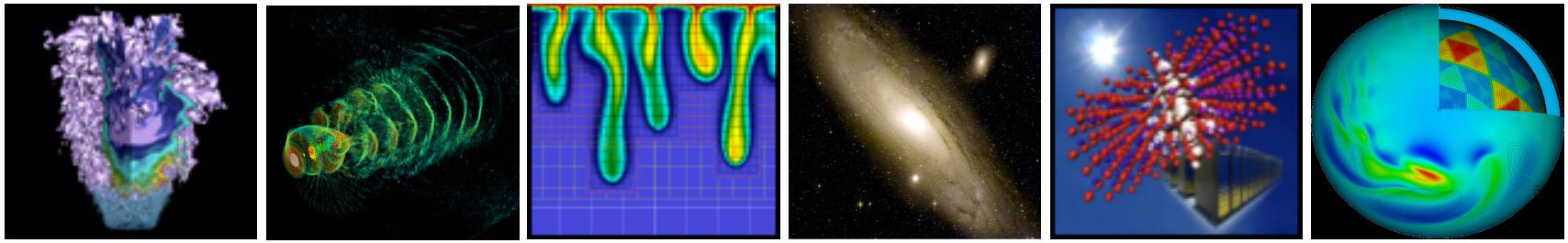


shibboleth@nersc.gov

Steve Chan

sychan@lbl.gov

NERSC National Energy Research Scientific Computing Center

BERKELEY LAB Lawrence Berkeley National Laboratory

Intro

- **What?**
  - What is Shib?
  - What has been Shib-Enabled?
- **Why?**
  - What problem is solved?
  - Why should I care?
- **Who? Where?**
  - Who is using it?

What is Shibboleth?

Gratuitous Biblical Exegesis:

The Gileadites captured the fords of the Jordan leading to Ephraim, and whenever a survivor of Ephraim said, "Let me cross over," the men of Gilead asked him, "Are you an Ephraimite?" If he replied, "No,", they said, "All right, say 'Shibboleth.'" If he said, "Sibboleth," because he could not pronounce the word correctly, they seized him and killed him at the fords of the Jordan. Forty-two thousand Ephraimites were killed at that time.

-Judges 12:5-6

What is Shibboleth?

Gratuitous Biblical Exegesis:

The Gileadites captured the fords of the Jordan leading to Ephraim, and whenever a survivor of Ephraim said, "Let me cross over," the men of Gilead asked him, "Are you an Ephraimite?" If he replied, "No,", they said, "All right, say 'Shibboleth.'" If he said, "Sibboleth," because he could not pronounce the word correctly, they seized him and killed him at the fords of the Jordan. Forty-two thousand Ephraimites were killed at that time.

-Judges 12:5-6

Ethnic Cleansing is in violation of LBL RPM section 7.01 ES&H:

A. Policy

It is the policy of Lawrence Berkeley National Laboratory to perform all work safely and with full regard to the well-being of workers, guests, the public, and the environment.

Keys to implementing this policy are the following core safety values:

[…]

Individuals demonstrate an awareness and concern for the safety of others.

Fatal Shibboleth Login failures are a STOP WORK situation!

What is Shibboleth?

Shibboleth®

The Shibboleth System is a standards based, open source software package for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

The Shibboleth software implements widely used federated identity standards, principally OASIS' Security Assertion Markup Language (SAML), to provide a federated single sign-on and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the browser user and their home site to control the attributes released to each application. Using Shibboleth-enabled access simplifies management of identity and permissions for organizations supporting users and applications. Shibboleth is developed in an open and participatory environment, is freely available, and is released under the Apache Software License.

From: http://shibboleth.internet2.edu/about.html

What is Shibboleth?

SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth

What is Shibboleth?

SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth

Attributes

Assertions about a user(principal) such as user id, name, organizational affiliation/roles. Much of it based on common x509/LDAP attributes. Attributes are encoded and transmited in SAML

What is Shibboleth?

SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth

Attributes

Assertions about a user(principal) such as user id, name, organizational affiliation/roles. Much of it based on common x509/LDAP attributes. Attributes are encoded and transmitted in SAML

Federation

Metadata standards supporting trust relationships to enable Federated Login

What is Shibboleth?

SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth

Attributes

Assertions about a user(principal) such as user id, name, organizational affiliation/roles. Much of it based on common x509/LDAP attributes. Attributes are encoded and transmited in SAML

Federation

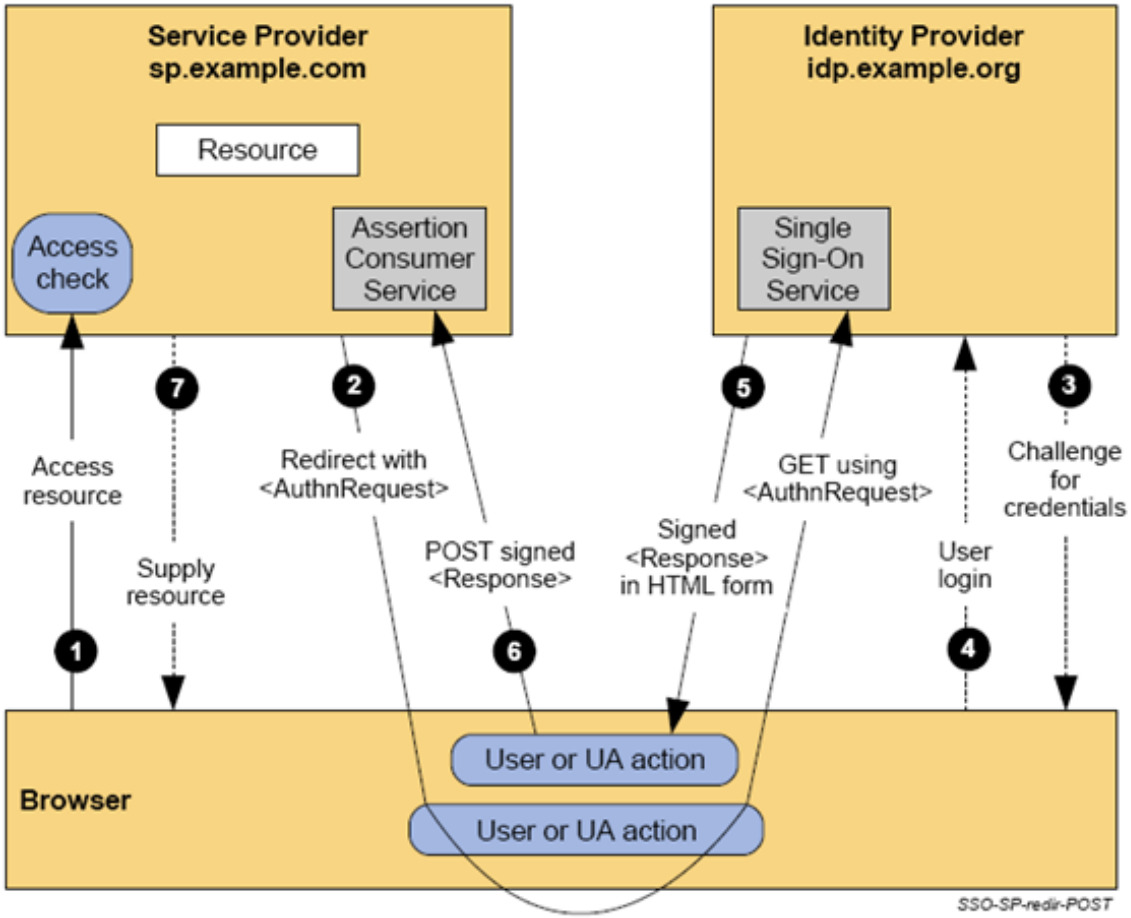
Metadata standards supporting trust relationships to enable Federated Login

Shibboleth/SAML

Shibboleth provides conventions for attributes, standards around metadata discovery and exchange, and policy controls to support privacy and other organizational goals to support the Research and Education community. Shibboleth 2.0 and SAML 2.0 converge on metadata standards

What is Shibboleth?

Shibboleth Web Login transaction



From: http://wiki.eclipse.org/SAML2_IdP

Why Single Sign On?

