



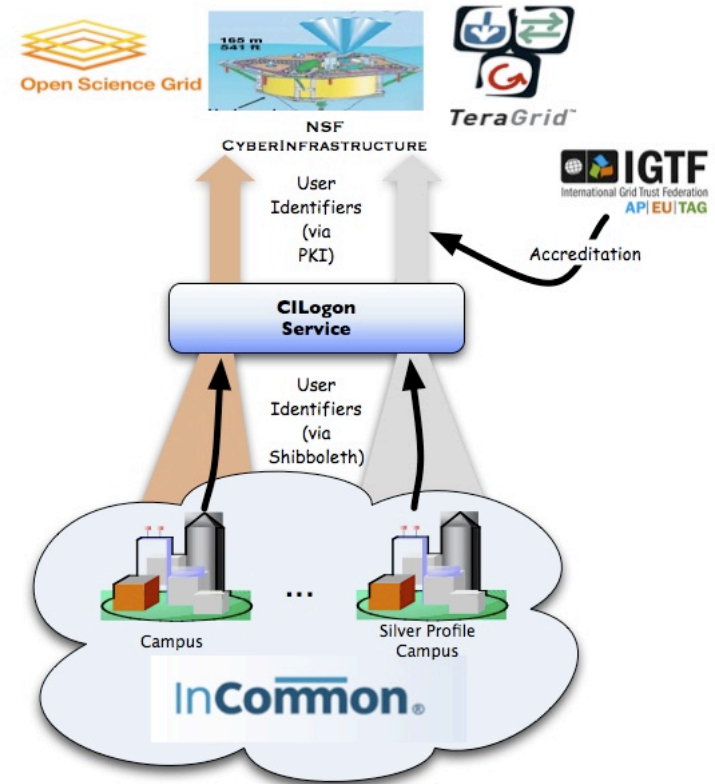
Federated Access to US CyberInfrastructure

Jim Basney
jbasney@ncsa.uiuc.edu

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.

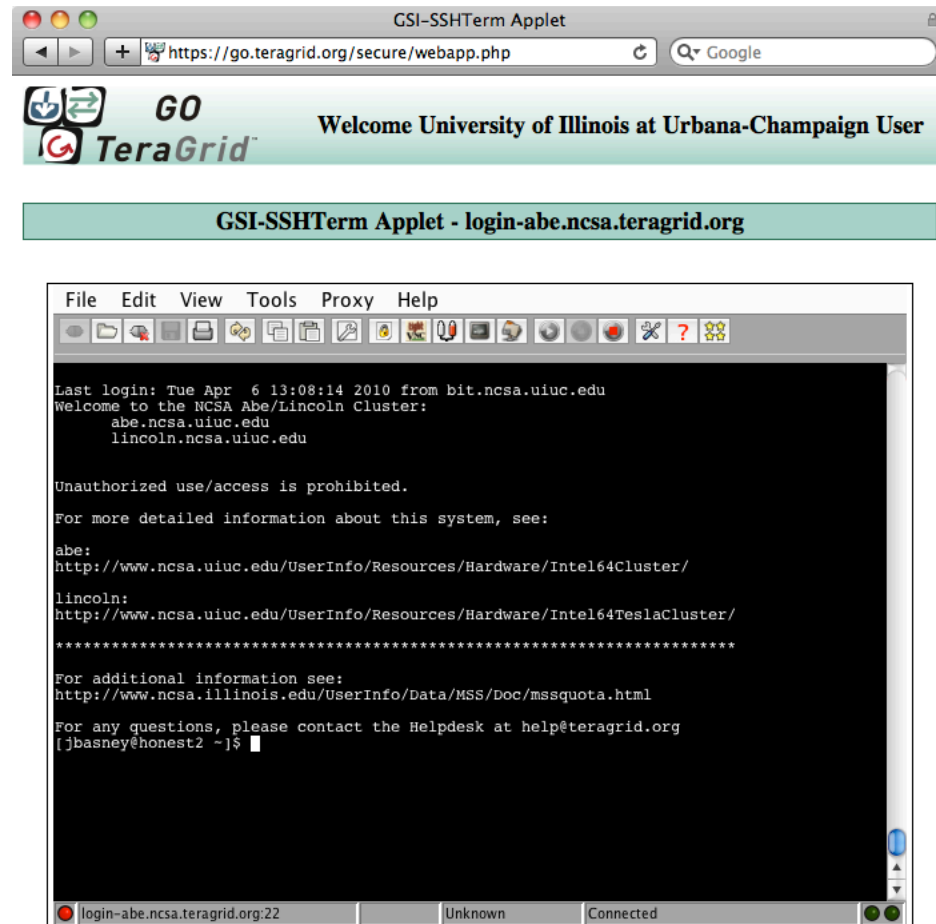
CILogon Project Goal

- Enable campus logon to CyberInfrastructure (CI)
 - Use researchers' existing security credentials at their home institution
 - Ease credential management for researchers and CI providers



