CILogon

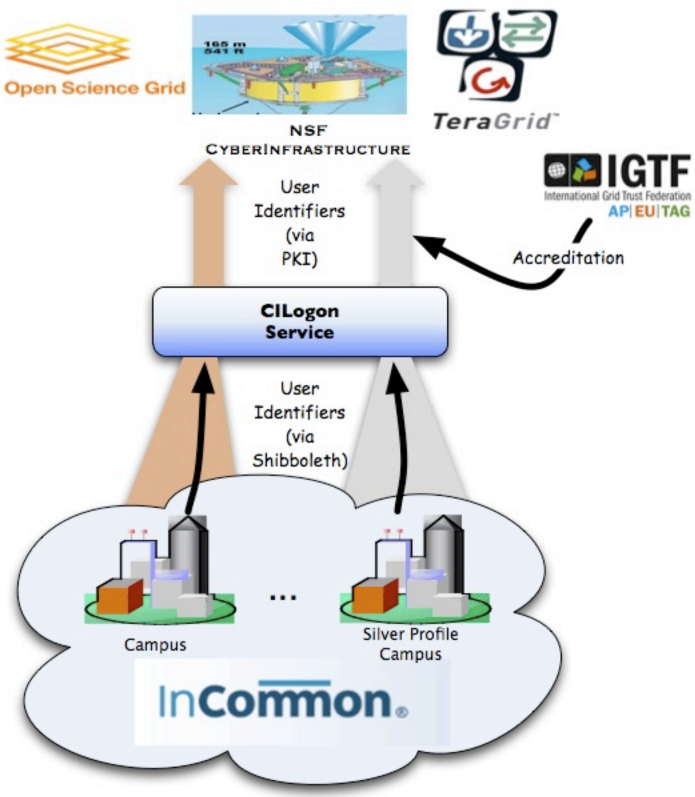
Federated Access to US CyberInfrastructure

Jim Basney
jbasney@illinois.edu

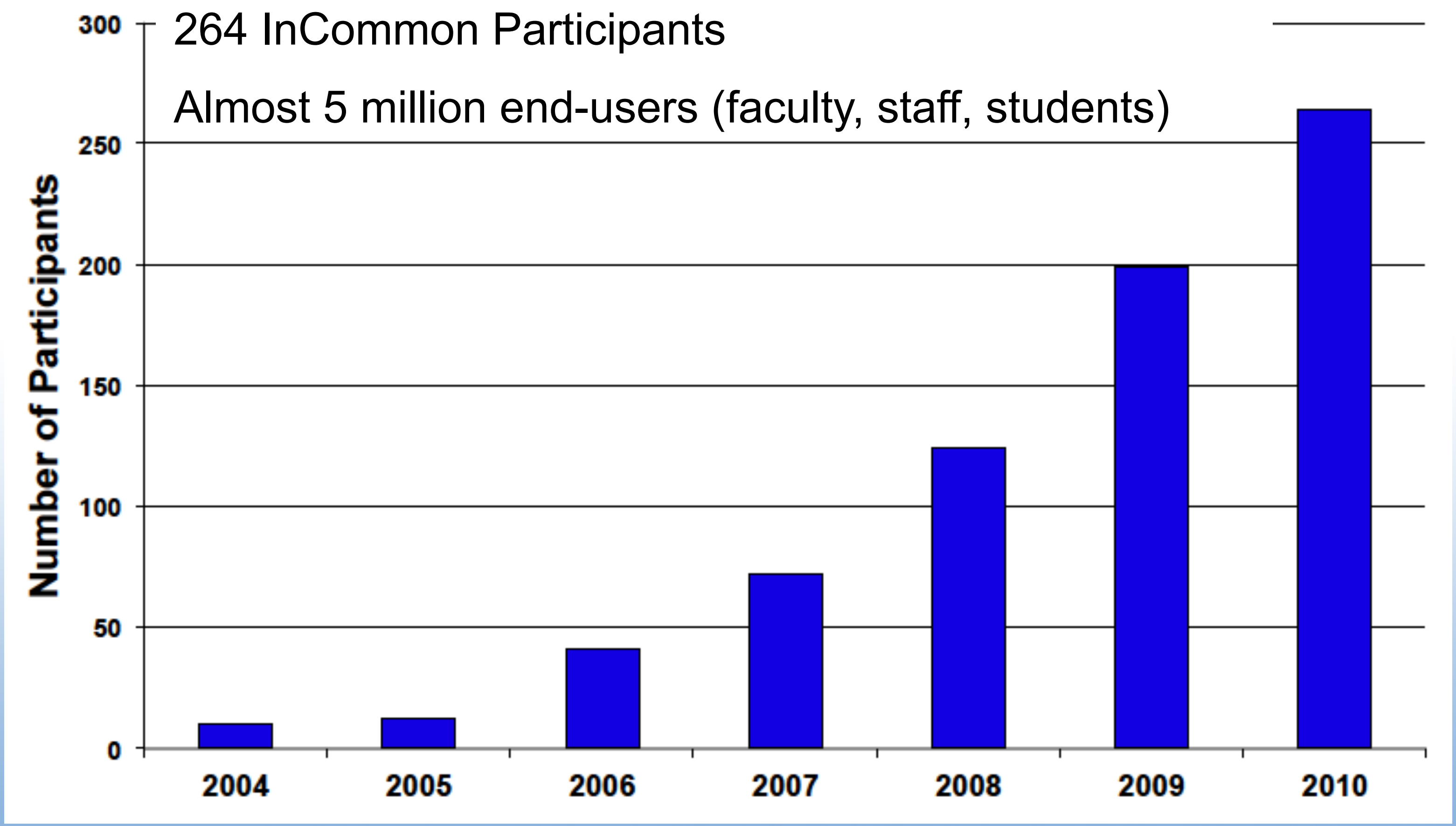
This material is based upon work supported by the National Science Foundation under grant number 0943633. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

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



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.



