Federated Identity Management for Research Organizations

Your Hosts Today

- Jim Basney
  - University of Illinois at Urbana-Champaign
  - National Center for Supercomputing Applications
  - CILogon
  - Center for Trustworthy Scientific Cyberinfrastructure (trustedci.org)
- Scott Koranda
  - Spherical Cow Group
  - Laser Interferometer Gravitational-wave Observatory (LIGO)
  - Center for Trustworthy Scientific Cyberinfrastructure (trustedci.org)
- Assistance from Terry Fleury (Thanks!)

Workshop Materials

https://registry.vo.idm.training/shared

Helpful to have today:

1. Browser you can use and "clear all history" repeatedly
    - Preferably Firefox
2. SSH key and SSH client to use with it
    - RSA or DSA key

Session Schedule and Break Times

8:00	Registration / Breakfast
9:00	Introduction / SAML / Shibboleth
11:00	Break
11:30	Shibboleth SP install continued
1:00	Lunch
2:00	SAML Federation Deep Dive / Application Integration
4:00	Break
4:30	OIDC / Collaboration Management
6:00	All done!

Federated Identity Management for Research Organizations

Identity Management?

For research organizations identity management (IdM) usually starts like this:

"Hey, you graduate student, we need a wiki to share some data and write a paper with our collaborators. Go make that happen."

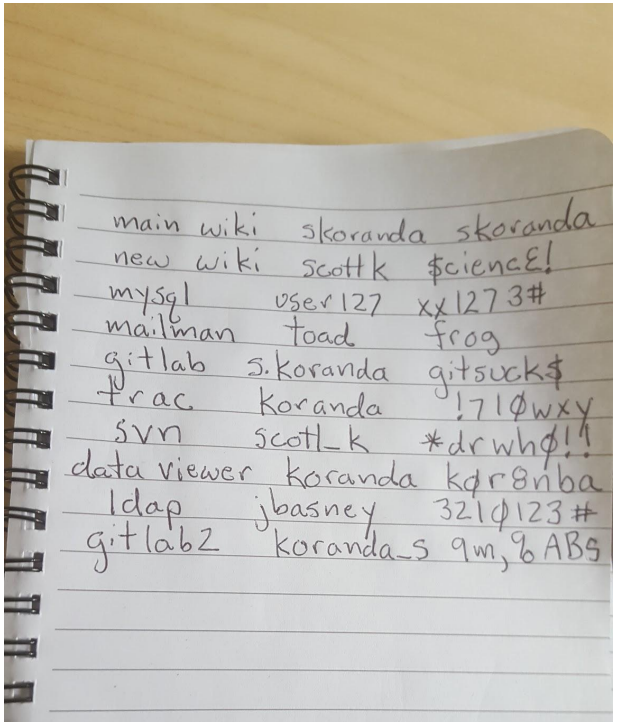
"Organic IdM" Happens

- Grad student deploys some wiki software
- Reads the "Creating users" documentation and provisions new accounts
- Sends email to collaborators:

  "Your new wiki account is skoranda and your password is skoranda. Please change it."

- Months go by...user never changes password.
- Next up: "We need a GitLab repository..."

Organization Grows and So Does Organic IdM



People Move On But Accounts and Access Persist

"Can somebody remove me from this mailing list? I left the project years ago but I continue to receive these emails that I don't think I should be seeing.

Oh, and it looks like I can still access the wiki. You might want to fix that too."

Somebody Will Eventually Suggest...

Google!

- Google Apps offers many interesting features
- But there are tradeoffs
  - Privacy concerns since your data is the product
  - Access for some collaborators may be impossible (or at least undesirable)
  - Less flexibility for later integration
  - Useful suite of products but still a walled garden

Better IdM for Research Organizations

We argue there are better approaches for IdM for research organizations

- Based on open standards
- Built from open source components
- Much more flexibility

The tradeoff is needing to make an intellectual investment in learning

- vocabulary
- architecture
- technical details
- community support channels

Presumably that is why you are here...

IdM Topics To Cover Today

- Authentication / credentials
- Authorization / access control
- Enrollment / onboarding and offboarding
- Collaboration management
- Federated identities including social identity

Problem/Solution Outline for the Day

- Problem: issuing too many accounts and credentials
  - Solution: leverage external or federated identity
  - Topics: SAML, Shibboleth, InCommon, eduGAIN, IdP Discovery, OIDC, CILogon
- Problem: no controlled access to services
  - Solution: leverage centralized access management tools
  - Topics: COmanage, Grouper, LDAP
- Problem: making the services we use fit into the infrastructure
  - Solution: application integration strategies
  - Topics: common architectures, provisioning and deprovisioning, command line solutions

Federated Identity

Federated Identity Definition

Wikipedia:

"...the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems."

"...serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration."

Software Assurance Marketpla ×

https://www.mir-swamp.org

SWAMP | About | Contact | Resources | Policies | ? Help | > Sign In

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.

Welcome to the SWAMP

The Software Assurance Marketplace (SWAMP) is a service that provides continuous software assurance capabilities to developers and researchers.

This no-cost code analysis service is open to the public. Let the SWAMP help you to build better, safer, and more secure code today!

Sign Up! | Sign Up with GitHub!

Get results in just three steps:

Rather than spending time installing, licensing and configuring software assessment tools on your own machine, let the SWAMP do the work for you.

1) Upload your package

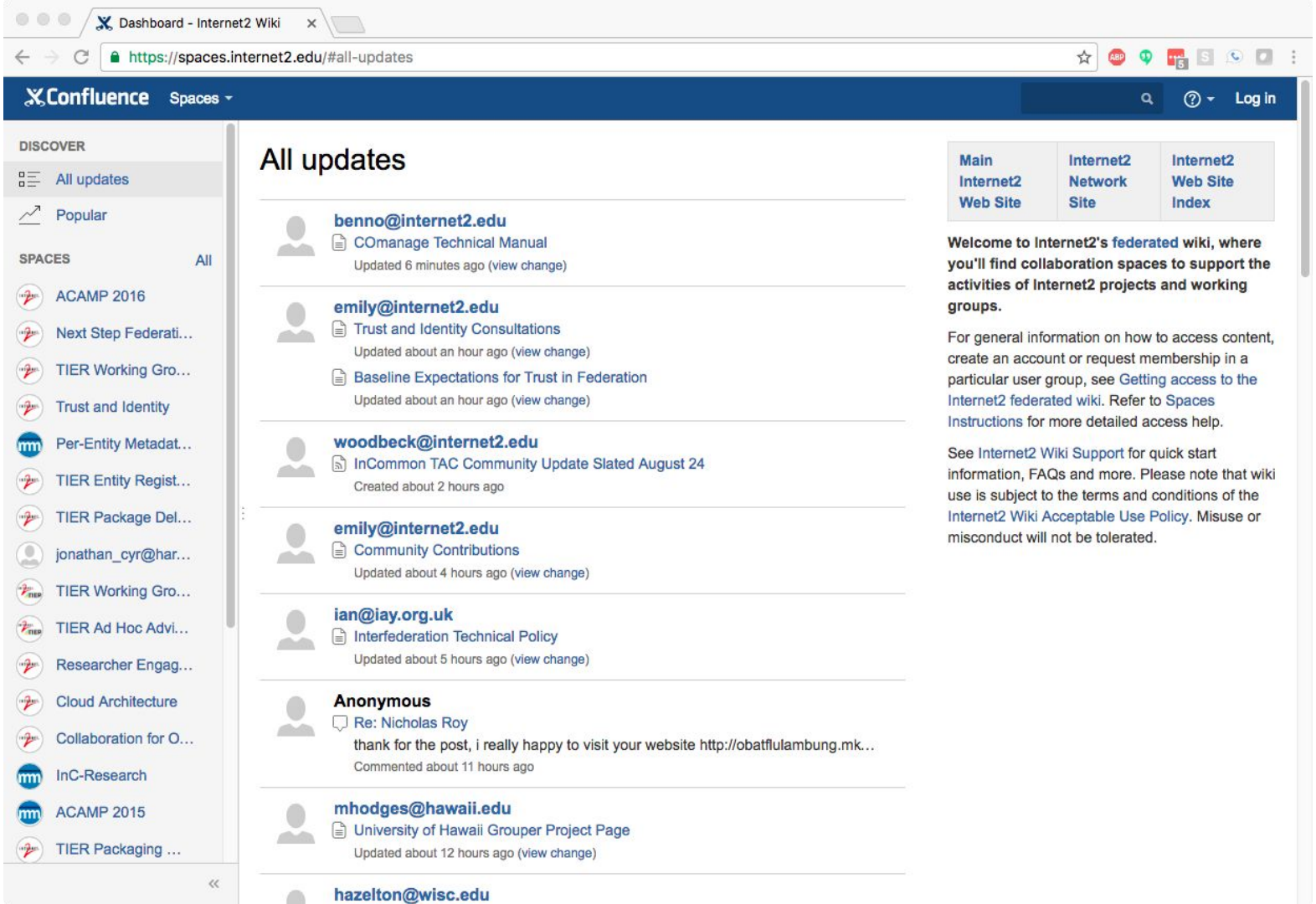
First, upload your code. Rest assured that it will remain private and secure.

2) Run your assessment

Next, create and run an assessment by choosing a package, tool, and platform.

3) View your results

Last, view your results using a native viewer or Code Dx™ for full featured analysis.


Dashboard - Internet2 Wiki
https://spaces.internet2.edu/#all-updates
Confluence
Spaces
Log in
DISCOVER
All updates
Popular
SPACES
All
ACAMP 2016
Next Step Federati…
TIER Working Gro…
Trust and Identity
Per-Entity Metadat…
TIER Entity Regist…
TIER Package Del…
jonathan_cyr@har…
TIER Working Gro…
TIER Ad Hoc Advi…
Researcher Engag…
Cloud Architecture
Collaboration for O…
InC-Research
ACAMP 2015
TIER Packaging …
All updates
benno@internet2.edu
COmanage Technical Manual
Updated 6 minutes ago (view change)
emily@internet2.edu
Trust and Identity Consultations
Updated about an hour ago (view change)
Baseline Expectations for Trust in Federation
Updated about an hour ago (view change)
woodbeck@internet2.edu
InCommon TAC Community Update Slated August 24
Created about 2 hours ago
emily@internet2.edu
Community Contributions
Updated about 4 hours ago (view change)
ian@iay.org.uk
Interfederation Technical Policy
Updated about 5 hours ago (view change)
Anonymous
Re: Nicholas Roy
thank for the post, i really happy to visit your website http://obatflulambung.mk…
Commented about 11 hours ago
mhodges@hawaii.edu
University of Hawaii Grouper Project Page
Updated about 12 hours ago (view change)
hazelton@wisc.edu
Main Internet2 Web Site
Internet2 Network Site
Internet2 Web Site Index
Welcome to Internet2's federated wiki, where you'll find collaboration spaces to support the activities of Internet2 projects and working groups.
For general information on how to access content, create an account or request membership in a particular user group, see Getting access to the Internet2 federated wiki. Refer to Spaces Instructions for more detailed access help.
See Internet2 Wiki Support for quick start information, FAQs and more. Please note that wiki use is subject to the terms and conditions of the Internet2 Wiki Acceptable Use Policy. Misuse or misconduct will not be tolerated.

Federated Identity: Hands-On Exercise

Task:

- Browse to https://spaces.internet2.edu
- Click "Login"
- Search for your home organization identity provider
- Choose "Do not remember" for session
- Click "Select"
- Authenticate to your home organization identity provider
- Verify you are "logged in" to the Internet2 Spaces wiki

Federated Identity: Hands-On Exercise

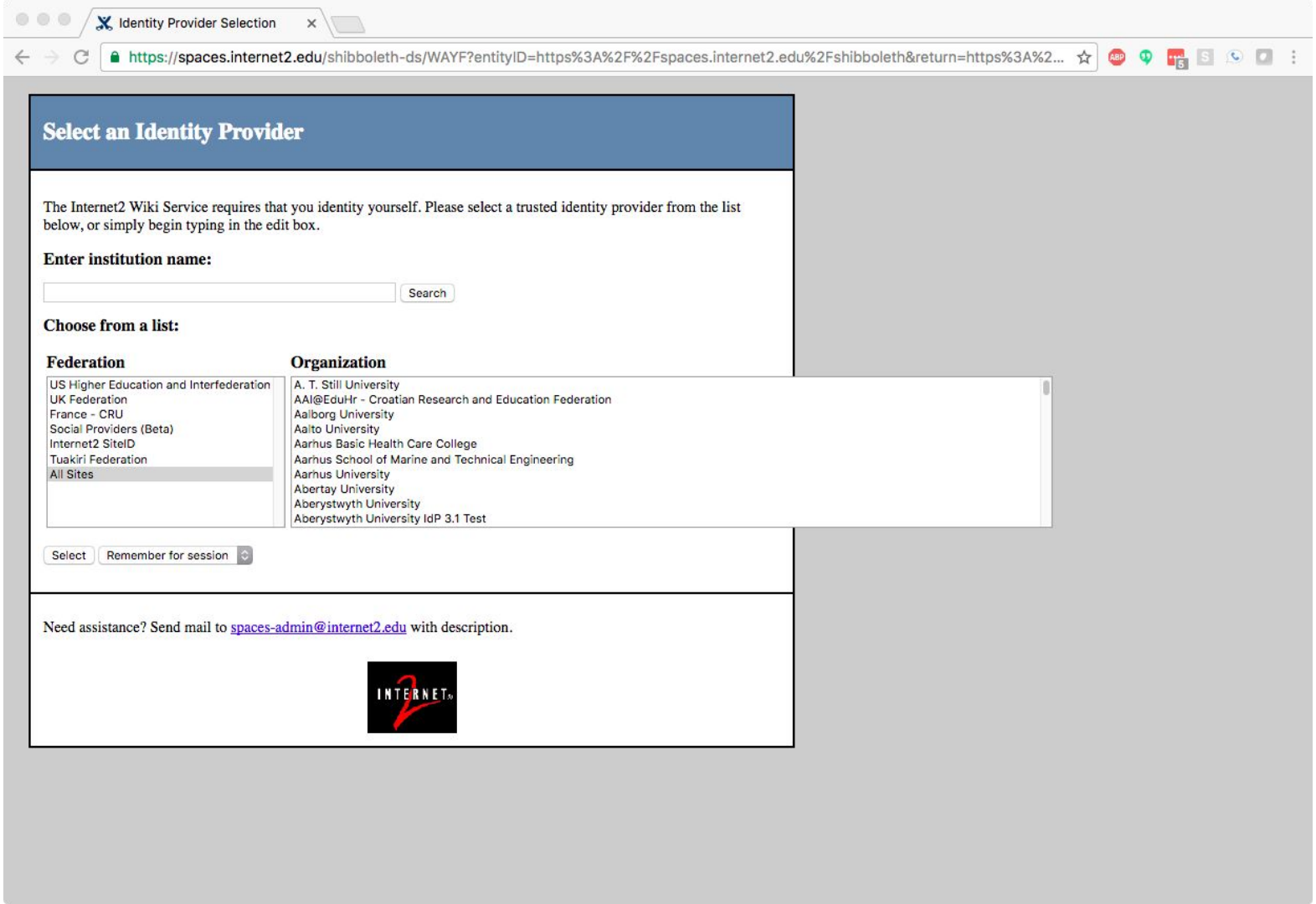
Cannot find your home organization?

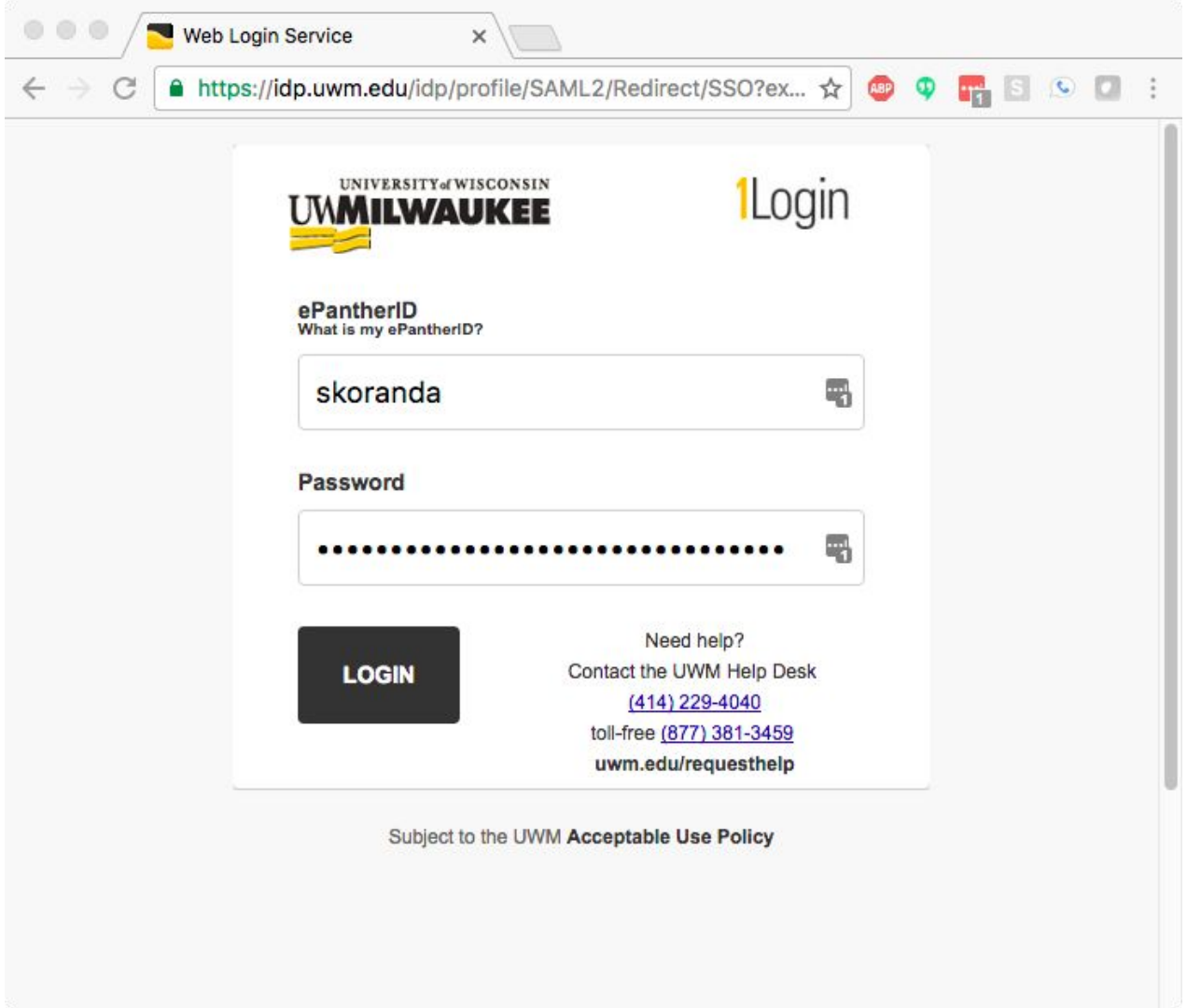
You need to first sign up for a (free) federated identity.