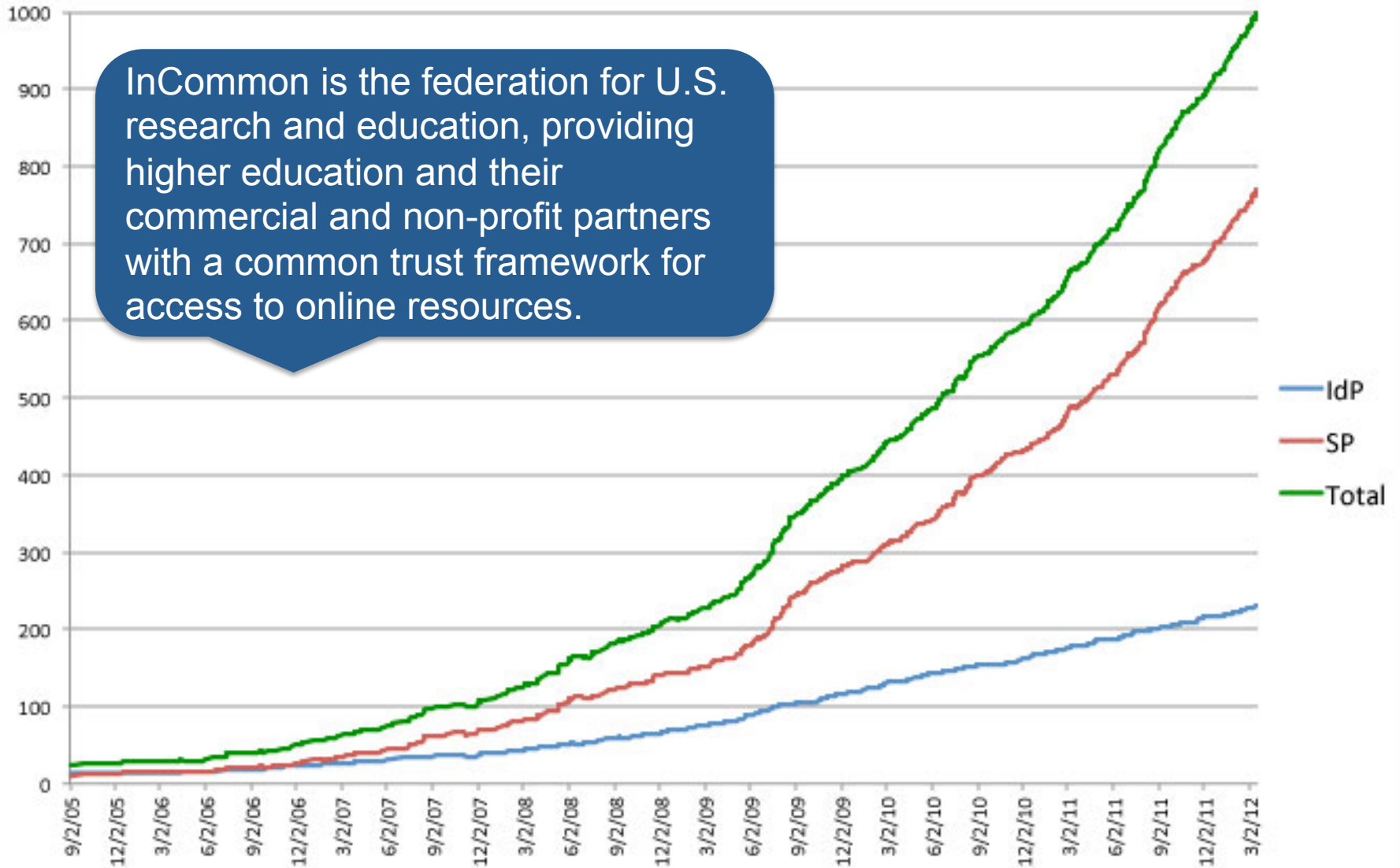
Why certificates?

- Command-line apps, non-web apps
- Multi-stage, unattended batch workflows
- Significant worldwide CI investment in PKI
 - Software, operations, standards, etc.