264 InCommon Participants

Almost 5 million end-users (faculty, staff, students)

A Roadmap for Using NSF Cyberinfrastructure with InCommon

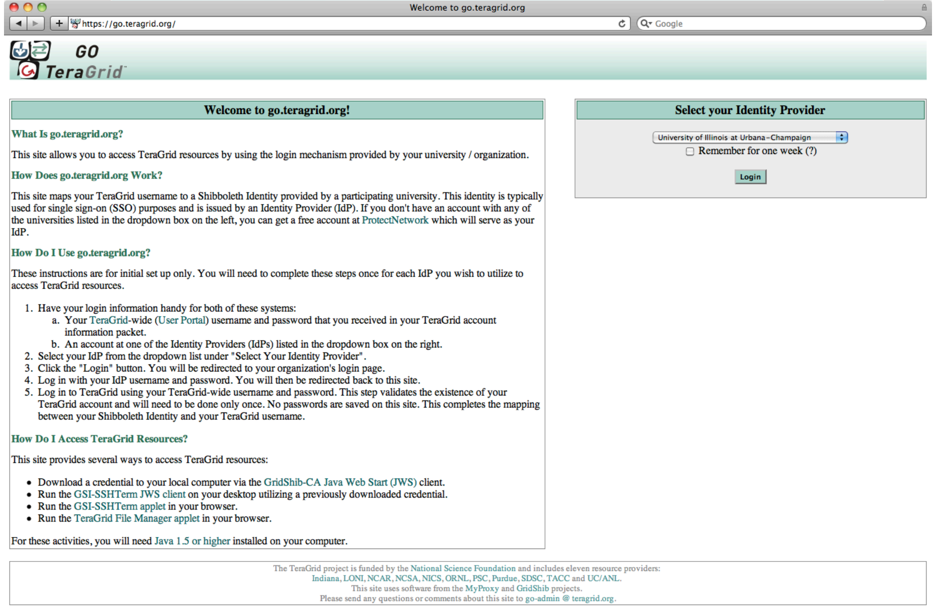
A helpful guide for CI projects

http://incommon.org/nsfroadmap

Prior Work: go.teragrid.org

- Campus login to TeraGrid
- 35 campuses so far
- Relies on TeraGrid identity vetting
- In production since September 2009
- 1000+ certificates issued so far to 65+ users
- IGTF accredited
- Integration with portal.teragrid.org underway
- IDtrust 2010 paper: “Federated Login to TeraGrid” (http://middleware.internet2.edu/idtrust/2010/)

TERAGRID
UC/ANL
PSC
NCSA
PU
NCAR
IU
ORNL
NICS
SDSC
LONI
TACC



Welcome to go.teragrid.org!

What Is 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 ProtectNetwork 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.

1. Have your login information handy for both of these systems:
   a. Your TeraGrid-wide (User Portal) username and password that you received in your TeraGrid account information packet.
   b. An account at one of the Identity Providers (IdPs) listed in the dropdown box on the right.
2. Select your IdP from the dropdown list under "Select Your Identity Provider".
3. Click the "Login" button. You will be redirected to your organization's login page.
4. Log in with your IdP username and password. You will then be redirected back to this site.
5. 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:

- Download 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.

Select your Identity Provider

University of Illinois at Urbana-Champaign

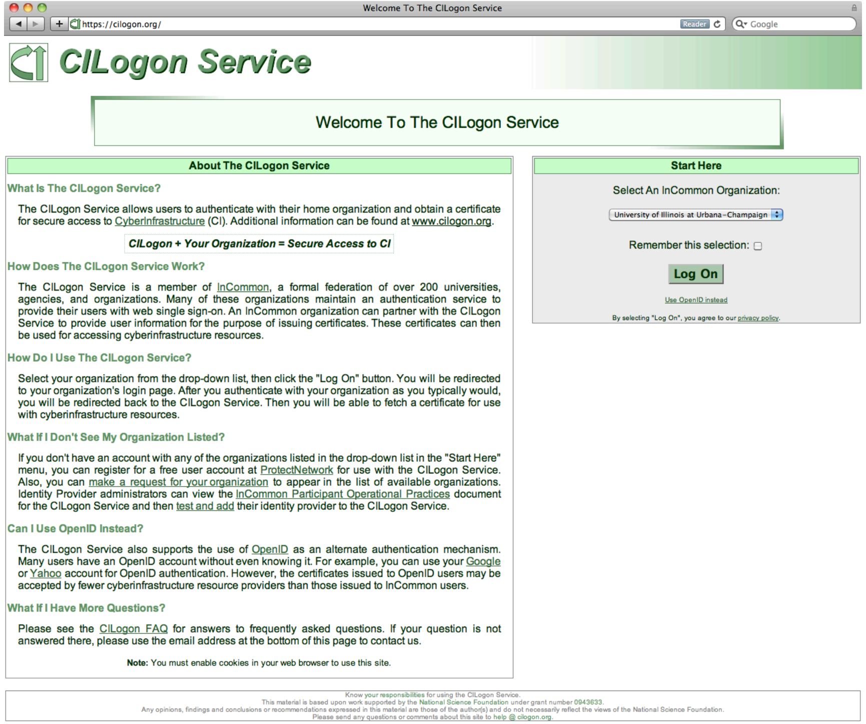
□ Remember for one week (?)

Login

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.

New Service: 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



Welcome To The CILogon Service

About The CILogon Service

What Is The CILogon Service?

The CILogon Service allows users to authenticate with their home organization and obtain a certificate for secure access to CyberInfrastructure (CI). Additional information can be found at www.cilogon.org.

CILogon + Your Organization = Secure Access to CI

How Does The CILogon Service Work?

The CILogon Service is a member of InCommon, a formal federation of over 200 universities, agencies, and organizations. Many of these organizations maintain an authentication service to provide their users with web single sign-on. An InCommon organization can partner with the CILogon Service to provide user information for the purpose of issuing certificates. These certificates can then be used for accessing cyberinfrastructure resources.

How Do I Use The CILogon Service?

Select your organization from the drop-down list, then click the "Log On" button. You will be redirected to your organization's login page. After you authenticate with your organization as you typically would, you will be redirected back to the CILogon Service. Then you will be able to fetch a certificate for use with cyberinfrastructure resources.

What If I Don't See My Organization Listed?

If you don't have an account with any of the organizations listed in the drop-down list in the "Start Here" menu, you can register for a free user account at ProtectNetwork for use with the CILogon Service. Also, you can make a request for your organization to appear in the list of available organizations. Identity Provider administrators can view the InCommon Participant Operational Practices document for the CILogon Service and then test and add their identity provider to the CILogon Service.

Can I Use OpenID Instead?

The CILogon Service also supports the use of OpenID as an alternate authentication mechanism. Many users have an OpenID account without even knowing it. For example, you can use your Google or Yahoo account for OpenID authentication. However, the certificates issued to OpenID users may be accepted by fewer cyberinfrastructure resource providers than those issued to InCommon users.

What If I Have More Questions?

Please see the CILogon FAQ for answers to frequently asked questions. If your question is not answered there, please use the email address at the bottom of this page to contact us.

Note: You must enable cookies in your web browser to use this site.