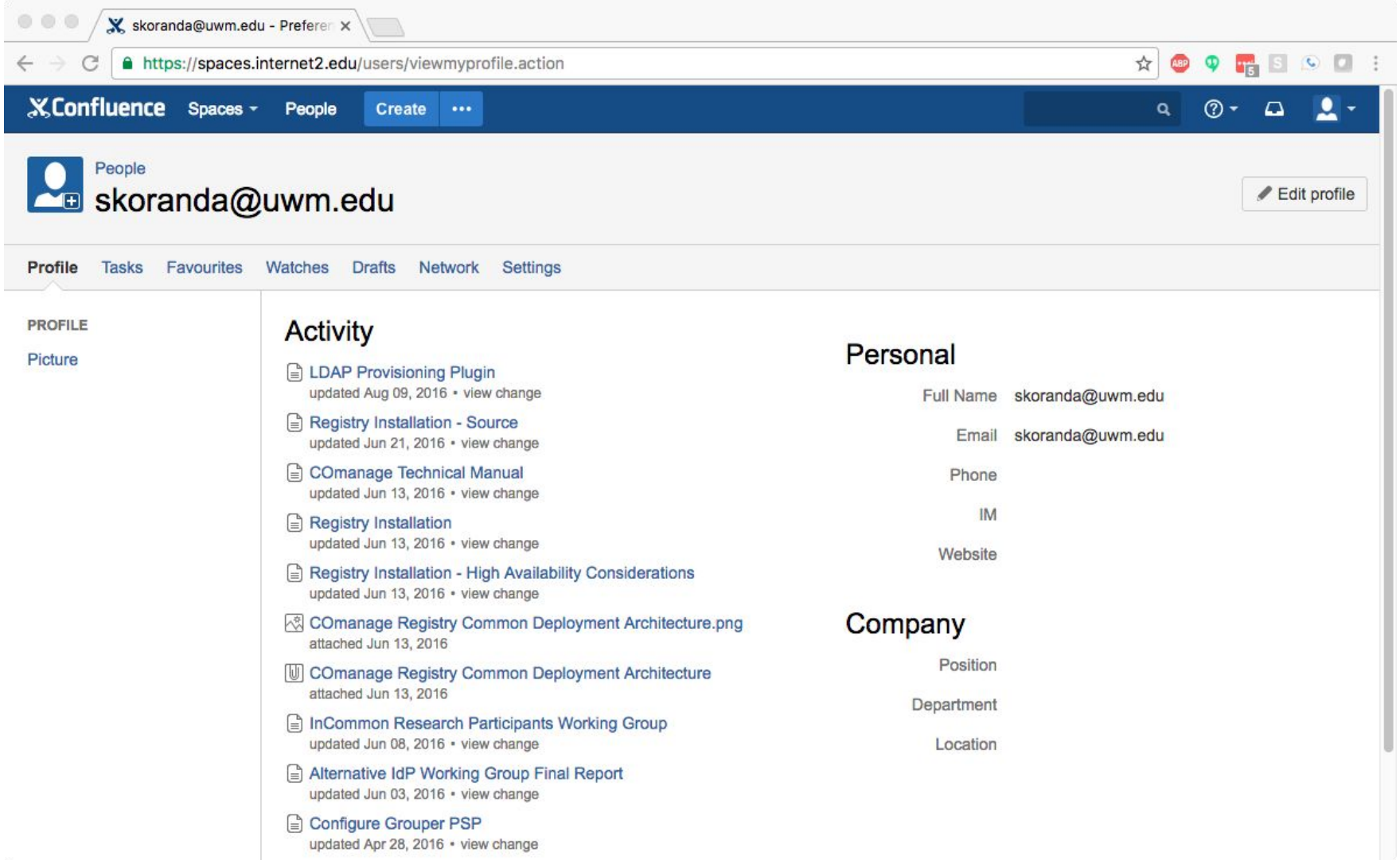
- Try NCSA: https://go.ncsa.illinois.edu/idp-guest

  or

- United ID: https://unitedid.org/
  - Requires a second factor like Google Authenticator on your phone


Identity Provider Selection
https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F%2Fspaces.internet2.edu%2Fshibboleth&return=https%3A%2...
Select an Identity Provider
The Internet2 Wiki Service requires that you identity yourself. Please select a trusted identity provider from the list below, or simply begin typing in the edit box.
Enter institution name:
Search
Choose from a list:
Federation
Organization
US Higher Education and Interfederation
UK Federation
France - CRU
Social Providers (Beta)
Internet2 SiteID
Tuakiri Federation
All Sites
A. T. Still University
AAI@EduHr - Croatian Research and Education Federation
Aalborg University
Aalto University
Aarhus Basic Health Care College
Aarhus School of Marine and Technical Engineering
Aarhus University
Abertay University
Aberystwyth University
Aberystwyth University IdP 3.1 Test
Select
Remember for session
Need assistance? Send mail to spaces-admin@internet2.edu with description.
INTERNET2


Web Login Service
https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?ex...
UNIVERSITY of WISCONSIN
UWMILWAUKEE
1Login
ePantherID
What is my ePantherID?
skoranda
Password
LOGIN
Need help?
Contact the UWM Help Desk
(414) 229-4040
toll-free (877) 381-3459
uwm.edu/requesthelp
Subject to the UWM Acceptable Use Policy

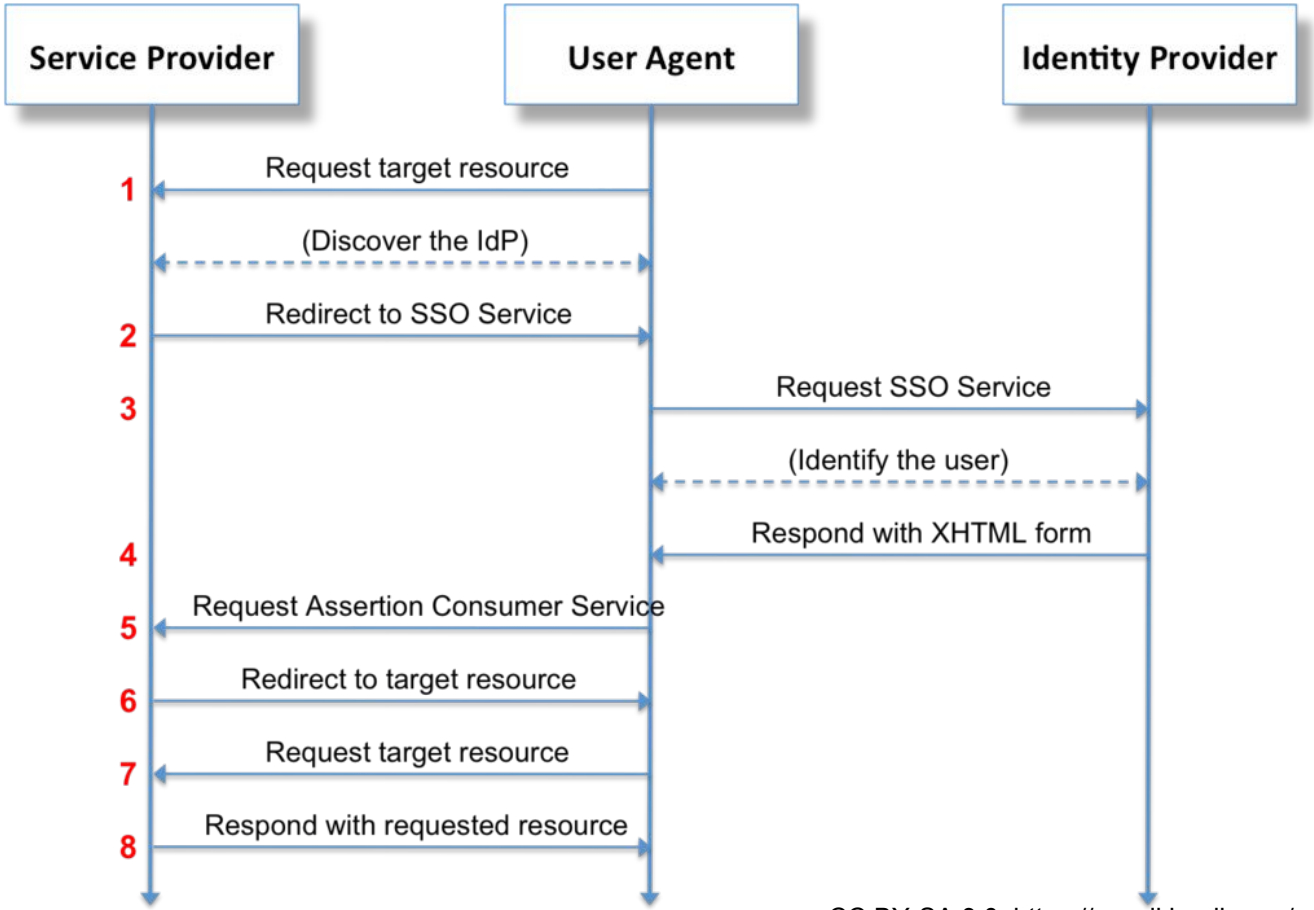

skoranda@uwm.edu - Preferen
https://spaces.internet2.edu/users/viewmyprofile.action
Confluence
Spaces
People
Create
People
skoranda@uwm.edu
Edit profile
Profile
Tasks
Favourites
Watches
Drafts
Network
Settings
PROFILE
Picture
Activity
LDAP Provisioning Plugin
updated Aug 09, 2016 • view change
Registry Installation - Source
updated Jun 21, 2016 • view change
COmanage Technical Manual
updated Jun 13, 2016 • view change
Registry Installation
updated Jun 13, 2016 • view change
Registry Installation - High Availability Considerations
updated Jun 13, 2016 • view change
COmanage Registry Common Deployment Architecture.png
attached Jun 13, 2016
COmanage Registry Common Deployment Architecture
attached Jun 13, 2016
InCommon Research Participants Working Group
updated Jun 08, 2016 • view change
Alternative IdP Working Group Final Report
updated Jun 03, 2016 • view change
Configure Grouper PSP
updated Apr 28, 2016 • view change
Personal
Full Name skoranda@uwm.edu
Email skoranda@uwm.edu
Phone
IM
Website
Company
Position
Department
Location

What just happened?

- Used identity from one security domain (your home organization) to access resources from another security domain (Internet2)
- Works because of pre-established trust between the identity provider (your home organization) and the service provider (Internet2 spaces wiki)
- Leveraged SAML protocol
  - Security Assertion Markup Language
  - Facilitates federated web browser single sign-on (SSO)
  - Most common (today) protocol used by higher education and research for federated SSO

SAML

SAML Web Browser SSO: Protocol Overview



SAML tracer :: Add-ons for ...

Mozilla Foundation (US) https://addons.mozilla.org/en-US/fire

Search

Register or Log in | Other Applications

mozilla

Add-ons

search for add-ons

EXTENSIONS THEMES COLLECTIONS MORE...

