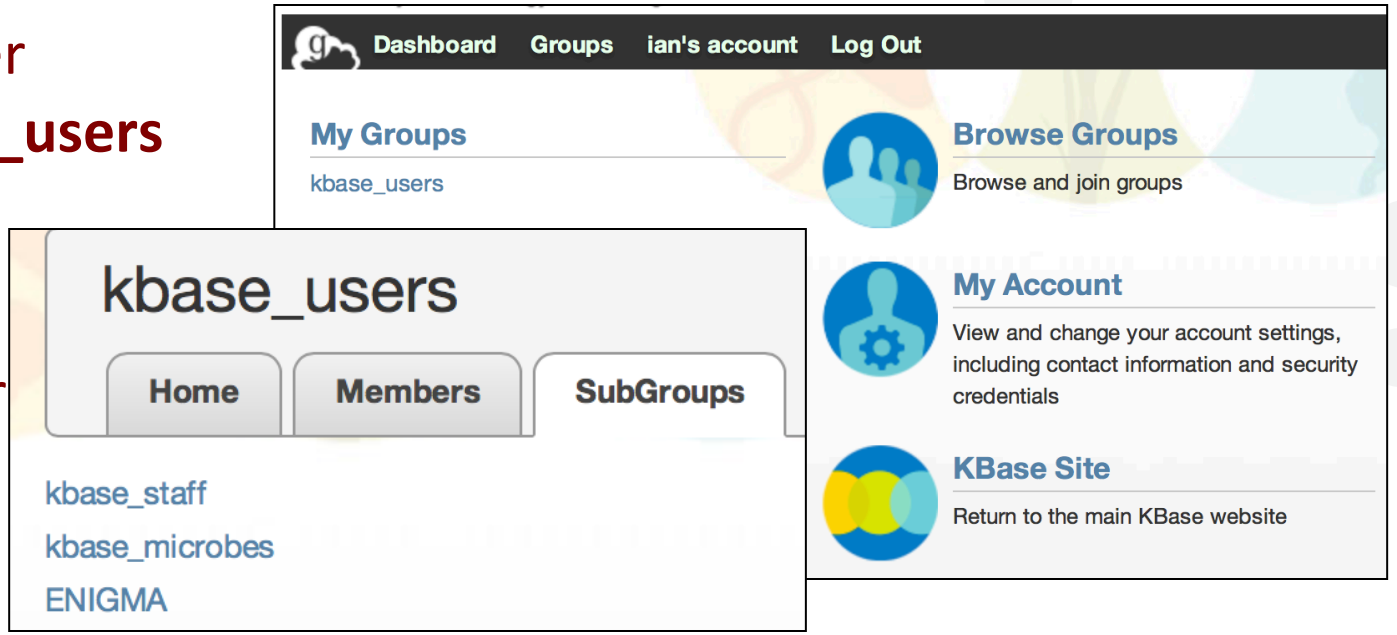


Group hub

- User-managed group creation, management
- Flexible control over admission policies and visibility
- Groups can be used in authorization decisions

Example: kBase

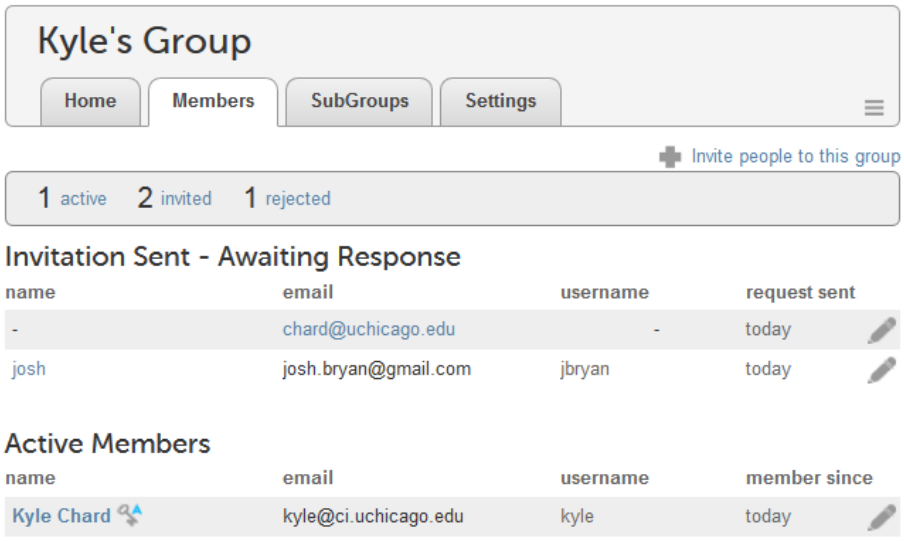
- Every kBase user added to **kbase_users**
- Subgroups also created
- Groups used for access control

