

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



NCSA



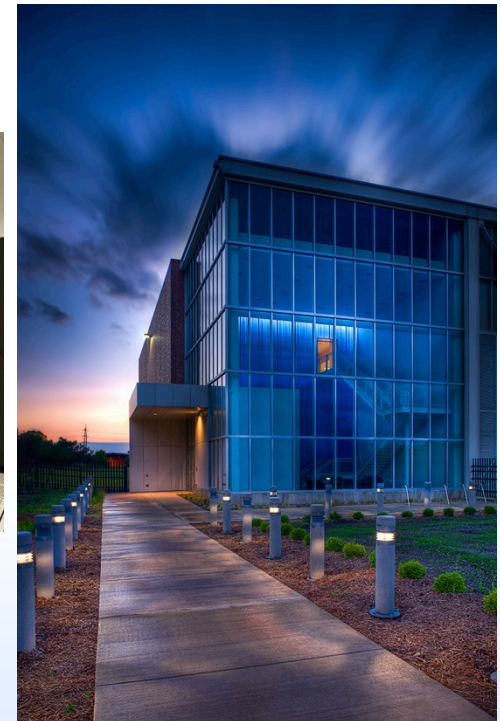
INDIANA UNIVERSITY



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

National Center for Supercomputing Applications (NCSA)

- Located at University of Illinois at Urbana-Champaign
- Established in 1986 by NSF Supercomputer Centers Program



www.ncsa.illinois.edu

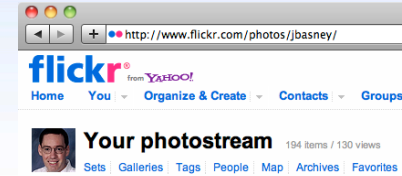
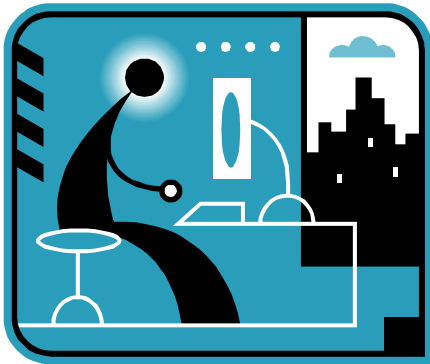
Distributed Web Security for Science Gateways



- Software Development for Cyberinfrastructure grant from the NSF Office of CyberInfrastructure (www.nsf.gov/oci)
 - 3 year project: August 2011 – July 2014
- Co-PIs: Marlon Pierce (IU), Rion Dooley (TACC)

- *What is cyberinfrastructure?*
 - Supercomputers, mass-storage systems, data repositories, networks, software and more
 - Supporting science and engineering research and education

Motivating Example: Photo Printing



2
Your
flickr
Password

3
Photos

1
Your
flickr
Password



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 photos on Flickr
 - Collaboratively edit an online Google doc
- **Credential:** *How security information is conveyed*
 - Also known as **Assertion** or **Token**

Delegated Authorization

Authenticate &
Grant Access
to Photos

2

3

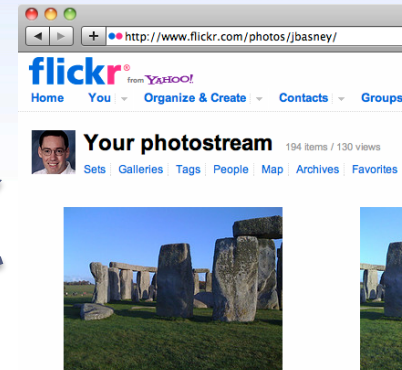
Token

4

Token

1

Request
Access to
Photos



5
Token

6
Photos



OAuth

- An open protocol for delegated authorization (oauth.net)
- Development
 - OAuth 1.0 released (October 2007)
 - OpenID+OAuth hybrid developed (2009)
 - OAuth 1.0a revision (June 2009)
 - RFC 5849 (Informational), April 2010
 - OAuth WRAP (2009-2010)
 - Basis for OAuth 2.0
 - OAuth 2.0 Standards Track RFC coming soon
 - OpenID Connect based on OAuth 2.0
- Used by Flickr, Twitter, Facebook, Google, Netflix, ...





NETFLIX

FeedFliks wants to access your Netflix Account.

To confirm, please login to Netflix:

Login

Password

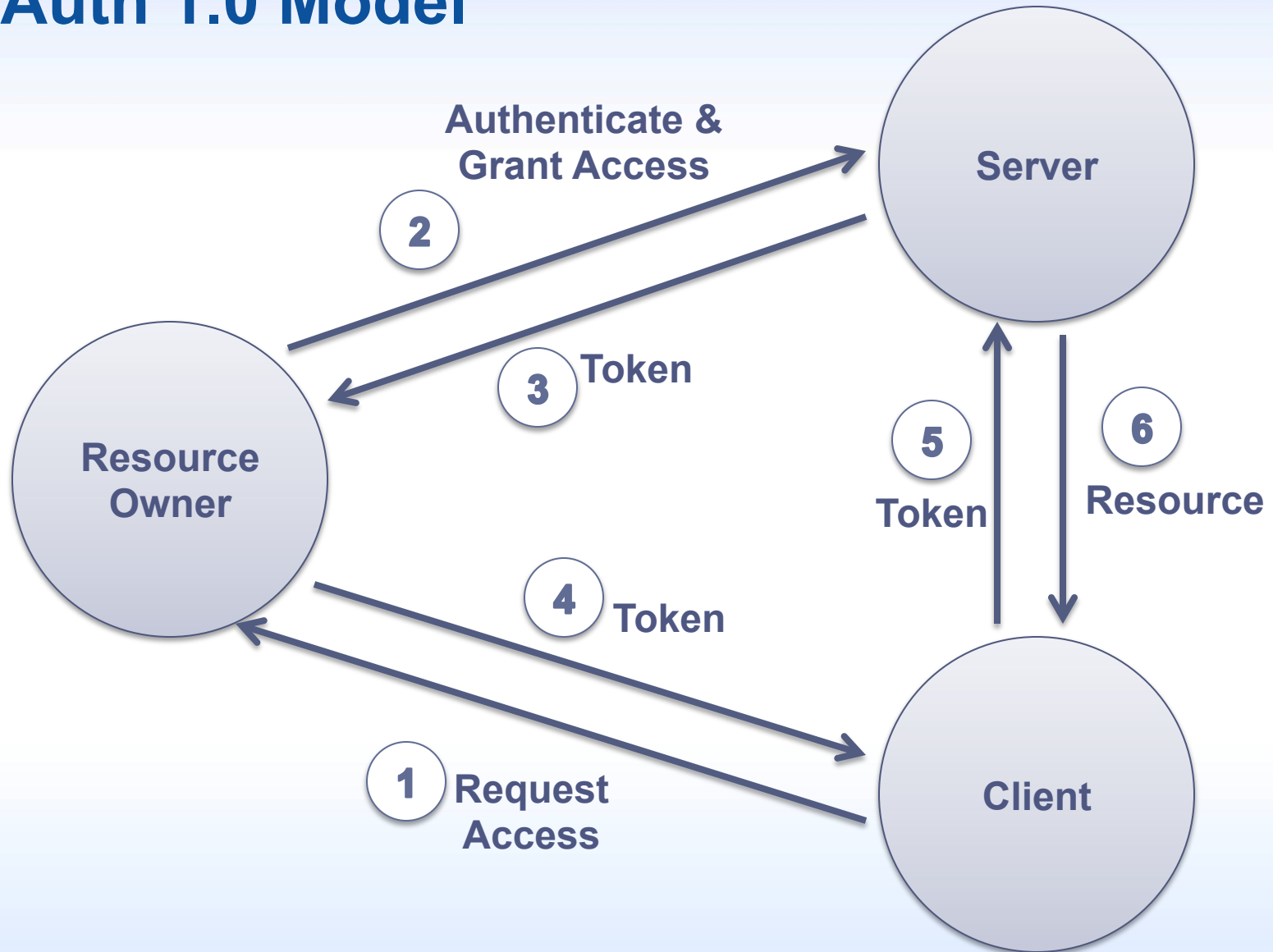
Yes, Link This Account

You should not authorize **FeedFliks** unless you trust them with access to your account. By confirming, you allow **FeedFliks** to access, share and update your Netflix data, including your queue, rental history, and ratings.