Pro:

Reduces "password fatigue" from too many different passwords

Sensitive/Secure information is centralized and less exposed

example: the web server gets compromised and used to harvest creds

Fewer locations where passwords are maintained

Convenience avoids possibly insecure workarounds by users

example: having the browser cache passwords

Centralized audit location

Con:

Training

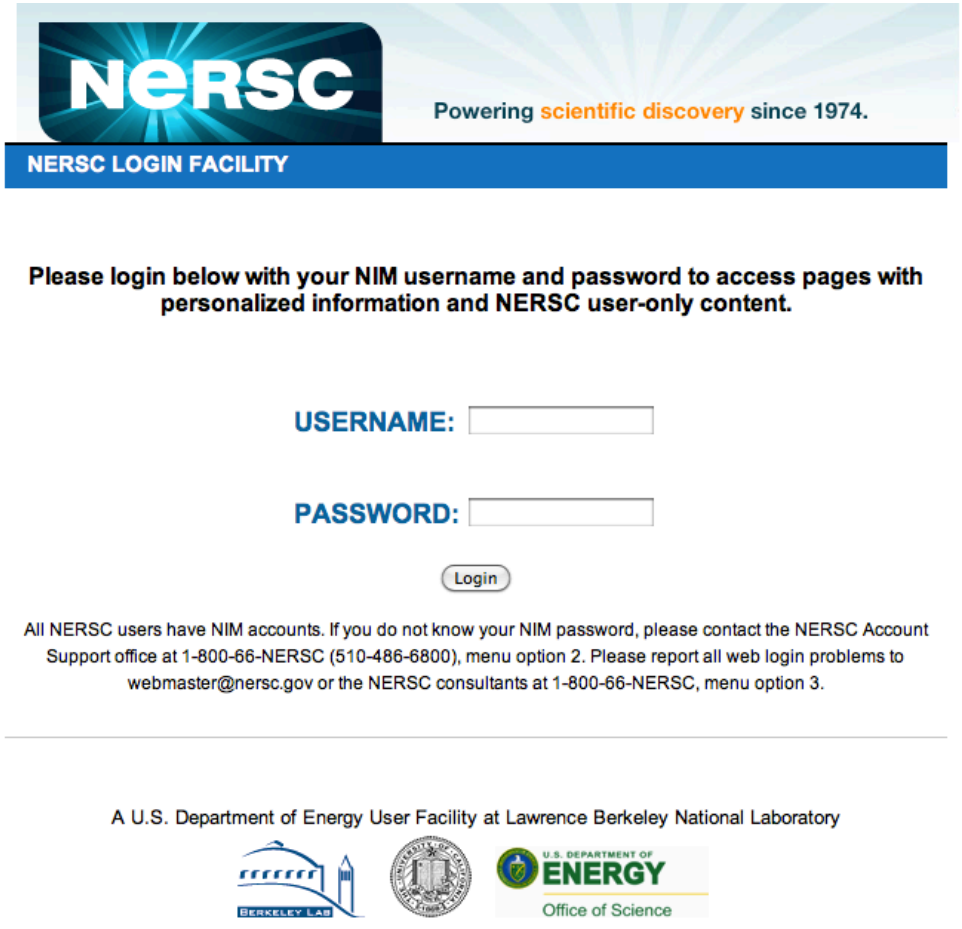
User is now logged into everything, and logout is more complex