Start Here

Select An InCommon Organization:

University of Illinois at Urbana-Champaign

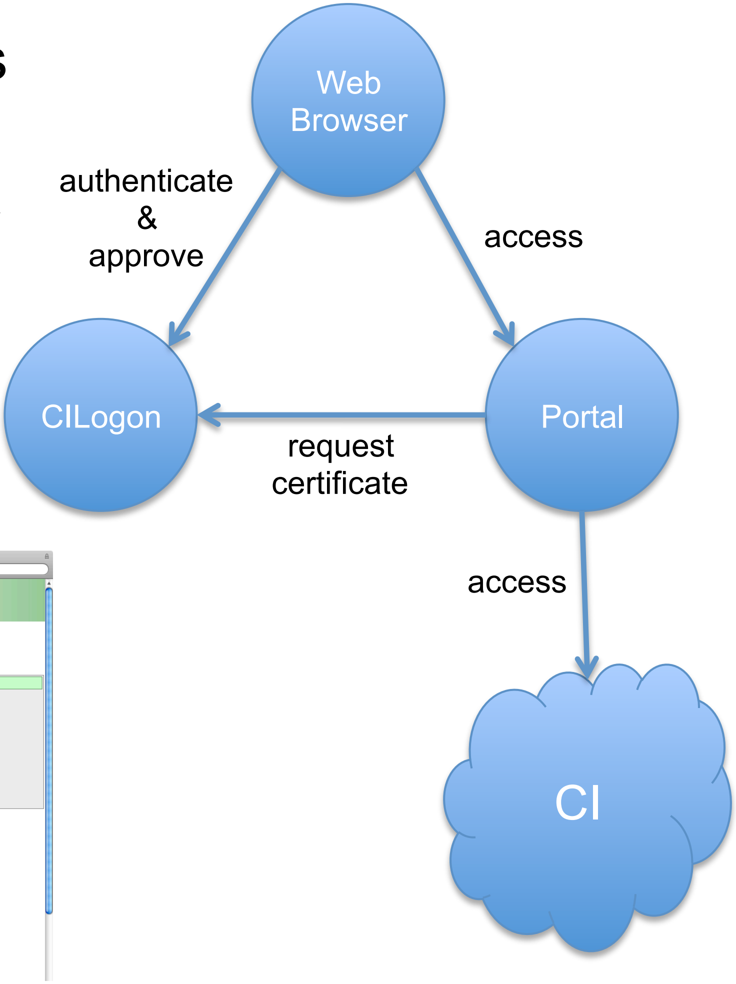
Remember this selection: □

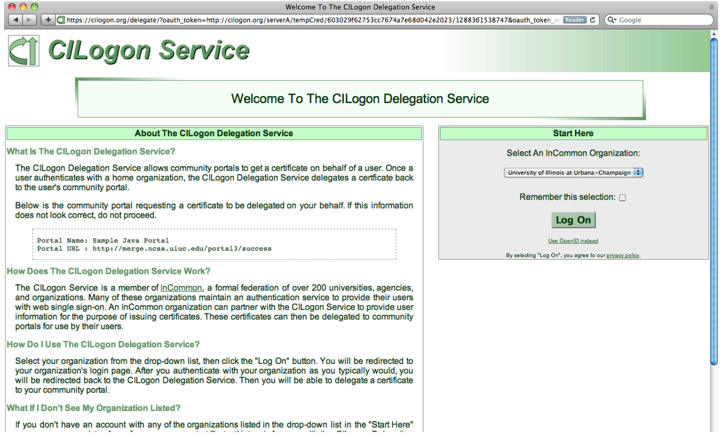
By selecting "Log On", you agree to our privacy policy.

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

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




Welcome To The CILogon Delegation Service
https://cilogon.org/delegate/?oauth_token=http://cilogon.org/serverA/tempCred/603029f62753cc7674a7e68d042e2023/1288361538747&oauth_token_s
Reader
Google
CILogon Service

Welcome To The CILogon Delegation Service

About The CILogon Delegation Service

What Is The CILogon Delegation Service?

The CILogon Delegation Service allows community portals to get a certificate on behalf of a user. Once a user authenticates with a home organization, the CILogon Delegation Service delegates a certficate back to the user's community portal.

Below is the community portal requesting a certificate to be delegated on your behalf. If this information does not look correct, do not proceed.

```
Portal Name: Sample Java Portal
Portal URL : http://merge.ncsa.uiuc.edu/portal3/success
```

How Does The CILogon Delegation Service Work?

The CILogon Service is a member of InCommon, a formal federation of over 200 universities, agencies, and organizations. Many of these organizations maintain an authentication service to provide their users with web single sign-on. An InCommon organization can partner with the CILogon Service to provide user information for the purpose of issuing certificates. These certificates can then be delegated to community portals for use by their users.

How Do I Use The CILogon Delegation Service?

Select your organization from the drop-down list, then click the "Log On" button. You will be redirected to your organization's login page. After you authenticate with your organization as you typically would, you will be redirected back to the CILogon Delegation Service. Then you will be able to delegate a certificate to your community portal.

What If I Don't See My Organization Listed?

If you don't have an account with any of the organizations listed in the drop-down list in the "Start Here"

Start Here

Select An InCommon Organization:

University of Illinois at Urbana-Champaign

Remember this selection: □

Log On

Use OpenID instead

By selecting "Log On", you agree to our privacy policy.

An OAuth Service for Issuing Certificates to Science Gateways for TeraGrid Users

Jim Basney and Jeff Gaynor
{jbasney,gaynor}@illinois.edu

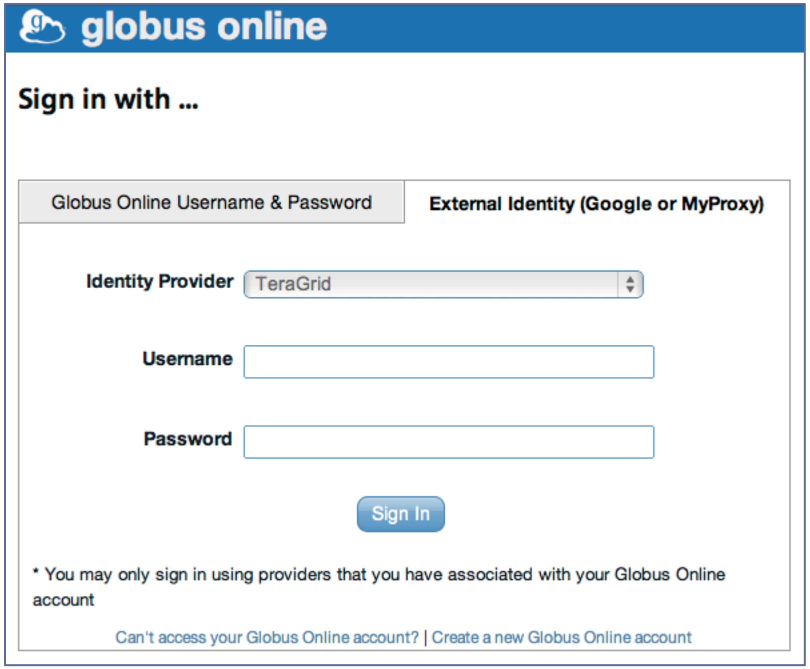
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign

This material is based upon work supported by the National Science Foundation under grant number 0932251.