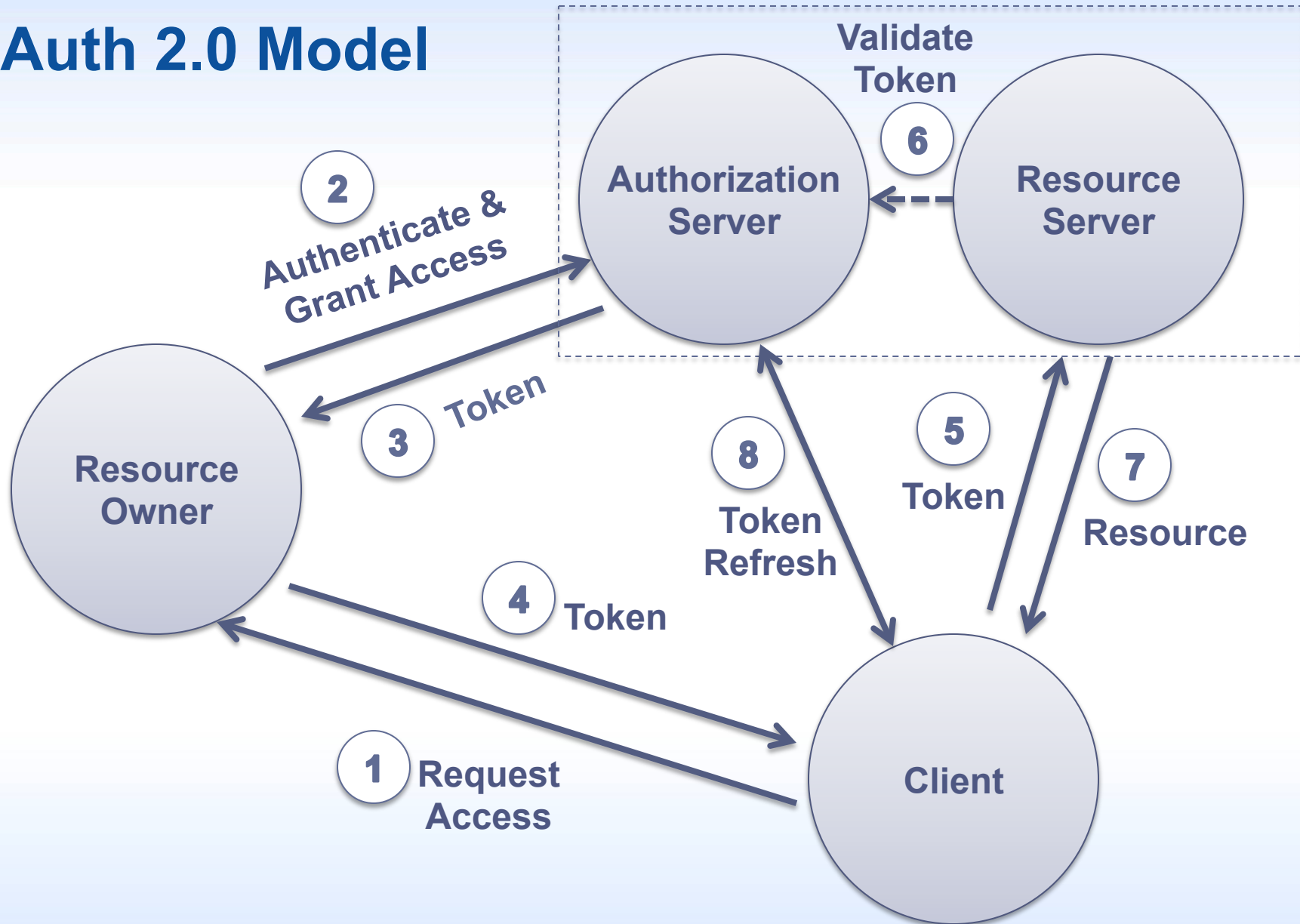
This page is provided by Netflix to authorize third-party applications, but has not been configured to send requests securely. If you grant access but you did not initiate this request at **FeedFliks**, it may be possible for other users of **FeedFliks** to access your data. We recommend you deny access unless you are certain that you initiated this request directly within **FeedFliks**.

Your password will always remain private, but **FeedFliks** will have ongoing access to your account. You can remove access at any time in [Your Account](#). Your usage of any third party application that interacts with Netflix is governed by the Netflix [Terms of Use](#).

OAuth 1.0 Model



OAuth 2.0 Model



[Home](#) / [Log in](#)

Log in with a SourceForge account

Enter your account info:

Username:

Password:

Remember Me [?](#)

Log in

[Forgot your username/password?](#)

Need an account on SourceForge.net?
[Create Account](#)

Log in with OpenID

Please click your account provider:



Remember Me [?](#)

Log in

[Problems logging in with OpenID?](#)

OpenID eliminates the need for multiple usernames across different websites.

[Learn more - Get an OpenID](#)



[Sign up for a new Google Account](#)

Accounts

Sign in to **Sourceforge.net** with your Google Account. [Learn more](#)

Sign in

Google

Email

jbasney@sciencegatewaysecurity.org

Password

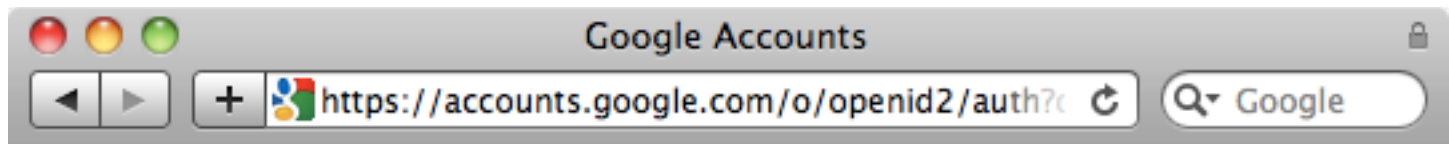
.....



Sign in

Stay signed in

[Can't access your account?](#)



Google accounts

[Sign in as a different user](#)

You are signing in to **Sourceforge.net** with your Google Account
jbasney@sciencegatewaysecurity.org



Remember me

You can always change your Google Account approval settings. Sourceforge.net is not owned, operated, or controlled by Google or its owners. [Learn more](#)



Find, Create, and Publish Open Source software for free

Search from thousands of software titles

Search

TODAY:

↓ 4,123,532 DOWNLOADS

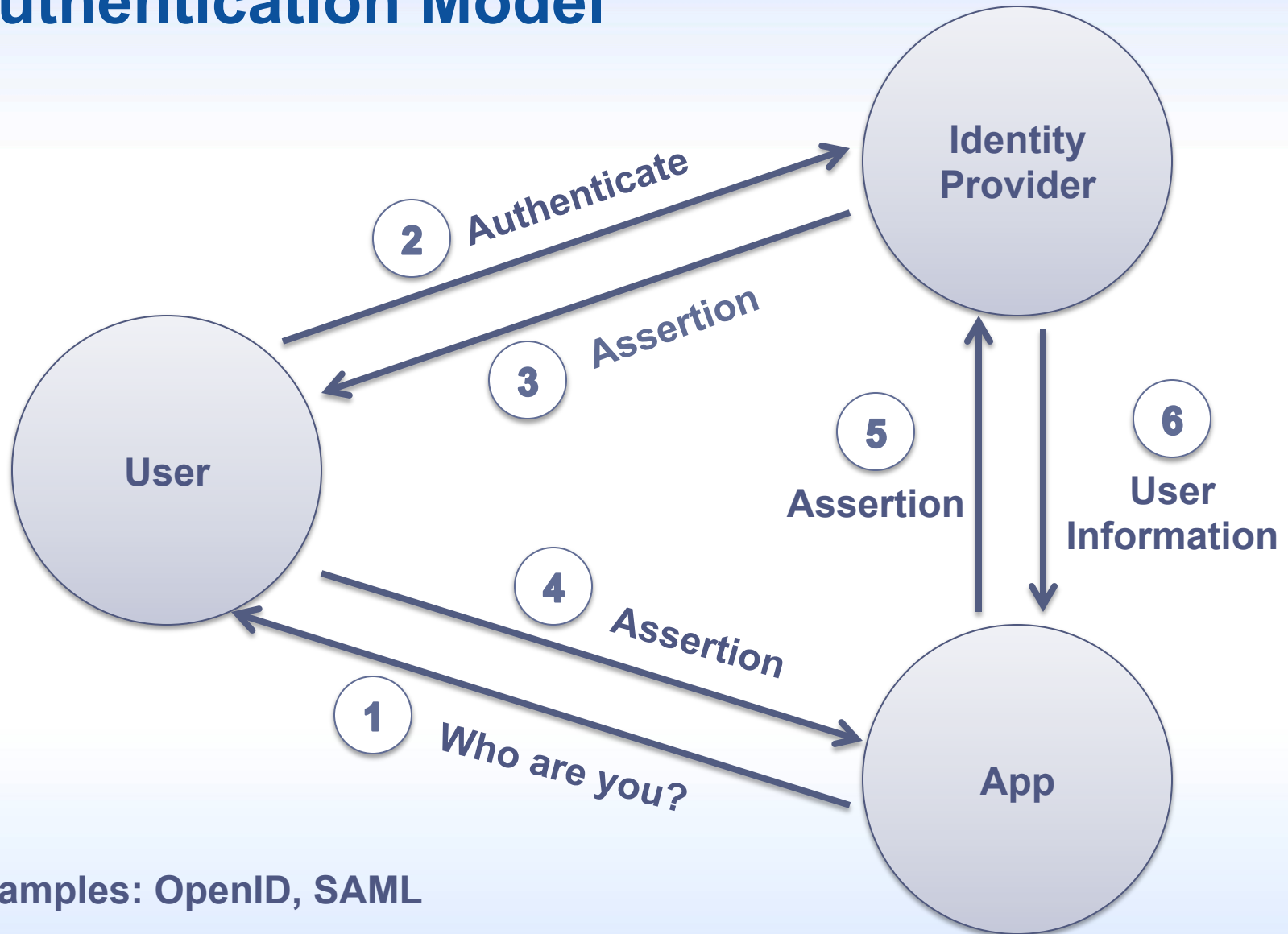
✓ 5,438 CODE COMMITS

💬 4,905 FORUM POSTS

🐛 743 BUGS TRACKED

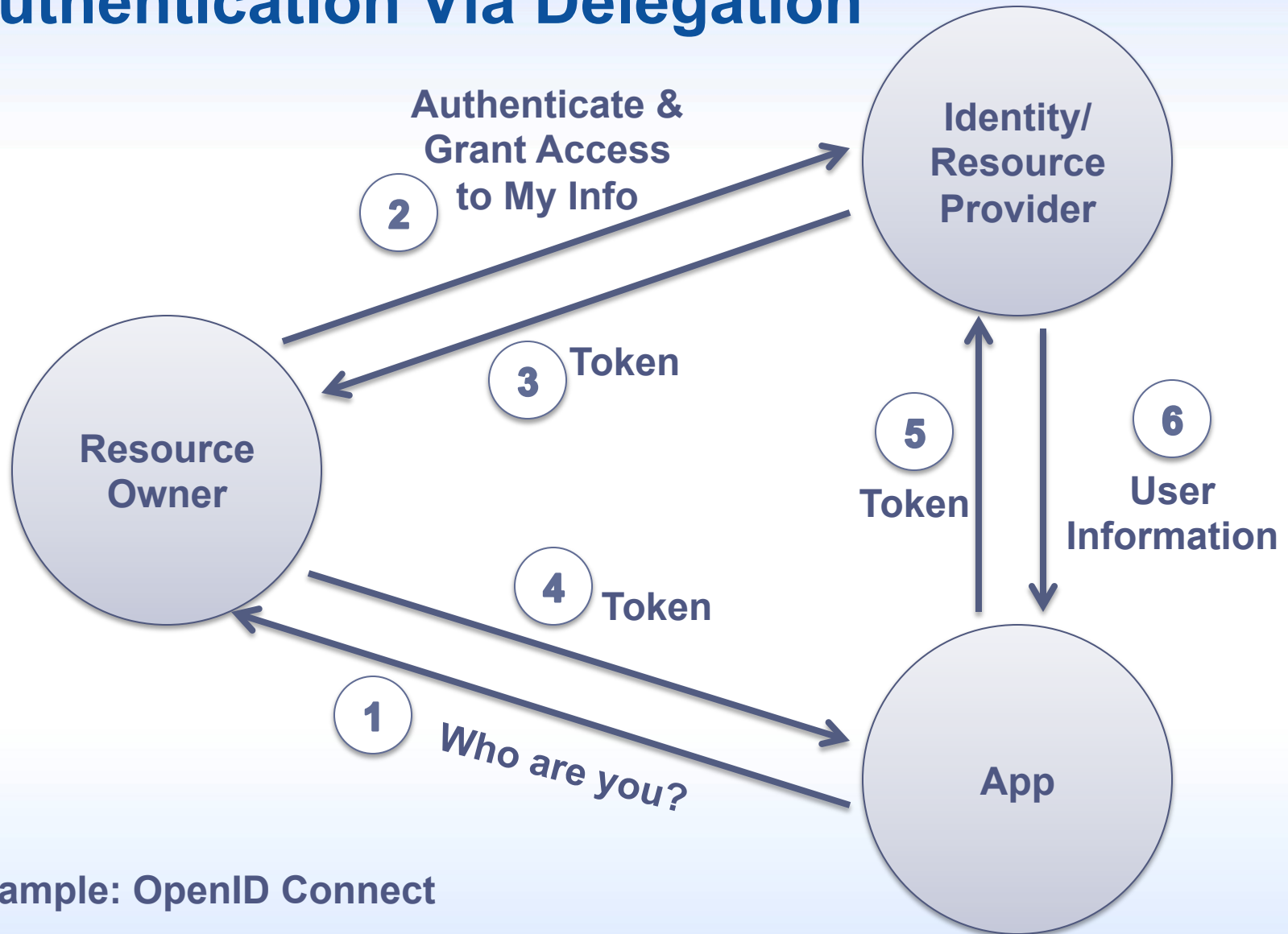
👁️ [MORE DETAILS](#)