Admins have to learn new technology

Single point of failure

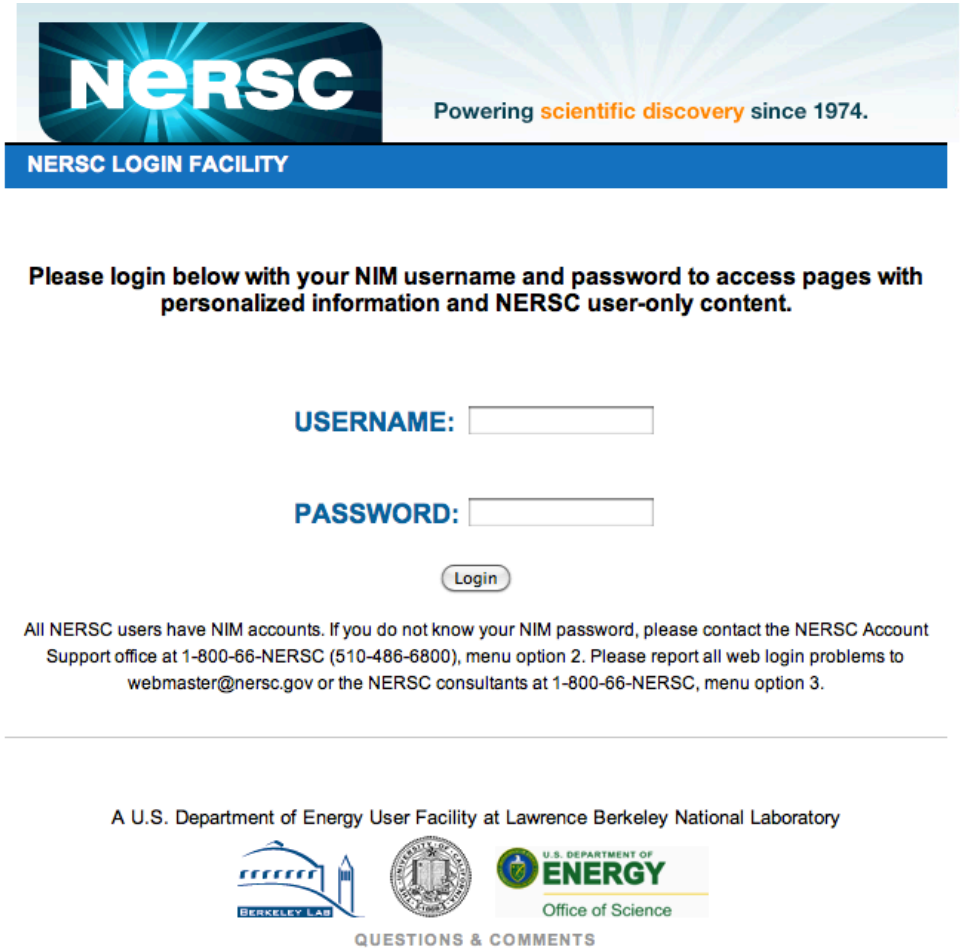
What is using shib at NERSC?

shib.nersc.gov is the Identity Provider (IdP)



What is using shib at NERSC?

Communicates with LDAP, handles all credentials, returns attributes



What is using shib at NERSC?

www.nersc.gov is a Service Provider (SP)

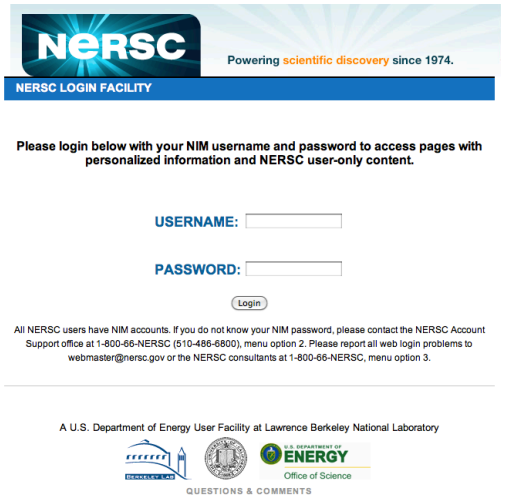
What is using shib at NERSC?

Service Provider is a web application dependent on IdP for authentication

What is using shib at NERSC?

