Distributed Web Security for Science Gateways

Jim Basney
jbasney@illinois.edu

In collaboration with:
Rion Dooley
dooley@tacc.utexas.edu
Jeff Gaynor
gaynor@illinois.edu
Suresh Marru
smarru@indiana.edu
Marlon Pierce
marpierc@indiana.edu

This material is based upon work supported by the National Science Foundation under grant number 1127210.

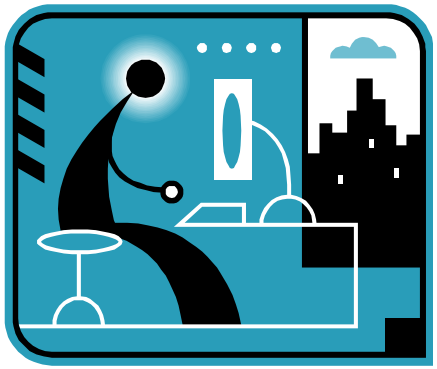
Distributed Web Security for Science Gateways

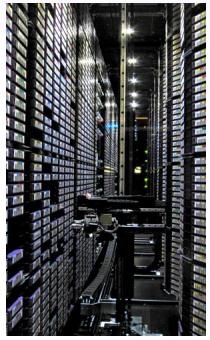
- Software Development for Cyberinfrastructure grant from the NSF Office of CyberInfrastructure (www.nsf.gov/oci)
  - 3 year project: August 2011 – July 2014
- Goal: Support use of OAuth by science gateways for distributed authentication, delegation, and authorization
- Develop OAuth “profiles” for science gateway use cases
  - Getting certificates from MyProxy servers
    - Both individual and “community” credentials
  - Delegating certificates between gateway components
  - Delegated access to REST services
  - Integration with external authentication (LDAP, Kerberos, SAML, OpenID)
  - Credential refresh
  - Web Single Sign-On (OpenID Connect)

Defining Terms

- **Authentication**: *Who are you?*
  - customer #83461234987
  - name: Jim Basney
  - email: jbasney@illinois.edu
- **Authorization**: *What are you allowed to do?*
  - Access private information
  - Charge purchases to your credit card
- **Delegated Authorization**: *Authorizations you grant to others*
  - Park your car (valet key)
  - View your private photos on Flickr
  - Collaboratively edit an online Google doc
- **Credential**: *How security information is conveyed*
  - Also known as **Assertion** or **Token**

Science Gateways: Tiered Access Models





user authenticates to science gateway

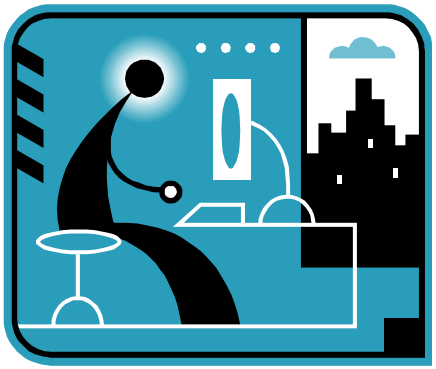
science gateway authenticates to service providers

NCSA

Science Gateways: Tiered Access Models

- Option A: Transitive Trust
  - Bilateral agreement between science gateway & service provider
    - Bulk allocation of service to the science gateway
    - Service provider may not know who the end users are
    - Users may not know who the underlying service providers are
  - Example: XSEDE Community Account model
    - User attributes in community credential provides user info to SP
- Option B: Delegation of Rights
  - End user has account at underlying service provider
  - Example: Individual XSEDE account with Globus Online
  - Science Gateway explicitly acts on the user's behalf when interacting with the underlying service providers
- Both options are useful (and can be combined)
  - Our recent work is focused on *Option B: Delegation of Rights*