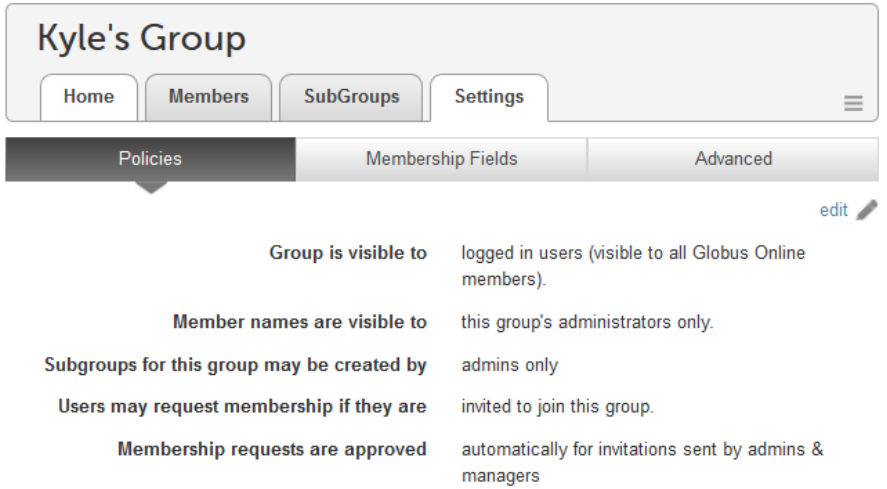


Group membership interface

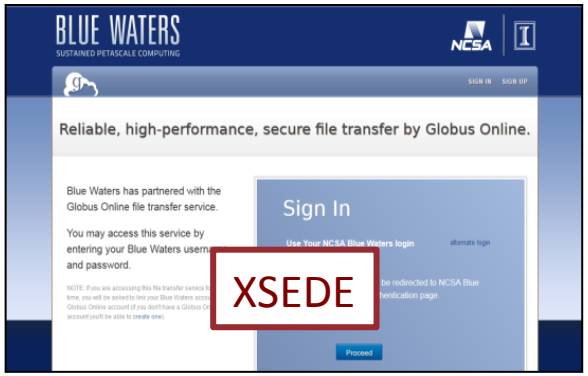
Group Membership

Group Name	Status
Cornell demo	Pending Admin Approval
Data Summit Slides	Administrator
Globus Team	Active Member
Ian's secret stuff group	Administrator
Ag-GRID	Active Member