Goals

- Support use of *individual TeraGrid accounts* via gateways
  - Independent of support for gateway *community accounts*
  - For more accurate accounting, greater resource access
- Avoid disclosing TeraGrid user passwords to gateways
  - Avoid risk to long-lived credentials (i.e., user passwords)
  - Use TeraGrid passwords only on systems operated by TeraGrid
- Use standard security protocols: TLS, OAuth
  - More trustworthy
  - Ease of integration for gateway developers

Current Approach → New Approach



globus online

Sign in with ...

Globus Online Username & Password | **External Identity (Google or MyProxy)**

Identity Provider TeraGrid

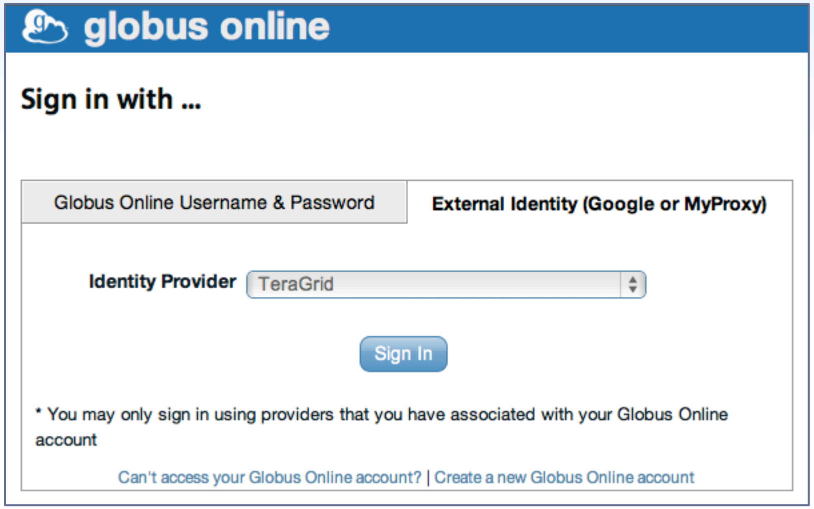
Username

Password

Sign In

* You may only sign in using providers that you have associated with your Globus Online account

Can't access your Globus Online account? | Create a new Globus Online account



globus online

Sign in with ...

Globus Online Username & Password | **External Identity (Google or MyProxy)**

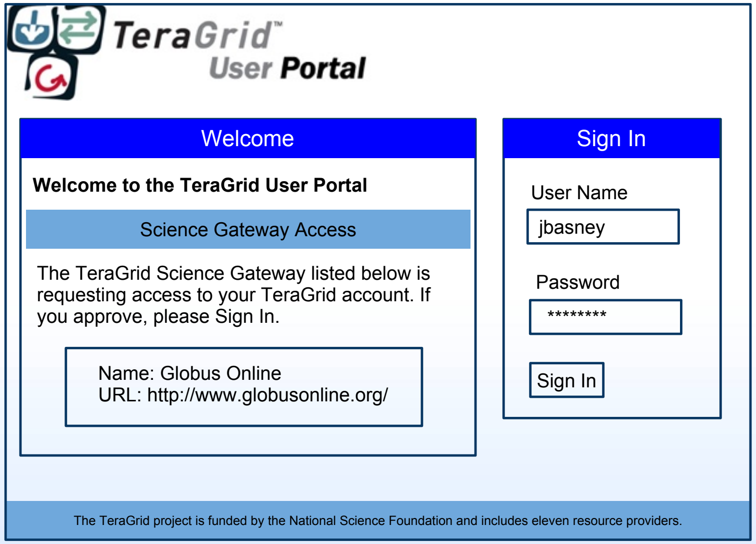
Identity Provider TeraGrid

Sign In

* You may only sign in using providers that you have associated with your Globus Online account

Can't access your Globus Online account? | Create a new Globus Online account

+



TeraGrid™ User Portal

Welcome

Welcome to the TeraGrid User Portal

Science Gateway Access

The TeraGrid Science Gateway listed below is requesting access to your TeraGrid account. If you approve, please Sign In.

Name: Globus Online
URL: http://www.globusonline.org/

Sign In

User Name: jbasney

Password: ********

Sign In

The TeraGrid project is funded by the National Science Foundation and includes eleven resource providers.

Benefits

- **Security WG** concerns about password disclosure to external science gateway sites are addressed
- **Science Gateways** can support individual TeraGrid account access via standard protocols
- **Resource Providers** can support user access via gateways using existing certificate-based interfaces
- **Users** can access their individual TeraGrid accounts via gateways using their TeraGrid Portal login

