



Federated Login to TeraGrid

Jim Basney
Terry Fleury
Von Welch


NCSA
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign

 TeraGrid

This material is based upon work supported by the
National Science Foundation under Grant No. 0503697


Goal


- Enable researchers to use the authentication method of their home organization for access to TeraGrid
 - Researchers don't need to use TeraGrid-specific credentials
 - Avoid distribution of TeraGrid-specific passwords
 - Avoid TeraGrid password reset requests
 - Better integrate TeraGrid with campus resources
 - Provision TeraGrid resources according to campus-based identity vetting and authorization


Federated Login to TeraGrid 

Challenges

- Support TeraGrid usage models
 - Interactive browser and command-line access
 - Multi-stage, unattended batch workflows
- Establish trust among campuses, TeraGrid members, and peer grids (OSG, EGEE)

Federated Login to TeraGrid 



Federated Login to TeraGrid 

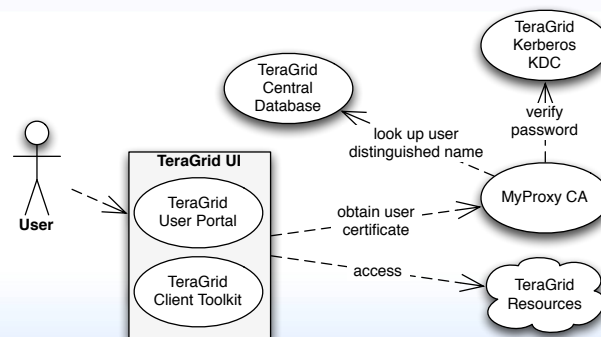
TeraGrid Allocations

- Resources allocated by peer review
- Project principal investigators add user accounts via the User Portal
- Central Database (TGCDDB) contains records for all users
- TeraGrid-wide username and password assigned to every user

Federated Login to TeraGrid



TeraGrid Single Sign-On



Federated Login to TeraGrid



TeraGrid PKI

- TeraGrid PKI consists of CAs operated by TeraGrid member institutions and other partners
- TeraGrid resource providers trust a consistent set of CAs
 - Provides consistent experience for users
 - Determined by consensus through Security Working Group
 - CAs accredited by International Grid Trust Federation (IGTF)



Federated Login to TeraGrid



InCommon Federation

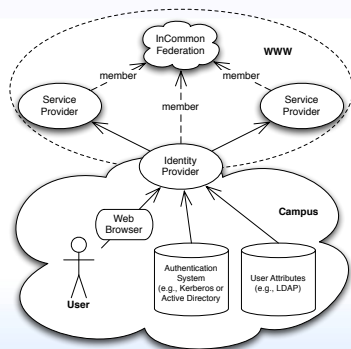
- InCommon facilitates use of campus identity with external service providers
 - By supporting adoption of standard mechanisms and policies
 - By distributing metadata that identifies members
- Uses SAML Web Browser Single Sign-On protocols
 - Shibboleth implementation from Internet2
 - Work well for browser-based applications, but not command-line or batch workflows
- InCommon represents >200 institutions (>4m users)
 - Of 38 institutions with over 50 TG users, 24 (67%) are currently InCommon members



Federated Login to TeraGrid



InCommon Federation



Federated Login to TeraGrid



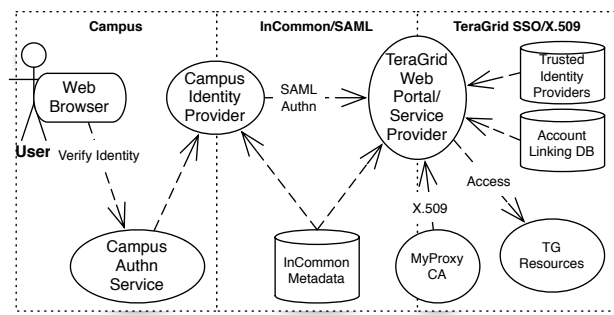
Our Approach

- Account Linking
 - Bind the researcher's campus identity (conveyed via InCommon/SAML) to his/her existing TeraGrid identity (TGCCDB)
 - InCommon motivates our use of SAML
 - Rely on the existing TeraGrid allocations process for identity vetting and authorization
 - Rely on campus for authentication of a persistent user identifier
- Credential Translation
 - Convert from a browser-based (SAML) credential to a certificate for command-line, workflow, and batch processes
 - Deliver certificate to desktop and web session
 - Rely on the existing TeraGrid PKI
 - Adding a new certificate authority

Federated Login to TeraGrid



Our Approach



Federated Login to TeraGrid



User Experience

Federated Login to TeraGrid



Welcome to go.teragrid.org!

This site allows you to access TeraGrid resources by using the login mechanism provided by your university / organization.