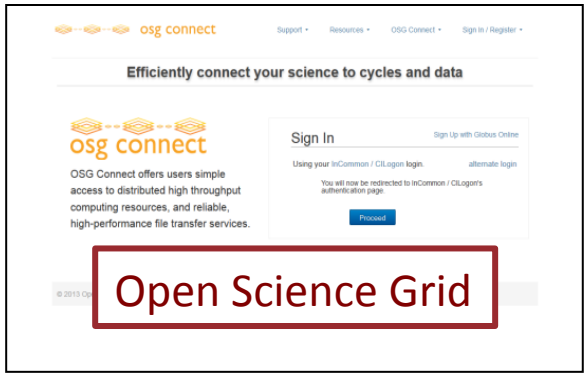




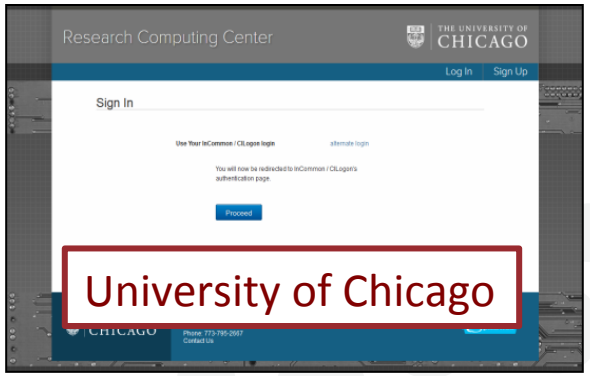
Branded sites



XSEDE

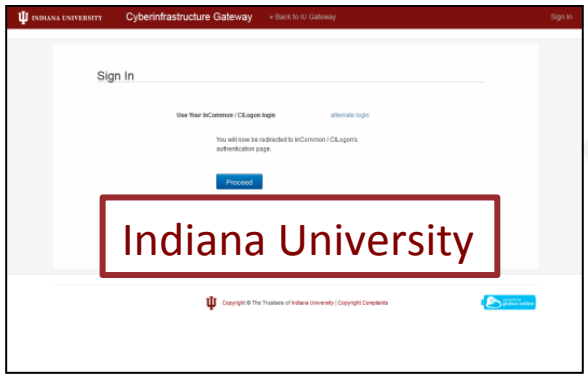


Open Science Grid

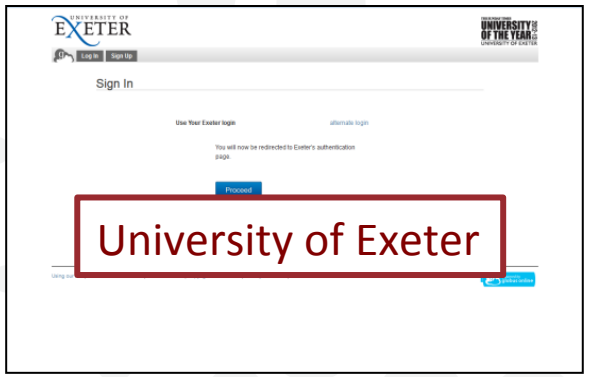


University of Chicago

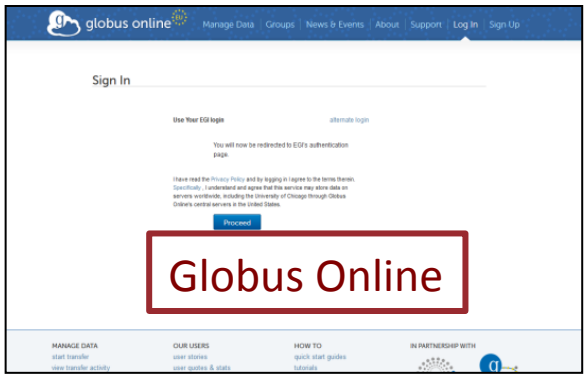
DOE kBase



Indiana University

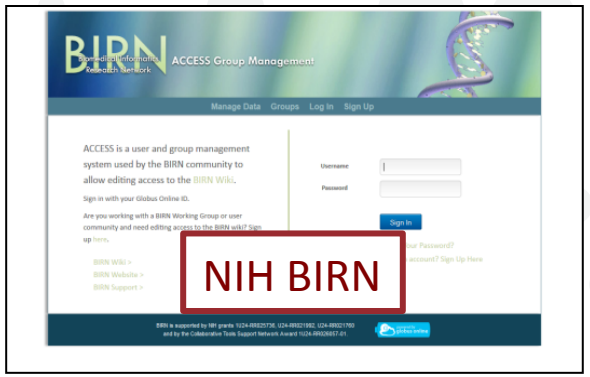


University of Exeter



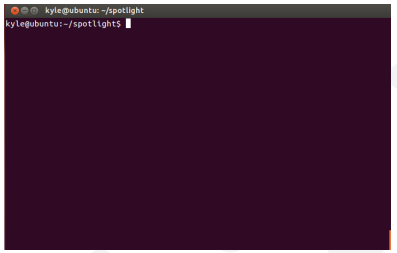
Globus Online

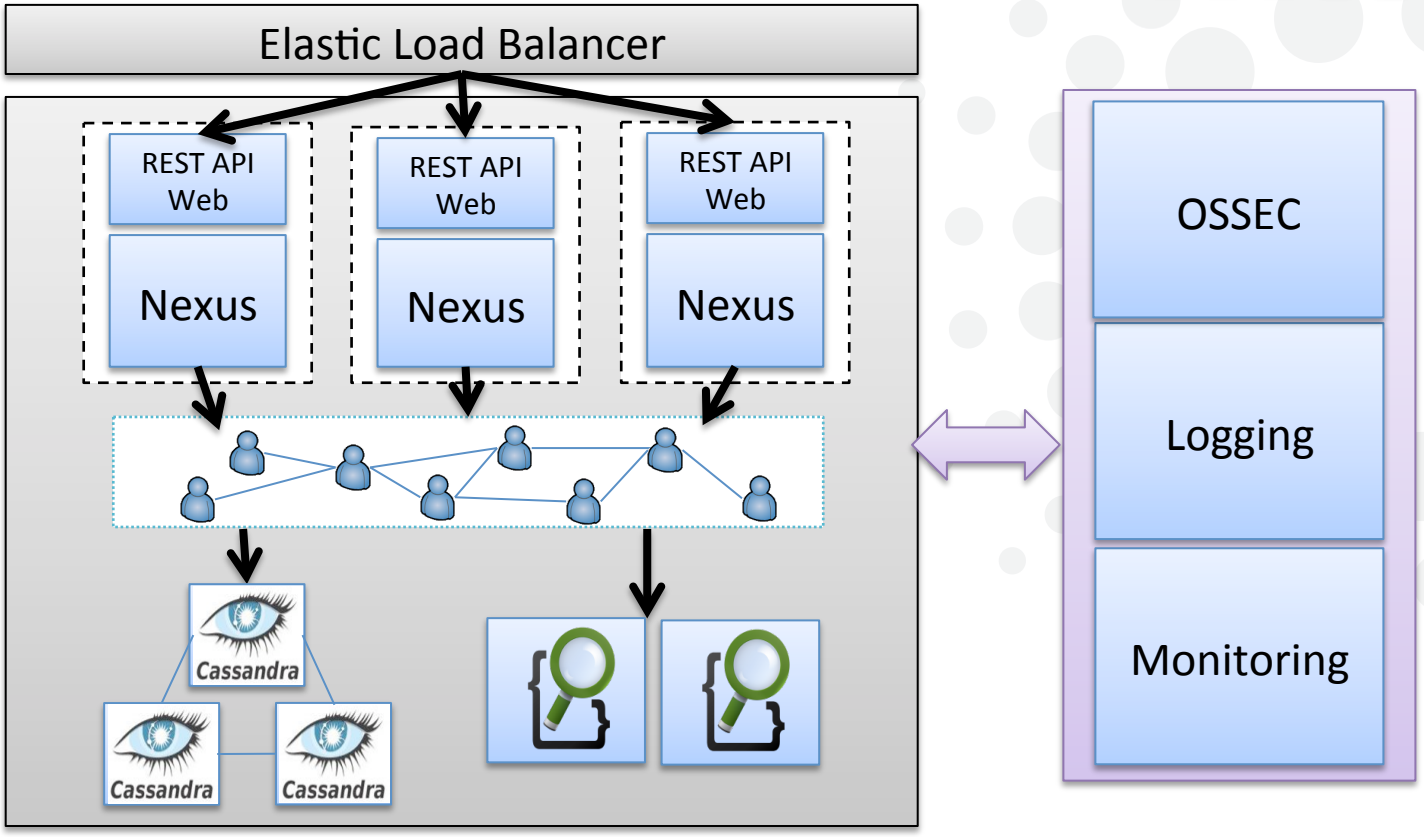
NERSC



NIH BIRN

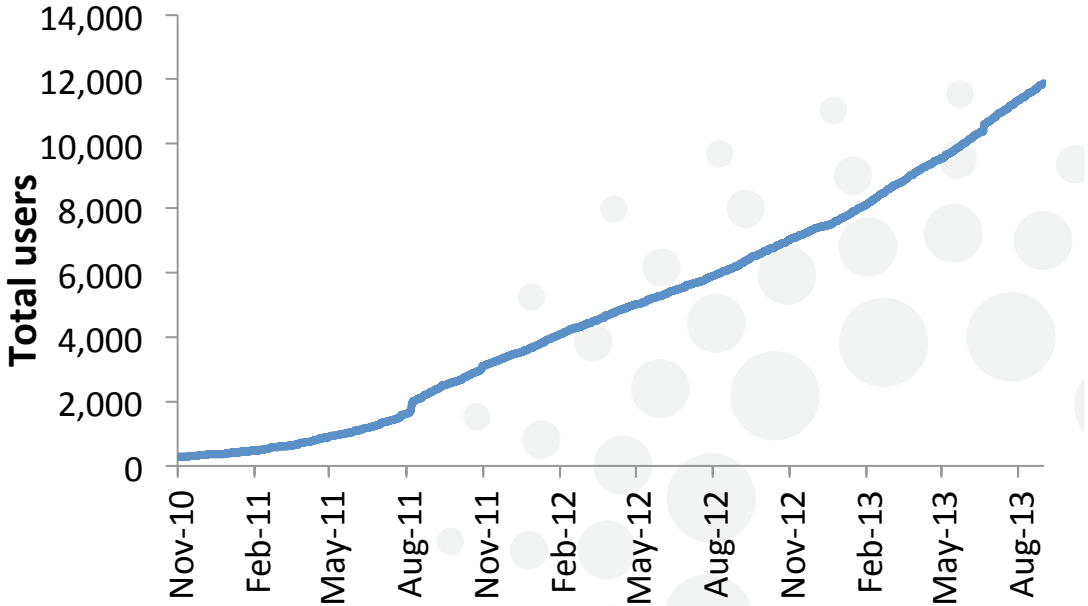
Implementation and deployment