Authentication Model



Examples: OpenID, SAML

Authentication Via Delegation



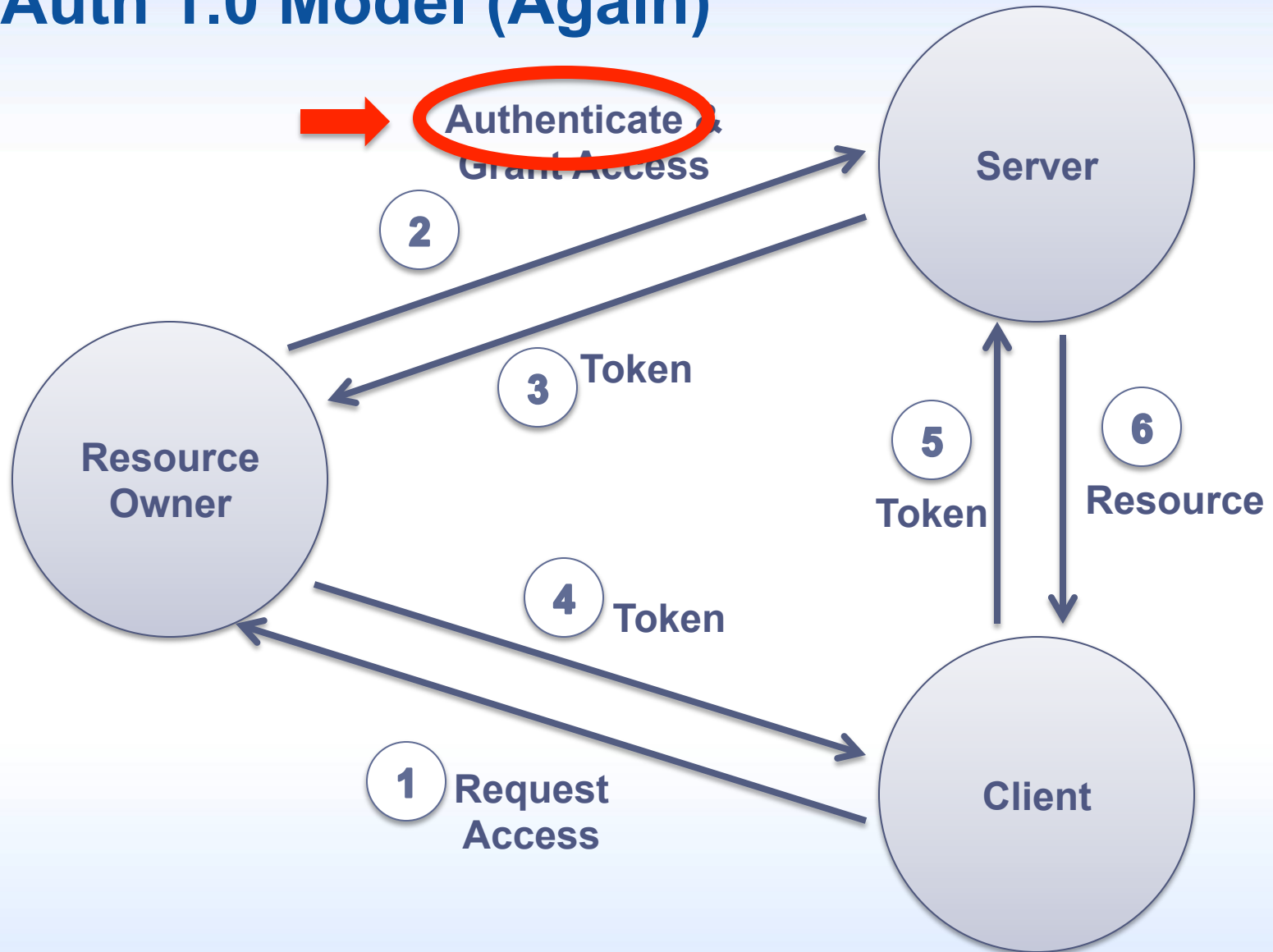
Example: OpenID Connect

Authentication Via Delegation

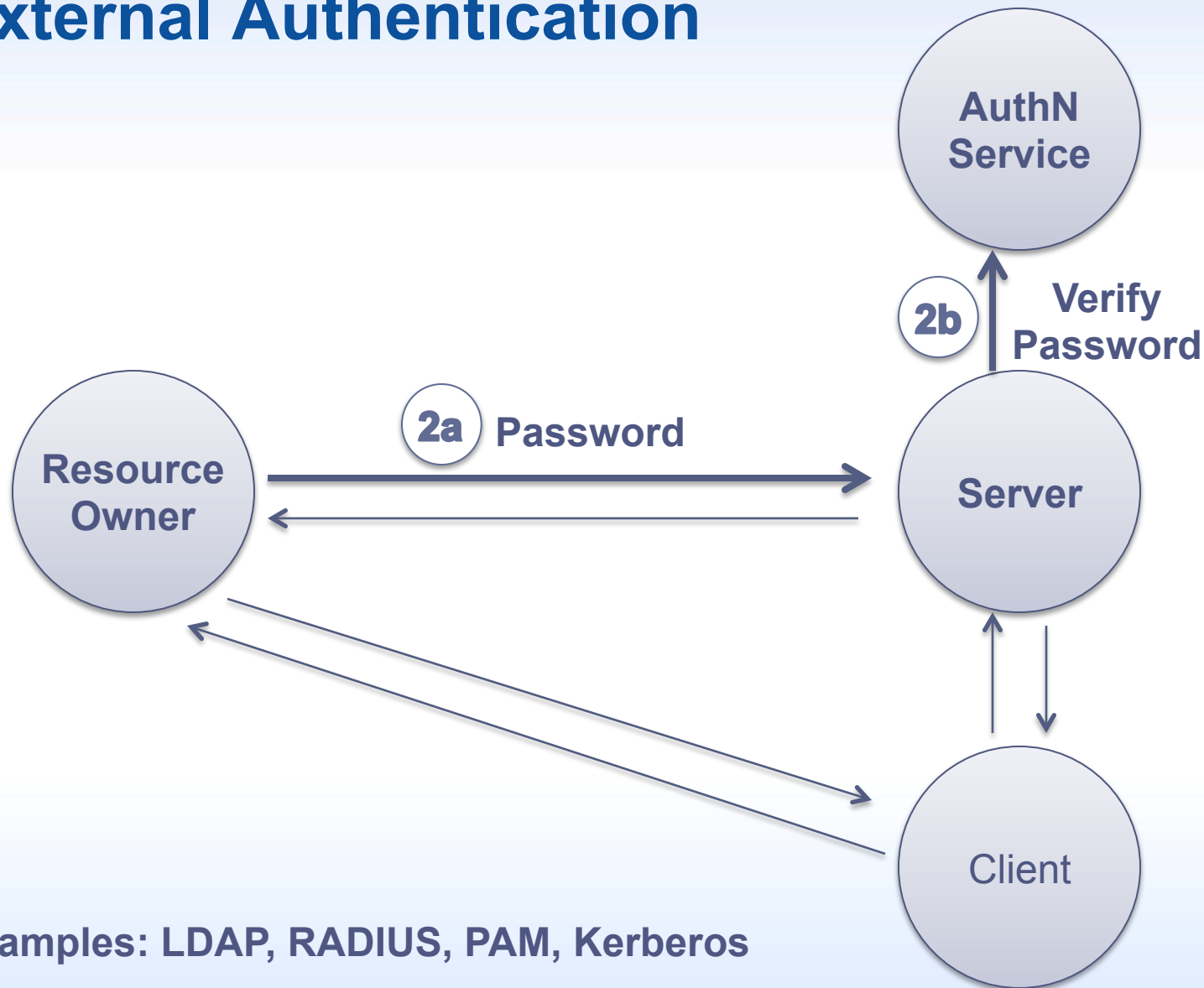
- Bad Idea
 - App: Who are you?
 - User: Here's full access to my Twitter account.
- Better Idea
 - App: Who are you?
 - User: Here's read access to my Twitter account profile.
- Delegated access to user's profile information
 - <http://nat.sakimura.org/2011/05/15/dummys-guide-for-the-difference-between-oauth-authentication-and-openid/>
- Example: **OpenID Connect** built on OAuth



OAuth 1.0 Model (Again)

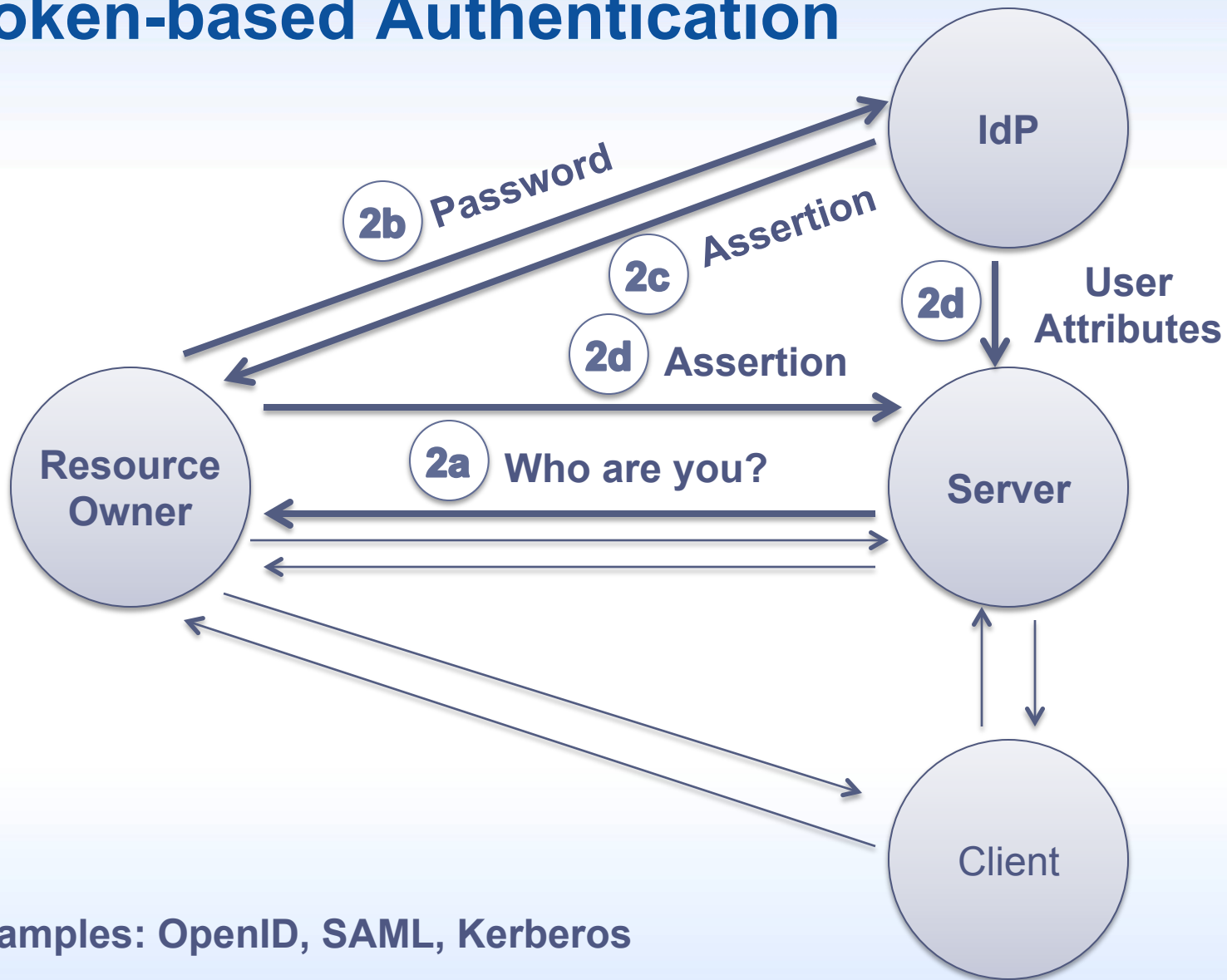


External Authentication



Examples: LDAP, RADIUS, PAM, Kerberos

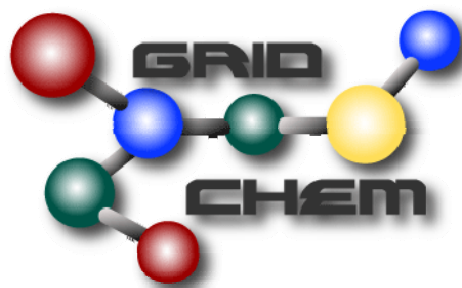
Token-based Authentication



Examples: OpenID, SAML, Kerberos

Science Gateways

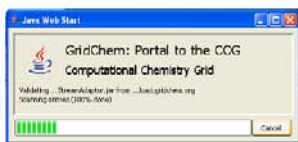
The image displays a collage of several science gateway web pages. At the top left is the **CyberGIS Gateway** page, which features a navigation menu with 'Home', 'Resources', 'Community', 'Support', and 'About'. Below the menu is a search bar and a 'Login' button. The main content area is titled 'Featured Applications' and includes a section for 'Computational Chemistry Grid' with a molecular structure graphic. To the right is the **Globus Online** page, which has a blue header with the text 'Reliable, high-performance, secure file transfer. Move files fast. No IT required.' and a large white arrow pointing upwards. Below this is a 'WATCH A VIDEO' button. In the center is the **iPlant Collaborative** page, which has a green header and a main banner with the text 'Challenge: iPlant develops a vision for plant science cyberinfrastructure'. Below the banner are several columns of content, including 'CHALLENGE', 'DISCOVER', 'LEARN', and 'CONNECT'. At the bottom left of the collage are logos for various institutions: **CCS** (Center for Computational Sciences, University of Kentucky), **ccit** (Center for Computation and Technology), **NCSA TACC** (National Center for Supercomputing Applications, Texas Advanced Computing Center), **OSC** (Ohio Supercomputer Center), and **Natio Science Found**. At the bottom right is the **UltraScan LIMS Portal** page, which has a dark header and a main section titled 'Welcome to the TeraGrid Science Gateway for UltraScan!'. Below this is a 'DISCLAIMER' section and a list of funding sources, including the Department of Biochemistry at the University of Texas Health Science Center at San Antonio, the National Science Foundation, and the National Institutes of Health.



Computational Chemistry Grid: Production Cyberinfrastructure for Computational Chemistry

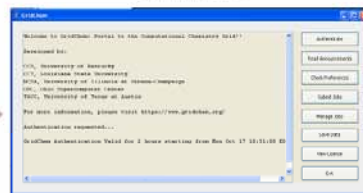
For more information, please visit www.gridchem.org or contact help@gridchem.org.