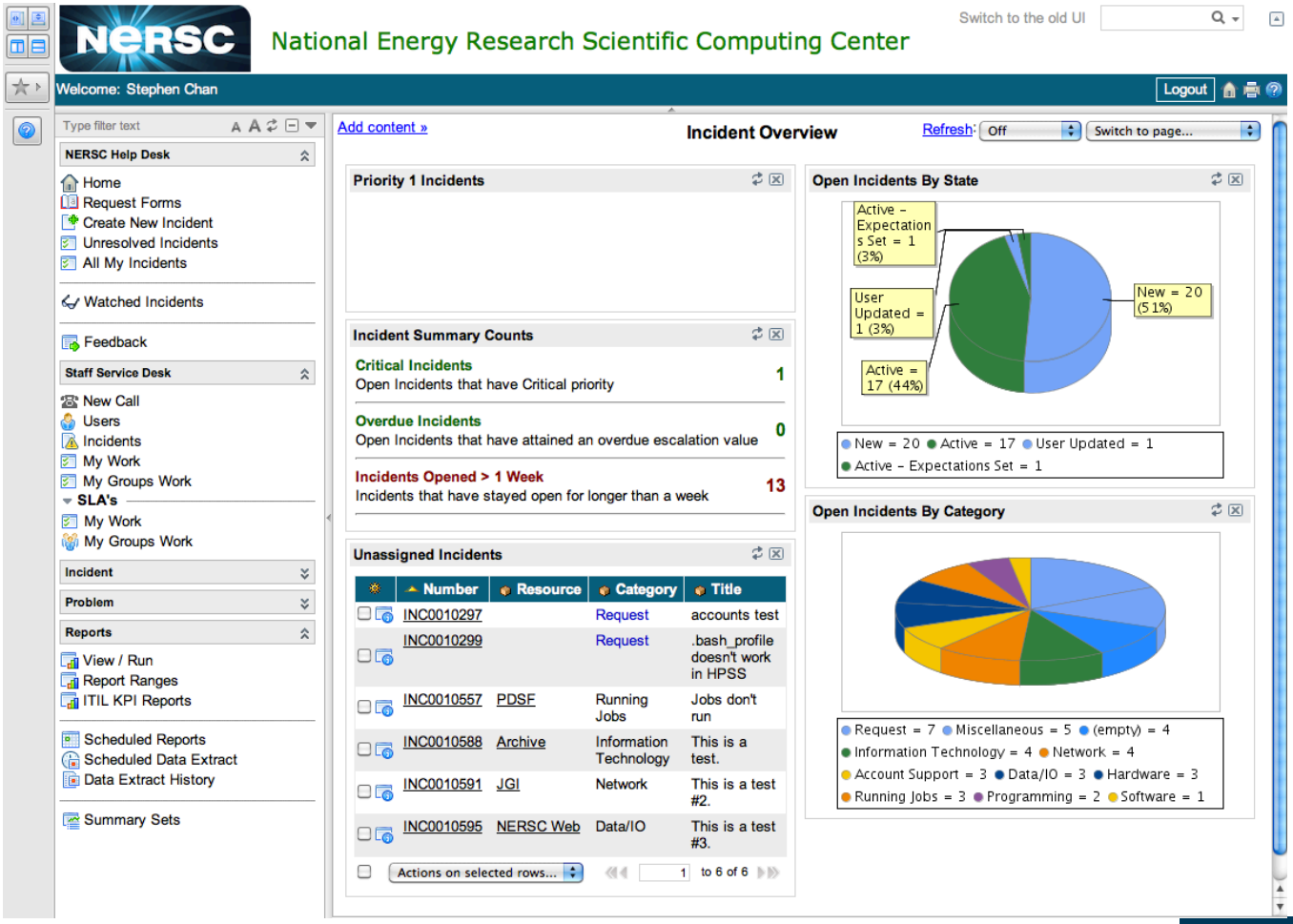
The Service Provider (www.nersc.gov) requests authentication attributes from the Identity Provider (shib.nersc.gov).

Once these attributes are received, the business logic in the SP decides on authorization for the user.



What is using shib at NERSC?

ServiceNow



What additional features?

- **Single Sign On** (currently disabled)
- **JAAS Authentication handler** (stackable)
  - **Radius Authentication (otp for Web SSO)**
    - Possibly useful when traveling to Cyber-Mordor (aka China)
  - **Kerberos Authentication**
  - **LDAP**
- **REMOTE_USER authentication**
  - **IdP looks for $REMOTE_USER for authentication**
- **Database backed attributes** (JDBC)

Who else is using shib?

Popular in R&E Communities:

UC Trust: UCB,UCLA, UCSD, UCD, UCM, UCSF, LBNL, UCI, UCR, UCSC, UCOP

Major Research Universities: Caltech, CMU, Columbia, Cornell, Duke, Georgetown, GA Tech, JHU, MIT, Princeton, Purdue, RPI, Stanford, U Chicago, UIUC, Penn, Yale, etc…

Companies with strong .edu ties and research institutions: Apple, CollegeNet, Internet2, NIH, Smithsonian, ANL, Globus, Teragrid, VOMS

Software As Service Providers: Google, Microsoft, Salesforce, Oracle, ServiceNow, IBM