SAML tracer 0.3.3

by Olav Morken, Jaime Perez

Debug and view SAML messages

+ Add to Firefox

★★★★☆

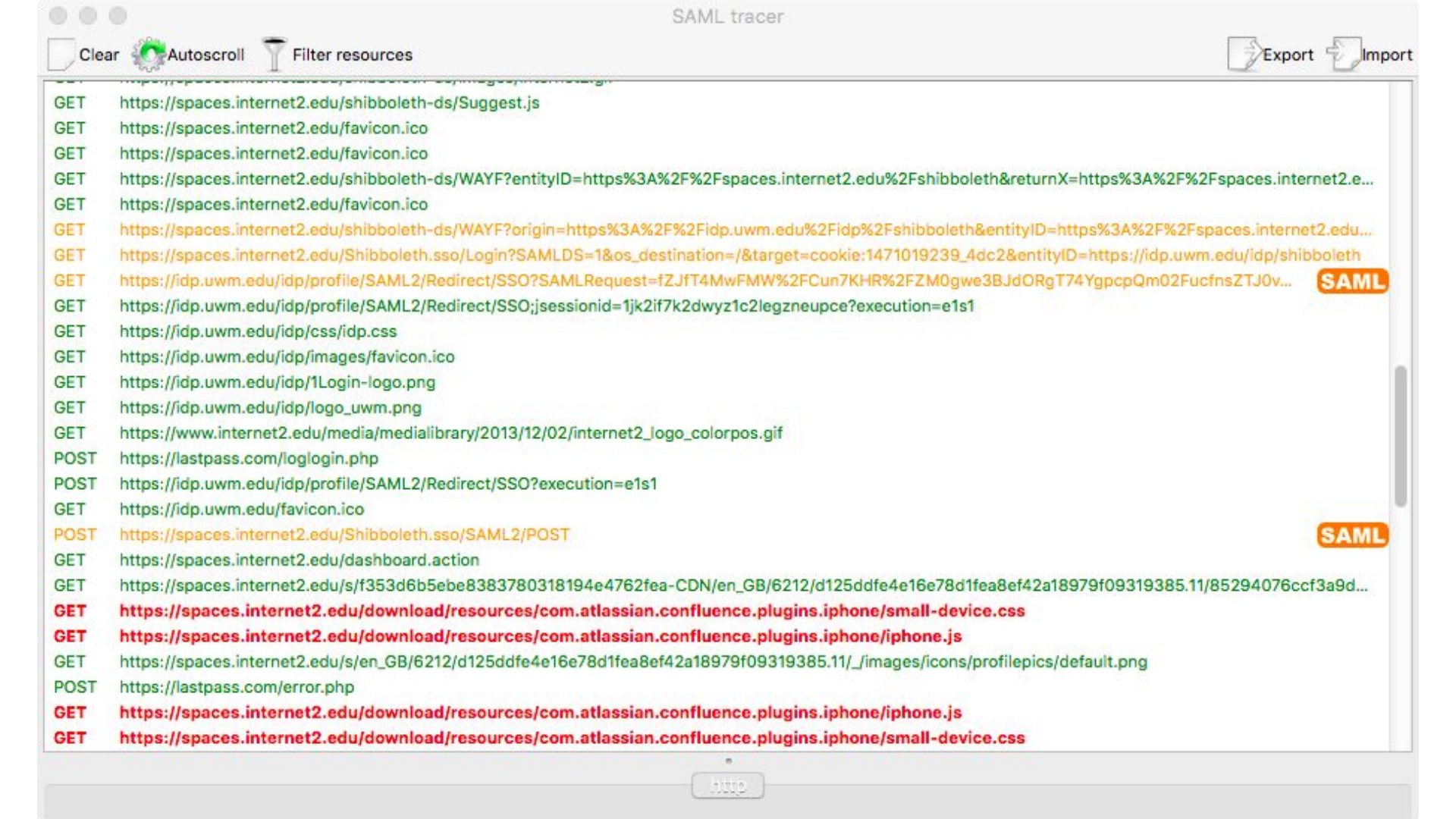
7 user reviews

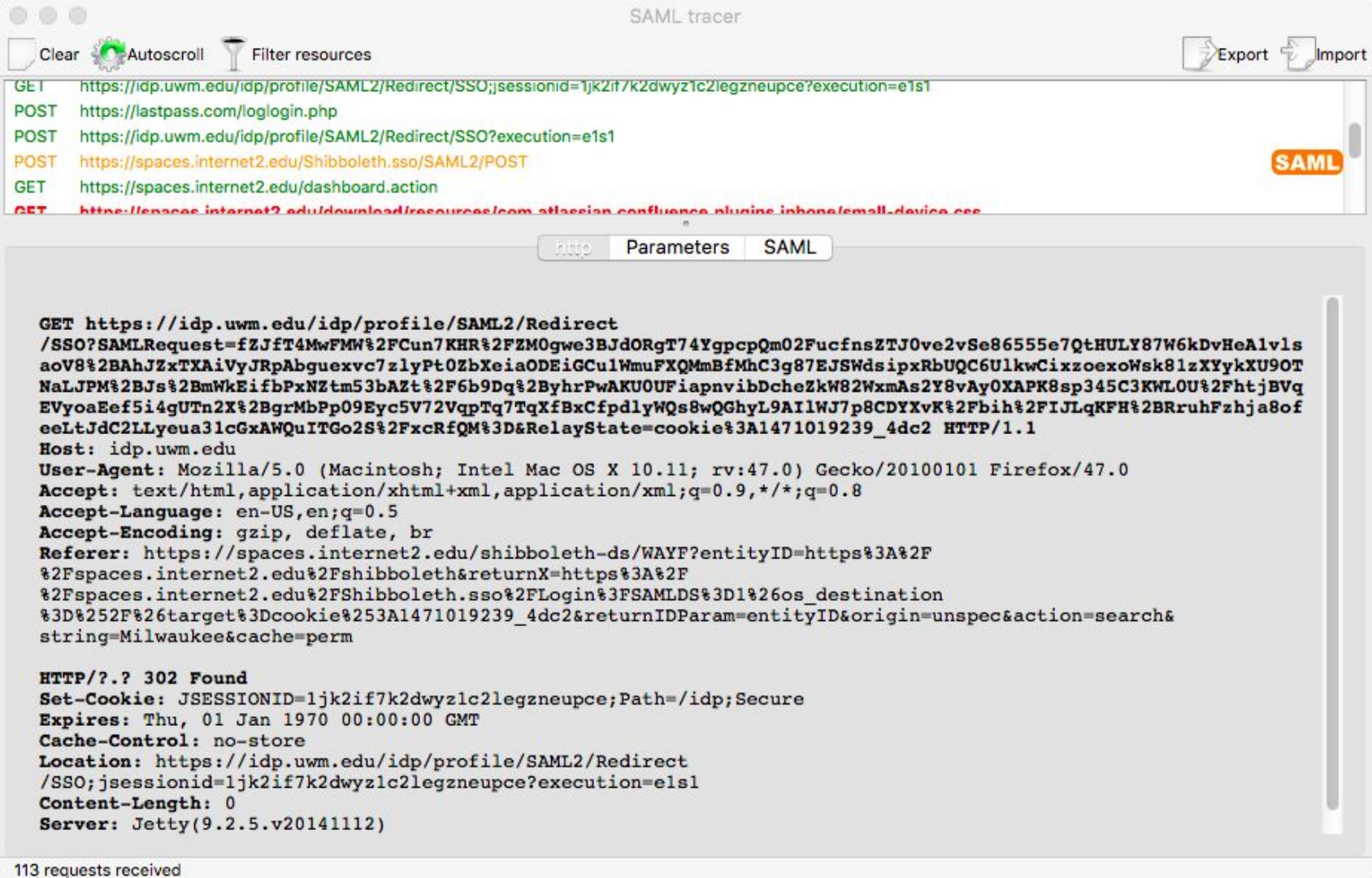
14,221 users

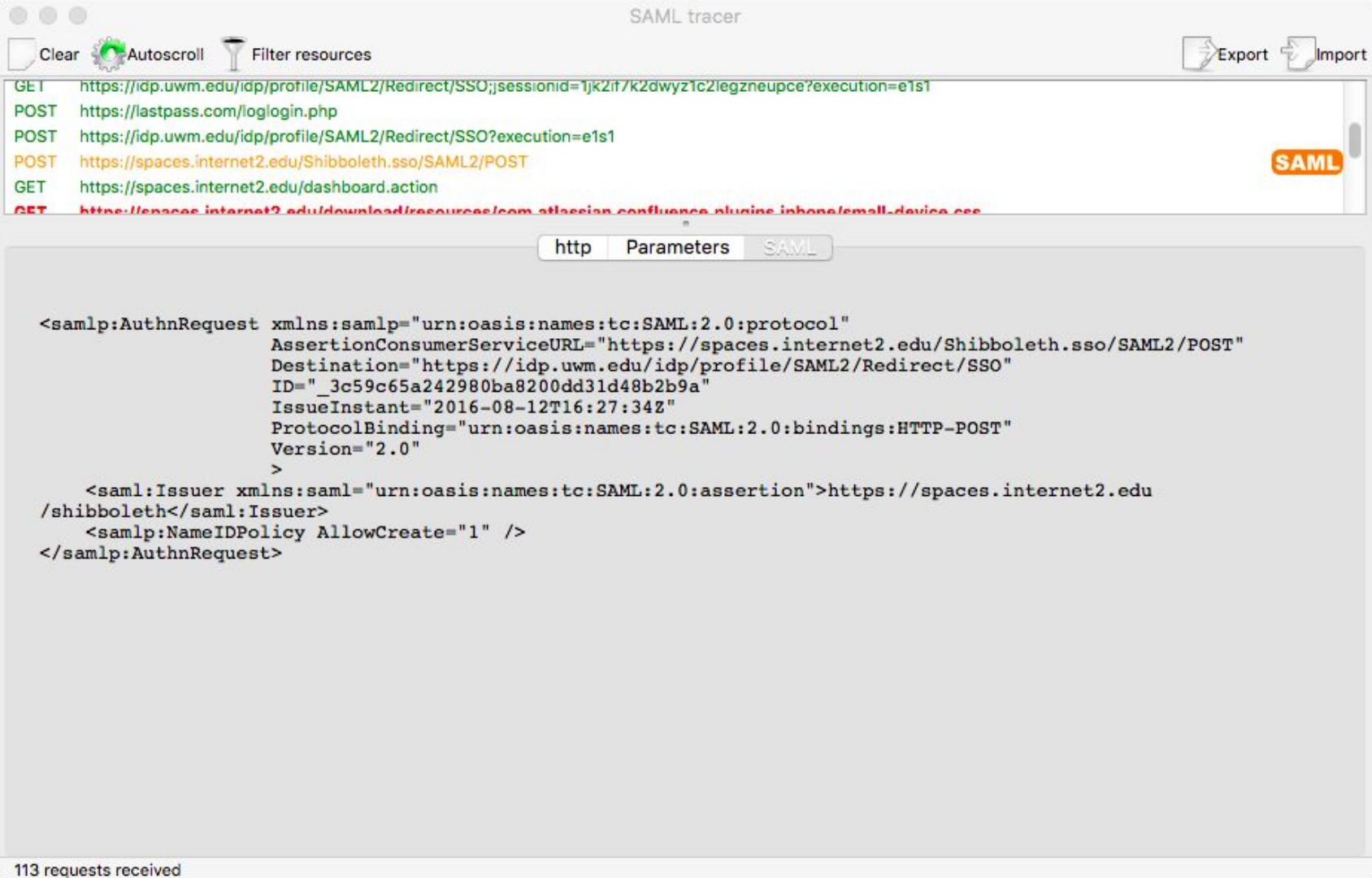
SAML: Hands-On Exercise

Task:

- Install SAML tracer Add-on for FireFox into your FireFox web browser
- SAML DevTools extension for Chrome is also available
- Other tools useable but involve more work
  - LiveHTTPHeaders
  - Safari Web Inspector
  - Fiddler
  - Often combined with https://www.samltool.com/ (scroll down)


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
GET https://spaces.internet2.edu/shibboleth-ds/Suggest.js
GET https://spaces.internet2.edu/favicon.ico
GET https://spaces.internet2.edu/favicon.ico
GET https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F%2Fspaces.internet2.edu%2Fshibboleth&returnX=https%3A%2F%2Fspaces.internet2.e...
GET https://spaces.internet2.edu/favicon.ico
GET https://spaces.internet2.edu/shibboleth-ds/WAYF?origin=https%3A%2F%2Fidp.uwm.edu%2Fidp%2Fshibboleth&entityID=https%3A%2F%2Fspaces.internet2.edu...
GET https://spaces.internet2.edu/Shibboleth.sso/Login?SAMLDS=1&os_destination=/&target=cookie:1471019239_4dc2&entityID=https://idp.uwm.edu/idp/shibboleth
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZJfT4MwFMW%2FCun7KHR%2FZM0gwe3BJdORgT74YgpcpQm02FucfnsZTJ0v...
SAML
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
GET https://idp.uwm.edu/idp/css/idp.css
GET https://idp.uwm.edu/idp/images/favicon.ico
GET https://idp.uwm.edu/idp/1Login-logo.png
GET https://idp.uwm.edu/idp/logo_uwm.png
GET https://www.internet2.edu/media/medialibrary/2013/12/02/internet2_logo_colorpos.gif
POST https://lastpass.com/loglogin.php
POST https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
GET https://idp.uwm.edu/favicon.ico
POST https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST
SAML
GET https://spaces.internet2.edu/dashboard.action
GET https://spaces.internet2.edu/s/f353d6b5ebe8383780318194e4762fea-CDN/en_GB/6212/d125ddfe4e16e78d1fea8ef42a18979f09319385.11/85294076ccf3a9d...
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/small-device.css
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/iphone.js
GET https://spaces.internet2.edu/s/en_GB/6212/d125ddfe4e16e78d1fea8ef42a18979f09319385.11/_/images/icons/profilepics/default.png
POST https://lastpass.com/error.php
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/iphone.js
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/small-device.css
http


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
POST https://lastpass.com/loglogin.php
POST https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
POST https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST
SAML
GET https://spaces.internet2.edu/dashboard.action
http
Parameters
SAML
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect
/SSO?SAMLRequest=fZJfT4MwFMW%2FCun7KHR%2FZM0gwe3BJdORgT74YgpcpQm02FucfnsZTJ0ve2vSe86555e7QtHULY87W6kDvHeA1vls
aoV8%2BAhJZxTXAiVyJRpAbguexvc7zlyPt0ZbXeiaODEiGCu1WmuFXQMmBfMhC3g87EJSWdsipxRbUQC6U1kwCixzoexoWsk81zXYykXU9OT
NaLJPM%2BJs%2BmWkEifbPxNZtm53bAZt%2F6b9Dq%2ByhrPwAKU0UFiapnvibDcheZkW82WxmAs2Y8vAy0XAPK8sp345C3KWL0U%2FhtjBVq
EVyoaEef5i4gUTn2X%2BgrMbPp09Eyc5V72VqpTq7TqXfBxCfpdlyWQs8wQGhyL9AIlWJ7p8CDYXvK%2Fbih%2FIJLqKFH%2BRruhFzhja8of
eeLtJdC2LLyeua31cGxAWQuITGo2S%2FxcRfQM%3D&RelayState=cookie%3A1471019239_4dc2 HTTP/1.1
Host: idp.uwm.edu
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F
%2Fspaces.internet2.edu%2Fshibboleth&returnX=https%3A%2F
%2Fspaces.internet2.edu%2FShibboleth.sso%2FLogin%3FSAMLDS%3D1%26os_destination
%3D%252F%26target%3Dcookie%253A1471019239_4dc2&returnIDParam=entityID&origin=unspec&action=search&
string=Milwaukee&cache=perm
HTTP/?.? 302 Found
Set-Cookie: JSESSIONID=1jk2if7k2dwyz1c2legzneupce;Path=/idp;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-store
Location: https://idp.uwm.edu/idp/profile/SAML2/Redirect
/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
Content-Length: 0
Server: Jetty(9.2.5.v20141112)
113 requests received


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
POST https://lastpass.com/loglogin.php
POST https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
POST https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST
SAML
GET https://spaces.internet2.edu/dashboard.action
http
Parameters
SAML
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
ID="_3c59c65a242980ba8200dd31d48b2b9a"
IssueInstant="2016-08-12T16:27:34Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Version="2.0"
>
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://spaces.internet2.edu
/shibboleth</saml:Issuer>
<samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
113 requests received

SAML tracer

Clear Autoscroll Filter resources Export Import

POST	https://lastpass.com/loglogin.php
POST	https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
POST	https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST SAML
GET	https://spaces.internet2.edu/dashboard.action
GET	https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/small-device.css

http Parameters SAML

```
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                 ID="_a7a2a544baf52cc9bf3e58e485249fde"
                 InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
                 IssueInstant="2016-08-12T16:27:36.448Z"
                 Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 >
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.uwm.edu
/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference URI="#_a7a2a544baf52cc9bf3e58e485249fde">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>rNZmtA7hjFiAyIROXhOTm3e7rN/Pz6Xe7kpQeuomYeE=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
gNxX+oP9qochqdNFsfhbtFlkXV8BMsvMtVbG5gFRLnLhdbayrTQ6WhQIaSAwk6RIIcnPfpYaF+jT
SPcVrvTO7F+gBPM0/9LvRJRGLaqDxJeLF49Fri9BG42I86LWJ7fLc5WKL4BUc+r3IiHk0GB5DgFy
```

210 requests received

SAML: Hands-on Exercise

Task:

- Open SAML tracer
- Browse to https://spaces.internet2.edu
- Click "Login" to kickoff SAML SSO flow
- Authenticate and complete SAML SSO flow
- Examine SAML exchanges using SAML tracer

SAML SP Initiated SSO Flow

- SP uses the Redirect Binding to redirect browser to the IdP
- Browser does a GET to the IdP Redirect URL endpoint
- Authentication request included as query string
    - Base64 and URL encoded

GET
https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZJfT4MwFMW%2FCun7KHR%2FZM0gwe3BJdORg
T74YgpcpQm02FucfnsZTJ0ve2vSe86555e7QtHULY87W6kDvHeA1vlsaoV8%2BAhJZxTXAiVyJRpAbguexvc7zlyPt0ZbXeiaODEi
GCu1WmuFXQMmBfMhC3g87EJSWdsipxRbUQC6UlkwCixzoexoWsk81zXYykXU9OTNaLJPM%2BJs%2BmWkEifbPxNZtm53b
AZt%2F6b9Dq%2ByhrPwAKU0UFiapnvibDcheZkW82WxmAs2Y8vAy0XAPK8sp345C3KWL0U%2FhtjBVqEVyoaEef5i4gUTn2X
%2BgrMbPp09Eyc5V72VqpTq7TqXfBxCfpdlyWQs8wQGhyL9AIlWJ7p8CDYXvK%2Fbih%2FIJLqKFH%2BRruhFzhja8ofeeLtJdC
2LLyeua31cGxAWQulTGo2S%2FxcRfQM%3D&RelayState=cookie%3A1471019239_4dc2

SAML SP Initiated SSO Flow

- SP may also include RelayState query parameter
  - Used by SP to "remember" initial resource or URL requested by browser
- IdP is obligated to return the RelayState untouched

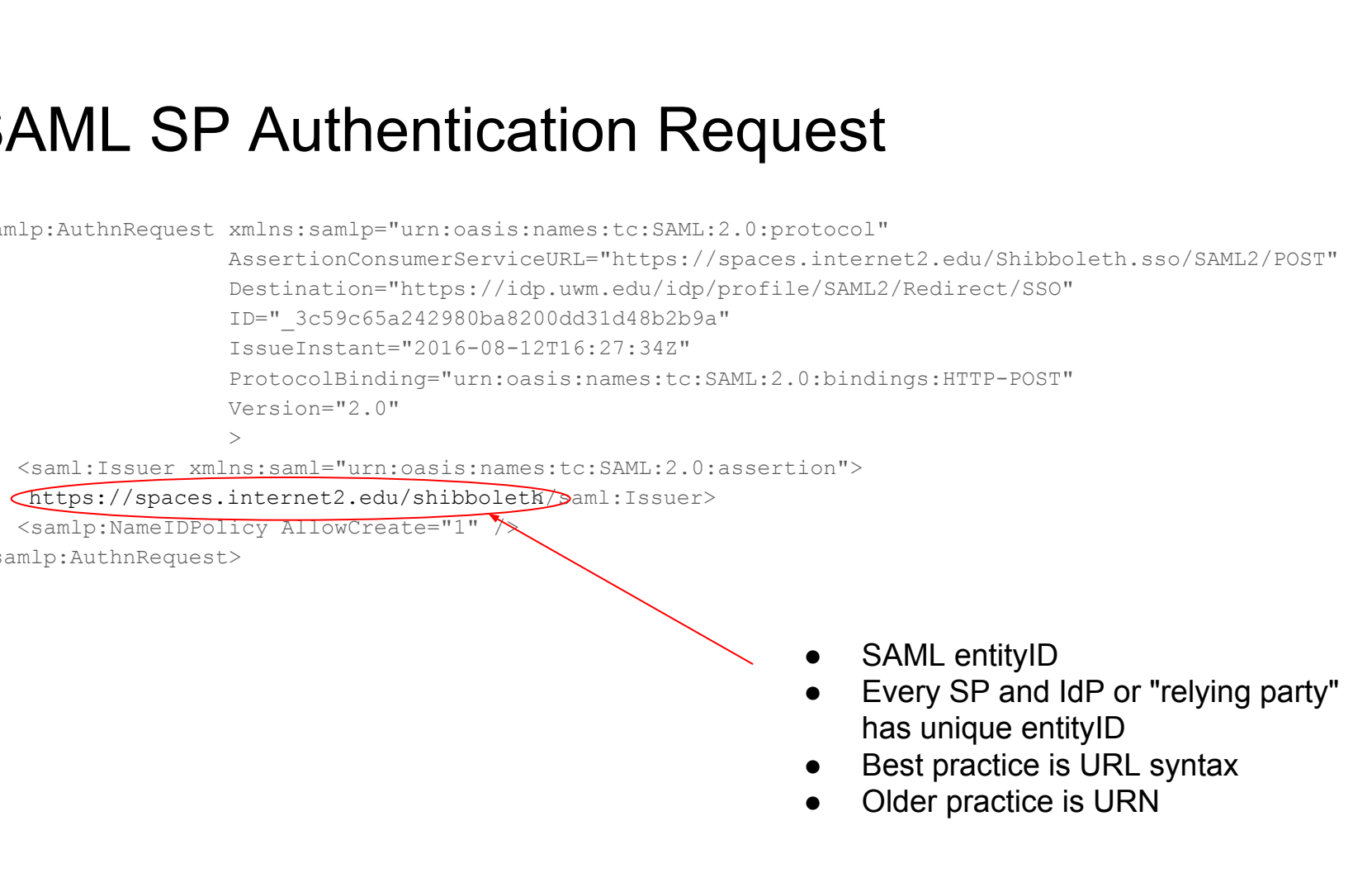
GET
https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZJfT4MwFMW%2FCun7KHR%2FZM0gwe3BJdORg
T74YgpcpQm02FucfnsZTJ0ve2vSe86555e7QtHULY87W6kDvHeA1vlsaoV8%2BAhJZxTXAiVyJRpAbguexvc7zlyPt0ZbXeiaODEi
GCu1WmuFXQMmBfMhC3g87EJSWdsipxRbUQC6UlkwCixzoexoWsk81zXYykXU9OTNaLJPM%2BJs%2BmWkEifbPxNZtm53b
AZt%2F6b9Dq%2ByhrPwAKU0UFiapnvibDcheZkW82WxmAs2Y8vAy0XAPK8sp345C3KWL0U%2FhtjBVqEVyoaEef5i4gUTn2X
%2BgrMbPp09Eyc5V72VqpTq7TqXfBxCfpdlyWQs8wQGhyL9AllWJ7p8CDYXvK%2Fbih%2FlJLqKFH%2BRruhFzhja8ofeeLtJdC
2LLyeua31cGxAWQulTGo2S%2FxcRfQM%3D&RelayState=cookie%3A1471019239_4dc2

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
                    ID="_3c59c65a242980ba8200dd31d48b2b9a"
                    IssueInstant="2016-08-12T16:27:34Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
                    ID="_3c59c65a242980ba8200dd31d48b2b9a"
                    IssueInstant="2016-08-12T16:27:34Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```



- SAML entityID
- Every SP and IdP or "relying party" has unique entityID
- Best practice is URL syntax
- Older practice is URN

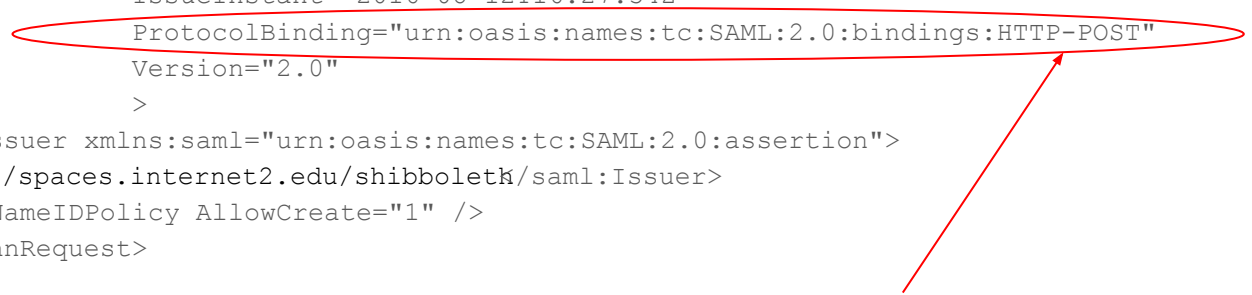
SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
                    ID="_3c59c65a242980ba8200dd31d48b2b9a"
                    IssueInstant="2016-08-12T16:27:34Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- AssertionConsumerServiceURL or "ACS"
- SP telling the IdP where it expects to receive response
- Most common is HTTP-POST binding
- Other bindings used rarely including artifact binding