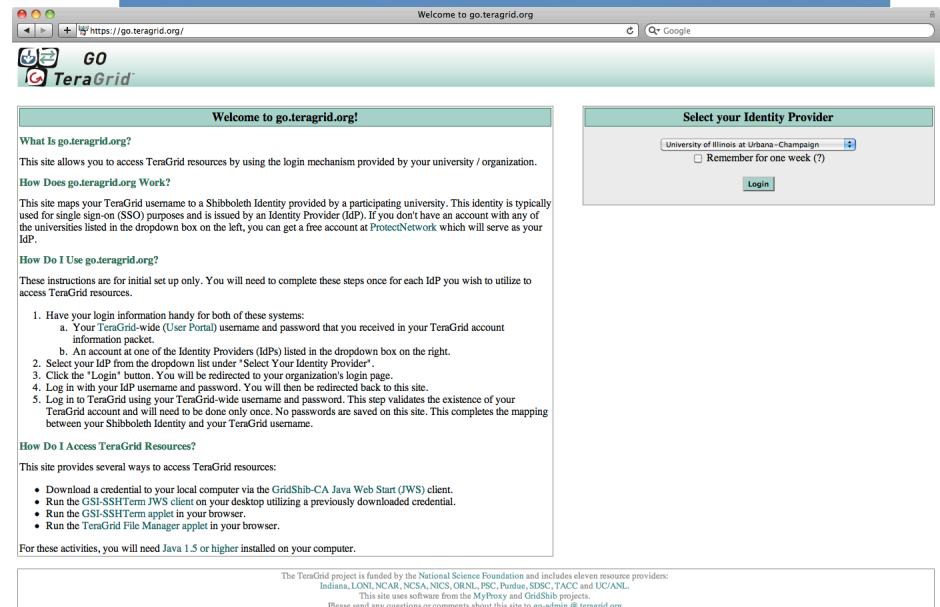
InCommon Entities: 2005-2012

InCommon is the federation for U.S. research and education, providing higher education and their commercial and non-profit partners with a common trust framework for access to online resources.



Prior Work: go.teragrid.org

- Campus login to TeraGrid
- 35 campus IdPs
- Relied on TeraGrid identity vetting
- In production since September 2009
- 1000+ certificates issued to 65+ users
- IGTF accredited
- IDtrust 2010 paper: “Federated Login to TeraGrid” (<http://middleware.internet2.edu/idtrust/2010/>)



Account Linking

MyProxy Login
 https://go.teragrid.org/secure/webapp.php

GO TeraGrid Welcome University of Illinois at Urbana-Champaign User

Associate Identity With TeraGrid Username

It appears that this is the first time you have logged on to this site with your Identity provided by University of Illinois at Urbana-Champaign. In order to utilize TeraGrid resources, you must first log in to your TeraGrid account. You will use the same username and password you use to log on to the TeraGrid User Portal.

This step needs to be performed only once for each identity. Future logins with your Identity will be associated with your TeraGrid username, thus bypassing this step.

Note that this step only verifies that you can log in to TeraGrid with a particular username. No password information is stored on this site.

Log in to TeraGrid

Username:

Password:

[Forgot your password?](#)

The TeraGrid project is funded by the National Science Foundation and includes eleven resource providers: Indiana, LONI, NCAR, NCSA, NICS, ORNL, PSC, Purdue, SDSC, TACC and UC/ANL. This site uses software from the MyProxy and GridShib projects. Please send any questions or comments about this site to go-admin@teragrid.org.

Manage Associations
 https://go.teragrid.org/secure/webapp.php

GO TeraGrid Welcome University of Illinois at Urbana-Champaign User

Manage Associations

Below is a table showing all identities associated with TeraGrid username "jbasney". If you want to delete any of them, check the appropriate box in the "Delete?" column and click the "Delete Checked" button.

If you delete the association for the current Identity (shown in *italics*), you will be required to log in to TeraGrid again to re-establish the association.

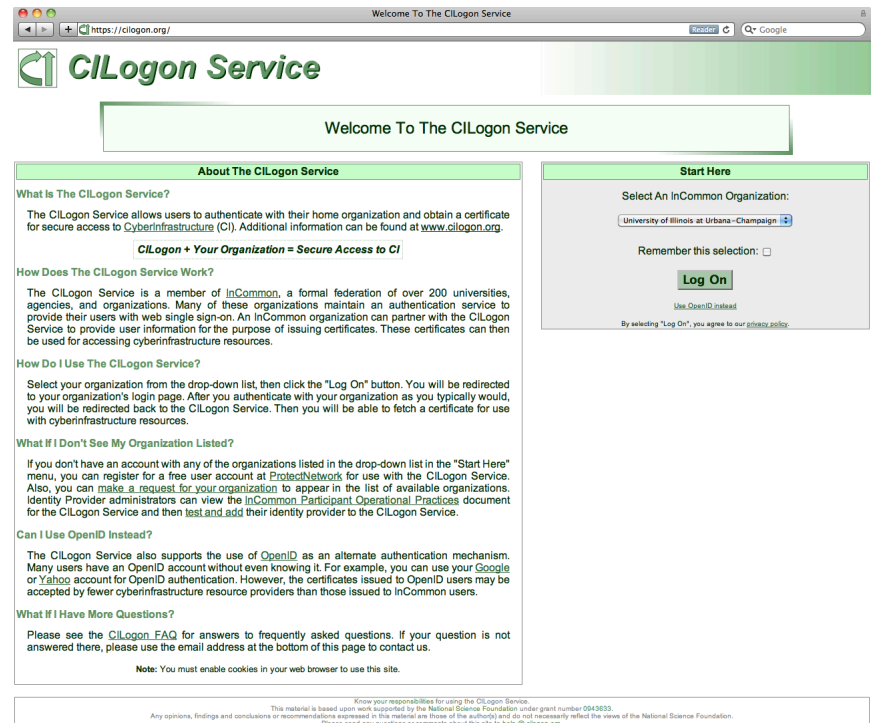
Delete?	Identity Provider	Created	Last Access
<input type="checkbox"/>	<i>University of Illinois at Urbana-Champaign</i>	2010-04-06 13:05:28-05	2010-04-06 13:09:47-05

The TeraGrid project is funded by the National Science Foundation and includes eleven resource providers: Indiana, LONI, NCAR, NCSA, NICS, ORNL, PSC, Purdue, SDSC, TACC and UC/ANL. This site uses software from the MyProxy and GridShib projects. Please send any questions or comments about this site to go-admin@teragrid.org.