Example: Photo Printing

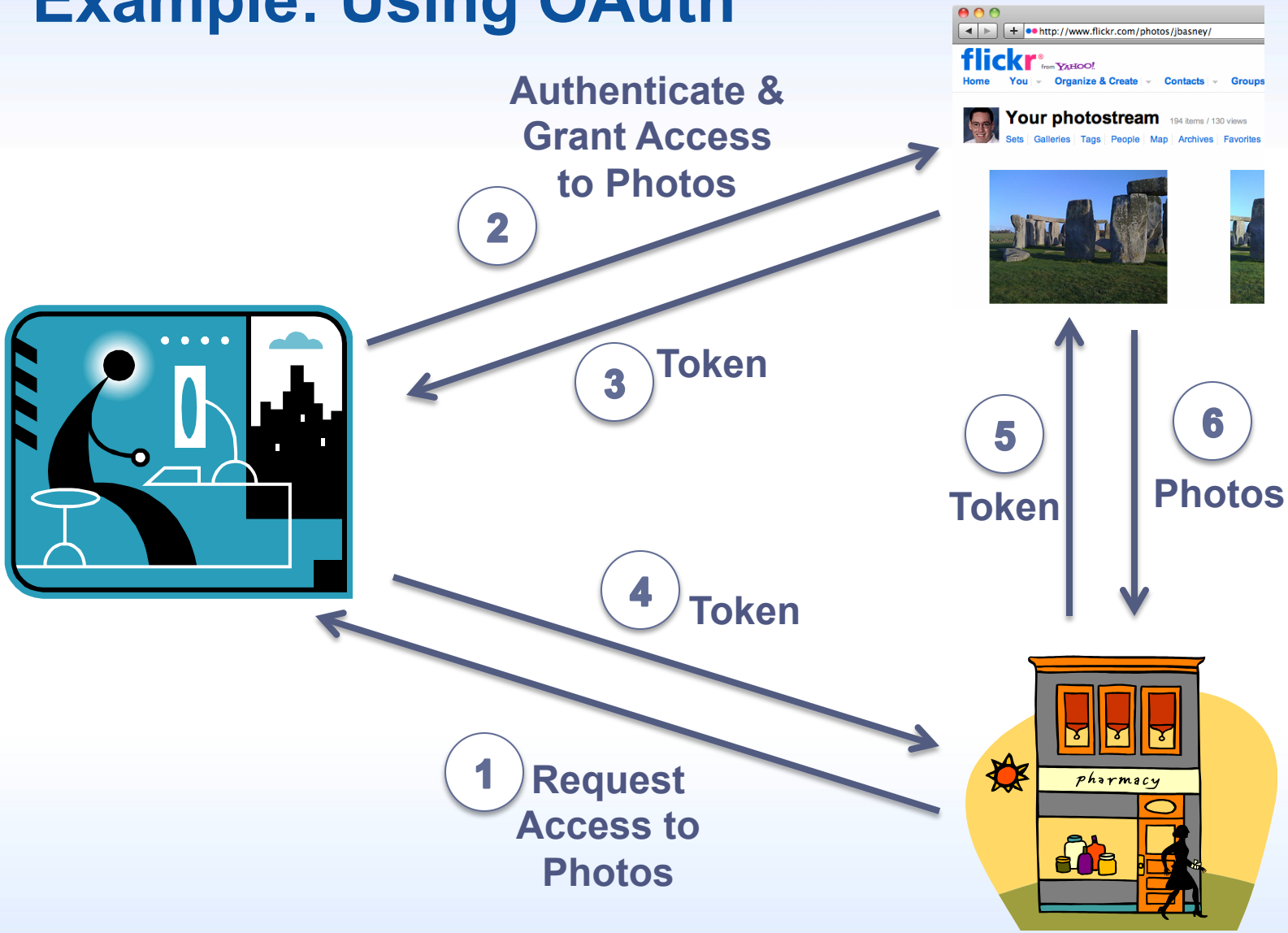


2 Your flickr Password

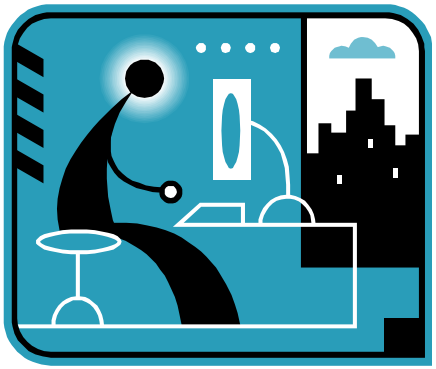
3 Photos

1 Your flickr Password

Example: Using OAuth



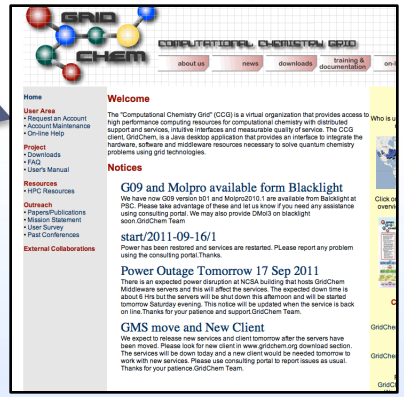
Example: Science Gateway



2 Your Password

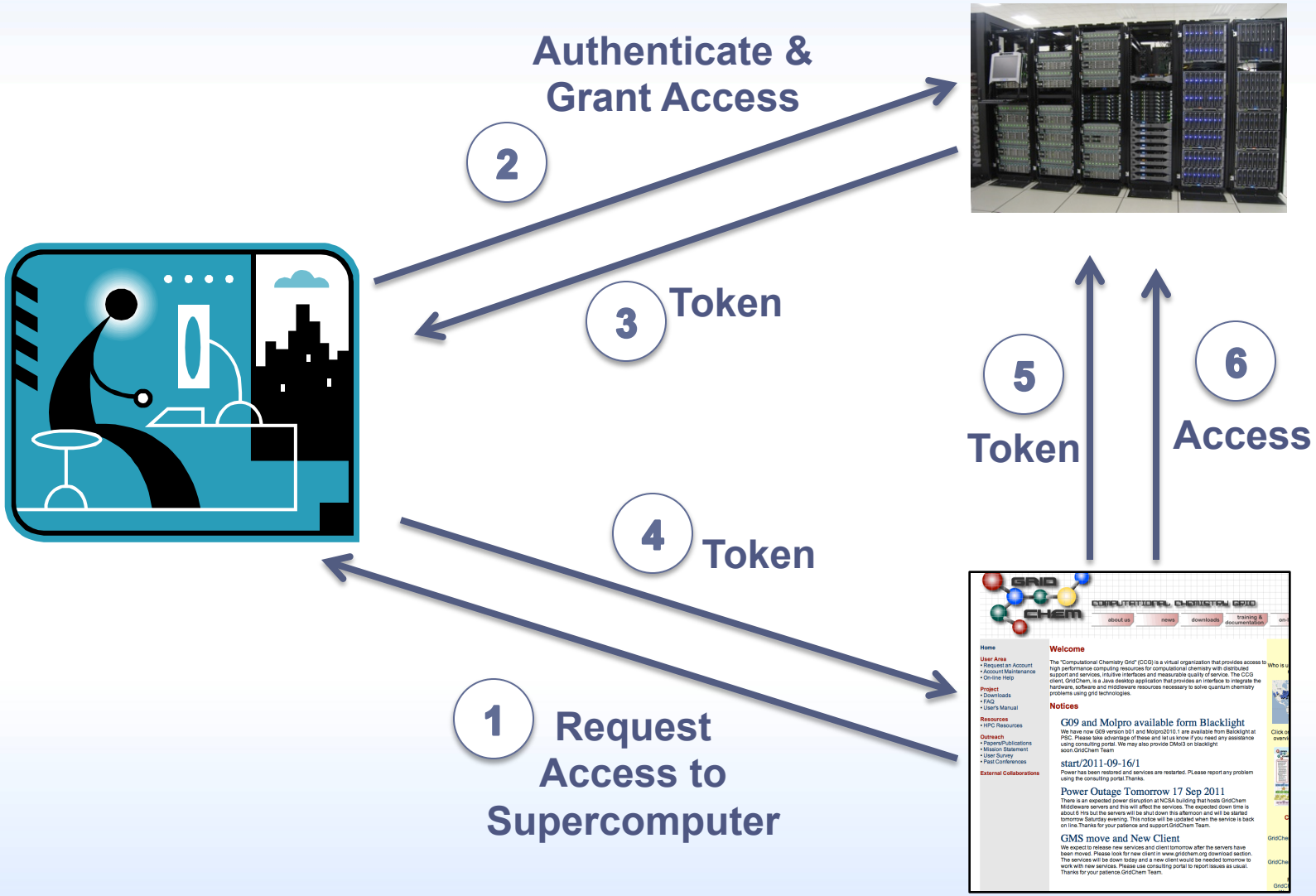
3 Access

1 Your Password

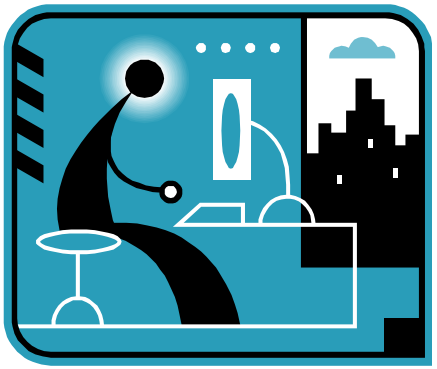


NCSA

Delegated Authorization via OAuth



Delegated Authorization via OAuth



Authenticate & Grant Access

2

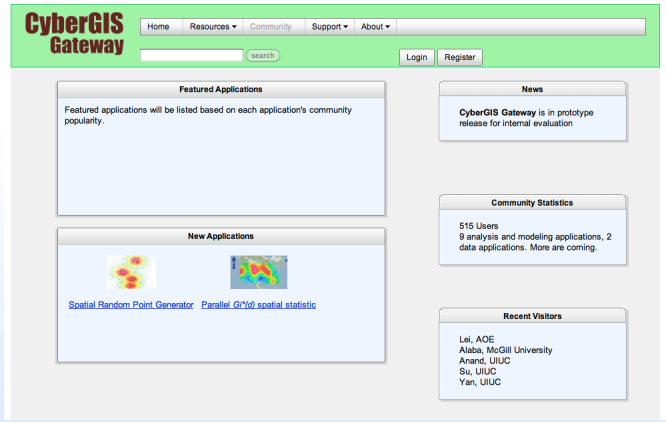
3 Token

4 Token

1 Request Access to iPlant Data

5 Token

6 Data

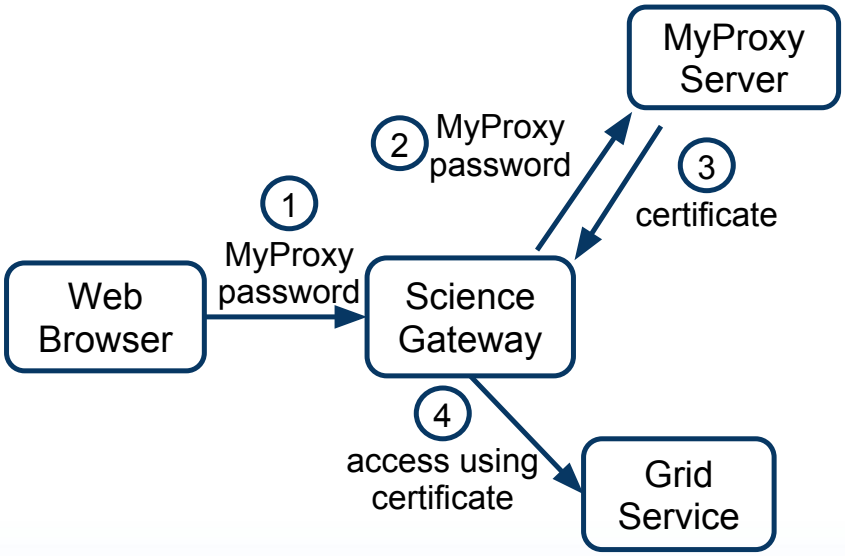


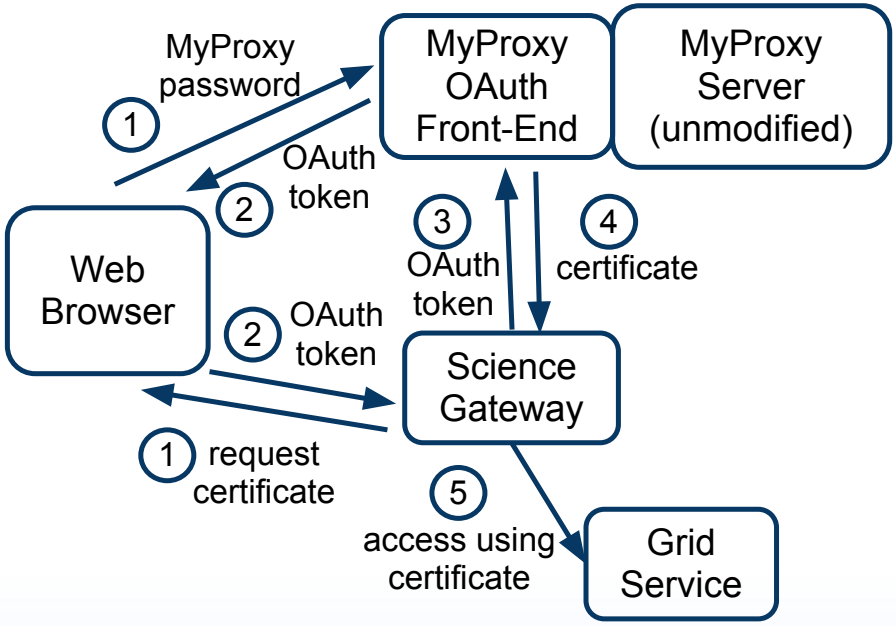
OAuth for MyProxy

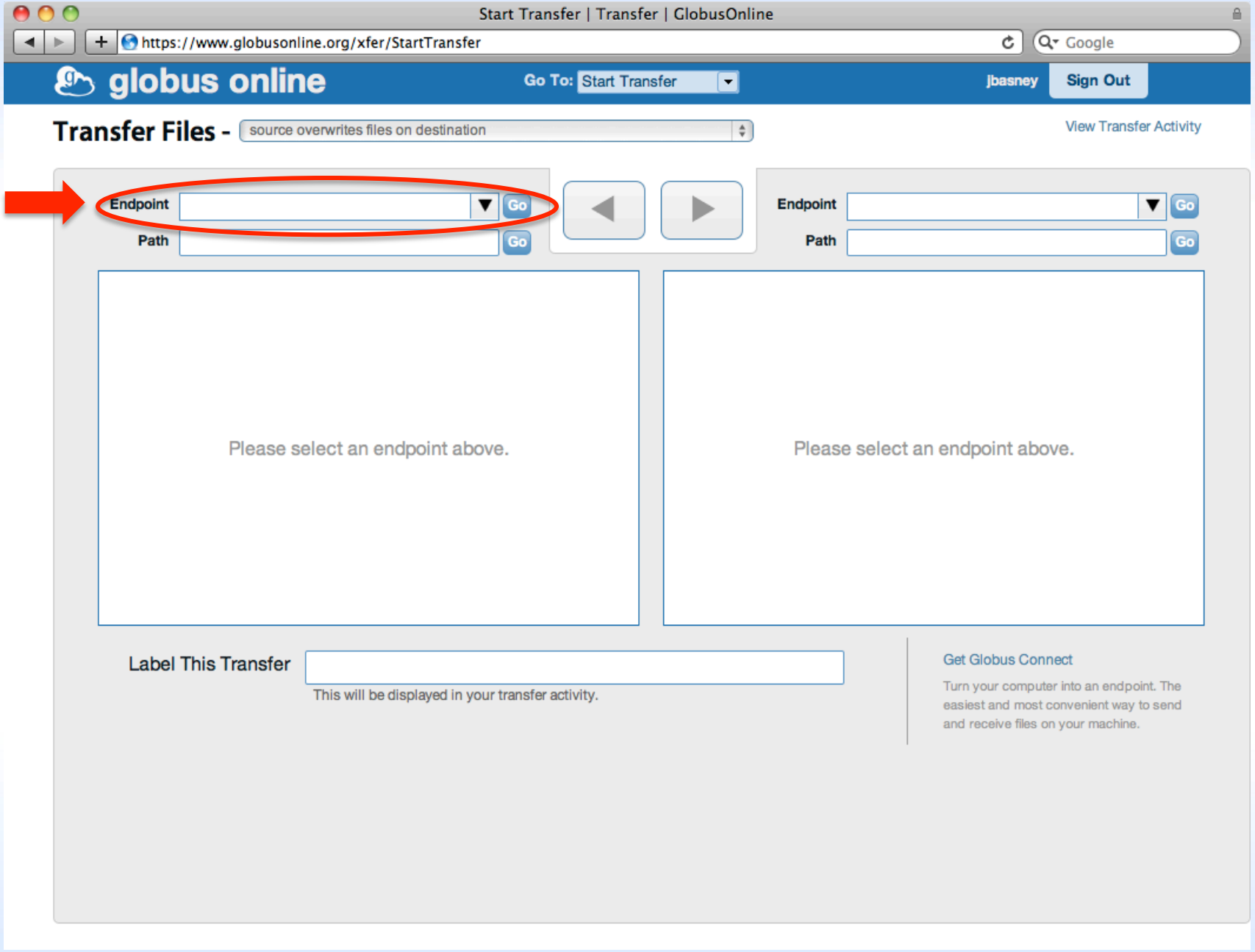
- Provides an OAuth 1.0a compliant REST web interface to MyProxy for providing user certificates to science gateways
  - Eliminates the need for users to disclose their MyProxy passwords to science gateways. Instead, gateway users authenticate to their MyProxy server's OAuth web interface to approve issuance of a certificate by MyProxy to the science gateway they are using.
- Java client & server implementations available now
  - http://www.sciencegatewaysecurity.org/oauth-for-myproxy
- XSEDE MyProxy OAuth Server
  - https://portal.xsede.org/oauth/
  - http://security.ncsa.illinois.edu/teragrid-oauth/
    - TG11 paper: http://dx.doi.org/10.1145/2016741.2016776
  - In use today by Globus Online
  - Supports using *individual* XSEDE accounts via science gateways