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
                    ID="_3c59c65a242980ba8200dd31d48b2b9a"
                    IssueInstant="2016-08-12T16:27:34Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```



- There is the declaration of the HTTP-POST binding

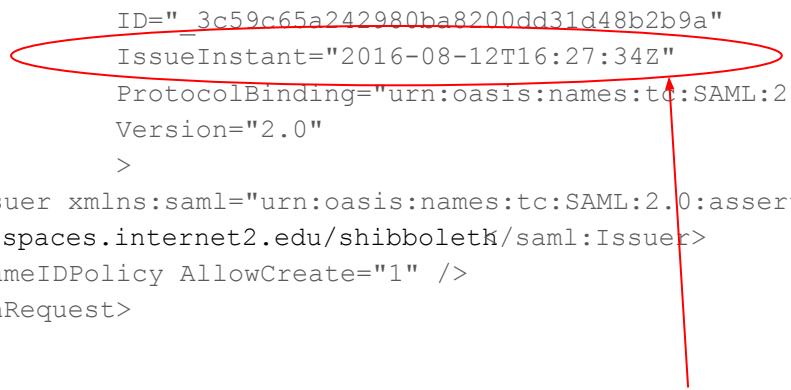
SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
                    ID="_3c59c65a242980ba8200dd31d48b2b9a"
                    IssueInstant="2016-08-12T16:27:34Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- SAML URL endpoint at the IdP the SP is targeting

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
                    ID="_3c59c65a242980ba8200dd31d48b2b9a"
                    IssueInstant="2016-08-12T16:27:34Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```



- Timestamp
- Prevent replay attacks
- Most systems tolerate some clock skew

SAML IdP Response

- IdP uses HTTP-POST binding to send response to SP
- Base64 encoded XML payload sent to browser and browser does POST
- Most IdPs include Javascript to automate the POST
  - Turn off Javascript and you will see a button to click to force the POST
- Response is usually digitally signed (XML digital signature)
  - SP can verify and trust the response
  - Prevent tampering
- Response includes an assertion about the authentication event
  - Assertion usually encrypted (XML encryption)
  - Encrypted using the SPs SAML key
  - Hides details about user from snooping browsers
  - TLS transport not usually required but usually used

SAML IdP Response

```
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
 ID="_a7a2a544baf52cc9bf3e58e485249fde"
 InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
 IssueInstant="2016-08-12T16:27:36.448Z"
 Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">

 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  https://idp.uwm.edu/idp/shibboleth
 </saml2:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  SNIP
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    SNIP
</saml2:EncryptedAssertion>
</saml2p:Response>
```

SAML IdP Response

```
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
 ID="_a7a2a544baf52cc9bf3e58e485249fde"
 InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
 IssueInstant="2016-08-12T16:27:36.448Z"
 Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">

 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  https://idp.uwm.edu/idp/shibboleth
 </saml2:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  SNIP
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    SNIP
</saml2:EncryptedAssertion>
</saml2p:Response>
```

- entityID of the IdP

SAML IdP Response

```
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
 ID="_a7a2a544baf52cc9bf3e58e485249fde"
 InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
 IssueInstant="2016-08-12T16:27:36.448Z"
 Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">

 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  https://idp.uwm.edu/idp/shibboleth
 </saml2:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  SNIP
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    SNIP
</saml2:EncryptedAssertion>
</saml2p:Response>
```

- Status is Success
- Could have been Failure

SAML IdP Response

```
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
 ID="_a7a2a544baf52cc9bf3e58e485249fde"
 InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
 IssueInstant="2016-08-12T16:27:36.448Z"
 Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">

 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  https://idp.uwm.edu/idp/shibboleth
 </saml2:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  SNIP
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    SNIP
</saml2:EncryptedAssertion>
</saml2p:Response>
```

- The SP's ACS endpoint to which the IdP is sending the response

SAML IdP Response

```
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
 ID="_a7a2a544baf52cc9bf3e58e485249fde"
 InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
 IssueInstant="2016-08-12T16:27:36.448Z"
 Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">

 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  https://idp.uwm.edu/idp/shibboleth
 </saml2:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  SNIP
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    SNIP
</saml2:EncryptedAssertion>
</saml2p:Response>
```

- Timestamp
- Prevent replay attacks
- Most systems tolerate some clock skew

SAML: Hands-on Exercise

- Use SAML tracer with SAML flow and IdP that does not encrypt
- Browse to https://registry.vo.idm.training/secure/
- Use the test user account provided to you for this training workshop
- Examine the unencrypted assertion in the IdP Response

SAML IdP Response

```
<saml2p:Response Destination="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"
                 ID="_801c5c74e66de16070b8694e897521d2"
                 InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 >
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
       https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      SNIP
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                     IssueInstant="2016-08-13T18:42:48.352Z"
                     Version="2.0"
                     xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   SEE NEXT SLIDE
    </saml2:Assertion>
</saml2p:Response>
```

SAML IdP Response

```
<saml2p:Response Destination="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"
                 ID="_801c5c74e66de16070b8694e897521d2"
                 InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 >
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
       https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      SNIP
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                     IssueInstant="2016-08-13T18:42:48.352Z"
                     Version="2.0"
                     xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   SEE NEXT SLIDE
    </saml2:Assertion>
</saml2p:Response>
```

SAML IdP Response

```
<saml2p:Response Destination="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"
                 ID="_801c5c74e66de16070b8694e897521d2"
                 InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 >
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
       https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      SNIP
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                     IssueInstant="2016-08-13T18:42:48.352Z"
                     Version="2.0"
                     xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   SEE NEXT SLIDE
    </saml2:Assertion>
</saml2p:Response>
```

SAML IdP Response

```
<saml2p:Response Destination="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"
                 ID="_801c5c74e66de16070b8694e897521d2"
                 InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 >
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
       https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      SNIP
    </ds:Signature>
    <saml2p:Status>
      <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                     IssueInstant="2016-08-13T18:42:48.352Z"
                     Version="2.0"
                     xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   SEE NEXT SLIDE
    </saml2:Assertion>
</saml2p:Response>
```

SAML IdP Response

```
<saml2p:Response Destination="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"
                 ID="_801c5c74e66de16070b8694e897521d2"
                 InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 >
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
       https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      SNIP
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                     IssueInstant="2016-08-13T18:42:48.352Z"
                     Version="2.0"
                     xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   SEE NEXT SLIDE
    </saml2:Assertion>
</saml2p:Response>
```

SAML IdP Assertion

```
<saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 >
    <saml2:Issuer>https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <saml2:Subject>
      SEE NEXT SLIDES
    </saml2:Subject>
    <saml2:Conditions NotBefore="2016-08-13T18:42:48.352Z" NotOnOrAfter="2016-08-13T18:47:48.352Z" >
      SNIP
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
                          SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9">
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
       SEE NEXT SLIDES
    </saml2:AttributeStatement>
</saml2:Assertion>
```

SAML IdP Assertion

```
<saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 >
    <saml2:Issuer>https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <saml2:Subject>
      SEE NEXT SLIDES
    </saml2:Subject>
    <saml2:Conditions NotBefore="2016-08-13T18:42:48.352Z" NotOnOrAfter="2016-08-13T18:47:48.352Z" >
      SNIP
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
                          SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9">
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
       SEE NEXT SLIDES
    </saml2:AttributeStatement>
</saml2:Assertion>
```

SAML IdP Assertion

```
<saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 >
    <saml2:Issuer>https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <saml2:Subject>
      SEE NEXT SLIDES
    </saml2:Subject>
    <saml2:Conditions NotBefore="2016-08-13T18:42:48.352Z" NotOnOrAfter="2016-08-13T18:47:48.352Z" >
      SNIP
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
                          SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9">
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
       SEE NEXT SLIDES
    </saml2:AttributeStatement>
</saml2:Assertion>
```

SAML IdP Assertion

```
<saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 >
    <saml2:Issuer>https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <saml2:Subject>
      SEE NEXT SLIDES
    </saml2:Subject>
    <saml2:Conditions NotBefore="2016-08-13T18:42:48.352Z" NotOnOrAfter="2016-08-13T18:47:48.352Z" >
      SNIP
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
                          SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9">
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
       SEE NEXT SLIDES
    </saml2:AttributeStatement>
</saml2:Assertion>
```

SAML IdP Assertion

```
<saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 >
    <saml2:Issuer>https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <saml2:Subject>
      SEE NEXT SLIDES
    </saml2:Subject>
    <saml2:Conditions NotBefore="2016-08-13T18:42:48.352Z" NotOnOrAfter="2016-08-13T18:47:48.352Z" >
      SNIP
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
                          SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9">
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
       SEE NEXT SLIDES
    </saml2:AttributeStatement>
</saml2:Assertion>
```

SAML IdP Assertion

```
<saml2:Assertion ID="_b4375f9e559f2b84bf2f2bc157c09ade"
                 IssueInstant="2016-08-13T18:42:48.352Z"
                 Version="2.0"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 >
    <saml2:Issuer>https://registry.vo.idm.training/idp/shibboleth</saml2:Issuer>
    <saml2:Subject>
      SEE NEXT SLIDES
    </saml2:Subject>
    <saml2:Conditions NotBefore="2016-08-13T18:42:48.352Z" NotOnOrAfter="2016-08-13T18:47:48.352Z" >
      SNIP
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
                          SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9">
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
       SEE NEXT SLIDES
    </saml2:AttributeStatement>
</saml2:Assertion>
```

SAML Subject

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                NameQualifier="https://registry.vo.idm.training/idp/shibboleth"

SPNameQualifier="https://registry.vo.idm.training/shibboleth">
AAdzZWNyZXQxXaGECb4BuVYo5GAEL+Jaw4bprqeMjVqgXNet/fHxs/3KSZD5Wpfi1yVhJdXoGHldCaC
Hwavf44snJIwM9fJjLuHxbYCbl9z78Xv1lVBvSw+m4RR28Y0idbgkJKY47ZCbkfk1Zrz+QJQJG8CCDtn3Aa3iz+k=
  </saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="75.86.142.120"
                          InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                          NotOnOrAfter="2016-08-13T18:47:48.495Z"
                          Recipient="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"/>
    </saml2:SubjectConfirmation>
</saml2:Subject>
```

SAML Subject

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                NameQualifier="https://registry.vo.idm.training/idp/shibboleth"

SPNameQualifier="https://registry.vo.idm.training/shibboleth">
AAdzZWNyZXQxXaGECb4BuVYo5GAEL+Jaw4bprqeMjVqgXNet/fHxs/3KSZD5Wpfi1yVhJdXoGHldCaC
Hwavf44snJIwM9fJjLuHxbYCbl9z78Xv1lVBvSw+m4RR28Y0idbgkJKY47ZCbkfk1Zrz+QJQJG8CCDtn3Aa3iz+k=
  </saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="75.86.142.120"
                          InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                          NotOnOrAfter="2016-08-13T18:47:48.495Z"
                          Recipient="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"/>
    </saml2:SubjectConfirmation>
</saml2:Subject>
```

SAML Subject

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                NameQualifier="https://registry.vo.idm.training/idp/shibboleth"

SPNameQualifier="https://registry.vo.idm.training/shibboleth">
AAdzZWNyZXQxXaGECb4BuVYo5GAEL+Jaw4bprqeMjVqgXNet/fHxs/3KSZD5Wpfi1yVhJdXoGHldCaC
Hwavf44snJIwM9fJjLuHxbYCbl9z78Xv1lVBvSw+m4RR28Y0idbgkJKY47ZCbkfk1Zrz+QJQJG8CCDtn3Aa3iz+k=
  </saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="75.86.142.120"
                          InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                          NotOnOrAfter="2016-08-13T18:47:48.495Z"
                          Recipient="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"/>
    </saml2:SubjectConfirmation>
</saml2:Subject>
```

- This is the value that identifies the subject.
- Transient NameIDs are opaque, privacy preserving, and will change each time subject authenticates (transient).

SAML2 NameID

- SAML2 spec defines a limited set of NameID formats
  - Transient - opaque, targeted (per SP), and temporary
  - Persistent - opaque, targeted, but not temporary
  - Email - value is in the form of an email address
  - Unspecified - interpretation left to implementations
  - A few others
- Not as flexible as using attributes about an authenticated subject
  - More on attributes later
- SAML2 NameID much less used by research organizations
  - Most often seen with commercial vendor services or SPs
    - WebEx, Google Apps, electronic journals, ...
  - Due to limitations of their SAML implementations
  - Heavy use of unhelpful "unspecified" format

SAML Subject

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                NameQualifier="https://registry.vo.idm.training/idp/shibboleth"

SPNameQualifier="https://registry.vo.idm.training/shibboleth">
AAdzZWNyZXQxXaGECb4BuVYo5GAEL+Jaw4bprqeMjVqgXNet/fHxs/3KSZD5Wpfi1yVhJdXoGHldCaC
Hwavf44snJIwM9fJjLuHxbYCbl9z78Xv1lVBvSw+m4RR28Y0idbgkJKY47ZCbkfk1Zrz+QJQJG8CCDtn3Aa3iz+k=
  </saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="75.86.142.120"
                          InResponseTo="_25b1cd853c94b075dda07511bd4572c3"
                          NotOnOrAfter="2016-08-13T18:47:48.495Z"
                          Recipient="https://registry.vo.idm.training/Shibboleth.sso/SAML2/POST"/>
    </saml2:SubjectConfirmation>
</saml2:Subject>
```

SAML AuthnStatement

```
<saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
  SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9" >
  <saml2:SubjectLocality Address="75.86.142.120" />
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>
       urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```

SAML AuthnStatement

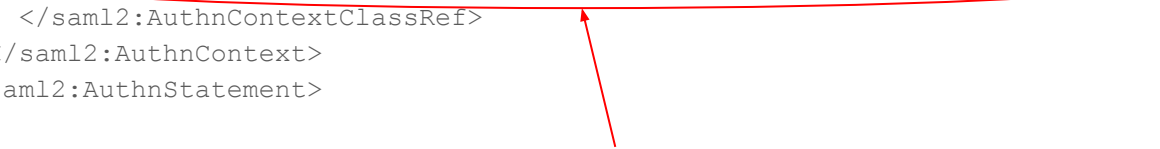
```
<saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
  SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9" >
  <saml2:SubjectLocality Address="75.86.142.120" />
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>
       urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```

SAML AuthnStatement

```
<saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
  SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9" >
  <saml2:SubjectLocality Address="75.86.142.120" />
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>
       urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```

SAML AuthnStatement

```
<saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
  SessionIndex="_6e20e8085b98cab86ef99afb6b9489b9" >
  <saml2:SubjectLocality Address="75.86.142.120" />
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```



- "How" the subject authenticated
- SAML2 defines a few standards
- Almost always see "PasswordProtectedTransport" in higher ed and research
  - Effectively "login and password over TLS"
- Higher ed and research community working on new international standards
  - Maybe see standards on MFA in the next year?