(one-time only)

CILogon Service (<https://cilogon.org>)

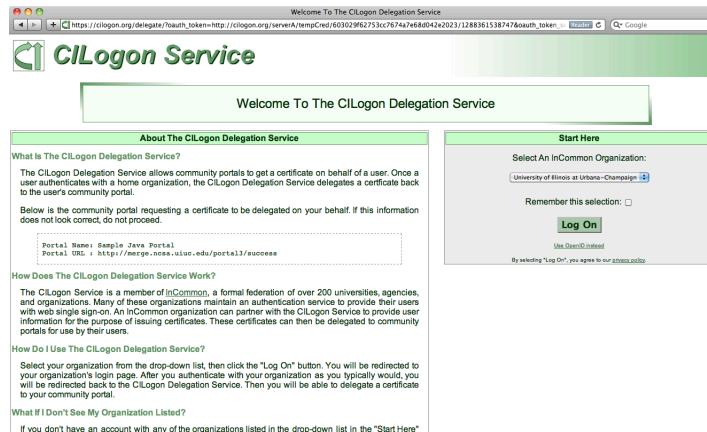
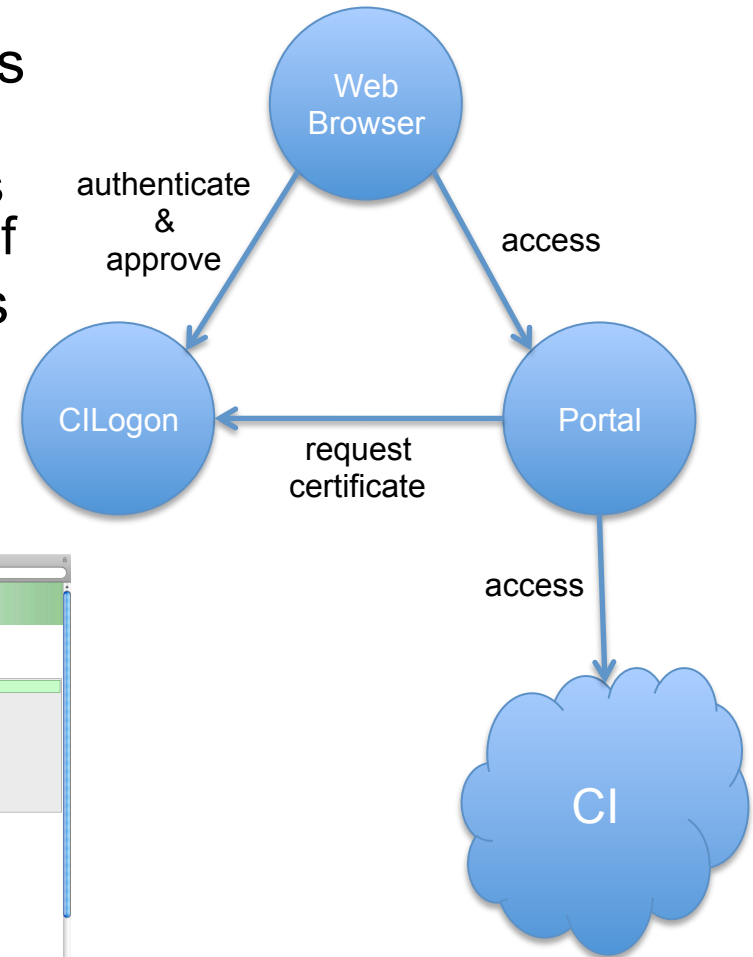
- No TeraGrid account required
- Supports InCommon and OpenID authentication
- Delivers certificates to desktop, browser, and portals
- Available certificate lifetimes: from 1 hour to 13 months
- Supports close integration with CI projects
- Available now!
- FAQ: www.cilogon.org/faq



The screenshot shows the CILogon Service homepage in a web browser. The browser address bar displays <https://cilogon.org/>. The page features a green header with the CILogon Service logo and a navigation bar with a "Welcome To The CILogon Service" button. The main content area is divided into two columns. The left column, titled "About The CILogon Service", contains sections for "What is The CILogon Service?", "How Does The CILogon Service Work?", "How Do I Use The CILogon Service?", "What if I Don't See My Organization Listed?", "Can I Use OpenID Instead?", and "What if I Have More Questions?". The right column, titled "Start Here", contains a "Select An InCommon Organization:" dropdown menu with "University of Illinois at Urbana-Champaign" selected, a "Remember this selection:" checkbox, a "Log On" button, and a "Use OpenID Instead" link. A footer section contains a disclaimer and contact information.