JAVA WEB START

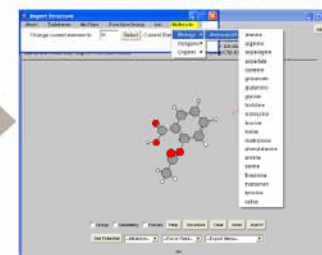


Client Application runs on Local Machine

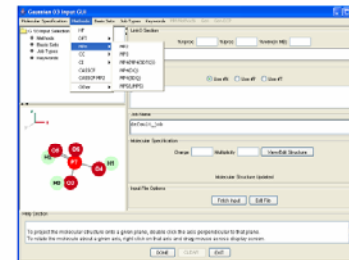
INTRO



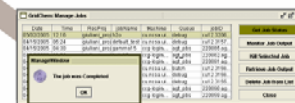
BUILD MOLECULE



BUILD INPUT FILE



SUBMIT



CLIENT

Graphical user interface (GUI) helps scientists:

- generate input
- submit and monitor quantum chemistry jobs
- remotely visualize output data

Client available for multiple platforms (Linux & Windows)

No Grid services needed on client system



Middleware Server

Middleware interface to the computational grid

- authentication
- data management
- resource specification
- routes jobs
- provides client with job status information
- provides access to job data for analysis
 - input, output, job details stored in mass storage archive
- resource discovery
- accounting management
- system and job monitoring

DOWNLOAD RESULTS



Grid Services
Leveraging NMI Software

CCG Resources

3,525,000 CPU hours available annually

POST PROCESS REVIEW

Supported by the NSF NMI Program under Award #04-38312

NCSA
www.ncsa.uiuc.edu

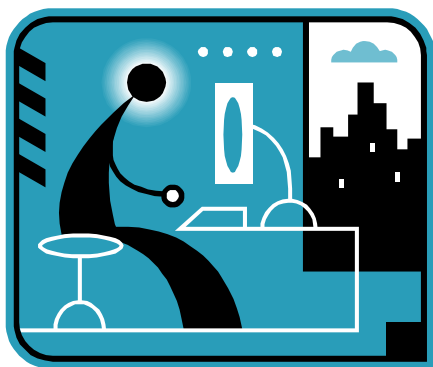
CCS
Center for Computational Sciences
UNIVERSITY OF KENTUCKY
www.ccs.uky.edu

CCT
www.cct.lsu.edu

OSC
www.osc.edu

TACC
www.tacc.utexas.edu

Science Gateways: Accessing Resources



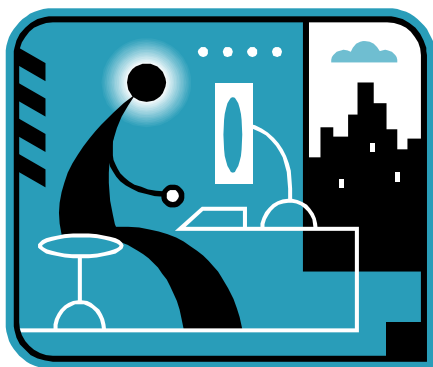
The screenshot shows the homepage of the Computational Chemistry Grid (CCG). The header includes the CCG logo and navigation links: 'about us', 'news', 'downloads', 'training & documentation', 'on-line help', and 'contact us'. The main content area is divided into several sections: 'Home' with a 'Welcome' message, 'User Area' with links for account management, 'Project' with links for downloads and manuals, 'Resources' with links for HPC resources and outreach, 'Notices' with announcements about G09 and Molpro availability and a power outage, and 'External Collaborations'. A 'Calendar of Events' is also visible on the right side of the page.



user accesses
science gateway

science gateway uses
external resources
(supercomputers,
compute clusters,
data stores)

Science Gateways: Tiered Access Models



user
authenticates to
science gateway

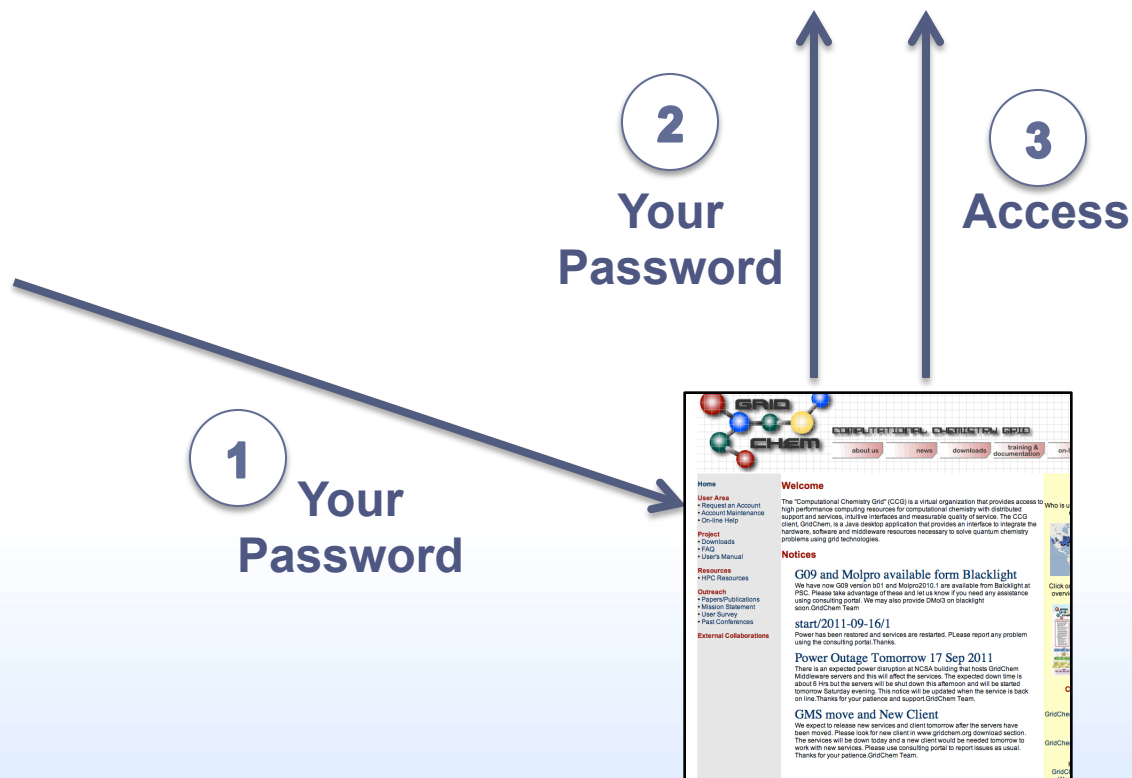


science gateway
authenticates to
service providers

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
- Option B: Delegation of Rights
 - End user has account at underlying service provider
 - Goal: Use underlying services via science gateway interfaces
 - Science Gateway explicitly acts on the user's behalf when interacting with the underlying service providers
- Both options are useful
 - Today let's focus on *Option B: Delegation of Rights*