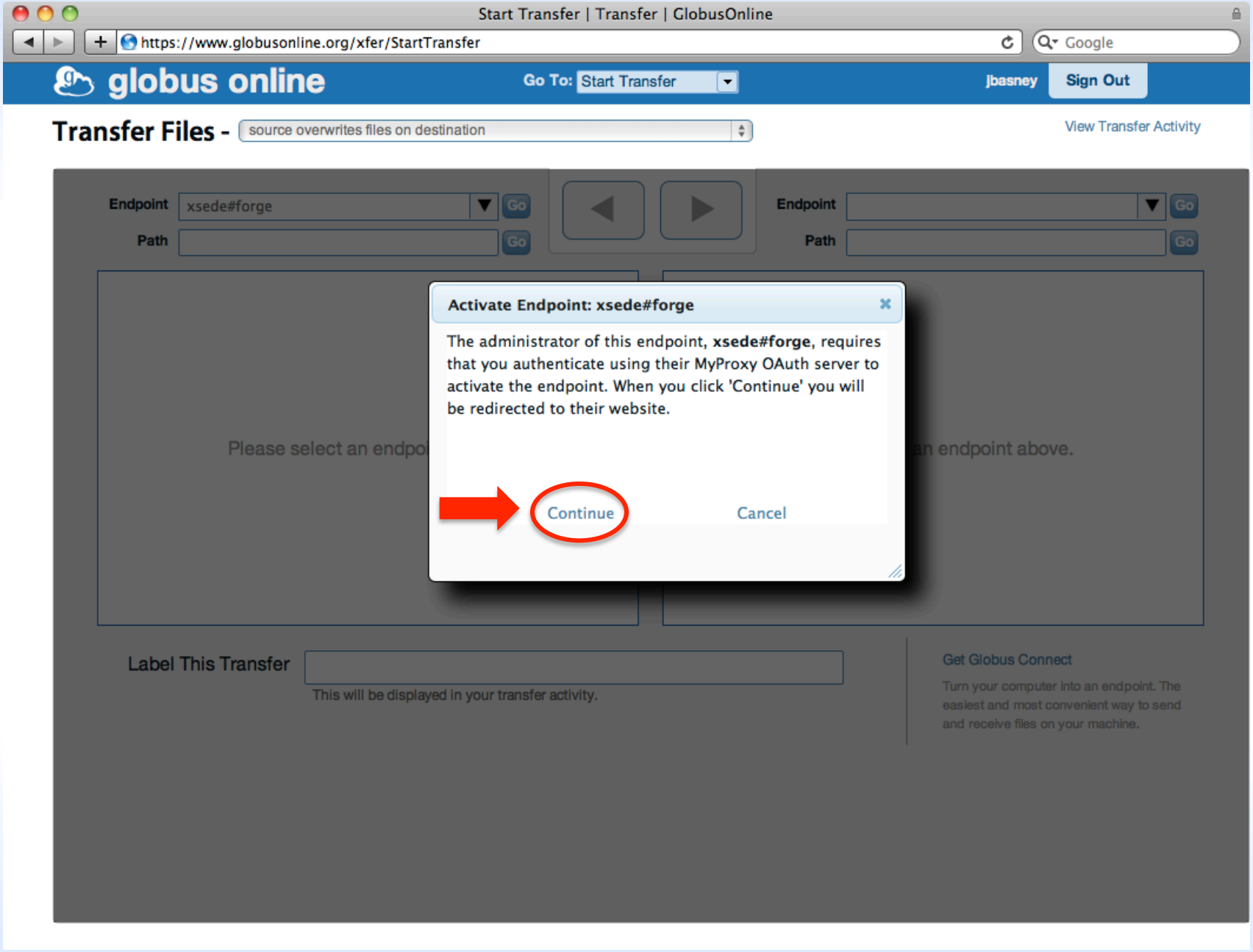
MyProxy Use Case

Old Approach ⟶ New Approach

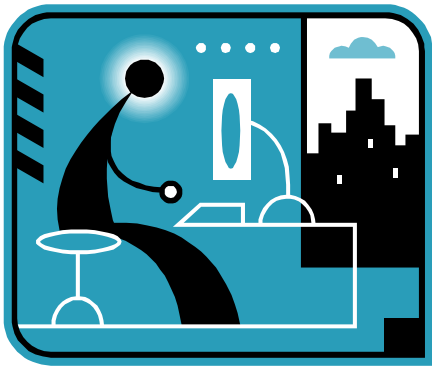


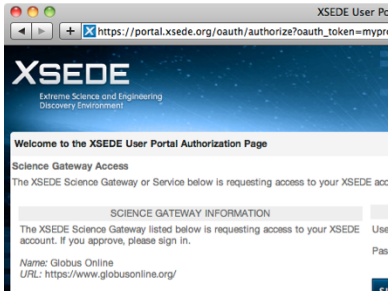


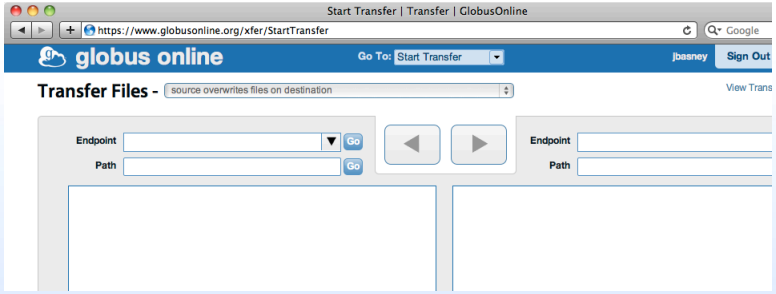

Start Transfer | Transfer | GlobusOnline
https://www.globusonline.org/xfer/StartTransfer
Google
globus online
Go To: Start Transfer
jbasney
Sign Out
Transfer Files -
source overwrites files on destination
View Transfer Activity
Endpoint
Go
Path
Go
Endpoint
Go
Path
Go
Please select an endpoint above.
Please select an endpoint above.
Label This Transfer
This will be displayed in your transfer activity.
Get Globus Connect
Turn your computer into an endpoint. The easiest and most convenient way to send and receive files on your machine.

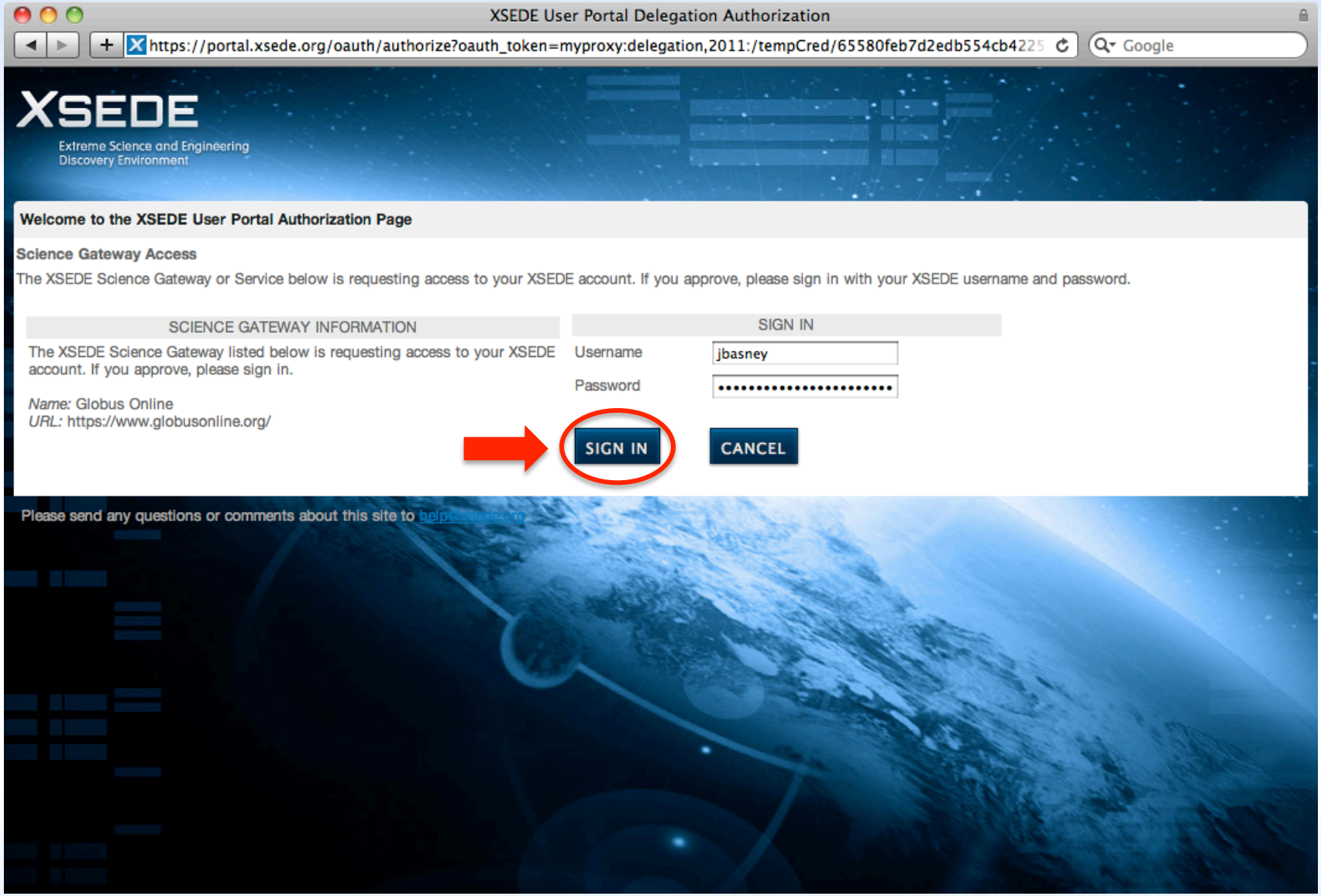

Start Transfer | Transfer | GlobusOnline
https://www.globusonline.org/xfer/StartTransfer
Google
globus online
Go To: Start Transfer
jbasney
Sign Out
Transfer Files -
source overwrites files on destination
View Transfer Activity
Endpoint
xsede#forge
Go
Path
Go
Endpoint
Go
Path
Go
Activate Endpoint: xsede#forge
The administrator of this endpoint, xsede#forge, requires that you authenticate using their MyProxy OAuth server to activate the endpoint. When you click 'Continue' you will be redirected to their website.
Continue
Cancel
Please select an endpo
an endpoint above.
Label This Transfer
This will be displayed in your transfer activity.
Get Globus Connect
Turn your computer into an endpoint. The easiest and most convenient way to send and receive files on your machine.

Globus Online Example

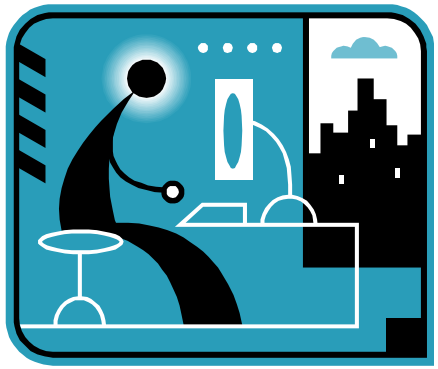




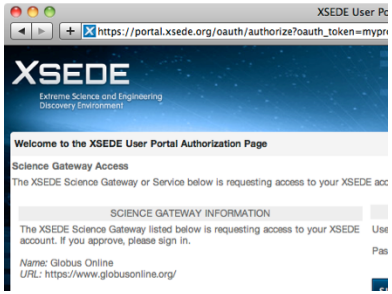


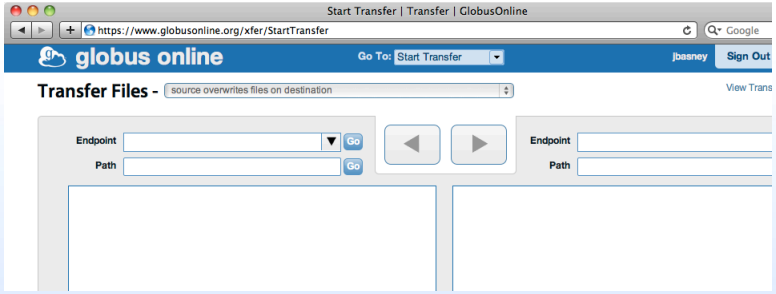

XSEDE User Portal Delegation Authorization
https://portal.xsede.org/oauth/authorize?oauth_token=myproxy:delegation,2011:/tempCred/65580feb7d2edb554cb4225
Google
XSEDE
Extreme Science and Engineering Discovery Environment
Welcome to the XSEDE User Portal Authorization Page
Science Gateway Access
The XSEDE Science Gateway or Service below is requesting access to your XSEDE account. If you approve, please sign in with your XSEDE username and password.
SCIENCE GATEWAY INFORMATION
The XSEDE Science Gateway listed below is requesting access to your XSEDE account. If you approve, please sign in.
Name: Globus Online
URL: https://www.globusonline.org/
SIGN IN
Username
jbasney
Password
SIGN IN
CANCEL
Please send any questions or comments about this site to