OAuth Example

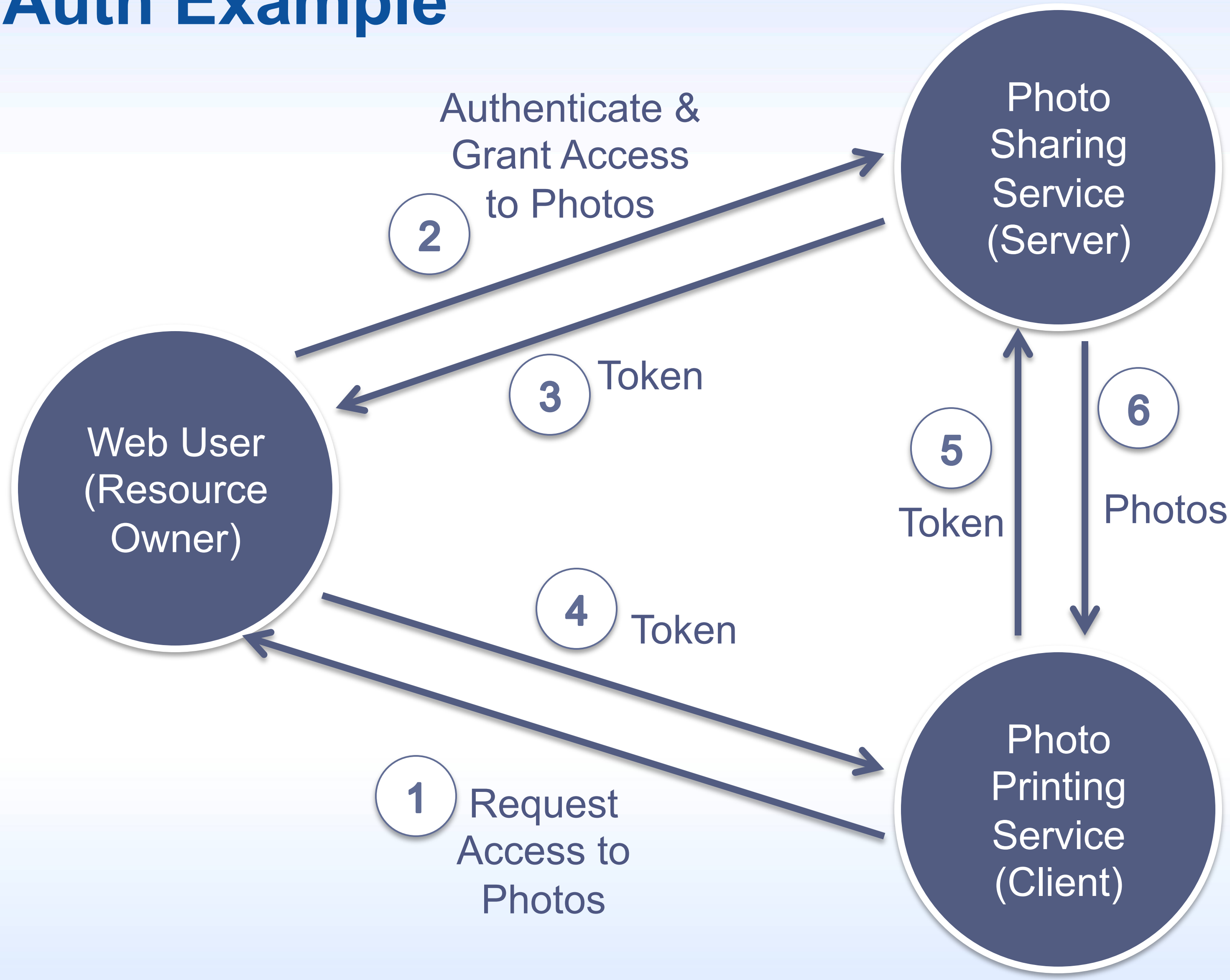
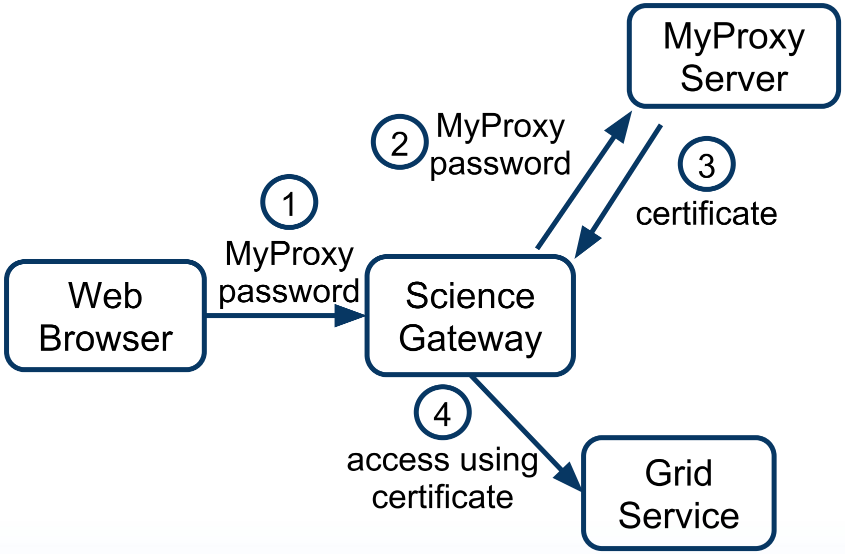
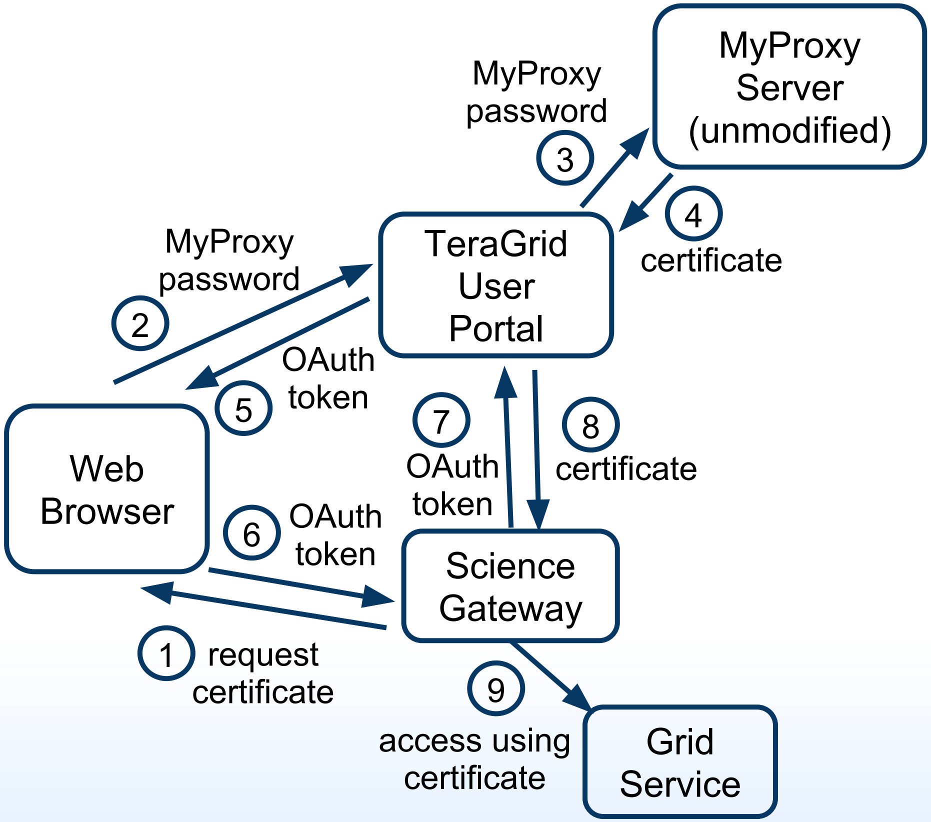
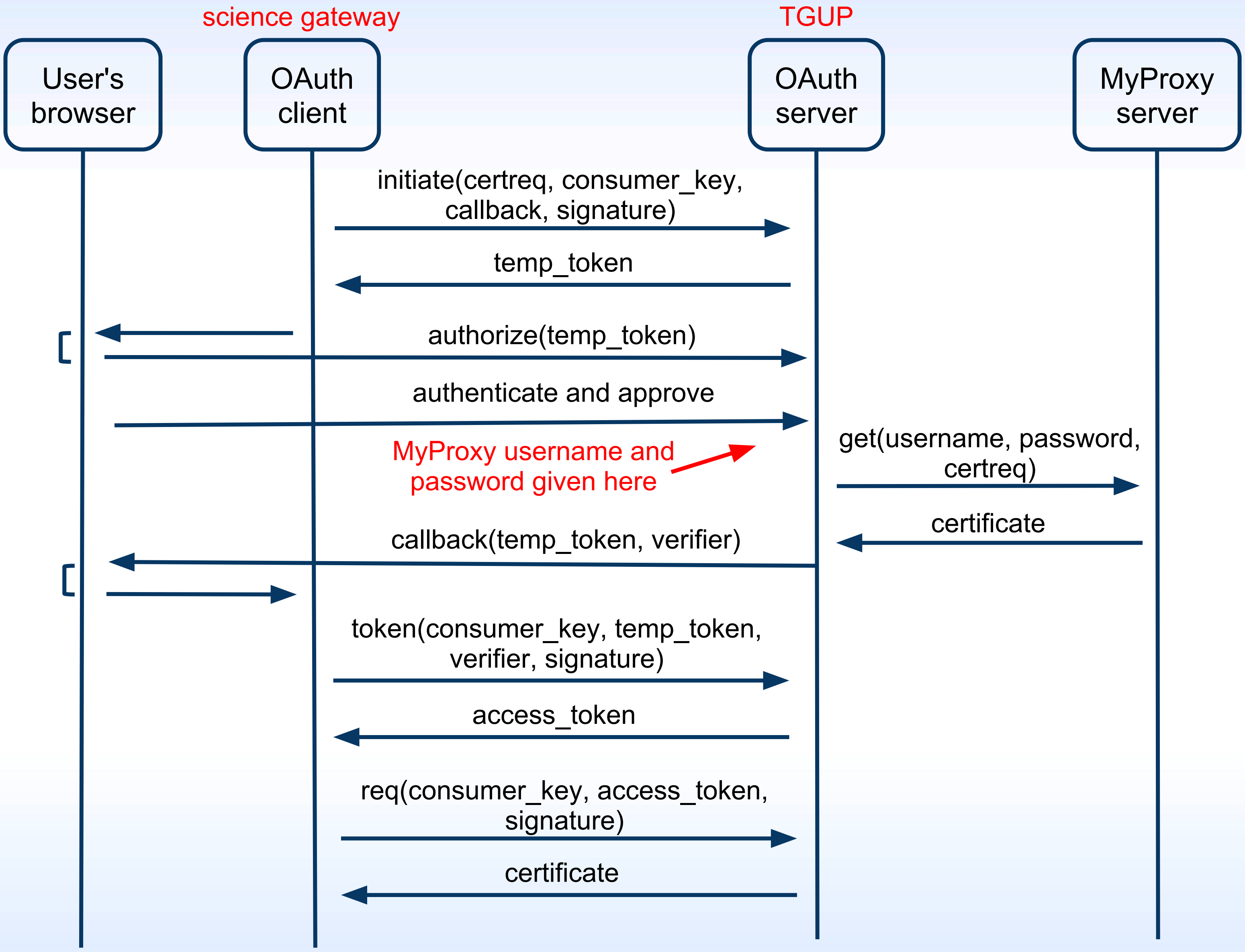