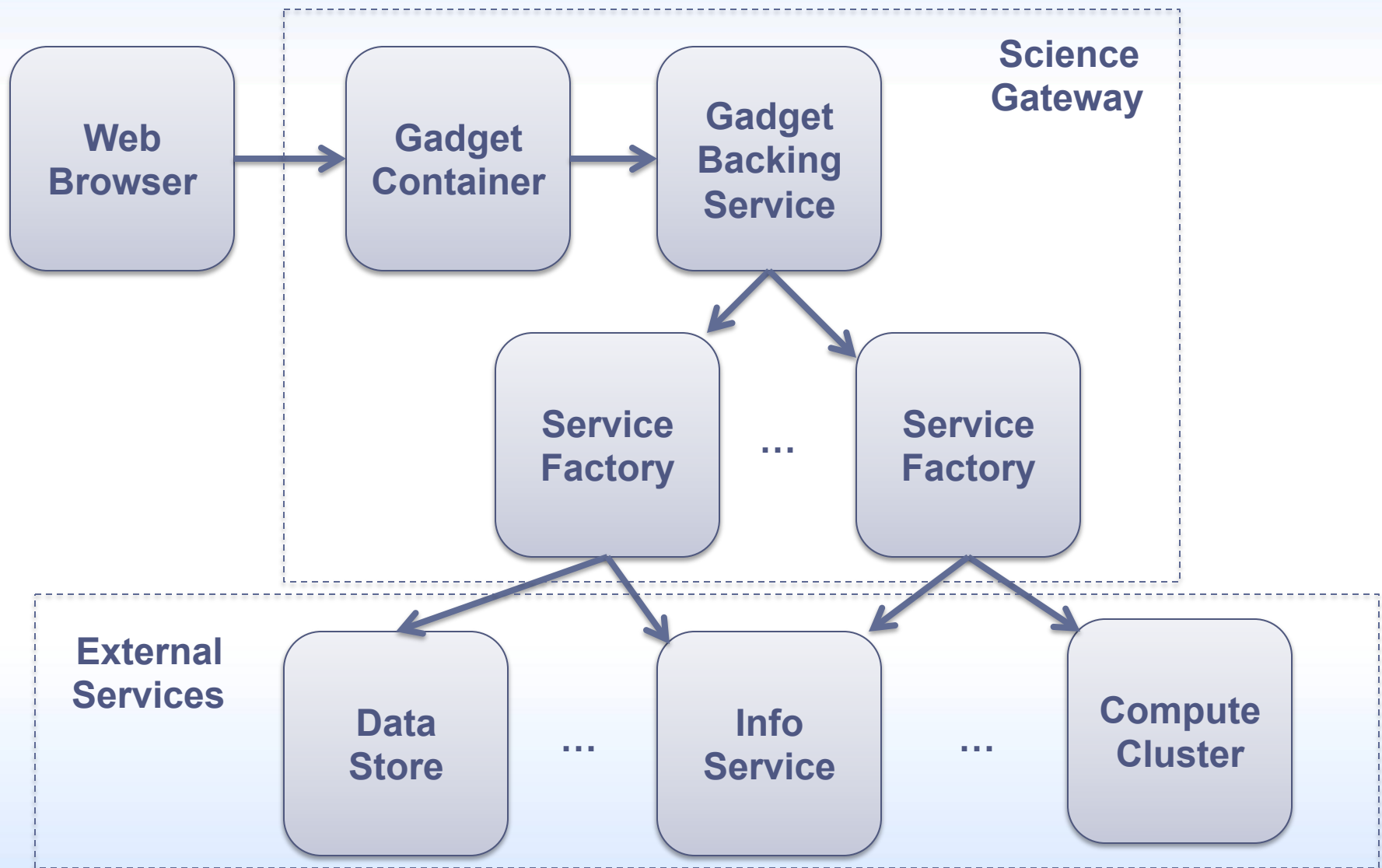
Motivating Example: Science Gateway



Delegated Authorization via OAuth



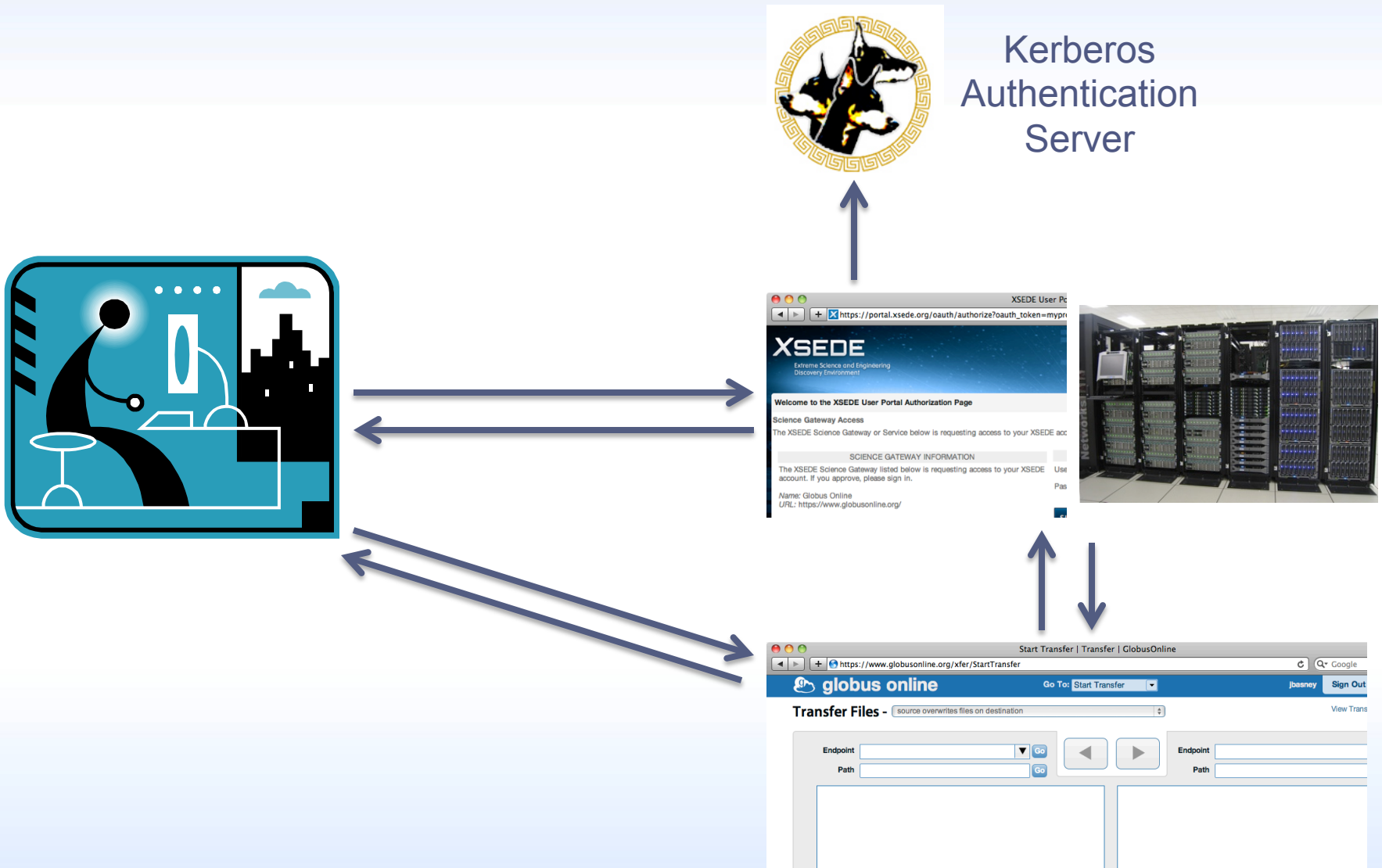
Challenge: Multi-Tier Science Gateways



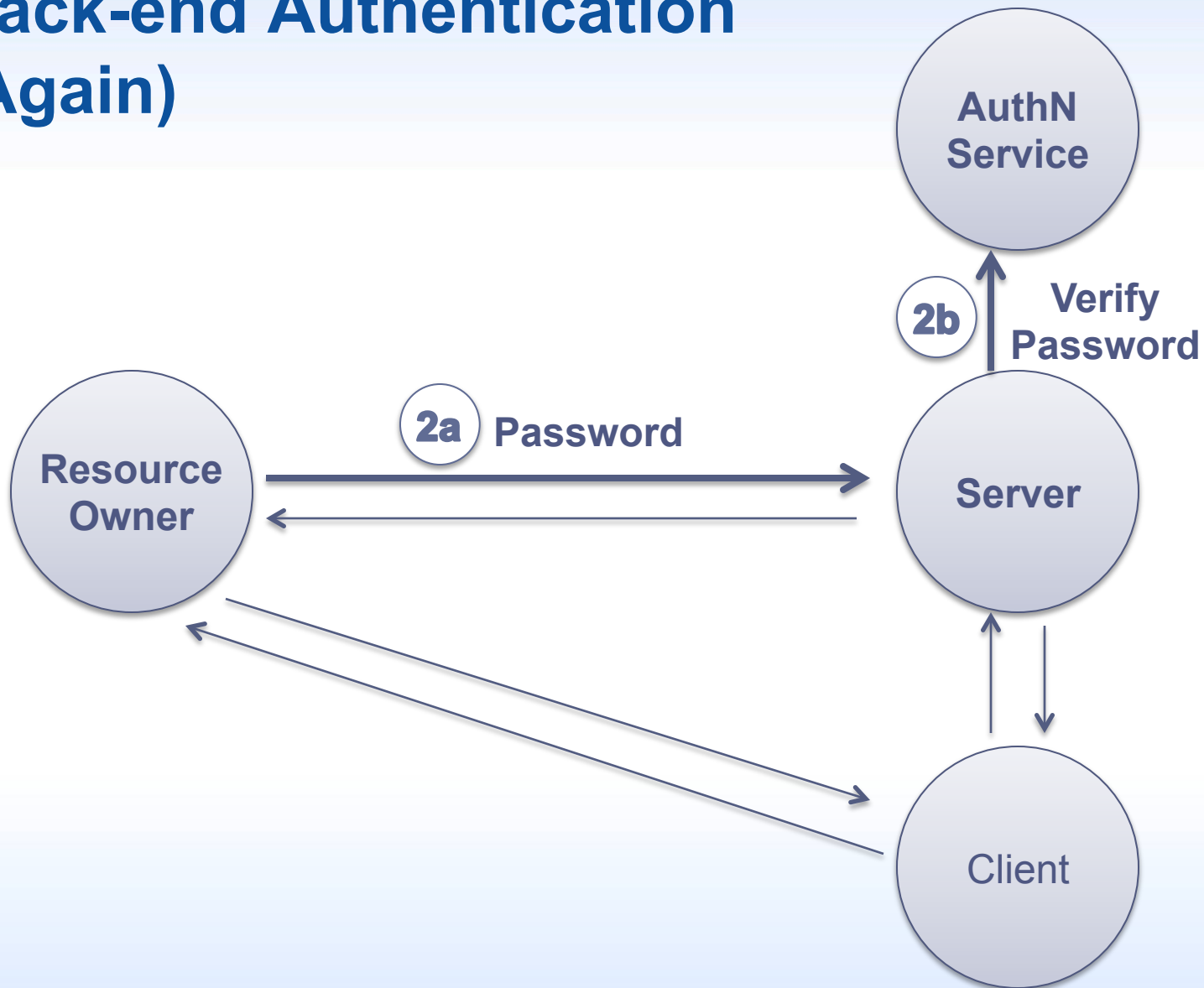
Long-Running Science Gateway Workflows

- Common Science Gateway Use Case:
 - Scientist launches workflow (computational simulation, data analysis, data movement/replication, visualization)
 - Workflow runs for hours/days/weeks
 - Scientist monitors workflow / receives notifications of completion
- Challenge: Duration of Delegation
 - “How long can the science gateway act on my behalf?”
 - Ideally: only as needed for the workflow to complete
 - Limit duration of delegation to minimize window of exposure
 - Difficult / inconvenient to predict workflow duration
 - Approaches: refresh / renewal / revocation
- **OAuth 2.0 refresh is needed!**

Globus Online Example



Back-end Authentication (Again)



Start Transfer | Transfer | GlobusOnline

https://www.globusonline.org/xfer/StartTransfer

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.

Transfer Files -

source overwrites files on destination

[View Transfer Activity](#)

Endpoint

Path




Endpoint

Path

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.



Please select an endpoint

an endpoint above.