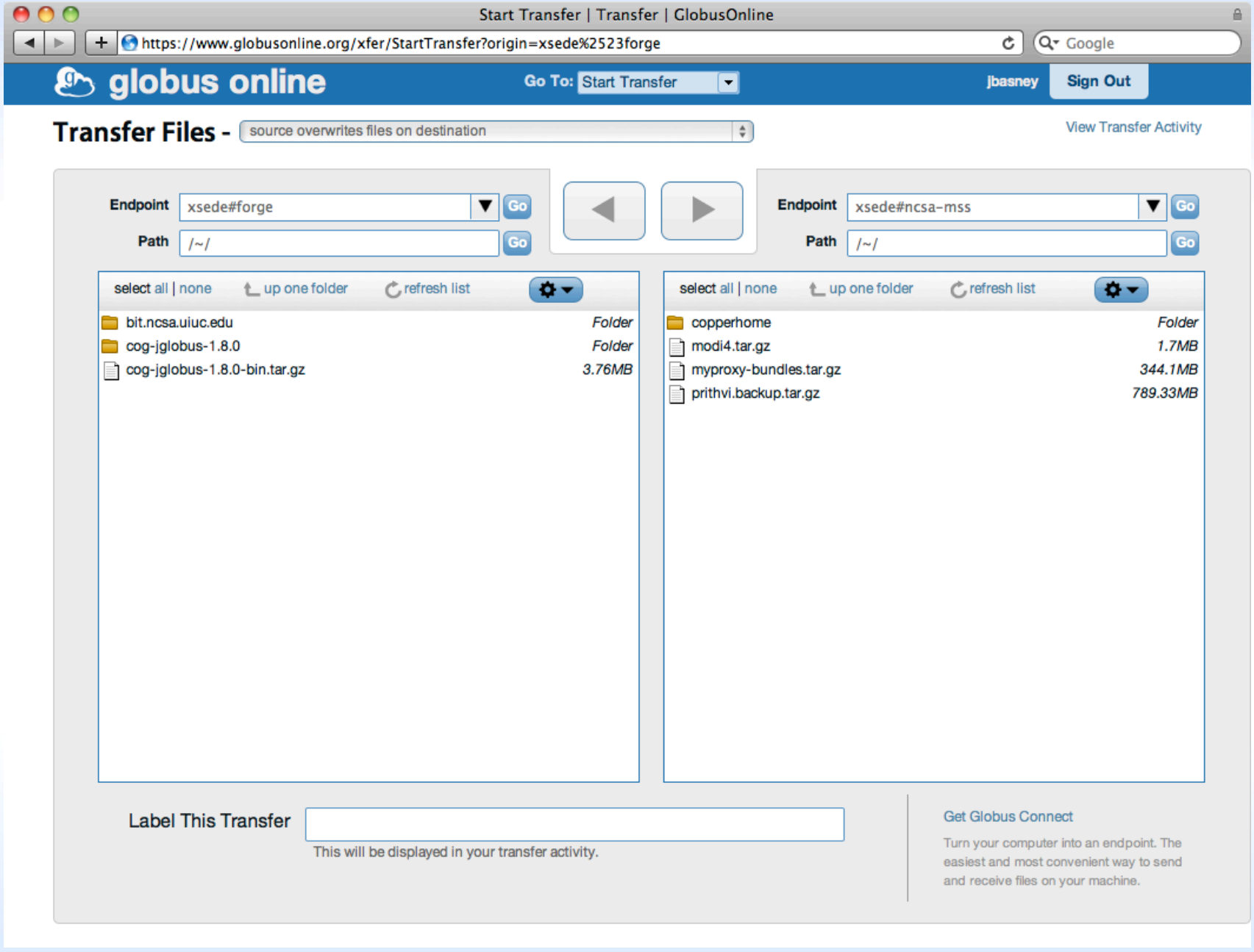
Globus Online Example

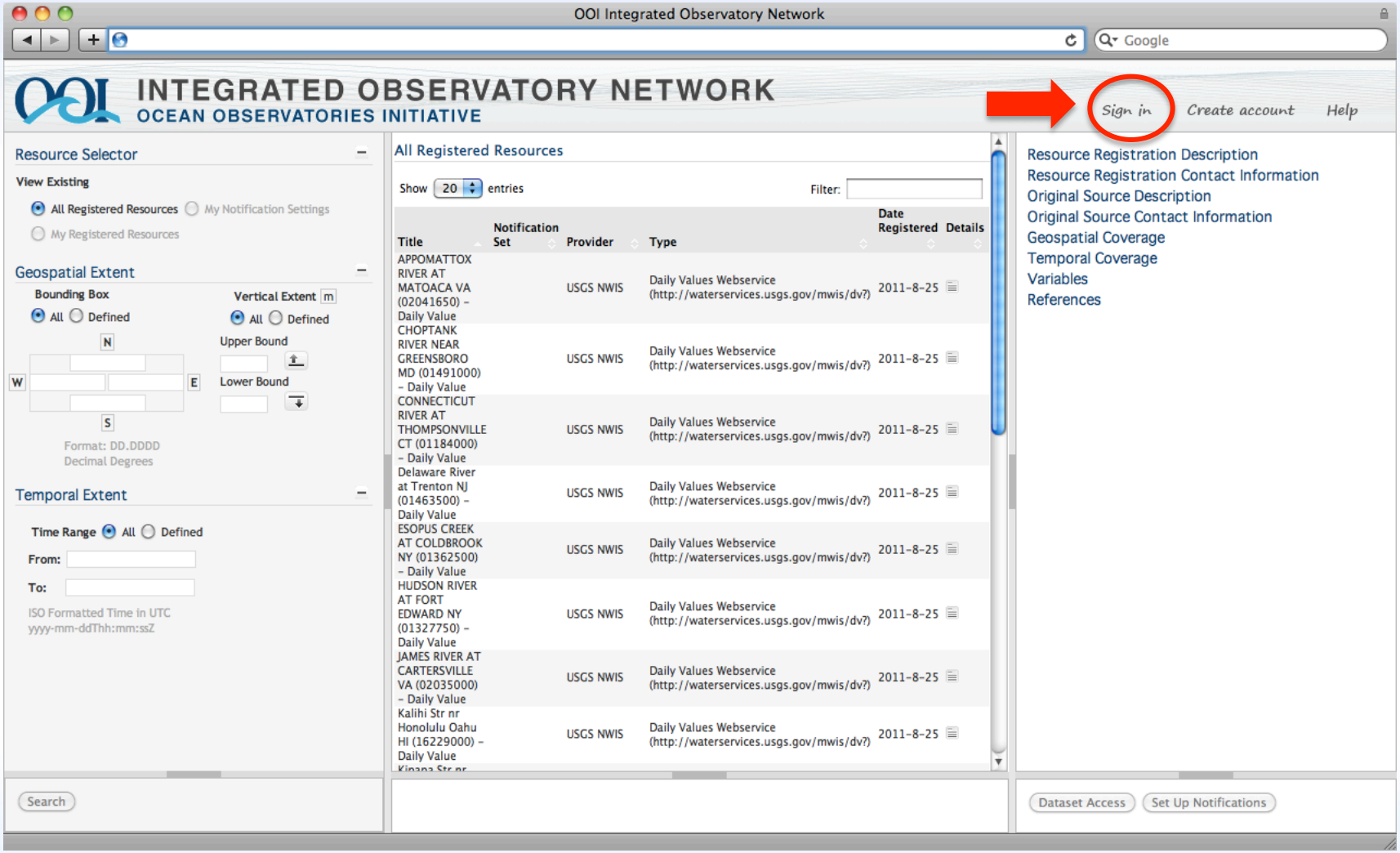


MyProxy
Credential Management Service

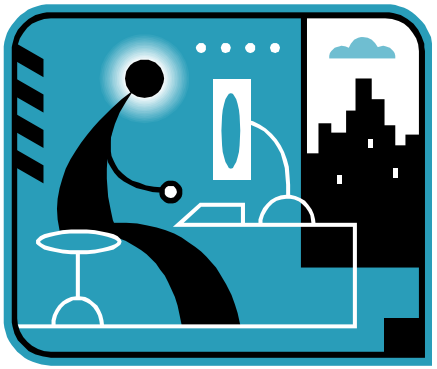


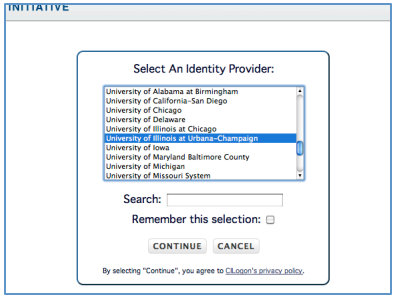


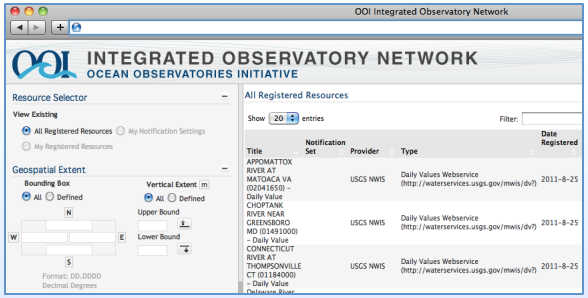

Start Transfer | Transfer | GlobusOnline
https://www.globusonline.org/xfer/StartTransfer?origin=xsede%2523forge
Google
globus online
Go To: Start Transfer
jbasney
Sign Out
Transfer Files -
source overwrites files on destination
View Transfer Activity
Endpoint
xsede#forge
Go
Path
/~/
Go
Endpoint
xsede#ncsa-mss
Go
Path
/~/
Go
select all | none
up one folder
refresh list
bit.ncsa.uiuc.edu Folder
cog-jglobus-1.8.0 Folder
cog-jglobus-1.8.0-bin.tar.gz 3.76MB
select all | none
up one folder
refresh list
copperhome Folder
modi4.tar.gz 1.7MB
myproxy-bundles.tar.gz 344.1MB
prithvi.backup.tar.gz 789.33MB
Label This Transfer
This will be displayed in your transfer activity.
Get Globus Connect
Turn your computer into an endpoint. The easiest and most convenient way to send and receive files on your machine.

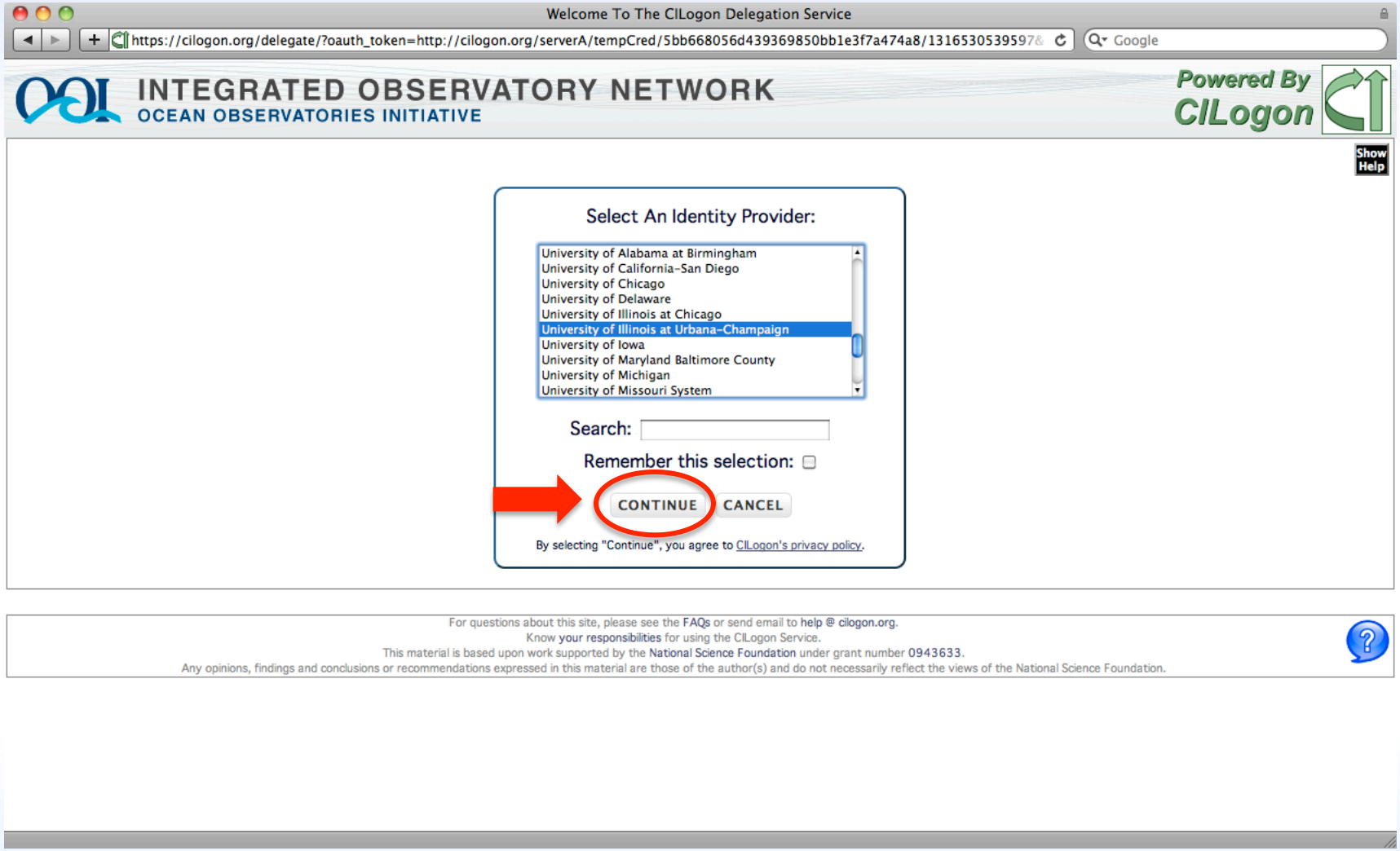

OOI Integrated Observatory Network
Google
INTEGRATED OBSERVATORY NETWORK
OCEAN OBSERVATORIES INITIATIVE
Sign in
Create account
Help
Resource Selector
View Existing
All Registered Resources
My Notification Settings
My Registered Resources
Geospatial Extent
Bounding Box
All
Defined
N
W
E
S
Format: DD.DDDD
Decimal Degrees
Vertical Extent m
All
Defined
Upper Bound
Lower Bound
Temporal Extent
Time Range
All
Defined
From:
To:
ISO Formatted Time in UTC