Photo Sharing Service (Server)
Web User (Resource Owner)
Photo Printing Service (Client)
1 Request Access to Photos
2 Authenticate & Grant Access to Photos
3 Token
4 Token
5 Token
6 Photos

Current Approach → New Approach






science gateway
TGUP
User's browser
OAuth client
OAuth server
MyProxy server
initiate(certreq, consumer_key, callback, signature)
temp_token
authorize(temp_token)
authenticate and approve
MyProxy username and password given here
get(username, password, certreq)
certificate
callback(temp_token, verifier)
token(consumer_key, temp_token, verifier, signature)
access_token
req(consumer_key, access_token, signature)
certificate

Distributed Web Security for Science Gateways

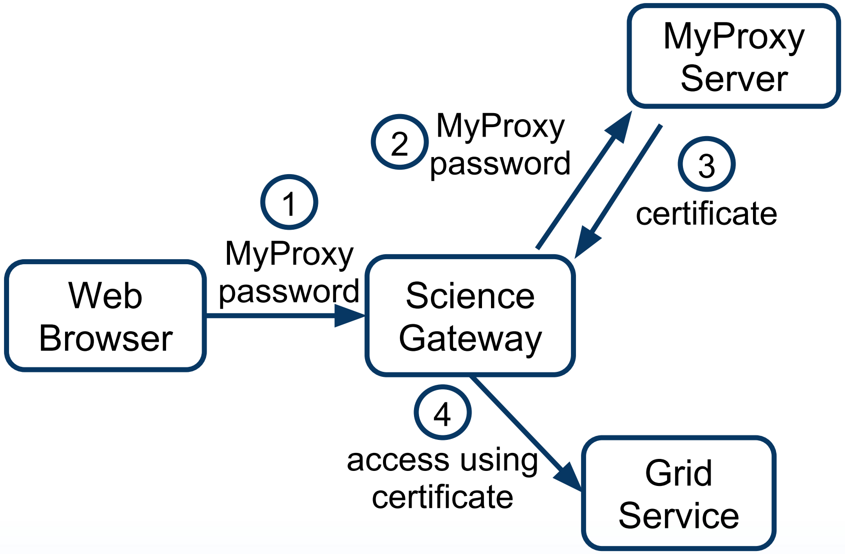
Jim Basney (NCSA)
Rion Dooley (TACC)
Jeff Gaynor (NCSA)
Suresh Marru (IU)
Marlon Pierce (IU)

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

Science Gateway Security Project

- Primary Deliverable: A standards-compliant **OAuth service** implementation to securely delegate, deliver, and renew credentials to science gateways on a user's behalf.
  - Including optional MyProxy integration
  - Including client libraries and modules for web frameworks
- Timeline:
  - August 2011: Project Start
  - February 2012: Initial MyProxy OAuth release
  - August 2012: Initial release of general software components
  - August 2013: Feature complete software releases
  - August 2014: Final software releases