CILogon Portal Delegation

- Grid Portals and Science Gateways provide web interfaces to CI
 - Portals/Gateways need certificates to access CI on researchers' behalf
- CILogon Delegation Service allows researchers to approve certificate issuance to portals (via **OAuth**)
- www.cilogon.org/portal-delegation



Integration Example: OOI

The screenshot displays the OOI Integrated Observatory Network interface. At the top, the logo and name "OOI INTEGRATED OBSERVATORY NETWORK OCEAN OBSERVATORIES INITIATIVE" are visible. A red arrow points to the "Sign in" link in the top right corner, which is circled in red. Other navigation links include "Create account" and "Help".

The main content area is titled "All Registered Resources" and features a table of resources. The table has columns for "Title", "Notification Set", "Provider", "Type", "Date Registered", and "Details". The "Show" dropdown is set to "20" entries, and there is a "Filter" input field.

Title	Notification Set	Provider	Type	Date Registered	Details
APPOMATTOX RIVER AT MATOACA VA (02041650) - Daily Value CHOPTANK RIVER NEAR GREENSBORO MD (01491000) - Daily Value CONNECTICUT RIVER AT THOMPSONVILLE CT (01184000) - Daily Value Delaware River at Trenton NJ (01463500) - Daily Value ESOPUS CREEK AT COLDBROOK NY (01362500) - Daily Value HUDSON RIVER AT FORT EDWARD NY (01327750) - Daily Value JAMES RIVER AT CARTERSVILLE VA (02035000) - Daily Value Kalihi Str nr Honolulu Oahu HI (16229000) - Daily Value Kinana Str nr		USGS NWIS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)	2011-8-25	
		USGS NWIS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)	2011-8-25	
		USGS NWIS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)	2011-8-25	
		USGS NWIS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)	2011-8-25	
		USGS NWIS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)	2011-8-25	
		USGS NWIS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)	2011-8-25	
		USGS NWIS	Daily Values Webservice (http://waterservices.usgs.gov/mwis/dv?)	2011-8-25	

On the left side, there are sections for "Resource Selector", "Geospatial Extent", and "Temporal Extent". The "Resource Selector" includes options for "View Existing" (All Registered Resources, My Notification Settings, My Registered Resources). "Geospatial Extent" includes "Bounding Box" and "Vertical Extent" options. "Temporal Extent" includes "Time Range" options (All, Defined) and "From" and "To" date pickers.

On the right side, there is a vertical menu with links: "Resource Registration Description", "Resource Registration Contact Information", "Original Source Description", "Original Source Contact Information", "Geospatial Coverage", "Temporal Coverage", "Variables", and "References".

At the bottom, there are "Search" and "Dataset Access" buttons, and a "Set Up Notifications" button.



INITIATIVE

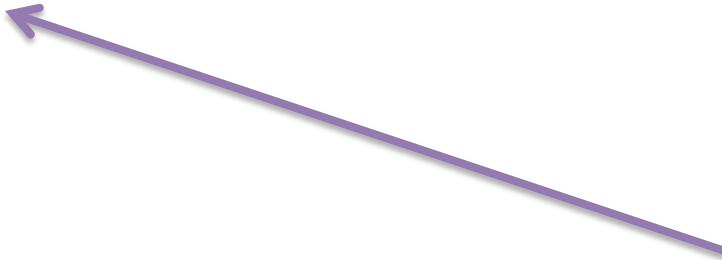
Select An Identity Provider:

- 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 [CILogon's privacy policy](#).



OOI Integrated Observatory Network

INTEGRATED OBSERVATORY NETWORK

OCEAN OBSERVATORIES INITIATIVE

Resource Selector

View Existing

All Registered Resources My Notification Settings

Geospatial Extent

Bounding Box

All Defined

Vertical Extent in:

Upper Bound Lower Bound

Format: DD.DDDD
Decimal Degrees

All Registered Resources

Show 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 (04910000) - 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


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](#).



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 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 [CI Logon's privacy policy.](#)



OOI Integrated Observatory Network

INTEGRATED OBSERVATORY NETWORK

OCEAN OBSERVATORIES INITIATIVE

Resource Selector

View Existing

All Registered Resources My Notification Settings

Geospatial Extent

Bounding Box

All Defined

Vertical Extent in:

Upper Bound Lower Bound

Format: DD.DDDD
Decimal Degrees

All Registered Resources

Show 20 entries

Title	Notification Set	Provider	Type	Date Registered
APKOMATTOX 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.