yyyy-mm-ddThh:mm:ssZ
Search
All Registered Resources
Show 20 entries
Filter:
Title
Notification Set
Provider
Type
Date Registered
Details
APPOMATTOX RIVER AT MATOACA VA (02041650) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
CHOPTANK RIVER NEAR GREENSBORO MD (01491000) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
CONNECTICUT RIVER AT THOMPSONVILLE CT (01184000) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
Delaware River at Trenton NJ (01463500) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
ESOPUS CREEK AT COLDBROOK NY (01362500) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
HUDSON RIVER AT FORT EDWARD NY (01327750) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
JAMES RIVER AT CARTERSVILLE VA (02035000) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
Kalihi Str nr Honolulu Oahu HI (16229000) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)
2011-8-25
Resource Registration Description
Resource Registration Contact Information
Original Source Description
Original Source Contact Information
Geospatial Coverage
Temporal Coverage
Variables
References
Dataset Access
Set Up Notifications

OOI Example



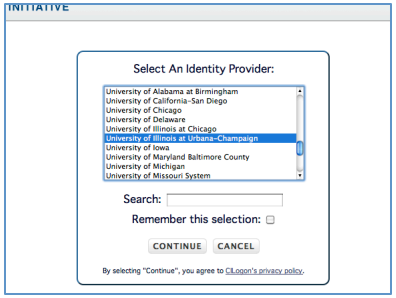

Select An Identity Provider:
University of Alabama at Birmingham
University of California-San Diego
University of Chicago
University of Delaware
University of Illinois at Chicago
University of Illinois at Urbana-Champaign
University of Iowa
University of Maryland Baltimore County
University of Michigan
University of Missouri System
Search:
Remember this selection:
CONTINUE
CANCEL