InCommon Federation

InCommon.org is a large identity federation

- Approx. 360 members
- Contains all of the members in previous slide

Assurance Program

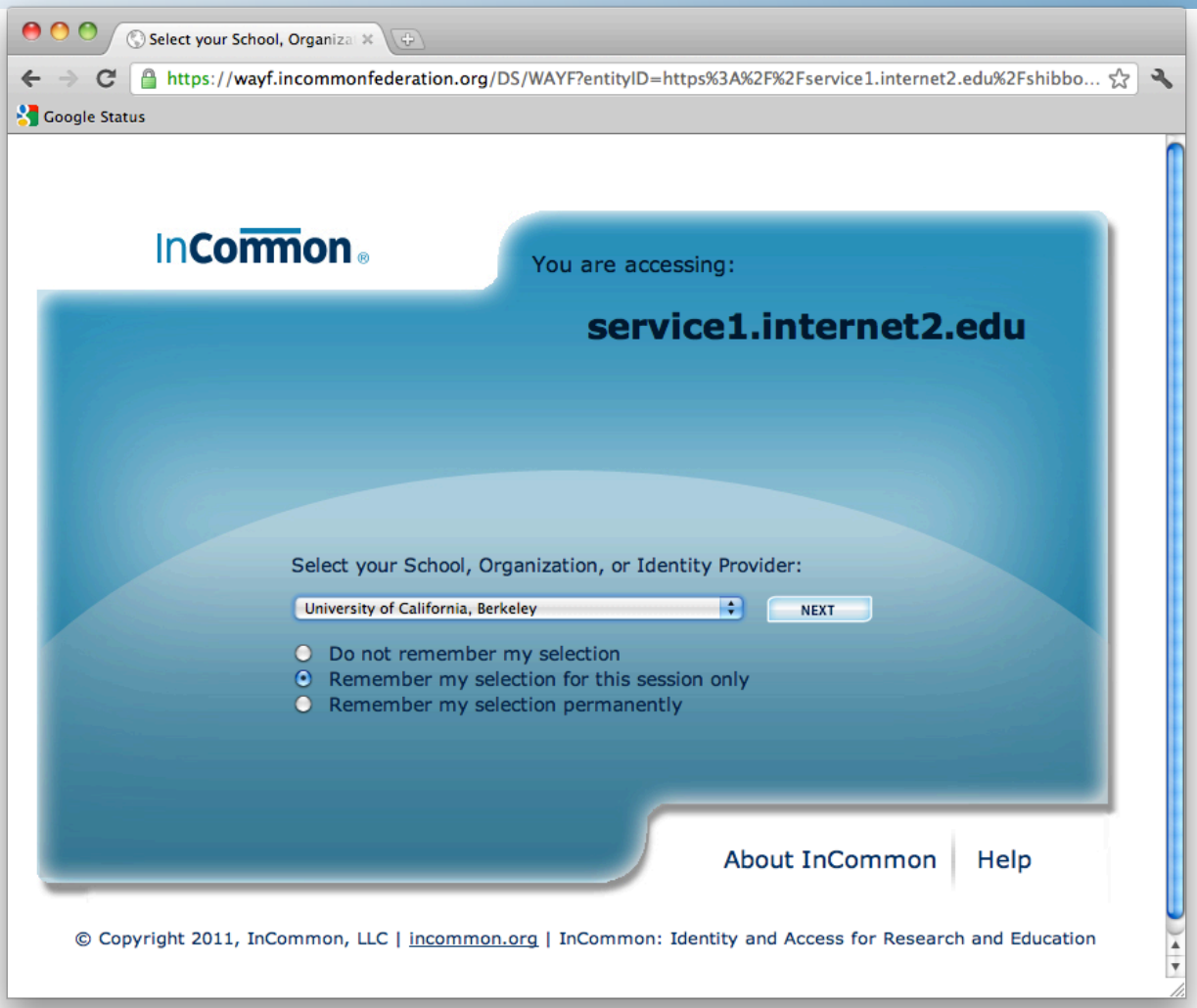
Certificate Service

NERSC is an affiliate

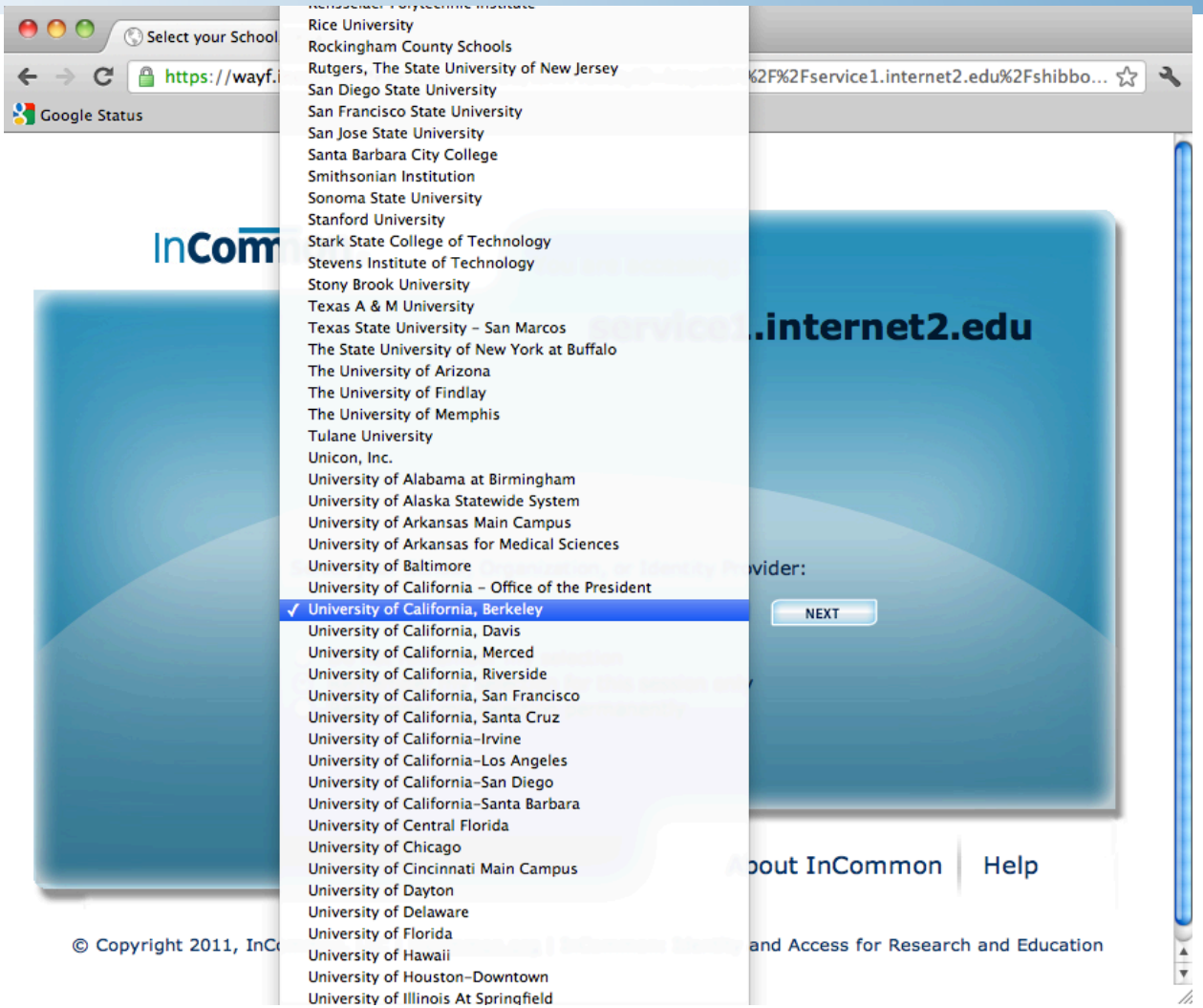
Provides a Discovery Service

- Login entry point for applications that makes available all the Identity Providers of members

InCommon Federation



InCommon Federation



Science Identity Federation

DOE Specific Federation

Led by Mike Helm M_Helm@lbl.gov

Mailing List:
http://groups.google.com/group/science

Basic discovery service

Interesting service – confluence.scifed.org

Several test IDPs

Blanket contract for InCommon membership

Training Events (Shib Install Fest)

NERSC is a member

What/Who else is Shib-Enabled?

Shibboleth Wiki is good resource:

https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled

Elsevier Science Direct
JSTOR
American Chemical Society
UC At Your Service Online
Apples iTunes U

Apache Webserver

Blackboard
Moodle
Sakai

Confluence Wiki
Drupal

Google Apps/Gmail
GridSphere
GridShib
Joomla
MediaWiki
MoinMoin Wiki
SYMPA
Twiki
Workpress
Silverstripe
ServiceNow

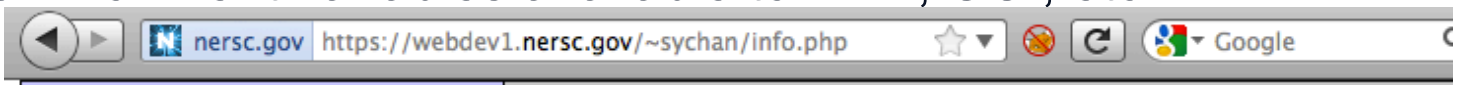
Oracle 10g/11g
BEA/Websphere

Who/What *could* be ShibEnabled?