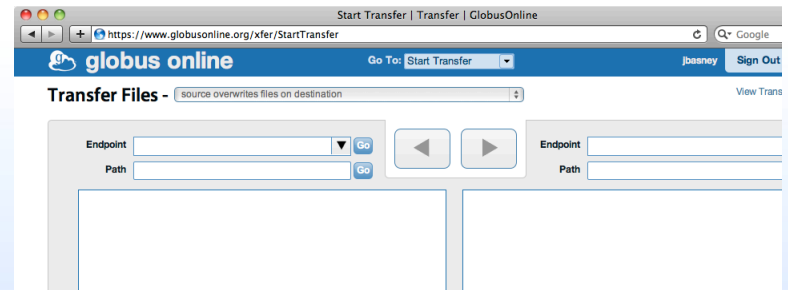
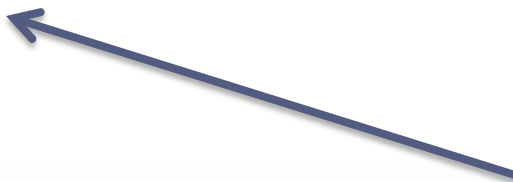
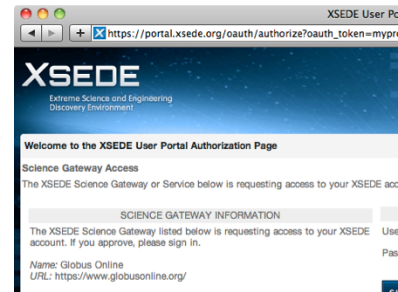
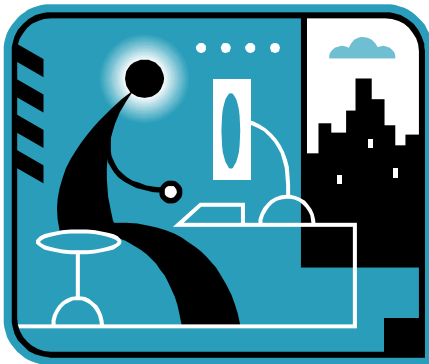
Label This Transfer

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

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

Password

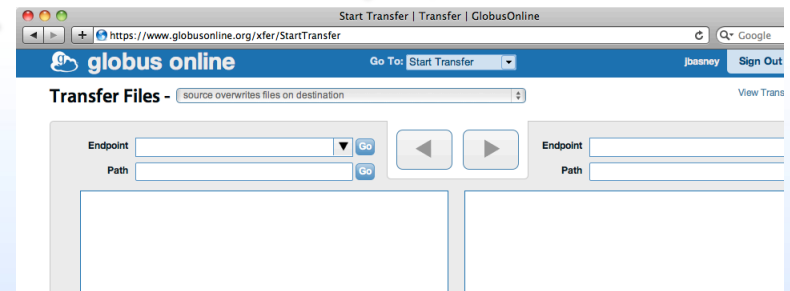
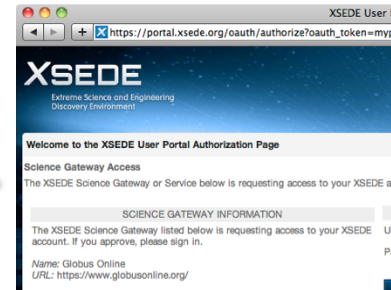


Please send any questions or comments about this site to help@xsede.org

Globus Online Example



Kerberos
Authentication
Server



Transfer Files -

source overwrites files on destination

[View Transfer Activity](#)

Endpoint xsede#forge



Path /~/



Endpoint xsede#nca-mss



Path /~/



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

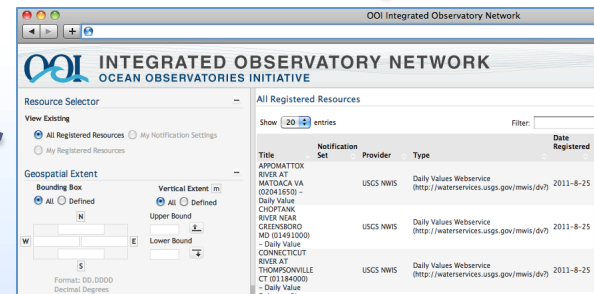
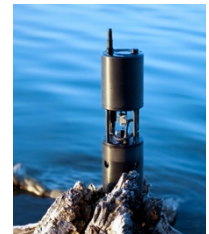
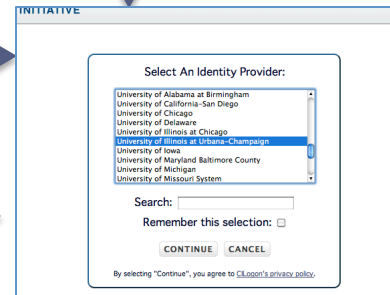
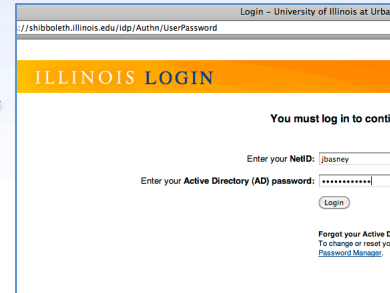
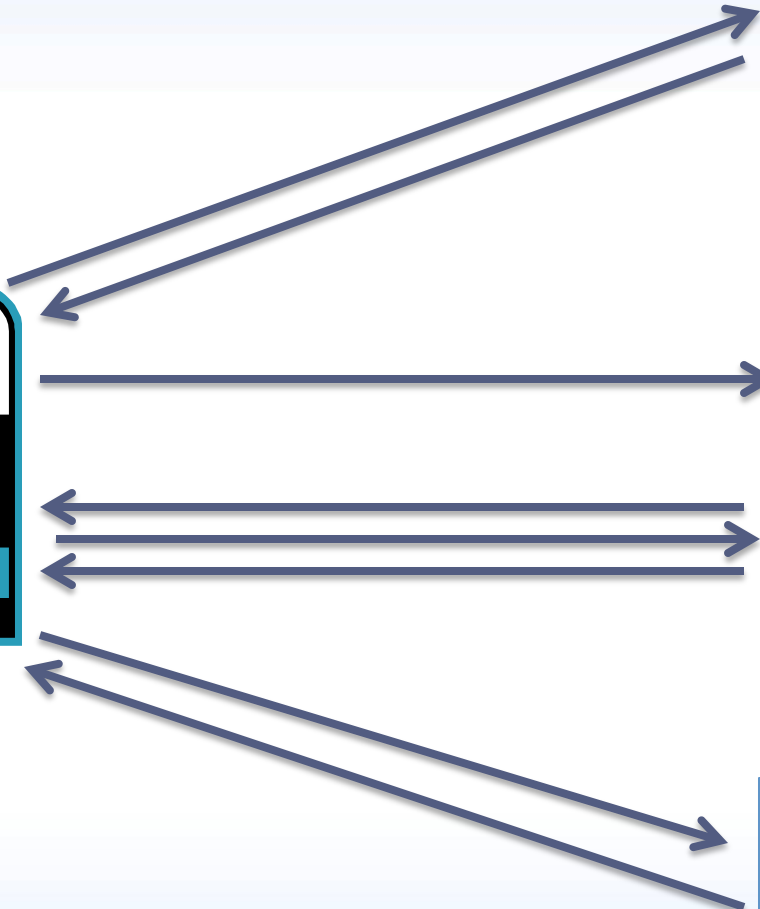
Label This Transfer

This will be displayed in your transfer activity.