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:

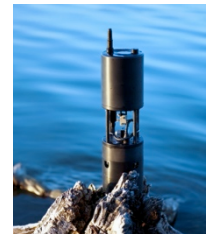
- University of Alabama at Birmingham
- University of California-San Diego
- University of Chicago
- University of Delaware
- University of Illinois at Chicago
- University of Illinois at Urbana-Champaign
- University of Iowa
- University of Maryland Baltimore County
- University of Michigan
- University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

Search: []

Remember this selection:

CONTINUE CANCEL

By selecting "Continue", you agree to [CI Logon'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 []

Format: DD.DDDD
Decimal Degrees

All Registered Resources

Show 20 entries

Title	Notification Set	Provider	Type	Date Registered
APKOMATTOX 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

OOI Integrated Observatory Network

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

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

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

Resource Registration Description

Resource Registration Contact Information

Resource Availability Settings

Resource Activation Settings

Original Source Description

Original Source Contact Information

Geospatial Coverage

Temporal Coverage

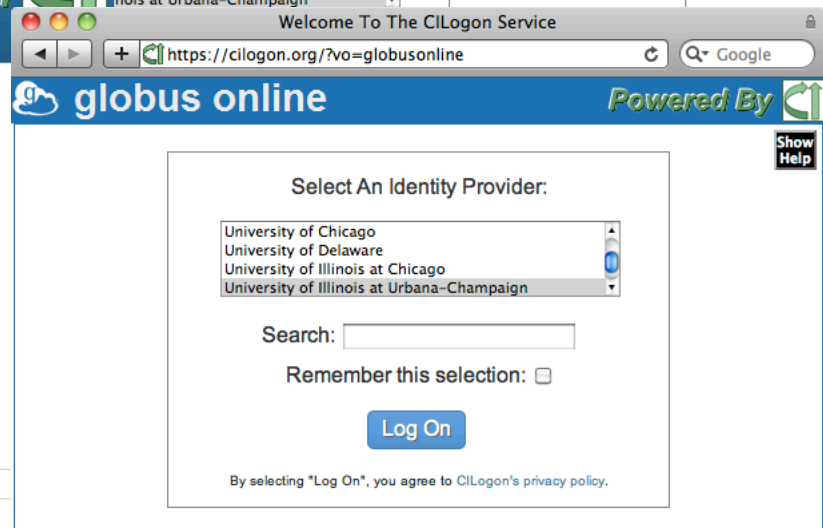
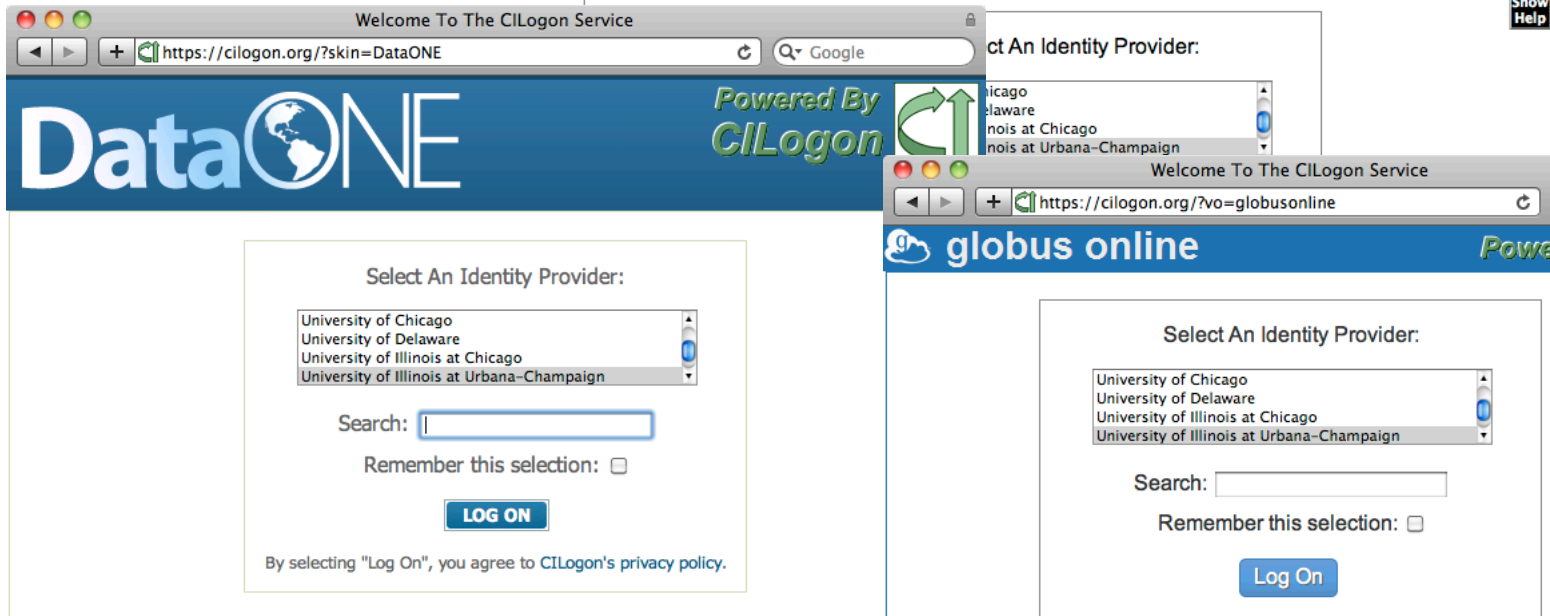
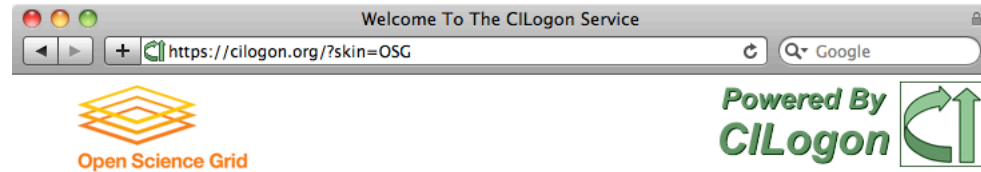
Variables

References

Search

Select All Deselect All Delete Selected Save Changes

More Integration Examples



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)
necessarily reflect the views of the National Science Foundation.