How Does go.teragrid.org Work?

This site maps your TeraGrid username to a Shibboleth Identity provided by a participating university. This identity is typically used for single-sign-on (SSO) purposes and is issued by an Identity Provider (IdP). If you don't have an account with any of the universities listed in the dropdown box on the left, you can get a free account at [Proton@Work](#) which will serve as your IdP.

How Do I Use go.teragrid.org?

These instructions are for initial set up only. You will need to complete these steps once for each IdP you wish to utilize to access TeraGrid resources.

- Have your login information handy for both of these systems:
 - Your TeraGrid-wide (User Portal) username and password that you received in your TeraGrid account information packet.
 - An account at one of the Identity Providers (IdPs) listed in the dropdown box on the right.
- Select your IdP from the dropdown list under "Select Your Identity Provider".
- Click the "Log In" button. You will be redirected to your organization's login page.
- Log in with your IdP username and password. You will then be redirected back to this site.
- Log in to TeraGrid using your TeraGrid-wide username and password. This step validates the existence of your TeraGrid account and will need to be done only once. No passwords are saved on this site. This completes the mapping between your Shibboleth identity and your TeraGrid username.

How Do I Access TeraGrid Resources?

This site provides several ways to access TeraGrid resources:

- Downloaded a credential to your local computer via the GridShib-CA Java Web Start (JWS) client.
- Run the GSI-SSHTerm JWS client on your desktop utilizing a previously downloaded credential.
- Run the GSI-SSHTerm applet in your browser.
- Run the TeraGrid File Manager applet in your browser.

For these activities, you will need Java 1.5 or higher installed on your computer.

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

Federated Login to TeraGrid

You must log in to continue.

Enter your NetID:

UIC and UIUC visitors: Add Shibboleth IdP links to your UIC or UIUC NetID. For details: [UIC NetID is Java](#), enter [jhuany@uic.edu](#).

Forgot your NetID password? To change or reset your NetID password, go to the CITES Password Manager page.

More Information

Where to Get Help

- Urbana campus: Contact the CITES Help Desk at [cites@uiuc.edu](#).
- Chicago campus: Contact AOCX at (312) 419-3000 or [cites@uiuc.edu](#).
- Bartlett campus: Contact Information Technology Services at (617) 306-6000 or [techsupport@uiuc.edu](#).

Technical Information

The server that has just now requested your NetID is shown below:

Server: shibboleth.illinois.edu
Server Operator: CITES Helpdesk Team Server

What is a NetID?

Your NetID serves as your right to many University computing and networking services and also determines your University email address, which is [netid@uiuc.edu](#).

For more information, see the [Your Network ID \(NetID\) page](#).

CITES Help Desk - [consult@uic.edu](#)

Federated Login to TeraGrid

MyProxy Login

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.

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

Log in to TeraGrid

Username:

Password:

Manage Associations

Below is a table showing all identities associated with TeraGrid username "jhuany". 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 *italic*), 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 13:05:24-05	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, NCSA, ORNL, PSC, Purdue, SDSC, TACC and UC/LAeN. 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)

Federated Login to TeraGrid

Connections and Management

Welcome University of Illinois at Urbana-Champaign User

Connections and Management

Your Identity is associated with the TeraGrid username "jhuany". You can now perform one of the following actions: connect to the command line of compute and visualization resources (two methods), manage your files with a drag-and-drop interface, or manage your identity associations. For most of these activities, you will need Java 1.5 or higher installed and enabled in your browser.

More Information About Desktop GSI-SSHTerm...

A. Connect To TeraGrid With A Desktop Version of GSI-SSHTerm

- Download a credential to your local computer.
- Click the "Launch GSI-SSHTerm JWS" button to start the desktop application.
- Select the "File->New Connection" menu and enter your desired target TeraGrid resource.

More Information About Desktop GSI-SSHTerm...

B. Connect To TeraGrid With A Browser-Based Version of GSI-SSHTerm

- Select the desired target TeraGrid resource from the dropdown box.
- Click the "Log In With GSI-SSHTerm" button.

More Information About The GSI-SSHTerm Applet...

C. Transfer Files Via A Drag-And-Drop Interface

- Click the "TeraGrid File Manager" button.
- Select the desired target TeraGrid resource for transferring files.

More Information About The File Manager...