Current Approach → New Approach



Web Browser

1 MyProxy password

Science Gateway

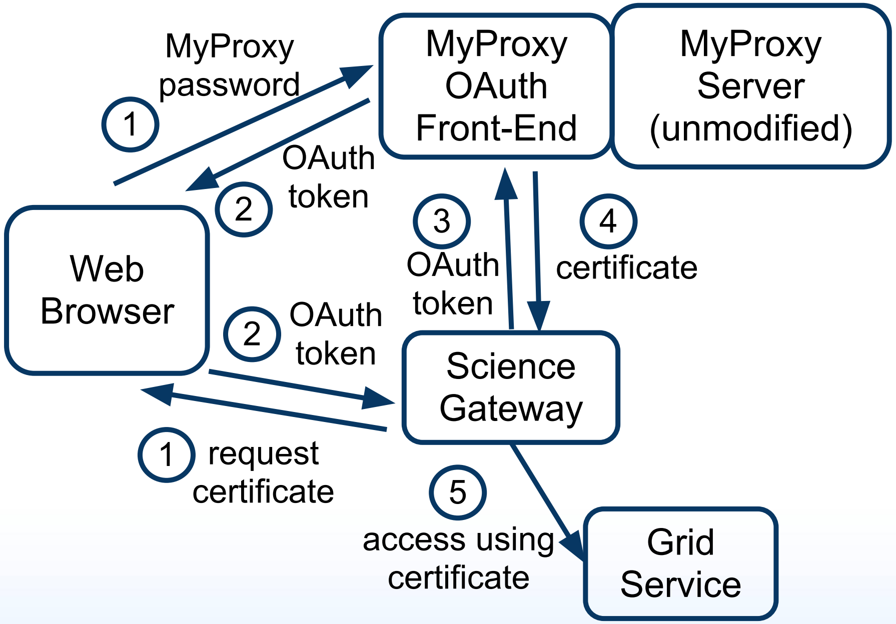
2 MyProxy password

MyProxy Server

3 certificate

4 access using certificate

Grid Service



1 MyProxy password

MyProxy OAuth Front-End

MyProxy Server (unmodified)

