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

Custom Web Application

- Allows developers to focus on core application logic
- Simplifies integration with campus infrastructure

Globus Nexus
(Identity, group, & profile management)
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

<table>
<thead>
<tr>
<th>Alias</th>
<th>Type</th>
<th>Authentication Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-generated openid alias</td>
<td>openid</td>
<td>google.com</td>
</tr>
<tr>
<td>CI</td>
<td>myproxy</td>
<td>grid.ci.uchicago.edu</td>
</tr>
<tr>
<td>MBook</td>
<td>ssh2</td>
<td>SSH Public Key</td>
</tr>
<tr>
<td>galaxy-climate</td>
<td>x509</td>
<td>/O=Grid/OU=DemoGroup</td>
</tr>
<tr>
<td>Ian Laptop</td>
<td>x509</td>
<td>/C=US/O=Globus Group</td>
</tr>
<tr>
<td>InCommon / CILogon Sign In</td>
<td>oauth</td>
<td>cilogon.org</td>
</tr>
</tbody>
</table>

Add External Identity

Add X.509 Certificate

Add SSH Public Key
• 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

## Group Name

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cornell demo</td>
<td>Pending Admin Approval</td>
</tr>
<tr>
<td>Data Summit Slides</td>
<td>Administrator</td>
</tr>
<tr>
<td>Globus Team</td>
<td>Active Member</td>
</tr>
<tr>
<td>Ian’s secret stuff group</td>
<td>Administrator</td>
</tr>
<tr>
<td>Ag-GRID</td>
<td>Active Member</td>
</tr>
</tbody>
</table>

## Kyle's Group

- **Active**: 1
- **Invited**: 2
- **Rejected**: 1

**Invitation Sent - Awaiting Response**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Username</th>
<th>Request Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td><a href="mailto:chard@uchicago.edu">chard@uchicago.edu</a></td>
<td>-</td>
<td>today</td>
</tr>
<tr>
<td>josh</td>
<td><a href="mailto:josh.bryan@gmail.com">josh.bryan@gmail.com</a></td>
<td>jbryan</td>
<td>today</td>
</tr>
</tbody>
</table>

**Active Members**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Username</th>
<th>Member Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kyle Chard</td>
<td><a href="mailto:kyle@ci.uchicago.edu">kyle@ci.uchicago.edu</a></td>
<td>kyle</td>
<td>today</td>
</tr>
</tbody>
</table>

**Group is visible to**: logged in users (visible to all Globus Online members)

**Member names are visible to**: this group's administrators only.

**Subgroups for this group may be created by**: admins only

**Users may request membership if they are invited to join this group.**

**Membership requests are approved automatically** for imitations sent by admins & managers.
Branded sites

- XSEDE
- Open Science Grid
- University of Chicago
- DOE kBase
- Indiana University
- University of Exeter
- Globus Online
- NERSC
- NIH BIRN
Implementation and deployment

Elastic Load Balancer

REST API Web
Nexus

REST API Web
Nexus

REST API Web
Nexus

OSSEC
Logging
Monitoring

Cassandra
Cassandra
Cassandra
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