D. Manage Identity Associations

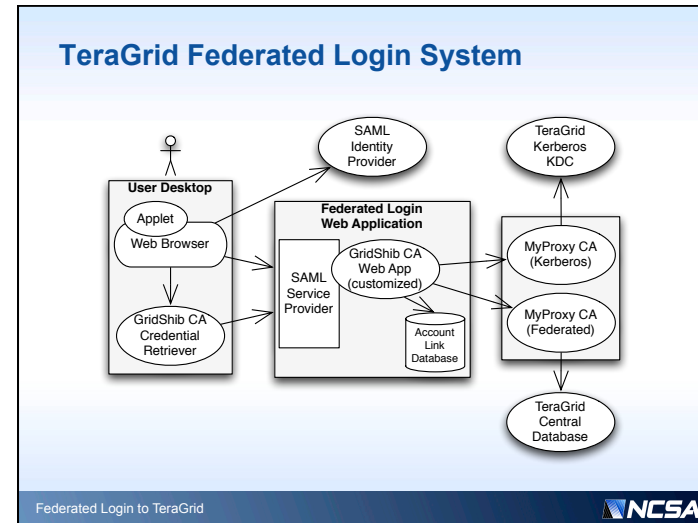
- Click the "Manage Associations" button to view or delete identity mappings.

More Information About Identity Management...

To end your secure session, click the "Log out" button.

Federated Login to TeraGrid

Federated Login to TeraGrid



Trust Establishment

- Campus and InCommon
- TeraGrid PKI

Federated Login to TeraGrid

Trust Establishment Process: Campus

- Join the InCommon Federation
- Add service provider to InCommon metadata
- Request identity providers to release identity information (a manual, campus-by-campus process)
 - Some released identifiers automatically to all InCommon members
 - Some released identifiers on email request
 - Some required local sponsorship and review
- Current status:
 - Targeted 38 campuses with over 50 TeraGrid users
 - 24 (67%) are InCommon members
 - 16 (of the 24) successfully federated to-date
 - 11 additional campuses federated outside the target list

Federated Login to TeraGrid

Trust Establishment Process: PKI

- Publish Certificate Policy and Certification Practices Statement (CP/CPS) according to RFC 3647
- Present CA to regional IGTF policy management authority – The Americas Grid PMA (TAGPMA)
- Checklist-based review by TAGPMA of CA's policies and operations
- Vote for acceptance by TAGPMA members
- Current status:
 - Submitted to TAGPMA (March 2009)
 - Approved by TAGPMA (May 2009)
- CA certificate included in TERENA Academic CA Repository (TACAR)

Federated Login to TeraGrid



Security Considerations

Federated Login to TeraGrid



Security Considerations

- Changes to TeraGrid trust architecture
 - Adding InCommon identity providers as trusted entities
 - Adding web authentication as a trusted method
- Peering with identity providers (IdPs)
 - IdP decides whether to release identifiers to TeraGrid
 - TeraGrid decides to accept IdP assertions – review includes:
 - IdP serves TeraGrid users
 - IdP is operated by a known and respected organization
 - IdP operates a trustworthy authentication service
 - IdP provides globally-unique and non-reassigned identifiers

Federated Login to TeraGrid



Security Considerations

- Web application security
 - Use HTTPS for privacy and authentication
 - Cross-Site Request Forgery (CSRF) attack protections (cookies and hidden form fields)
 - Locked down servers (firewalls, OTP for admin access, etc.)
- CA security
 - FIPS 140 level 2 rated hardware security modules
 - Locked down servers

Federated Login to TeraGrid



Security Considerations

- Disallowing account sharing
 - Account sharing complicates incident response
 - Allow only one identifier per identity provider to be linked with a given TeraGrid identity
- Incident response
 - Actions may include:
 - Disable account links
 - Disable identity provider trust
 - Revoke certificates
 - Coordinate response with TeraGrid security working group, InCommon, and IGTF

Federated Login to TeraGrid



Related Work

- Federated CAs (some accredited by IGTF) in Europe:
 - Switzerland: SWITCH SLCS CA for SWITCHaai federation
 - Germany: DFN-SLCS CA for DFN-AAI federation
 - UK: SARoNGS Credential Translation Service for UK Access Management federation
 - TERENA Certificate Service for national federations (Denmark, Finland, Netherlands, Norway, Sweden, and more)
- TeraGrid Science Gateways
 - Web-based community access to TeraGrid resources
 - Gateways manage their own user registration and authentication
 - May independently support federated login

Federated Login to TeraGrid



Status

- In production at <https://go.teragrid.org> since Sep 2009
 - Supporting logins from 27 institutions
 - Issued >800 certificates so far
- Work in progress:
 - Integrate with TeraGrid User Portal (<https://portal.teragrid.org>)
 - CILogon Project (www.cilogon.org)
 - Provide certificates to all InCommon members (not just TeraGrid users)
- Other possible future work for TeraGrid:
 - Phase out TeraGrid passwords
 - Attribute-based authorization
 - Support for OpenID

Federated Login to TeraGrid



- Questions? Comments?
- Contact: jbasney@illinois.edu

Federated Login to TeraGrid