SAML AttributeStatement

```
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="sn" Name="urn:oid:2.5.4.4" NameFormat=SNIP>
    <saml2:AttributeValue>User01</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat=SNIP>
    <saml2:AttributeValue>Test User01</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="givenName" Name="urn:oid:2.5.4.42" NameFormat=SNIP>
    <saml2:AttributeValue>Test</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat=SNIP>
    <saml2:AttributeValue>testuser01@vo.idm.training</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat=SNIP>
    <saml2:AttributeValue>testuser01@vo.idm.training</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

SAML2 Attributes

- Higher ed and research leverage well defined standards
  - eduPerson schema managed by MACE-DIR
  - Standard LDAP schema like sn, givenName, mail
    - Borrow OIDs rather than reinvent new
- More later on attributes in higher ed and research federations like InCommon

Deploying a SAML Service Provider

SAML Capable Applications and Services

- Writing a SAML consumer is hard
  - Don't do it
  - Even the best SAML libraries have significant limitations
    - Large part of why commercial vendor implementations so limited
  - As a ***LAST RESORT***:
    - OpenSAML from Shibboleth team (used to build Shibboleth IdP implementation)
      - Java
      - Documentation, if it exists, aimed at internal use by Shibboleth team
    - Spring Security SAML Extension - Java
    - pySAML2 - Python
    - Python-SAML by OneLogin
    - .NET SAML by Microsoft

- Don't do it (really, please do not do it)

SAML Application Integration

Better approach is to integrate applications with existing SAML consumers

Web applications that consume SAML and provision details about subject and authentication to applications

Quite strong options from higher ed and research community:

- Shibboleth Native SP for Apache (Linux and Windows)
- Shibboleth Native SP for IIS (Windows)
- SimpleSAMLphp (any environment PHP can run in)

Today we will focus on Shibboleth Native SP for Apache on Linux

SAML Application Integration

Other options outside of higher education and research:

- Cloud services like Auth0, OneLogin
- Microsoft AD FS

The primary issue with these solutions is that they focus on bi-lateral federations (small "f") between a single IdP and perhaps a few SPs

Focused on more traditional enterprise use cases

You lose much of what you can gain from Federations (large "F") like InCommon

We do see organizations leverage AD FS but life is hard for them...

- Not the same as using Microsoft AD as person registry
- That is fairly common across higher education and research

SAML SP: Hands-On Exercise

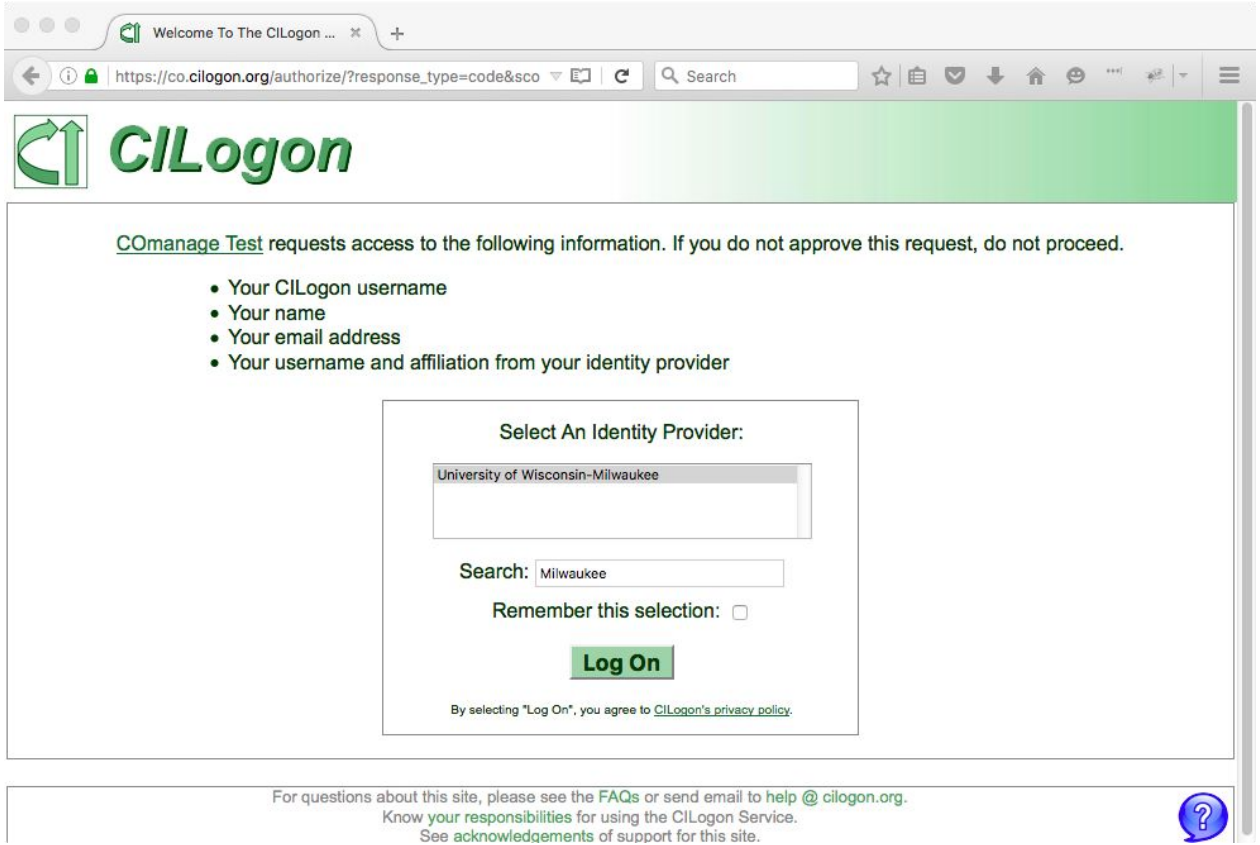
Task:

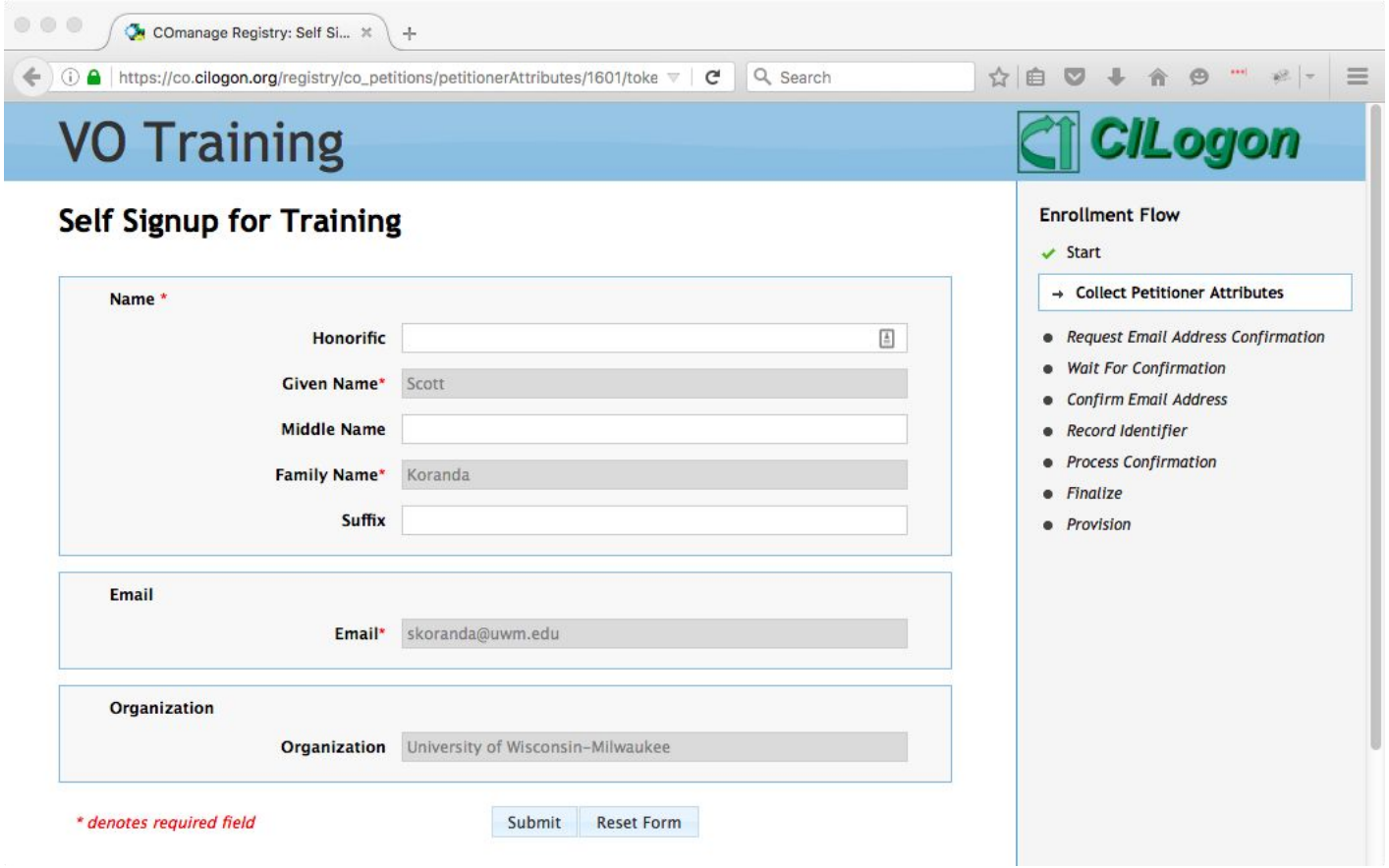
- Browse to https://registry.vo.idm.training/enroll
- When prompted choose your login provider
  - Google available as option
- Authenticate
- Edit form if some fields not supplied by your login provider
- Read email with subject "Please verify email for VO training session"
- Click link in email then "Accept"
- Click "Login" to login again to COmanage
- Click "VO Training"
- Click on your name/the gear icon choose "My VO Training Identity"

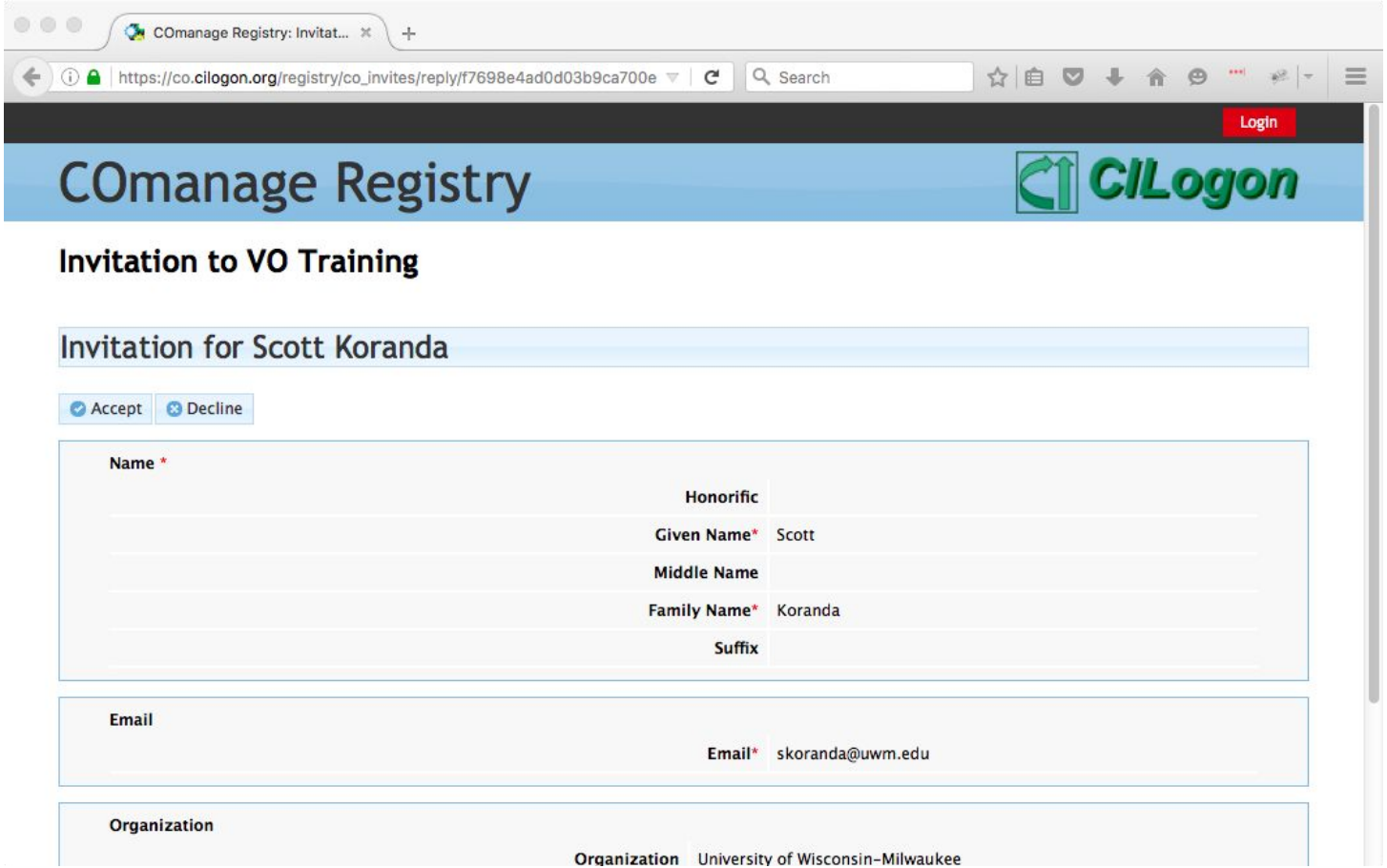
SAML SP: Hands-On Exercise

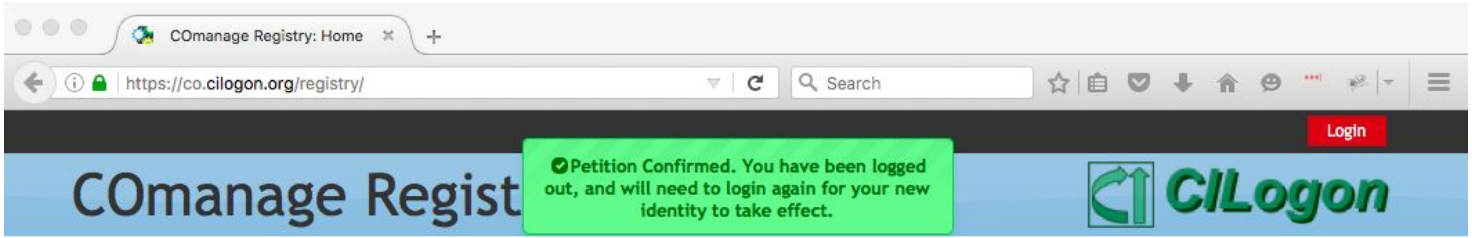
Task (continued):

- Note the UID COmanage provisioned for you
- Scroll down and click "Add" next to "SSH Keys"
- Click "Browse" to choose and upload an SSH key
  - Use an RSA or DSA key
- SSH using key and the provisioned UID into host assigned to you
  - For example: `ssh skoranda@sp01.vo.idm.training`
- Use sudo to gain root access
  - `sudo bash`


Welcome To The CILogon ...
https://co.cilogon.org/authorize/?response_type=code&sco
Search
CILogon
COmanage Test requests access to the following information. If you do not approve this request, do not proceed.
• Your CILogon username
• Your name
• Your email address
• Your username and affiliation from your identity provider
Select An Identity Provider:
University of Wisconsin-Milwaukee
Search: Milwaukee
Remember this selection:
Log On
By selecting "Log On", 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.
See acknowledgements of support for this site.

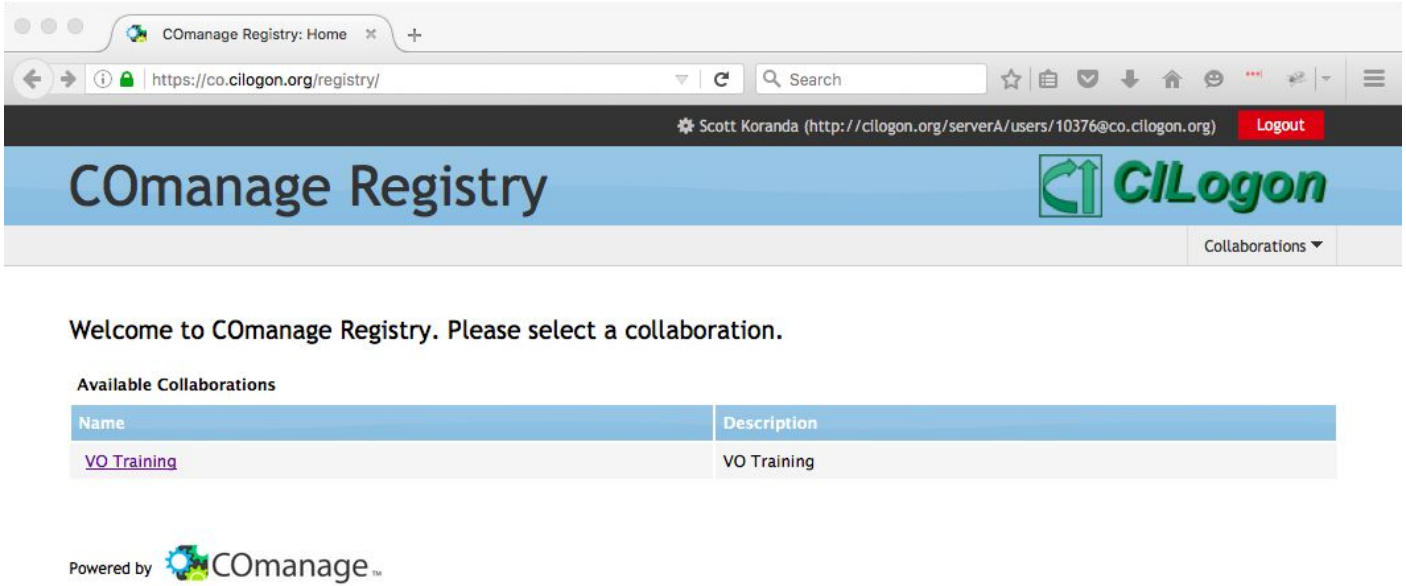