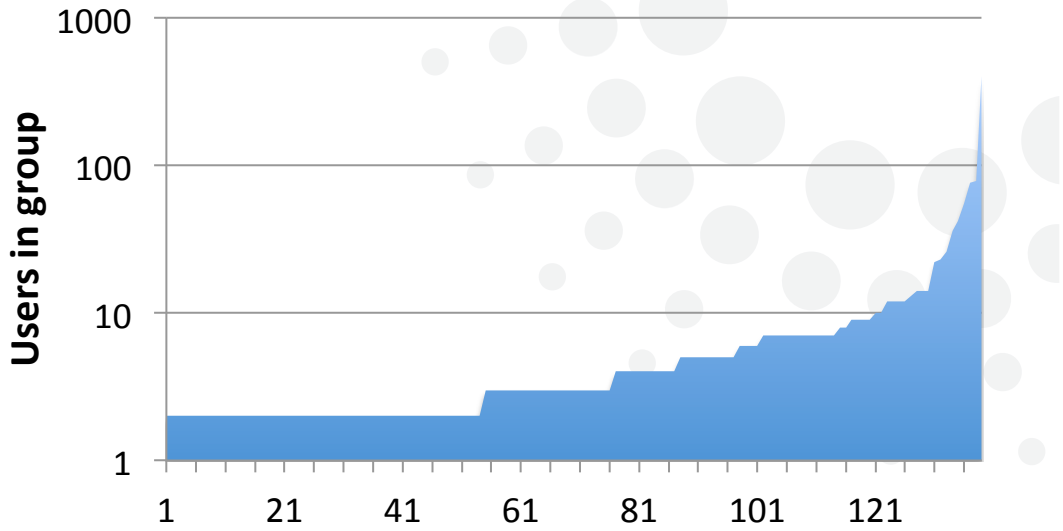




Globus Nexus usage as of 9/13

- >12,000 users and 4977 linked identities
- 557 groups totaling:
  - 1638 active members
  - 229 pending or invited members
  - 162 rejected or suspended members
- Largest group (kbase) has 402 members





User profiles

- Profile = set of attributes/values about a user
  - E.g., name, email, address, field of science, etc.
- Types of profile attributes:
  - Self-asserted (e.g., name)
  - Validated (e.g., email, linked identity)
  - Asserted by other user
- Sources of profile attributes:
  - Social sites (e.g., LinkedIn, Facebook, Google+)
  - Campus Shibboleth servers
  - Nexus users

Identities and groups in XSEDE

- Proposal: Replace current ad-hoc systems with Globus Nexus identity and group service
  - Reduce complexity, reduce cost, increase capability
- Careful process of documentation and review
  - "Architecture and development requirements: User and identity management"
  - "User management proposal: Affected use cases"
  - "User management proposal: Motivating stories"
  - "Proposal: Refactoring XSEDE identity and group capabilities"
- Hope to reach closure by end of 2013