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.

Challenges

- Level of Assurance
- Non-Browser Apps
- IdP-SP On-Boarding
- User Catch-All IdPs

Levels of Assurance

- LOA requirements differ across scientific collaborations
 - 2-factor authentication
 - IGTF accreditation
 - Open access with usage statistics
- CILogon LOA options:
 - InCommon Silver: US Gov't ICAM Level 2
 - OpenID OIX: US Gov't ICAM Level 1
 - InCommon “Basic”



CILogon and IGTF



- CILogon CA operations, key management, and certificate profiles meet IGTF standards
- Issue: subscriber ID vetting & authentication
 - Goal: rely on campuses for this
 - Need minimum standards for campus practices
 - Approach: rely on InCommon Identity Assurance
- Status:
 - CILogon Silver CA accredited October 2010
 - Now waiting for InCommon Silver campuses...
 - CILogon Basic & OpenID CAs operating w/o IGTF accreditation

Support for Non-Browser Apps

- Option #1:
 - Use browser-based authentication (SAML, OpenID)
 - Get URL for certificate download (wget/curl)
 - Or use Java Web Start, etc.
 - Use certificate for non-browser authentication
 - *Unfortunately still requires a browser*
- Option #2
 - Use SAML Enhanced Client or Proxy (ECP) authentication *outside the browser* to download certificate
 - ECP adoption by InCommon campuses beginning
 - Successfully tested with U Washington, U Chicago, LIGO, LTER, and ProtectNetwork
 - For more info: <http://www.cilogon.org/ecp>

ECP Example

```
$ curl -sSO https://cilogon.org/ecp.pl
```

```
$ perl ecp.pl --get cert -c create -k userkey.pem -o usercert.pem -t 12
```

```
Select an Identity Provider (IdP):
```

```
1> LTER Network
```

```
2> ProtectNetwork
```

```
3> University of Chicago
```

```
4> University of Washington
```

```
5> Specify the URL of another IdP
```

```
Choose [2]: 2
```

```
Enter a username for the Identity Provider: jbasney
```

```
Enter a password for the Identity Provider: *****
```

```
$ grid-proxy-init -cert usercert.pem -key userkey.pem -hours 4
```

```
Your identity: /DC=org/DC=cilogon/C=US/O=ProtectNetwork/CN=Jim Basney A685
```

```
Creating proxy ..... Done
```

```
$ gsissh citest.example.edu
```

```
[jbasney@citest ~]$
```

SP On-Boarding

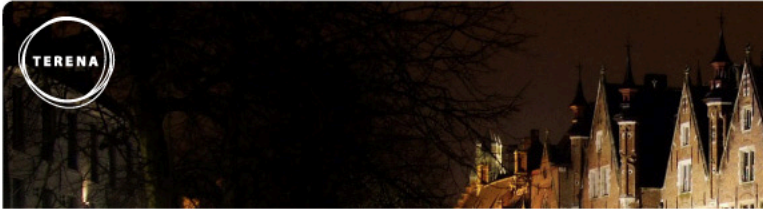
- Goal: Enable successful use of SPs by users from many IdPs
 - Particularly difficult for “no contract” SPs (“user-driven” SPs)
- Challenge: Attribute release
 - Technical solutions: user consent, attribute requirements in metadata, IdP filtering
 - Policy: privacy, FERPA, SP trust
 - Policies differ for students versus faculty/staff
 - Scaling: attribute bundles, default release policies

SP On-Boarding

Unhandled exception

https://login.terena.org/wayf/module.php/saml/sp/saml2-acis.php/default-sp

UNHANDLED EXCEPTION



Unhandled exception

An unhandled exception was thrown.
If you report this error, please also report this tracking number which makes it possible to locate administrator: 62104052f1

Debug information

The debug information below may be of interest to the administrator / help desk:


```
SimpleSAML_Error_Error: UNHANDLED EXCEPTION

Backtrace:
0 /usr/share/simplesamlphp/wayf/www/module.php:180 (N/A)
Caused by: SimpleSAML_Error_Exception: This service needs an attribute to identify
users, but it did not find any of eduPersonTargetedID, eduPersonPrincipalName, or mail.
Please ask your institution administrator to release at least one of those attributes.

Backtrace:
11 /usr/share/simplesamlphp/idp/modules/terena/lib/Auth/Process/SmartAttrs.php:84 (sspmod_terena_Auth_Process_SmartAttrs::getSmartID)
10 /usr/share/simplesamlphp/idp/modules/terena/lib/Auth/Process/SmartAttrs.php:307 (sspmod_terena_Auth_Process_SmartAttrs::process)
```

Login Unsuccessful

https://wiki.shibboleth.net/confluence/c



Shibboleth

Login Unsuccessful

Your Identity Provider did not release enough information for our services to properly identify you. You will need to contact an Identity Provider administrator to enable the release of the appropriate information, or alternatively use an alternative Identity Provider with a more liberal policy.