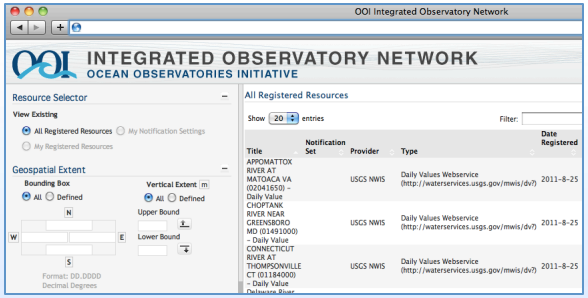

OOI Integrated Observatory Network
INTEGRATED OBSERVATORY NETWORK
OCEAN OBSERVATORIES INITIATIVE
Resource Selector
View Existing
All Registered Resources
Geospatial Extent
Bounding Box
Vertical Extent
Upper Bound
Lower Bound
All Registered Resources
Show 20 entries
Filter:
Title
Notification Set
Provider
Type
Date Registered

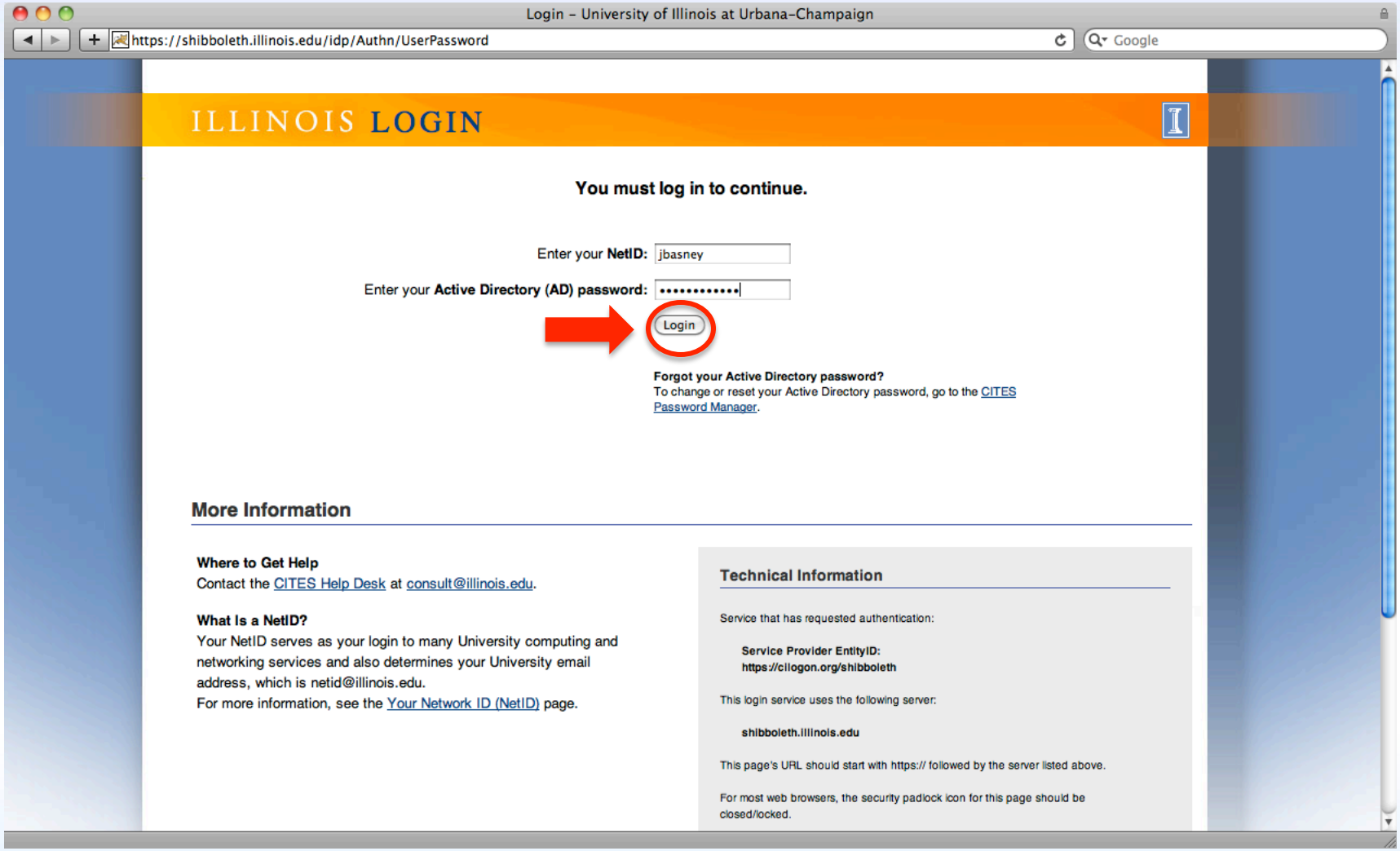

Welcome To The CILogon Delegation Service
https://cilogon.org/delegate/?oauth_token=http://cilogon.org/serverA/tempCred/5bb668056d439369850bb1e3f7a474a8/1316530539597&
Google
INTEGRATED OBSERVATORY NETWORK
OCEAN OBSERVATORIES INITIATIVE
Powered By CILogon
Show Help
Select An Identity Provider:
University of Alabama at Birmingham
University of California-San Diego
University of Chicago
University of Delaware
University of Illinois at Chicago
University of Illinois at Urbana-Champaign
University of Iowa
University of Maryland Baltimore County
University of Michigan
University of Missouri System
Search:
Remember this selection:
CONTINUE
CANCEL
By selecting "Continue", you agree to CILogon's privacy policy.
For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.
This material is based upon work supported by the National Science Foundation under grant number 0943633.
Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

OOI Example

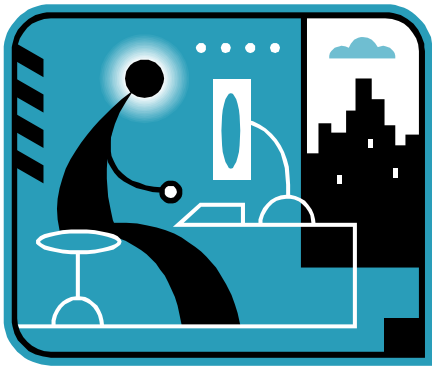

Login – University of Illinois at Urbana
://shibboleth.illinois.edu/idp/Authn/UserPassword
ILLINOIS LOGIN
You must log in to continu
Enter your NetID:
jbasney
Enter your Active Directory (AD) password:
Login
Forgot your Active Dire
To change or reset your
Password Manager.

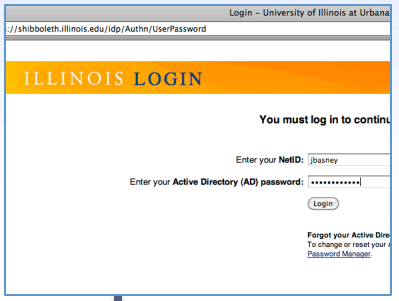

INITIATIVE
Select An Identity Provider:
University of Alabama at Birmingham
University of California-San Diego
University of Chicago
University of Delaware
University of Illinois at Chicago
University of Illinois at Urbana-Champaign
University of Iowa
University of Maryland Baltimore County
University of Michigan
University of Missouri System
Search:
Remember this selection:
CONTINUE
CANCEL
By selecting "Continue", you agree to CILogon's privacy policy.

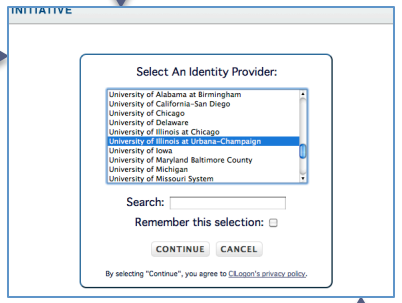

OOI Integrated Observatory Network
INTEGRATED OBSERVATORY NETWORK
OCEAN OBSERVATORIES INITIATIVE
Resource Selector
View Existing
All Registered Resources
My Notification Settings
My Registered Resources
Geospatial Extent
Bounding Box
All
Defined
Vertical Extent
Upper Bound
Lower Bound
Format: DD.DDDD
Decimal Degrees
All Registered Resources
Show 20 entries
Filter:
Title
Notification Set
Provider
Type
Date Registered
APPOMATTOX RIVER AT MATOACA VA (02041650) - Daily Value
CHOPTANK RIVER NEAR GREENSBORO MD (01491000) - Daily Value
CONNECTICUT RIVER AT THOMPSONVILLE CT (01184000) - Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/nwis/dv/)
2011-8-25

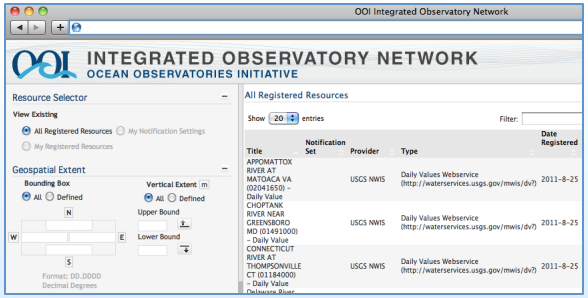

Login – University of Illinois at Urbana-Champaign
https://shibboleth.illinois.edu/idp/Authn/UserPassword
Google
ILLINOIS LOGIN
You must log in to continue.
Enter your NetID: jbasney
Enter your Active Directory (AD) password:
Login
Forgot your Active Directory password?
To change or reset your Active Directory password, go to the CITES Password Manager.
More Information
Where to Get Help
Contact the CITES Help Desk at consult@illinois.edu.
What Is a NetID?
Your NetID serves as your login to many University computing and networking services and also determines your University email address, which is netid@illinois.edu.
For more information, see the Your Network ID (NetID) page.
Technical Information
Service that has requested authentication:
Service Provider EntityID:
https://cilogon.org/shibboleth
This login service uses the following server:
shibboleth.illinois.edu
This page's URL should start with https:// followed by the server listed above.
For most web browsers, the security padlock icon for this page should be closed/locked.