Web applications are easily ShibEnabled with Apache Shib Module

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLinuxInstall

Once module is configured, shibboleth login info is passed in via CGI environment variables available to PHP, CGI, etc…



_SERVER["Shib-Shib-Session-ID"]	_7a82077fcdd2b965d8118826c2bd9dfd
_SERVER["Shib-Shib-Identity-Provider"]	https://login.lbl.gov/idp/shibboleth
_SERVER["Shib-Shib-Authentication-Instant"]	2011-12-14T23:11:09.137Z
_SERVER["Shib-Shib-Authentication-Method"]	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
_SERVER["Shib-Shib-AuthnContext-Class"]	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
_SERVER["Shib-Shib-Session-Index"]	63c5159b8880ffaa8b4ed85992379d11b8bb35627d1a75c893d5c30dcc0d01f2
_SERVER["Shib-affiliation"]	Staff@lbl.gov;Member@lbl.gov
_SERVER["Shib-cn"]	Steve Chan;Stephen Chan
_SERVER["Shib-displayName"]	Chan, Stephen (Steve)
_SERVER["Shib-employeeNumber"]	004285
_SERVER["Shib-entitlement"]	lbnlUser
_SERVER["Shib-eppn"]	SYChan@lbl.gov
_SERVER["Shib-givenName"]	Stephen
_SERVER["Shib-mail"]	SYChan@lbl.gov
_SERVER["Shib-sn"]	Chan
_SERVER["Shib-uid"]	SYChan

Multidomain Login Demo

Demo Wordpress instance at:

https://webdev1.nersc.gov/~sychan/wpdemo/

WordPress 3.3

http://wordpress.org/download/

Shib Module 1.4:

http://wordpress.org/extend/plugins/shibboleth/

Apache 2.2 and Shibboleth NativeSP

Customized Login Page

Multidomain Login Demo

Apache directives for shib:

```
<Location /~sychan/>
  AuthType shibboleth
  ShibRequireSession Off
  require shibboleth
</Location>
```

Significant config directives for shibd – back end to apache module. Documented at:

https://sites.google.com/a/lbl.gov/csd-silverstripe/web-administrator/shibboleth-sp-configuration/apache-nativesp

Shibboleth uses lots and lots of XML – bring XML allergy meds

You are in a maze of twisty little XML stanzas, all alike

Multidomain Login Demo

Login Domain Director Page logindemo.php:

```
<?php


echo "<center>Test login from the following authentication domains:<br/><br/><br/
    >";
echo '<a href="https://webdev.nersc.gov/Shibboleth.sso/Login?entityID=https%3A//
    login.lbl.gov/idp/shibboleth&' . $_SERVER['QUERY_STRING'] . '"><img
    src="http://www.berkeleyside.com/wp-content/uploads/2011/03/berkeley-lab-
    logo.gif" alt="Berkeley Lab" height="20%" width="20%"/></a><br/><br/><br/>';
echo '<a href="https://webdev.nersc.gov/Shibboleth.sso/Login?entityID=https%3A//
    shib.nersc.gov/idp/shibboleth&' . $_SERVER['QUERY_STRING'] .'"><img
    src="http://www.nersc.gov/themes/nersc-sass/images/logo.png" alt="NERSC
    Shib" /></a><br/><br/><br/><br/>';
echo '<a href="https://webdev.nersc.gov/Shibboleth.sso/Login?entityID=https%3A//
    shib.nersc.gov/idpJGI/shibboleth&' . $_SERVER['QUERY_STRING'] .'"><img
    src="https://www.llnl.gov/news/news_images/logo_JGI_new.gif" height="10%"/></
    a><br/>';


echo "</center>";


?>
```

Questions? Brainstorming

Do we have users that want to access resources at NERSC, but don't have NIM accounts?

Are there applications at other sites that NERSC users want to access without getting account at remote site?

Are there applications where we want groups from multiple sites to have access too, without consolidating user db?

Do we want to allow some form of NERSC authentication on hosts that we don't really trust, or on remote networks where LDAP access would be undesirable?