You may direct your technical staff to this [infrastructure page](#) for specific technical details on configuration and our policies regarding the information we receive.



Test Your Organization's Identity Provider

Verify SAML Attribute Release Policy

Thank you for your interest in the CILOGON Service. This page allows the administrator of an Identity Provider (IdP) to verify that all necessary SAML attributes have been released to the CILOGON Service Provider (SP). Below you will see the various attributes required by the CILOGON Service and their values as released by your IdP. If all required attributes are present, you can add your IdP to the list of organizations available to the CILOGON Service (assuming it has not already been added).

Summary

✔ All required attributes have been released by your IdP. For details of the various attributes utilized by the CILOGON Service and their current values, see the sections below.

[Add Your IdP to the CILOGON Service](#)

▼ SAML Attributes

Identity Provider (entityID): urn:mace:incommon:uiuc.edu
ePTID:
ePPN: jbasney@illinois.edu
First Name (givenName): James
Last Name (sn): Basney
Display Name (displayName): James Alan Basney
Email Address (email): jbasney@illinois.edu
Level of Assurance (assurance):

▼ Metadata Attributes

Organization Name: University of Illinois at Urbana-Champaign
Home Page: http://www.uiuc.edu/index.html
Technical Contact: Mike Grady <m-grady@uiuc.edu>
Administrative Contact: Mike Grady <m-grady@uiuc.edu>

User Catch-All

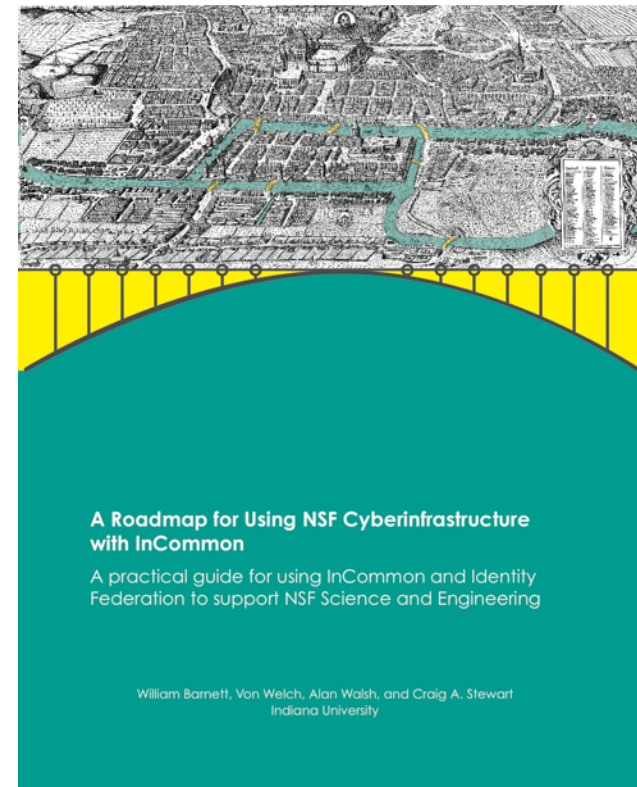
- Handling users w/o institutional logins
 - Home institution not (yet) in InCommon federation
 - Home institution not (yet) on-boarded w/ SP
- go.teragrid.org
 - TeraGrid username/password
- cilogon.org
 - “Request a New Organization” page
 - OpenID (Google, PayPal, VeriSign)
 - ProtectNetwork
 - Project logins (LTER, LIGO, ...)

CILogon: Lessons Learned

- InCommon today supports **browser SSO**
 - SAML->X.509 bridges are common for non-web apps (CILogon, TERENA Certificate Service, etc.)
 - SAML ECP adopted by ~5 InCommon IdPs so far (<http://www.cilogon.org/ecp>)
- Attribute release is a major challenge today for SPs that want to support many IdPs
 - New InCommon effort to address this challenge: <https://spaces.internet2.edu/display/InCCollaborate/Research+and+Scholarship+Category>
- Google OpenID is a popular “catch-all” IdP
 - US ICAM LOA 1 certified (<http://openididentityexchange.org/certified-providers>)

References

- A Roadmap for Using NSF CyberInfrastructure with InCommon
(<http://www.incommon.org/nsfroadmap>)
- An Analysis of the Benefits and Risks to LIGO When Participating in Identity Federations
(<http://www.google.com/search?q=LIGOIdentityFederationRiskAnalysis.pdf>)
- Federated Security Incident Response
(<https://spaces.internet2.edu/x/8o6KAQ>)



Thanks

For more information:

www.cilogon.org

info@cilogon.org