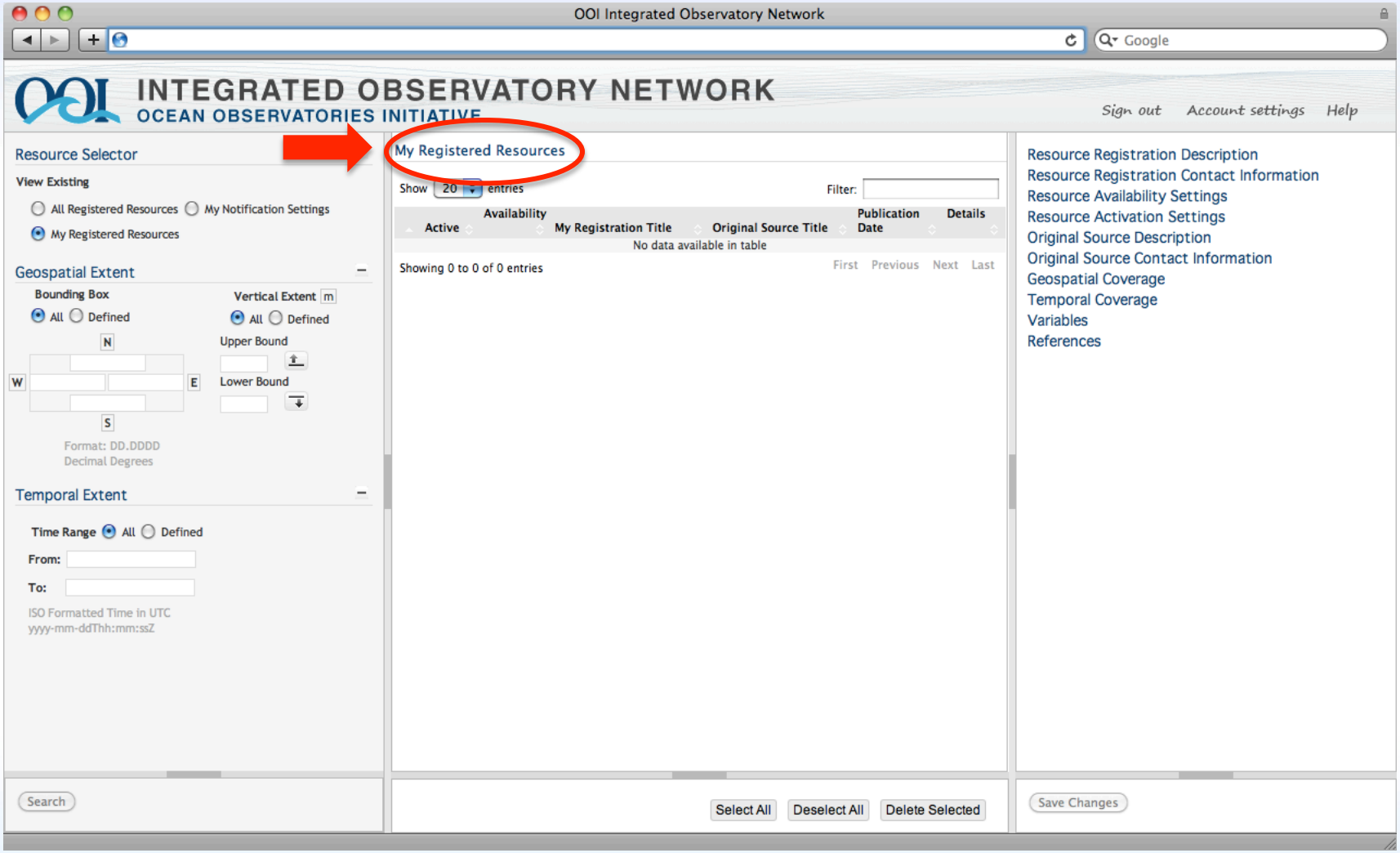
OOI Example




Login – University of Illinois at Urbana
://shibboleth.illinois.edu/idp/Authn/UserPassword
ILLINOIS LOGIN
You must log in to continu
Enter your NetID:
jbasney
Enter your Active Directory (AD) password:
Login
Forgot your Active Dire
To change or reset your
Password Manager.


INITIATIVE
Select An Identity Provider:
University of Alabama at Birmingham
University of California-San Diego
University of Chicago
University of Delaware
University of Illinois at Chicago
University of Illinois at Urbana-Champaign
University of Iowa
University of Maryland Baltimore County
University of Michigan
University of Missouri System
Search:
Remember this selection:
CONTINUE
CANCEL
By selecting "Continue", you agree to CILogon's privacy policy.


OOI Integrated Observatory Network
INTEGRATED OBSERVATORY NETWORK
OCEAN OBSERVATORIES INITIATIVE
Resource Selector
View Existing
All Registered Resources
My Notification Settings
My Registered Resources
Geospatial Extent
Bounding Box
All
Defined
Vertical Extent
Upper Bound
Lower Bound
Format: DD.DDDD
Decimal Degrees
All Registered Resources
Show 20 entries
Filter:
Title
Notification Set
Provider
Type
Date Registered
APPOMATTOX RIVER AT MATOACA VA (02041650) – Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/nwis/dv/)
2011-8-25
CHOPTANK RIVER NEAR GREENSBORO MD (01491000) – Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/nwis/dv/)
2011-8-25
CONNECTICUT RIVER AT THOMPSONVILLE CT (01184000) – Daily Value
USGS NWIS
Daily Values Webservice (http://waterservices.usgs.gov/nwis/dv/)
2011-8-25


OOI Integrated Observatory Network
Google
INTEGRATED OBSERVATORY NETWORK
OCEAN OBSERVATORIES INITIATIVE
Sign out
Account settings
Help
Resource Selector
View Existing
All Registered Resources
My Notification Settings
My Registered Resources
Geospatial Extent
Bounding Box
All
Defined
Vertical Extent
m
All
Defined
N
W
E
S
Upper Bound
Lower Bound
Format: DD.DDDD
Decimal Degrees
Temporal Extent
Time Range
All
Defined
From:
To:
ISO Formatted Time in UTC
yyyy-mm-ddThh:mm:ssZ
Search
My Registered Resources
Show
20
entries
Filter:
Active
Availability
My Registration Title
Original Source Title
Publication Date
Details
No data available in table
Showing 0 to 0 of 0 entries
First
Previous
Next
Last
Select All
Deselect All
Delete Selected
Resource Registration Description
Resource Registration Contact Information
Resource Availability Settings
Resource Activation Settings
Original Source Description
Original Source Contact Information
Geospatial Coverage
Temporal Coverage
Variables
References
Save Changes

Starting the Discussion

- What are science gateways doing today for web security?
  - Using OAuth, OpenID, SAML?
  - Supporting both individual and community accounts?
  - Authenticating to REST services?
  - Sharing data across multiple gateways?
- What are current/future science gateway security needs?
  - What is your input on our project plans?
    - Getting certificates from MyProxy servers
    - Delegating certificates between gateway components
    - Delegated access to REST services
    - Integration with external authentication (LDAP, Kerberos, SAML, OpenID)
    - OAuth 2.0 update
    - Credential refresh
    - Web Single Sign-On (OpenID Connect)
  - What is your input on the XSEDE architecture?

Continuing the Discussion

- Please join our discuss@sciencegatewaysecurity.org mailing list:
  - Send email to: discuss+subscribe@sciencegatewaysecurity.org
  - Or visit: https://groups.google.com/a/sciencegatewaysecurity.org/group/discuss/subscribe