COmanage Registry: Self Si...
https://co.cilogon.org/registry/co_petitions/petitionerAttributes/1601/toke
Search
VO Training
CILogon
Self Signup for Training
Name *
Honorific
Given Name*
Scott
Middle Name
Family Name*
Koranda
Suffix
Email
Email*
skoranda@uwm.edu
Organization
Organization
University of Wisconsin-Milwaukee
* denotes required field
Submit
Reset Form
Enrollment Flow
Start
Collect Petitioner Attributes
Request Email Address Confirmation
Wait For Confirmation
Confirm Email Address
Record Identifier
Process Confirmation
Finalize
Provision

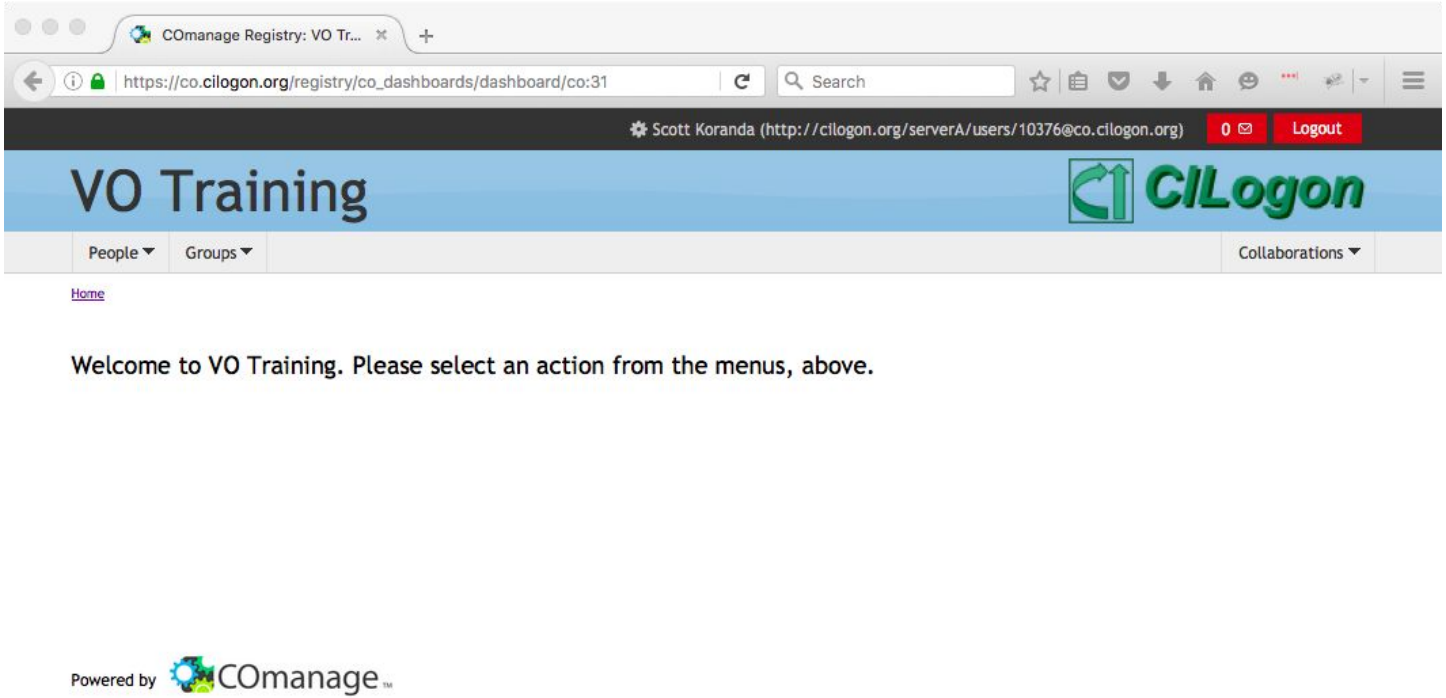

COmanage Registry: Invitat...
https://co.cilogon.org/registry/co_invites/reply/f7698e4ad0d03b9ca700e
Search
Login
COmanage Registry
CILogon
Invitation to VO Training
Invitation for Scott Koranda
Accept
Decline
Name *
Honorific
Given Name* Scott
Middle Name
Family Name* Koranda
Suffix
Email
Email* skoranda@uwm.edu
Organization
Organization University of Wisconsin-Milwaukee

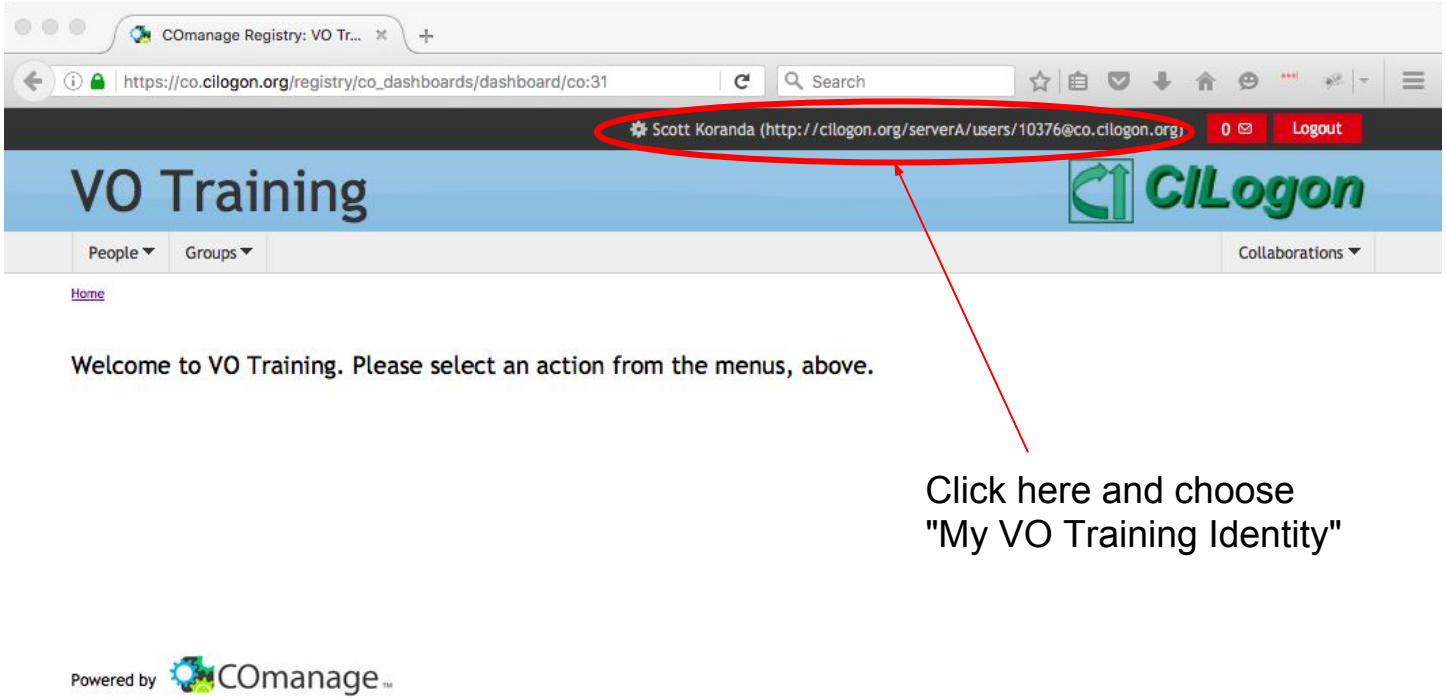


Welcome to COmanage Registry. Please login.

Powered by COmanage

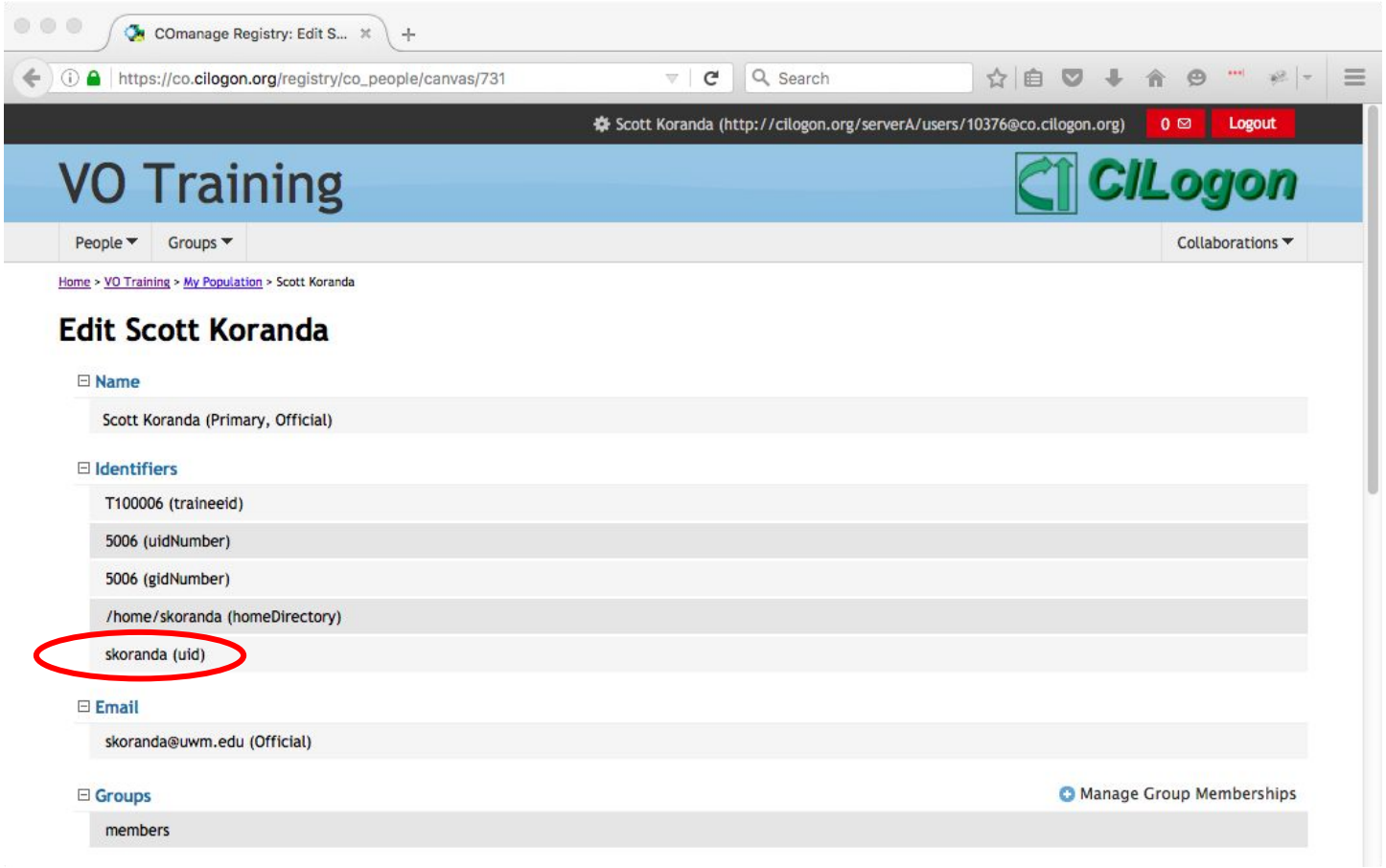

COmanage Registry: Home
https://co.cilogon.org/registry/
Search
Scott Koranda (http://cilogon.org/serverA/users/10376@co.cilogon.org)
Logout
COmanage Registry
CILogon
Collaborations
Welcome to COmanage Registry. Please select a collaboration.
Available Collaborations
Name
Description
VO Training
VO Training
Powered by
COmanage

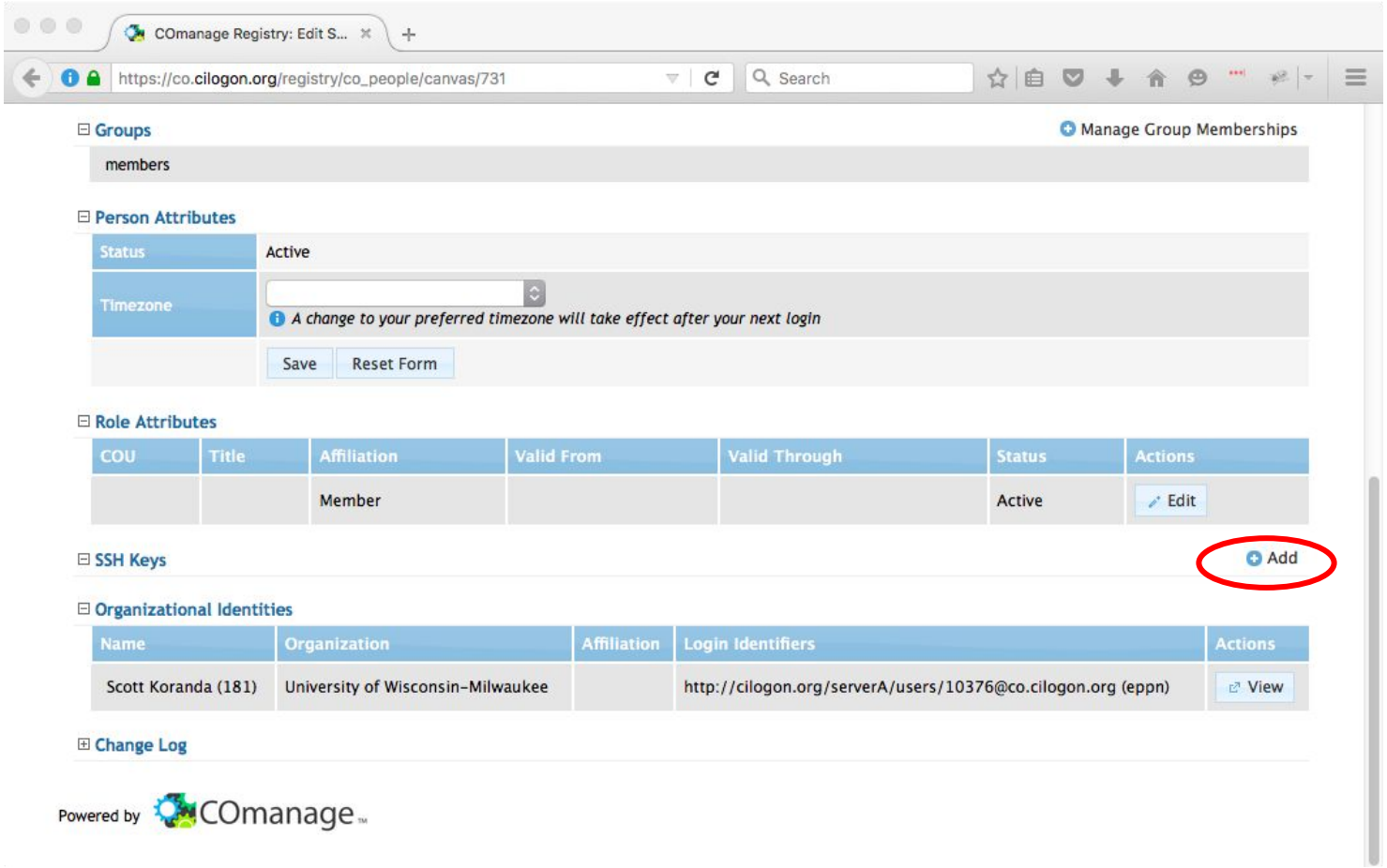

COmanage Registry: VO Tr...
https://co.cilogon.org/registry/co_dashboards/dashboard/co:31
Search
Scott Koranda (http://cilogon.org/serverA/users/10376@co.cilogon.org)
0
Logout
VO Training
CILogon
People
Groups
Collaborations
Home
Welcome to VO Training. Please select an action from the menus, above.
Powered by COmanage



Click here and choose
"My VO Training Identity"

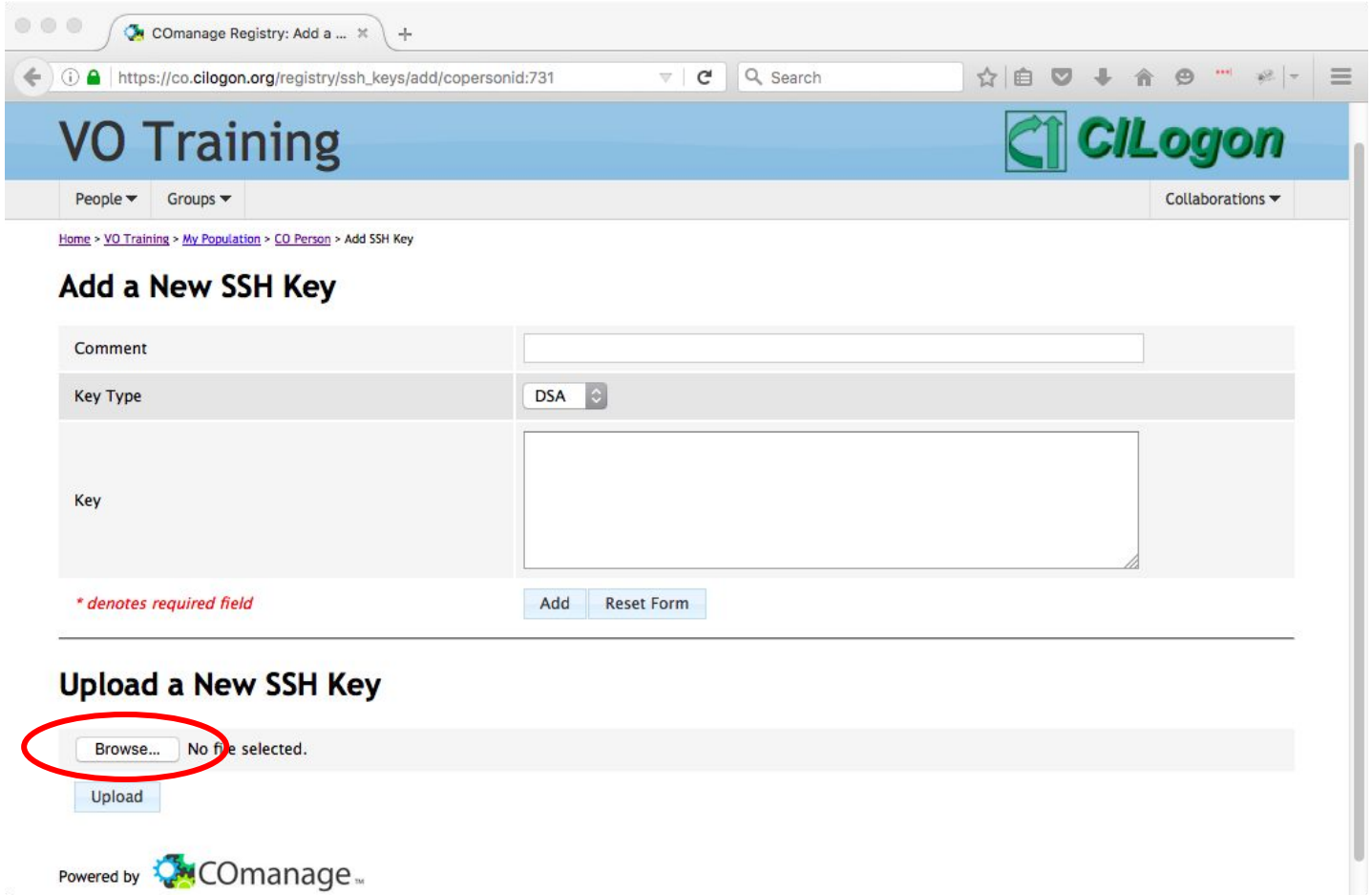
Note the UID automatically provisioned for you



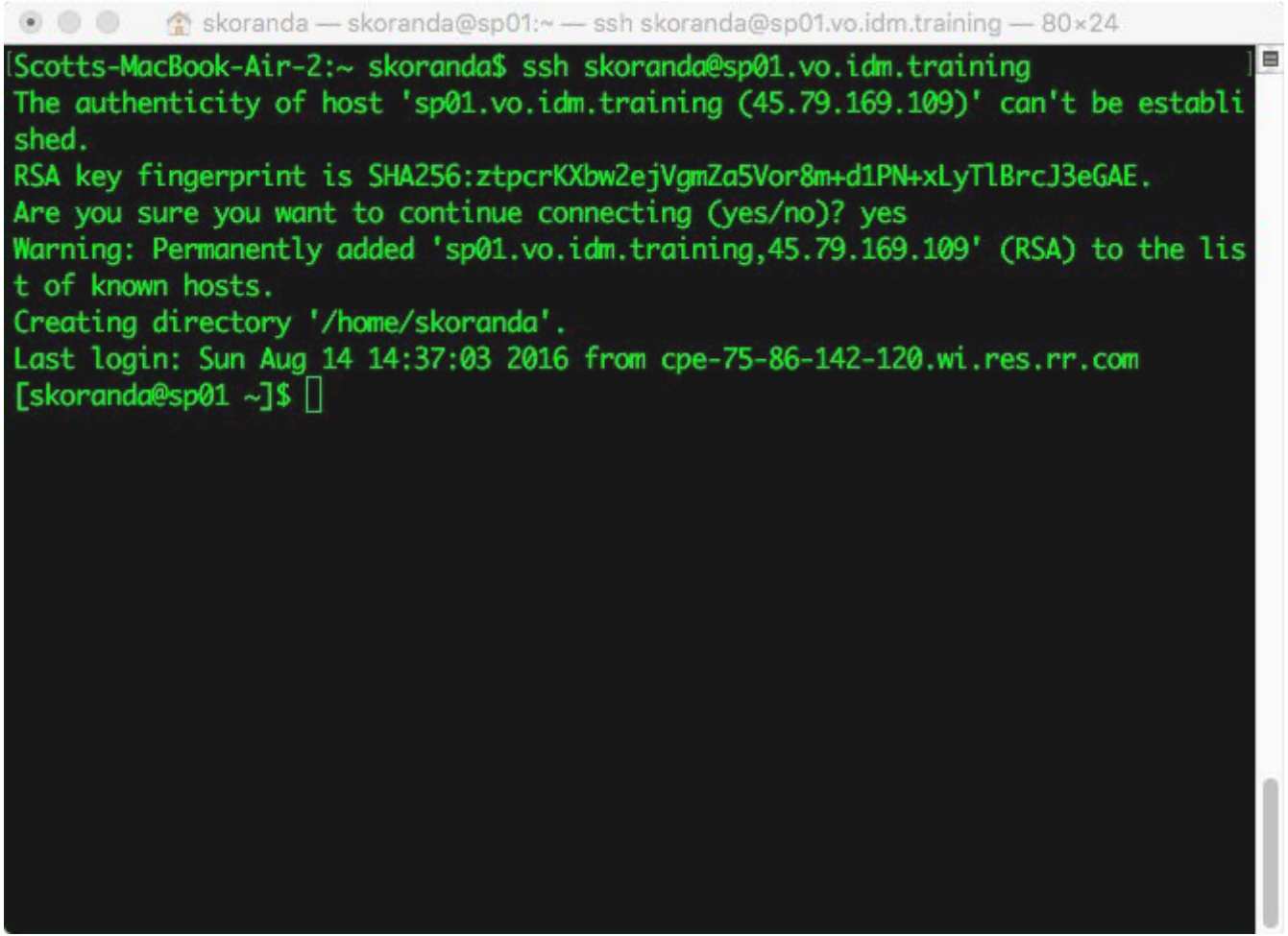


Scroll down and click "Add" next to "SSH Keys"

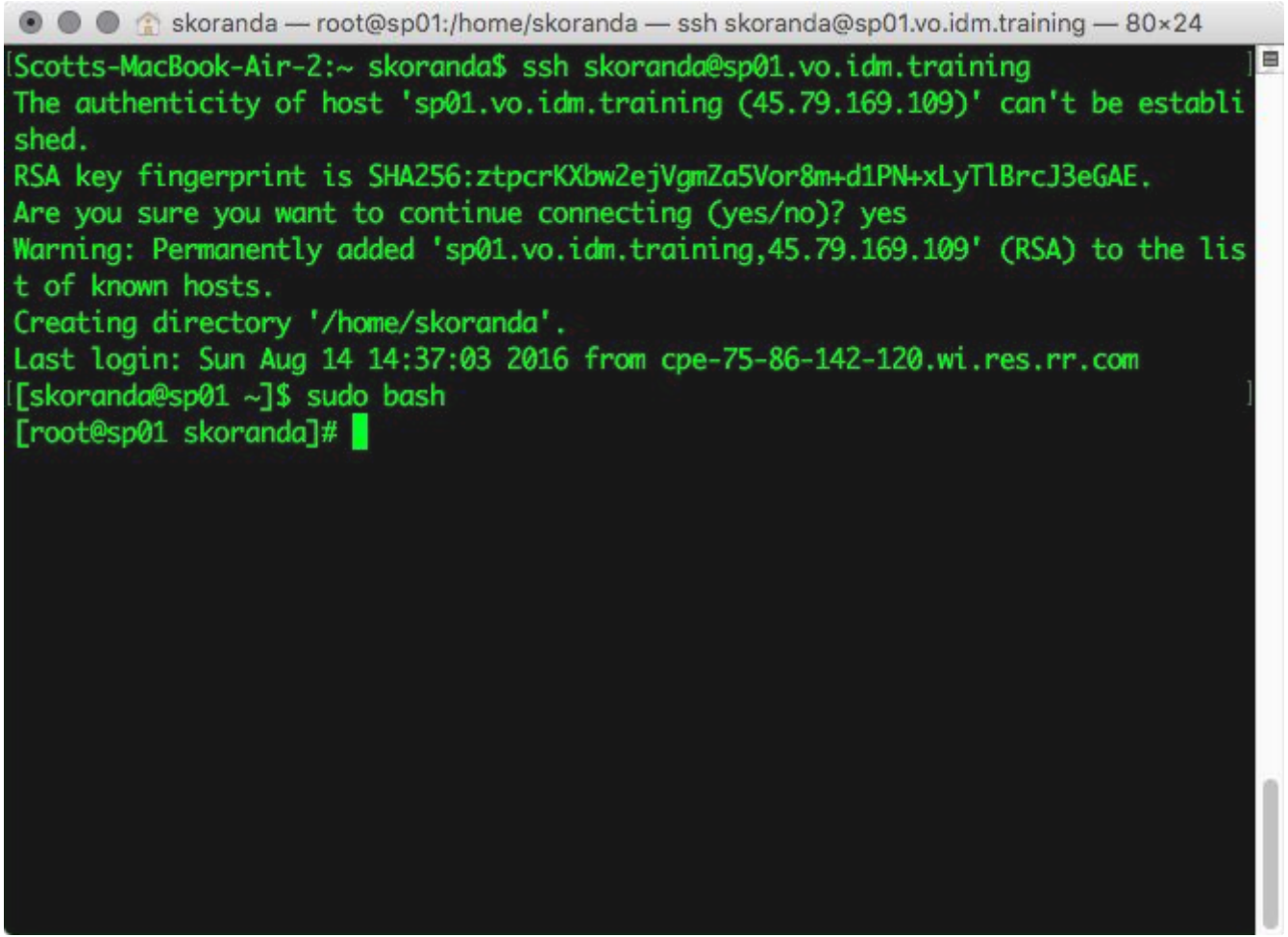
Click "Browse" to find and then upload your SSH key.



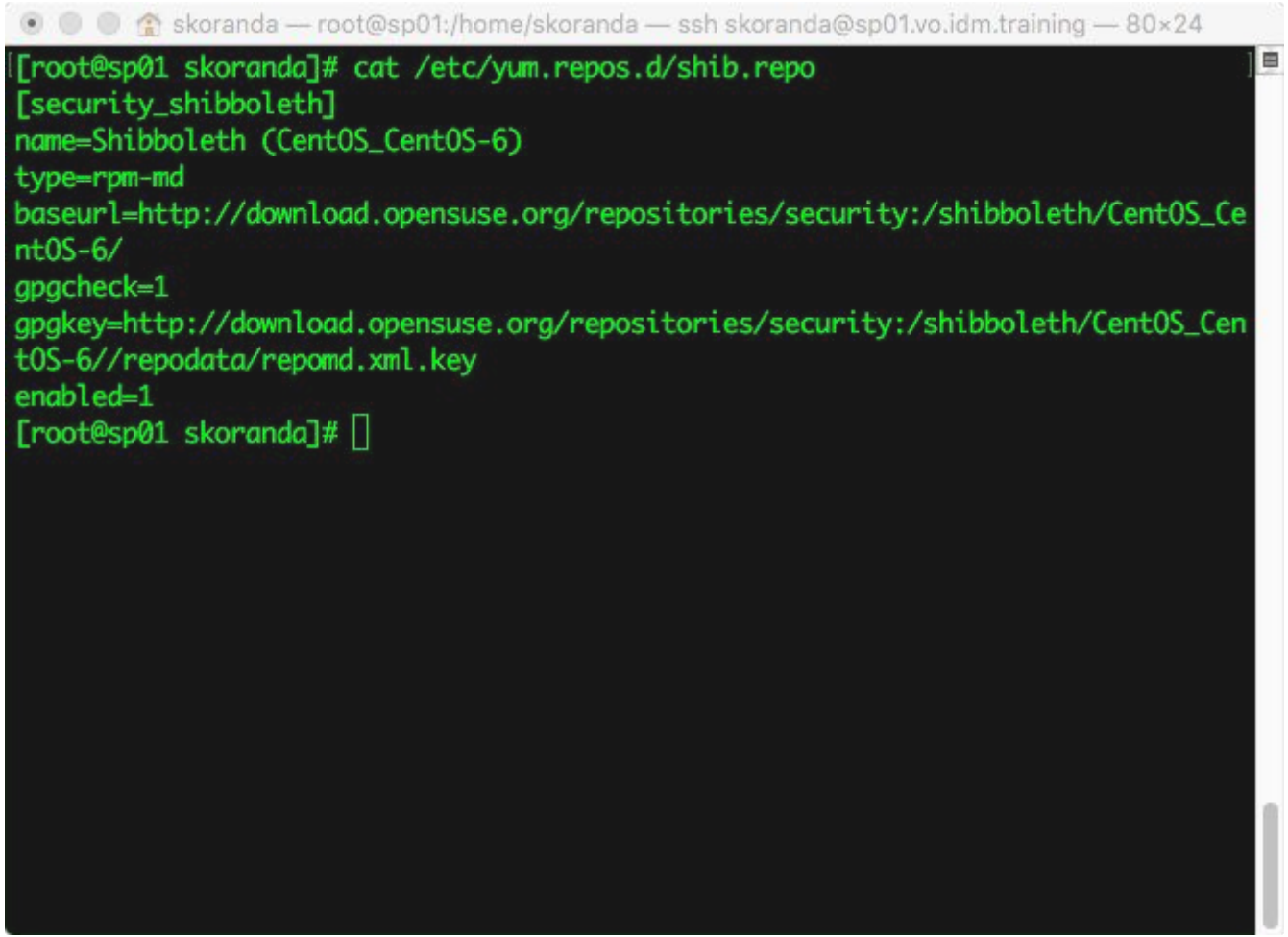
SSH to your assigned host using the UID COmanage provisioned for you



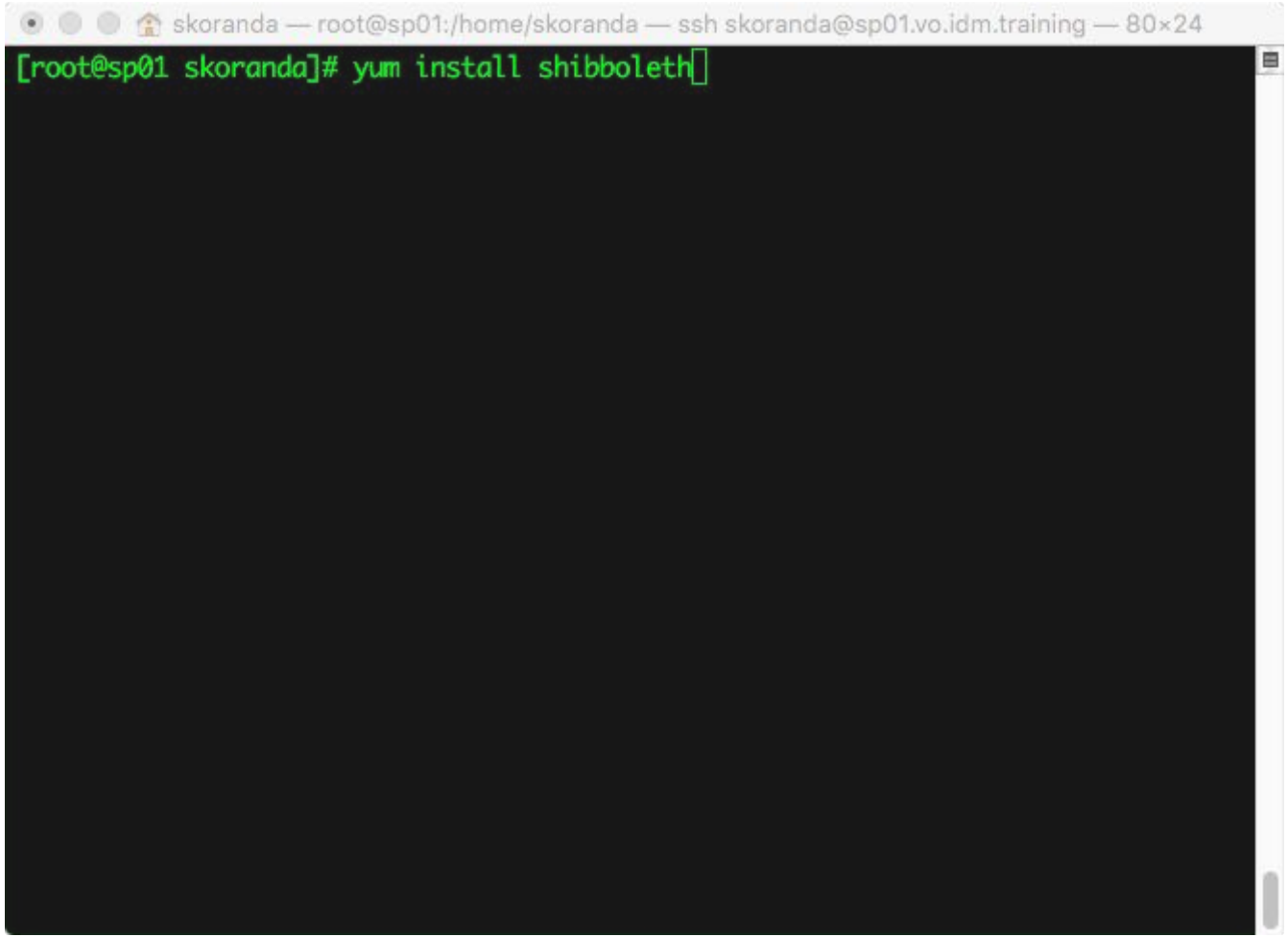
Execute "sudo bash" to obtain root access to the host



Shibboleth Yum repo has been pre-configured for you.



Use yum to install the shibboleth package and its dependencies



Shibboleth SP Deployment

- Shibboleth project officially supports RHEL and CentOS with yum repositories
- No official support for Debian and Ubuntu
  - Do not use the Debian/Ubuntu standard repository versions--too old
  - Recommend the SWITCH Federation Repositories
    - No official support outside of SWITCH but you are welcome to use repositories
    - https://www.switch.ch/aai/guides/sp/installation/

Break

Shibboleth SP Architecture

Shibboleth SP includes two primary components

1. Shibboleth daemon 'shibd'
    - Most of the SAML "heavy lifting"
    - Maintains session state
    - Listens on UNIX socket
    - Independent daemon process usually managed with init script
2. Shibboleth Apache module 'mod_shib'
    - Runs "inside" of Apache like any other Apache module
    - Exposes the SAML URL endpoints for consuming SAML
    - Includes semantics for authorization and access control
    - Communicates with shibd via the UNIX socket

Shibboleth SP Configuration

Two primary places to configure Shibboleth SP:

1. /etc/shibboleth/shibboleth2.xml
    - Configure SAML details including SP entityID
    - Configure session details
    - Configure application integration
    - Loads some other auxiliary files in /etc/shibboleth/
    - Platform-independent access control (usually not used with Linux)
2. Apache HTTP Server configuration files
    - Details of how SAML URL endpoints "mounted" into URL space
    - Access control for directories and locations

Shibboleth SP: Hands-On Exercise

Task:

- Configure the Shibboleth SP
  - Including federating with the training IdP
- Configure Apache to protect a simple static web page

Shibboleth SP: Hands-On Exercise

Edit /etc/shibboleth/shibboleth2.xml

Replace

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
     REMOTE_USER="eppn persistent-id targeted-id">
```