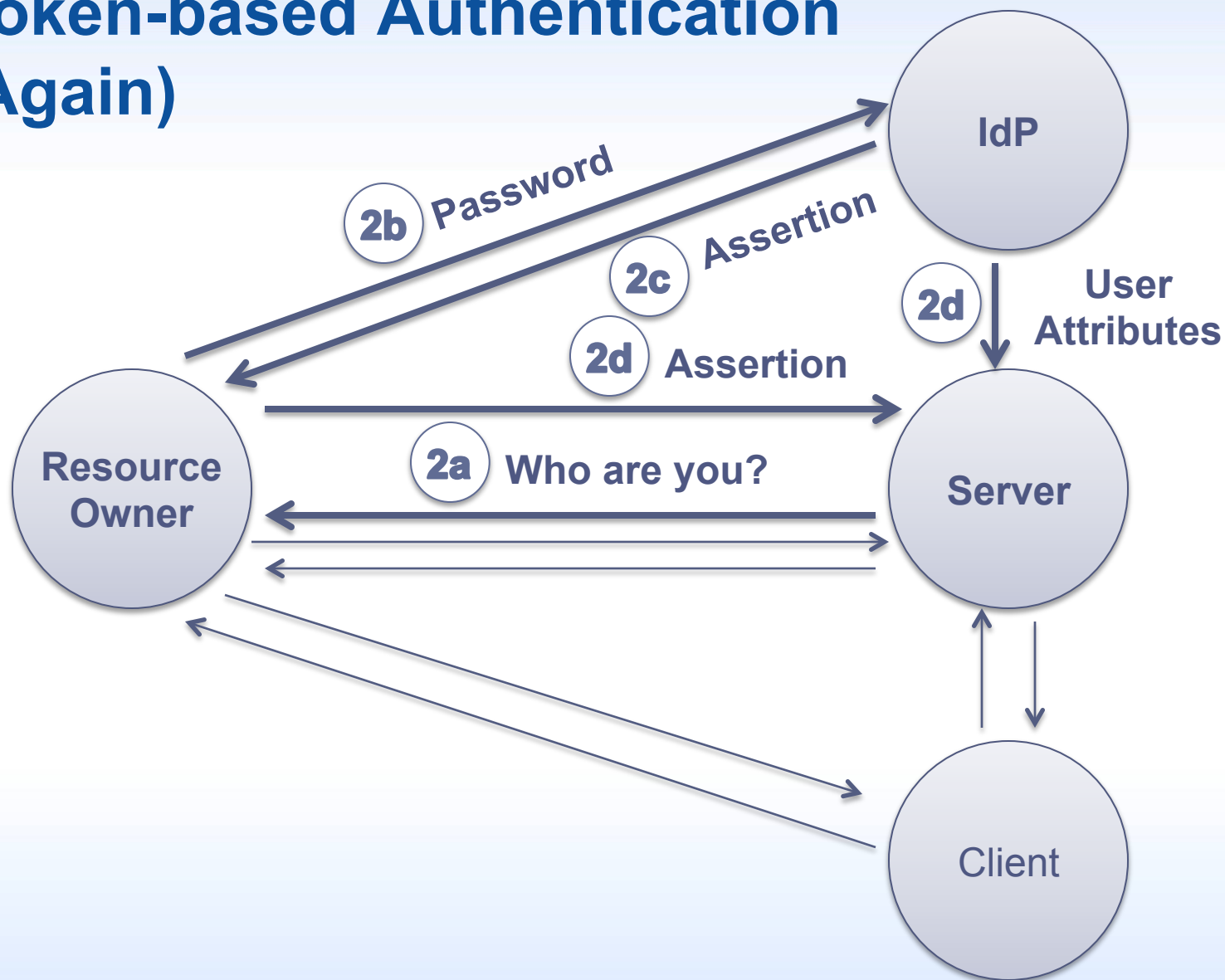
Get Globus Connect

Turn your computer into an endpoint. The easiest and most convenient way to send and receive files on your machine.

OOI Example



Token-based Authentication (Again)



OOI Integrated Observatory Network

Google

OOI 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 [m]

All Defined

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

All Registered Resources

Show 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	
Kinana Str nr					

[Resource Registration Description](#)
[Resource Registration Contact Information](#)
[Original Source Description](#)
[Original Source Contact Information](#)
[Geospatial Coverage](#)
[Temporal Coverage](#)
[Variables](#)
[References](#)

OOI Example



INITIATIVE

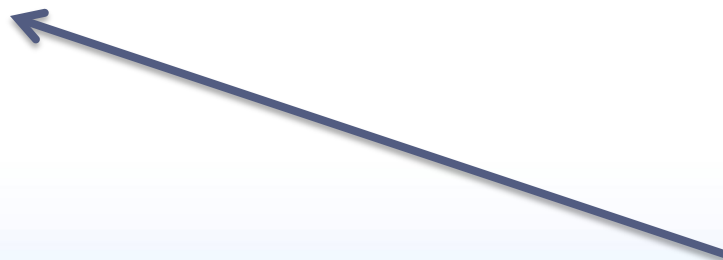
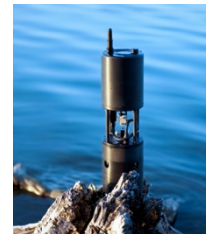
Select An Identity Provider:

- 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:

By selecting "Continue", you agree to [CLLeon's privacy policy](#).



OOI Integrated Observatory Network

INTEGRATED OBSERVATORY NETWORK

OCEAN OBSERVATORIES INITIATIVE

Resource Selector

View Existing All Registered Resources My Registered Resources My Notification Settings

Geospatial Extent

Bounding Box All Defined

Vertical Extent in: All Defined

Upper Bound Lower Bound

Format: DD.DDDD
Decimal Degrees

All Registered Resources

Show entries Filter:

Title	Notification Set	Provider	Type	Date Registered
APPOMATTOX RIVER AT MATOCCA VA (02041550) - Daily Value		USGS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25
CHOPFANK RIVER NEAR GREENSBORO MD (0491000) - Daily Value		USGS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25
CONNECTICUT RIVER AT THOMPSONVILLE CT (01186000) - Daily Value		USGS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25

Delete Rows

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 continue.

Enter your NetID: [jbasney]

Enter your Active Directory (AD) password: [*****]

Login

Forgot your Active Directory Username or Password? [Click here to reset your Password Manager.](#)

INITIATIVE

Select An Identity Provider:

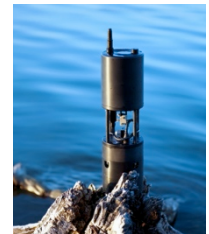
- University of Alabama at Birmingham
- University of California-San Diego
- University of Chicago
- University of Delaware
- University of Illinois at Chicago
- University of Illinois at Urbana-Champaign
- University of Iowa
- University of Maryland Baltimore County
- University of Michigan
- University of Missouri System

Search: []

Remember this selection:

CONTINUE CANCEL

By selecting "Continue", you agree to [CLLeon'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 in:

All Defined

Upper Bound [] Lower Bound []

Filter: []

Show 20 entries

Title	Notification Set	Provider	Type	Date Registered
APPOMATTOX RIVER AT MATOCCA VA (02041950) - Daily Value		USCS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25
CHOPFANK RIVER NEAR GREENSBORO MD (01491000) - Daily Value		USCS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25
CONNECTICUT RIVER AT THOMPSONVILLE CT (01186000) - Daily Value		USGS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25

Login - University of Illinois at Urbana-Champaign


https://shibboleth.illinois.edu/idp/Authn/UserPassword

ILLINOIS LOGIN

You must log in to continue.

Enter your **NetID**:

Enter your **Active Directory (AD) password**:



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>

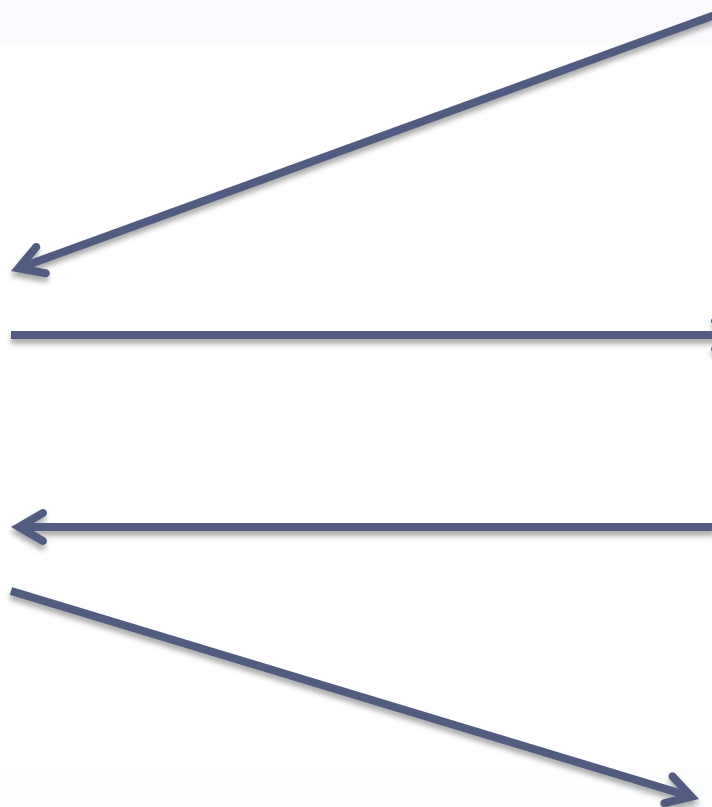
This login service uses the following server:

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 continue.

Enter your NetID: [jbasney]

Enter your Active Directory (AD) password: [.....]

Login

Forgot your Active Directory (AD) password? [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 [ILLIUM'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 in:

All Defined

Upper Bound [] Lower Bound []

Filter: []

Show 20 entries

Title	Notification Set	Provider	Type	Date Registered
APPOMATTOX RIVER AT MATOCCA VA (02041950) - Daily Value		USCS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25
CHOPFANK RIVER NEAR GREENSBORO MD (01491000) - Daily Value		USCS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25
CONNECTICUT RIVER AT THOMPSONVILLE CT (01186000) - Daily Value		USGS NWS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv/)	2011-8-25

Wrap Up

Thanks
for your
interest!

- More info

- www.sciencegatewaysecurity.org
- jbasney@illinois.edu

- References

Jim Basney, Rion Dooley, Jeff Gaynor, Suresh Marru, and Marlon Pierce, "Distributed Web Security for Science Gateways," Gateway Computing Environments Workshop (GCE11), November 17, 2011, Seattle, WA.

Jim Basney and Jeff Gaynor, "An OAuth Service for Issuing Certificates to Science Gateways for TeraGrid Users," TeraGrid Conference, July 18-21, 2011, Salt Lake City, UT. <http://dx.doi.org/10.1145/2016741.2016776>

Jim Basney, Von Welch, and Nancy Wilkins-Diehr, "TeraGrid Science Gateway AAAA Model: Implementation and Lessons Learned," TeraGrid Conference, August 2-5, 2010, Pittsburgh, PA. <http://dx.doi.org/10.1145/1838574.1838576>

Von Welch, Jim Barlow, James Basney, Doru Marcusiu, Nancy Wilkins-Diehr, "A AAAA model to support science gateways with community accounts," Concurrency and Computation: Practice and Experience, Volume 19, Issue 6, March 2007. <http://dx.doi.org/10.1007/s10586-007-0033-8>