2 OAuth token

Web Browser

3 OAuth token

4 certificate

2 OAuth token

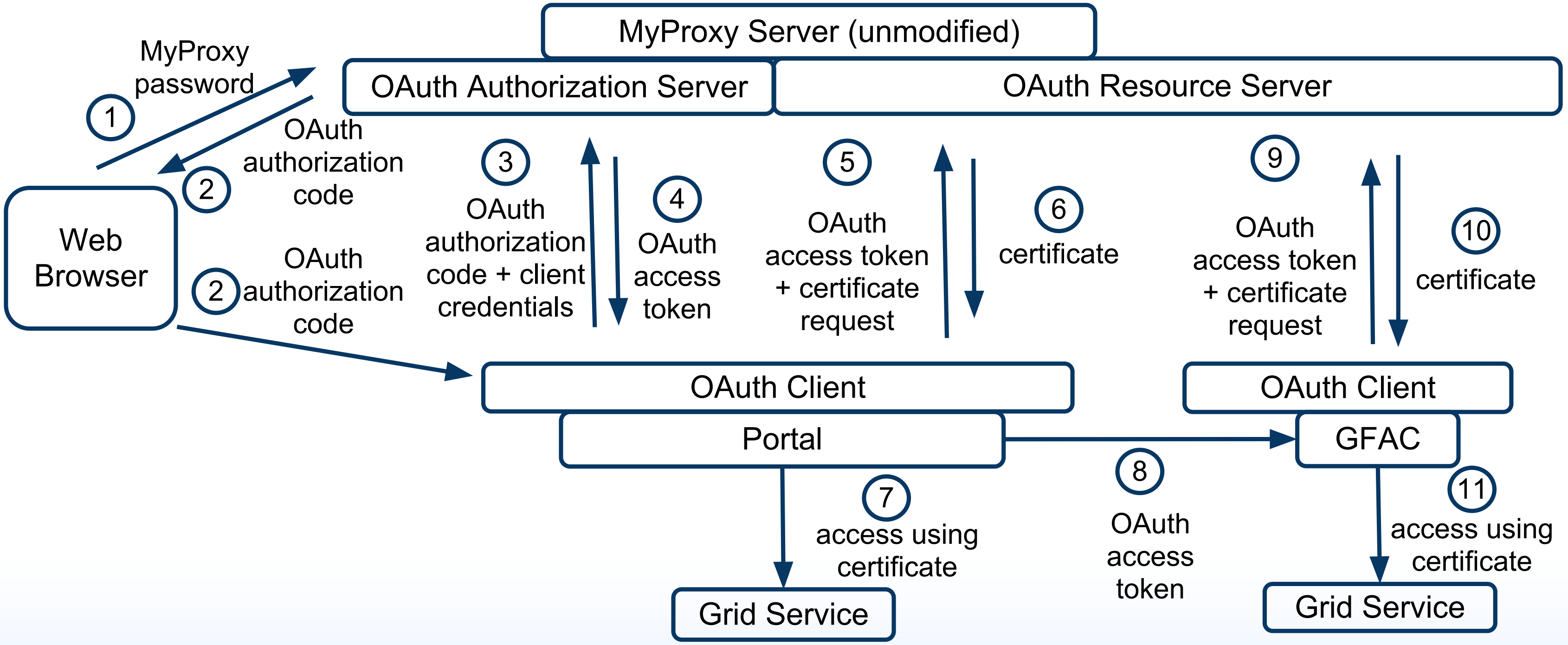
1 request certificate

Science Gateway

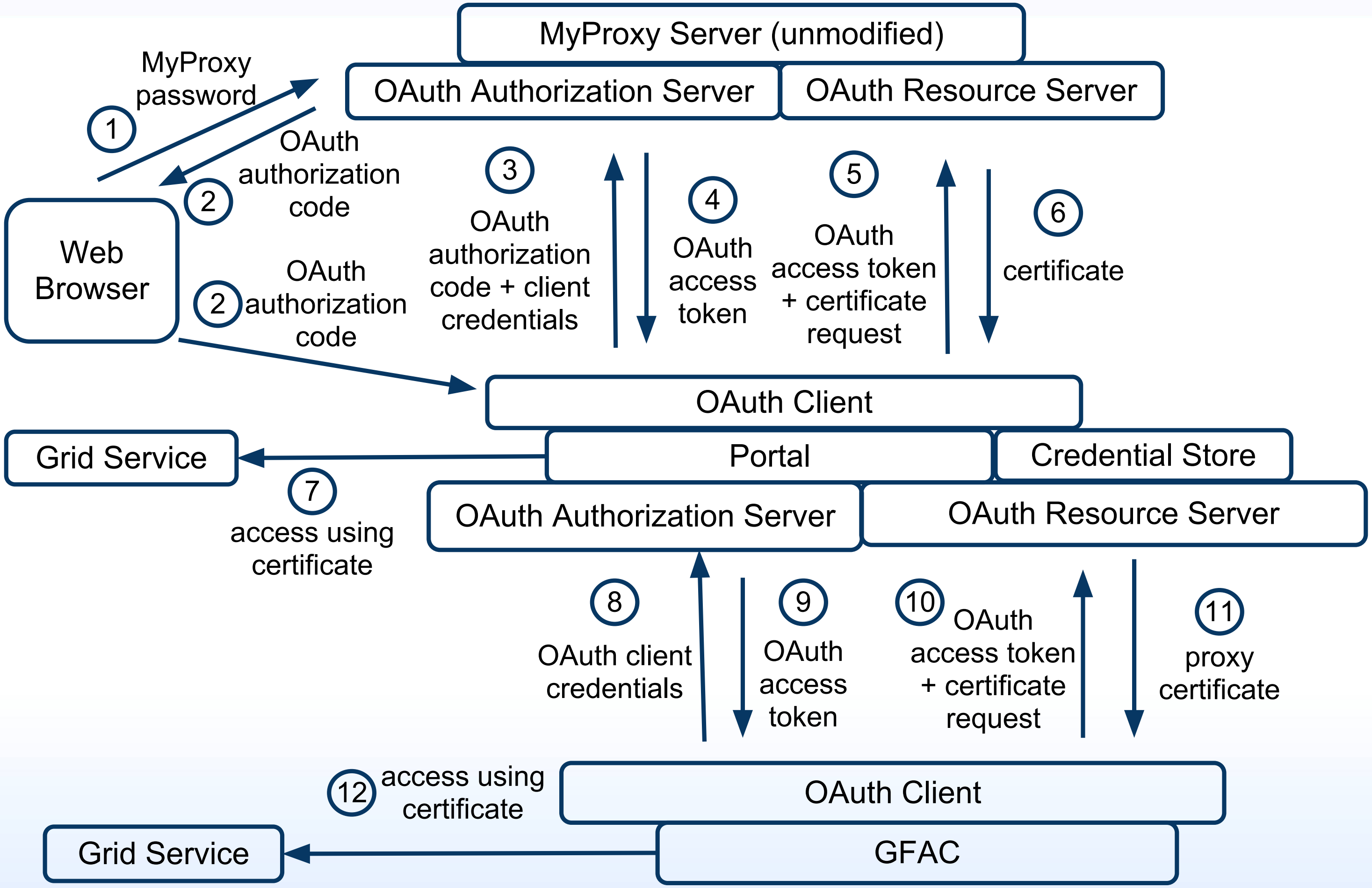
5 access using certificate

Grid Service

Certificate Delegation via OAuth (Option A)



Certificate Delegation via OAuth (Option B)



MyProxy Server (unmodified)

OAuth Authorization Server

OAuth Resource Server

1 MyProxy password

2 OAuth authorization code

Web Browser

2 OAuth authorization code

3 OAuth authorization code + client credentials

4 OAuth access token

5 OAuth access token + certificate request

6 certificate

OAuth Client

Grid Service

Portal

Credential Store

7 access using certificate

OAuth Authorization Server

OAuth Resource Server

8 OAuth client credentials

9 OAuth access token

10 OAuth access token + certificate request

11 proxy certificate

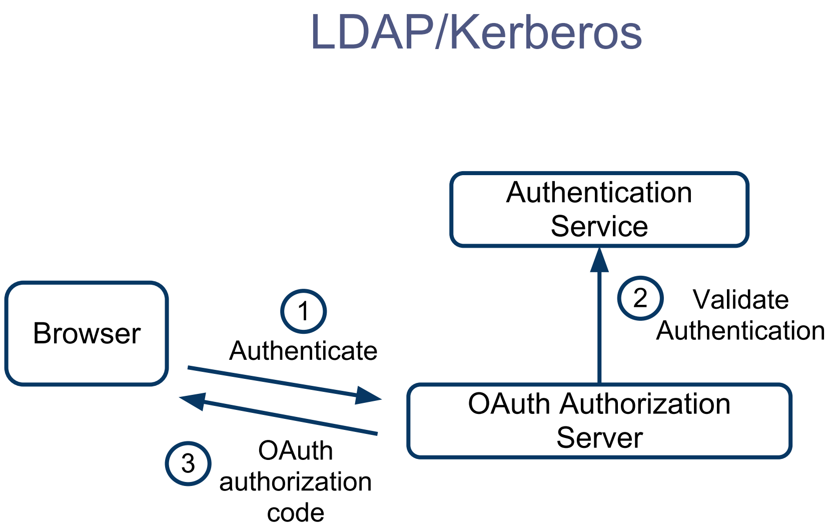
12 access using certificate

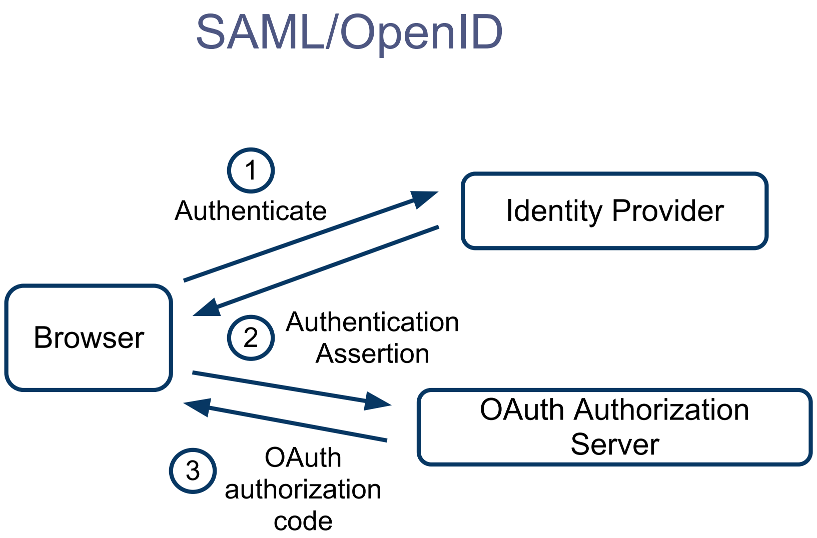
OAuth Client

Grid Service

GFAC

Integration with External Authentication





Science Gateway Security Project

- Other planned OAuth deliverables
  - Secure access to gateway REST services
    - Authorizing access to services via OAuth tokens instead of certs
  - Certificate renewal
    - Using OAuth refresh tokens
- Community engagement
  - UltraScan, iPlant, GridChem/ParamChem
  - XSEDE, Globus Online