with

```
<ApplicationDefaults entityID="https://spN.vo.idm.training/shibboleth"
     REMOTE_USER="eppn persistent-id targeted-id">
```

where 'spN' is the hostname for your assigned host, eg. 'sp01'

Shibboleth SP: Hands-On Exercise

Edit /etc/shibboleth/shibboleth2.xml

Replace

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
    checkAddress="false" handlerSSL="false" cookieProps="http">
```

with

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
    checkAddress="false" handlerSSL="true" cookieProps="https">
```

Shibboleth SP: Hands-On Exercise

Edit /etc/shibboleth/shibboleth2.xml

Replace

```
<SSO entityID="https://idp.example.org/idp/shibboleth"
  discoveryProtocol="SAMLDS" discoveryURL="https://ds.example.org/DS/WAYF">
  SAML2 SAML1
</SSO>
```

with

```
<SSO entityID="https://registry.vo.idm.training/idp/shibboleth">
  SAML2
</SSO>
```

Shibboleth SP: Hands-On Exercise

Edit /etc/shibboleth/shibboleth2.xml

Below

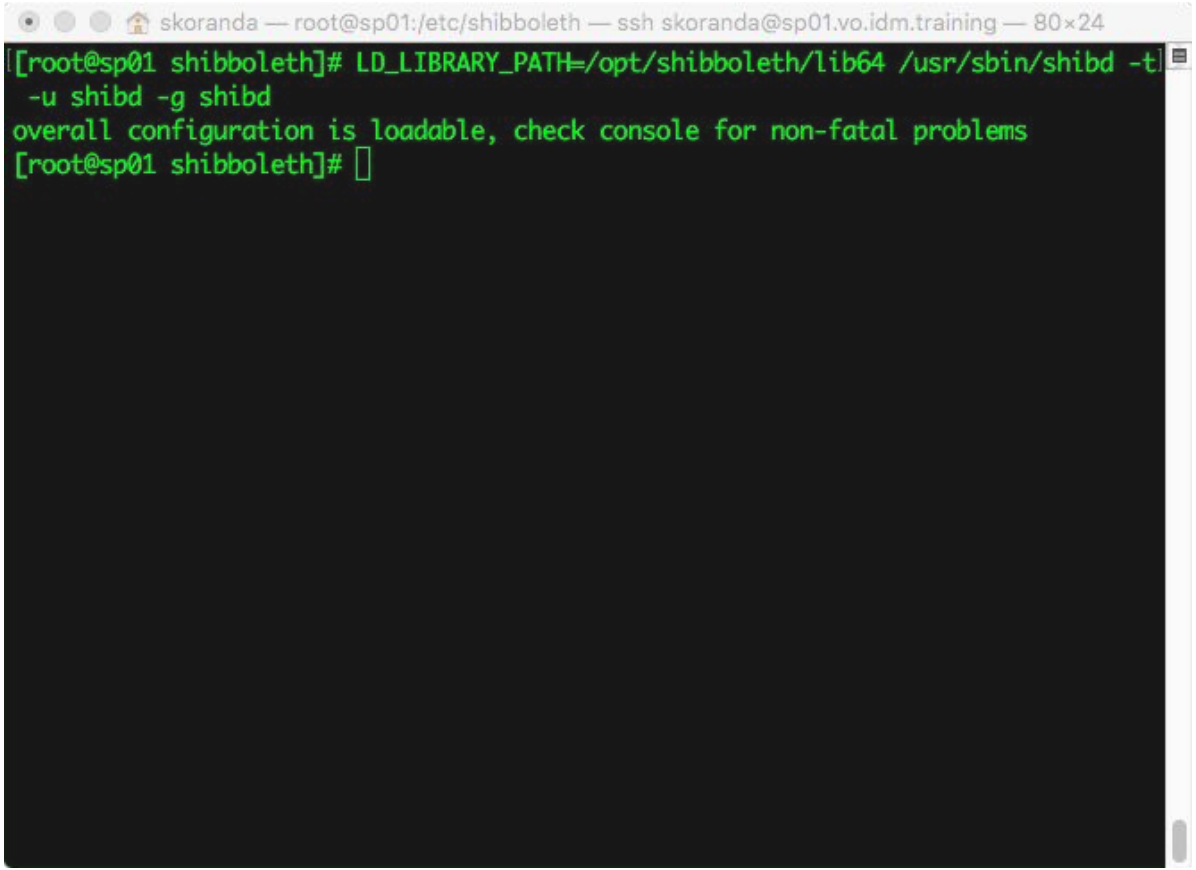
```
<!-- Example of locally maintained metadata. -->
```

insert

```
<MetadataProvider type="XML" validate="true" file="vo-idm-training-idp-metadata.xml"/>
```

Shibboleth SP: Hands-On Exercise

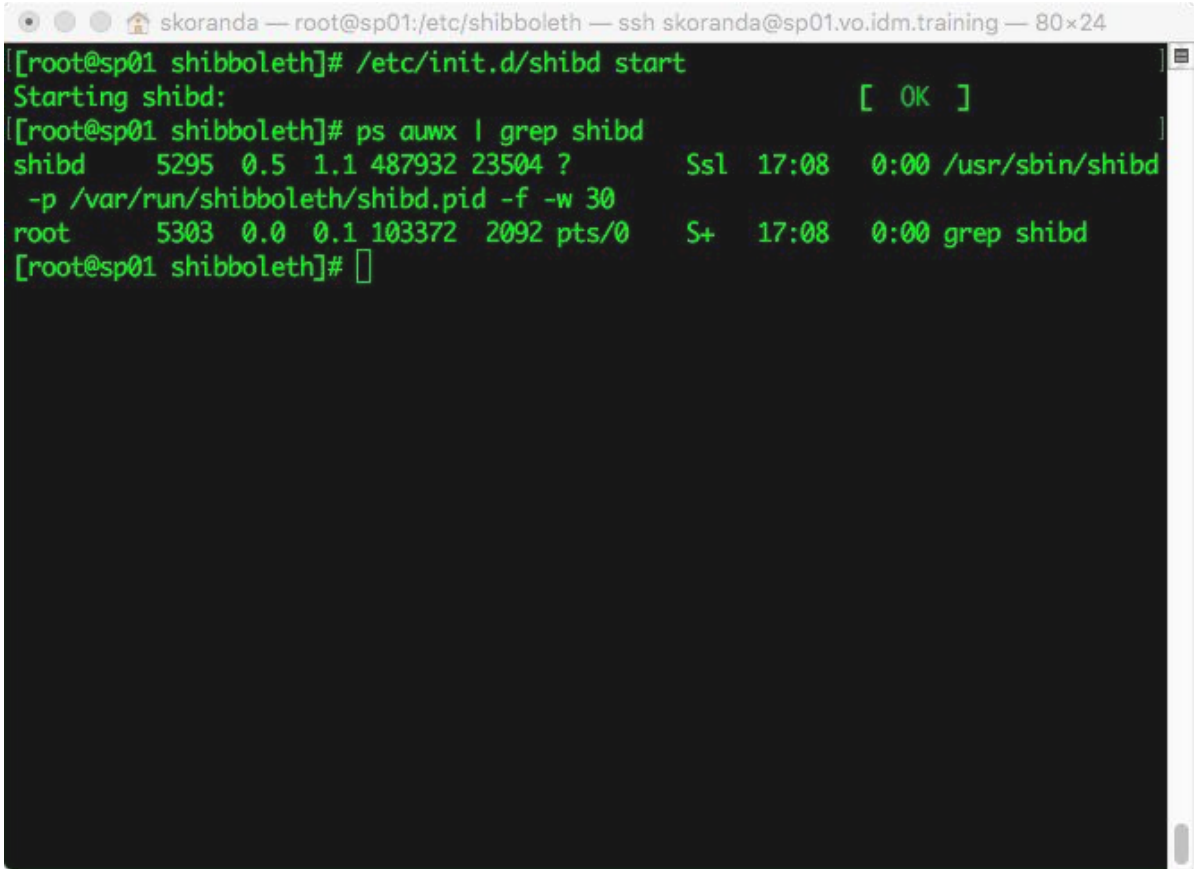
Check the syntax of the configuration file using shibd with the -t, -u, and -g options



Shibboleth SP: Hands-On Exercise

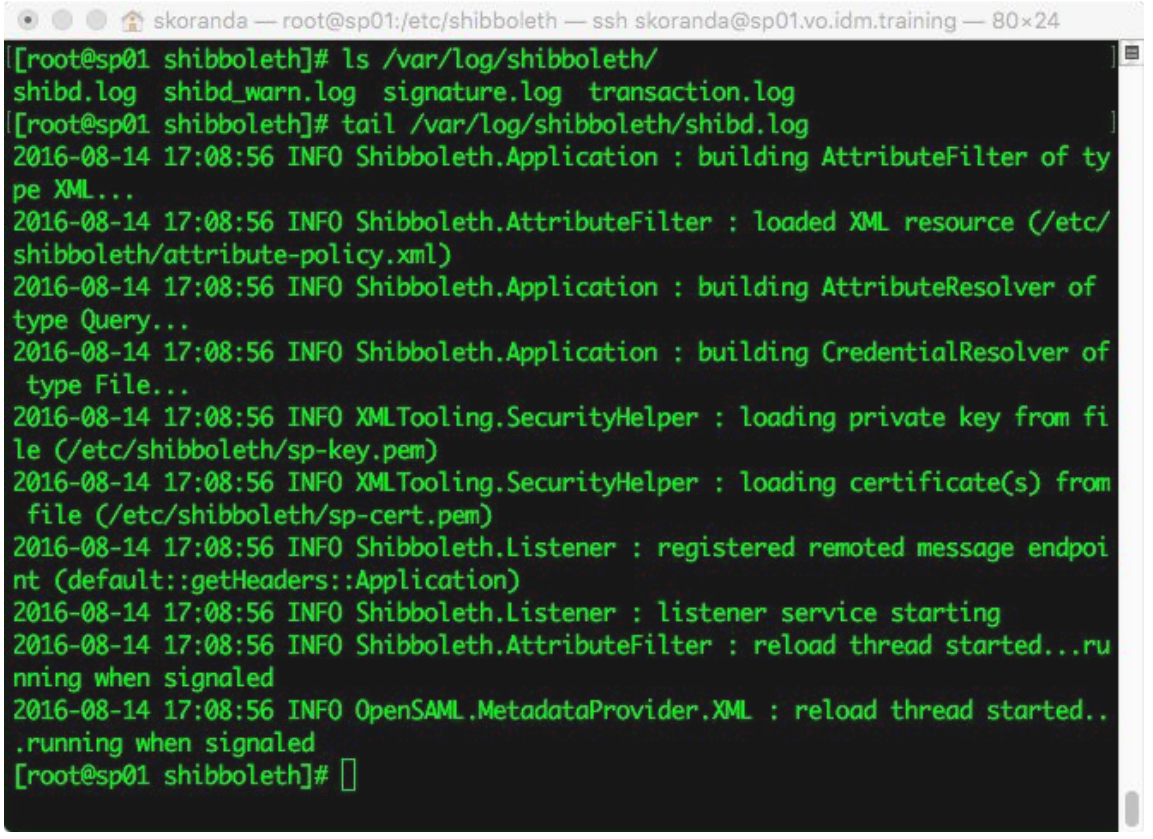
Start the shibd daemon using init script

On RHEL and CentOS shibd runs as user 'shibd'



Shibboleth SP: Hands-On Exercise

shibd logs to files in /var/log/shibboleth

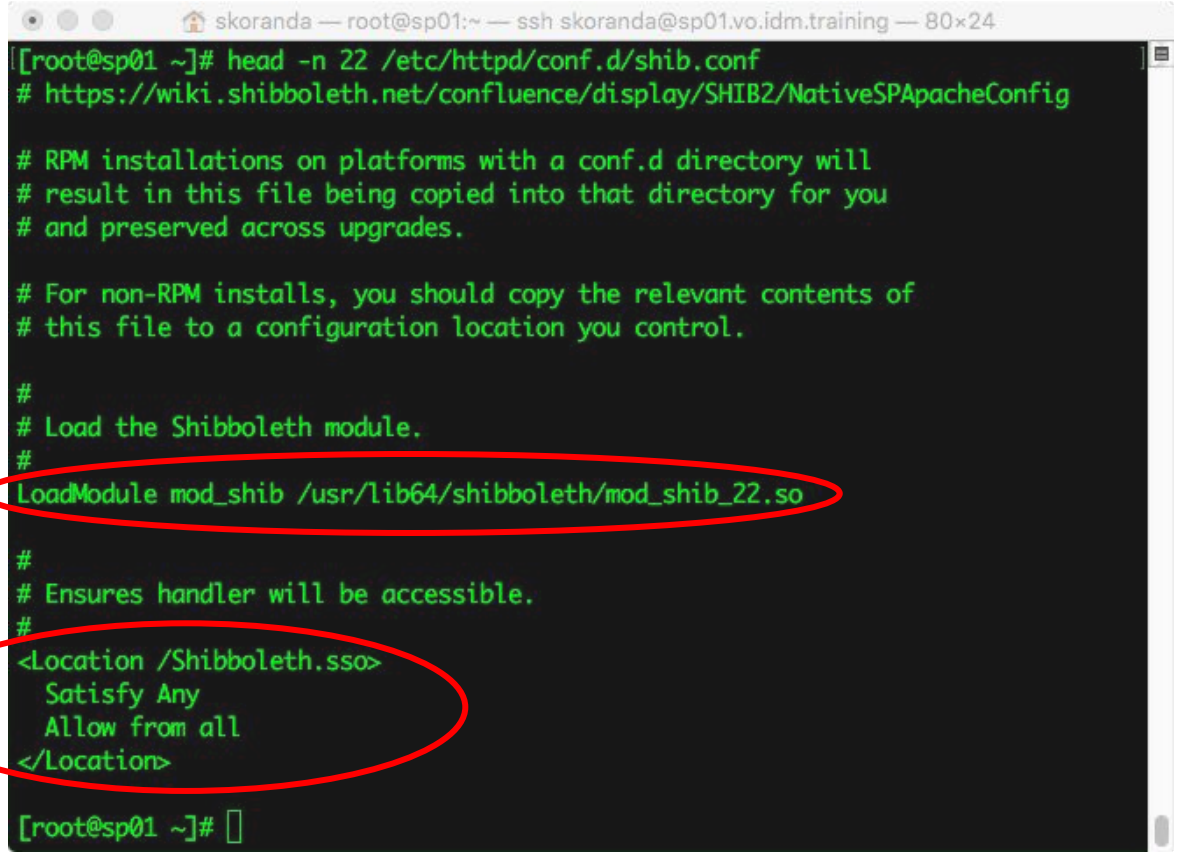


Shibboleth SP: Hands-On Exercise

The Shibboleth RPM puts a minimal Apache configuration into /etc/httpd/conf.d/shib.conf

Loads the mod_shib Apache module

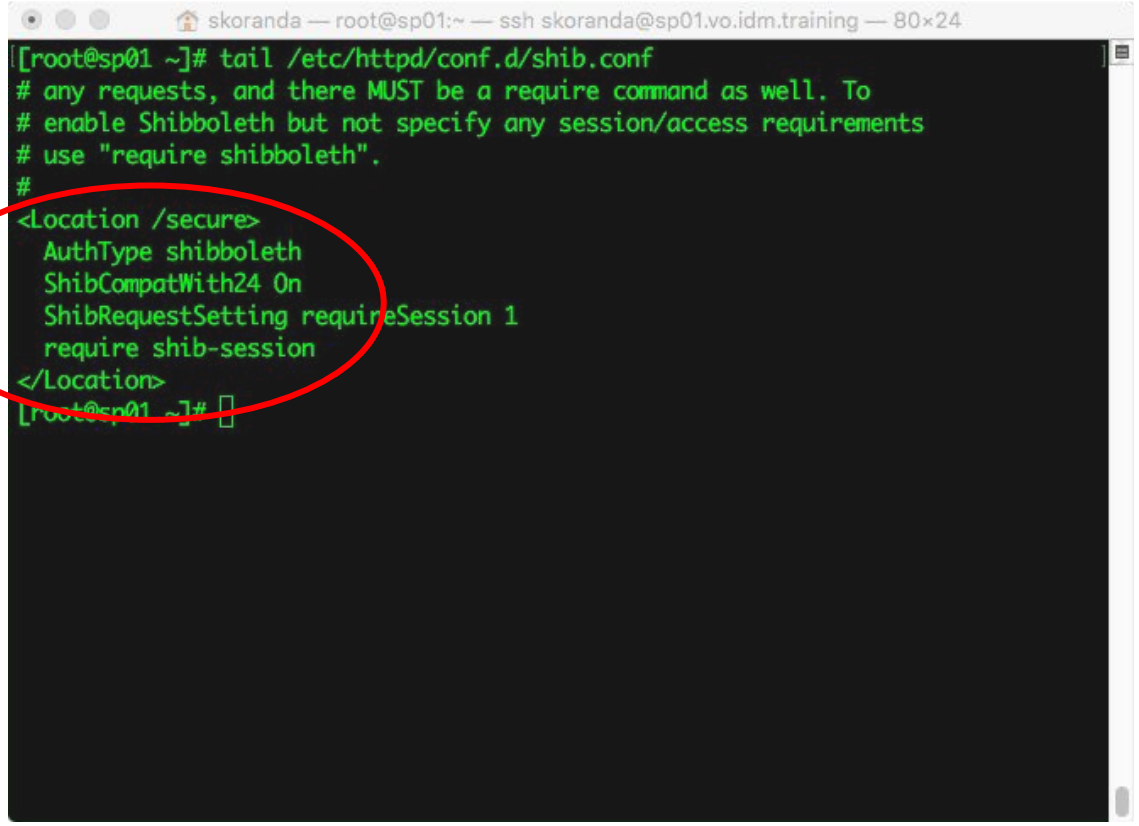
"Mounts" the SAML URL endpoint listener



Shibboleth SP: Hands-On Exercise

Simple access control example:

- AuthType shibboleth invokes the module
- ShibCompatWith24 helps prepare for syntax change with Apache 2.4
- ShibRequestSetting requireSession 1
  requires a valid Shibboleth "session" for access, meaning a SAML Web SSO flow has happened
- require shib-session necessary syntax for Apache module



Shibboleth SP: Hands-On Exercise

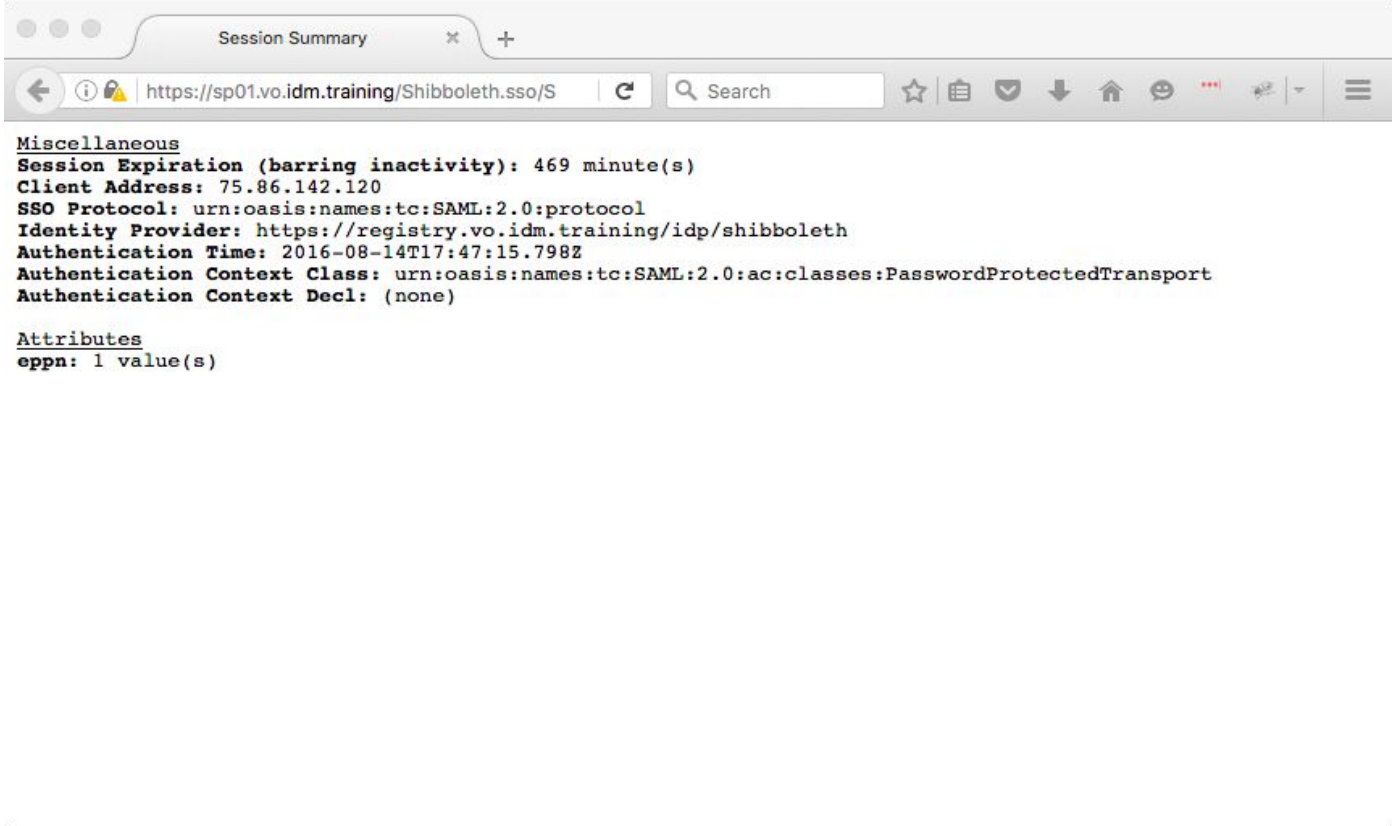
- Restart both shibd and httpd
  - mod_shib Apache module also reads /etc/shibboleth/shibboleth2.xml
  - Easiest if you restart both shibd and httpd after edits
  - If in production you can get away with restarting one or the other if you know which components you have affected
    - Can also reload httpd if just changing access control details
- Browse to https://sp0N.vo.idm.training/secure
  - SAML tracer might be helpful for debugging

Shibboleth SP: Hands-On Exercise

Some Shibboleth SP "Tips and Tricks"

- Browse to https://sp0N.vo.idm.registry/Shibboleth.sso/Session

Shibboleth SP: Hands-On Exercise



Shibboleth SP: Hands-On Exercise

Edit shibboleth2.xml and change

```
<Handler type="Session" Location="/Session" showAttributeValues="false"/>
```

to be instead

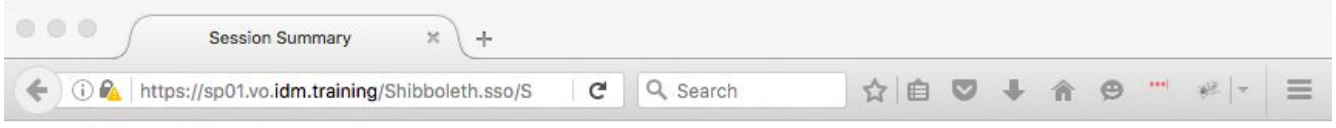
```
<Handler type="Session" Location="/Session" showAttributeValues="true"/>
```

then restart shibd and httpd and browse in order to

1. https://sp0N.vo.idm.training/Shibboleth.sso/Session
2. https://sp0N.vo.idm.training/secure/
3. https://sp0N.vo.idm.training/Shibboleth.sso/Session

Shibboleth SP: Hands-On Exercise

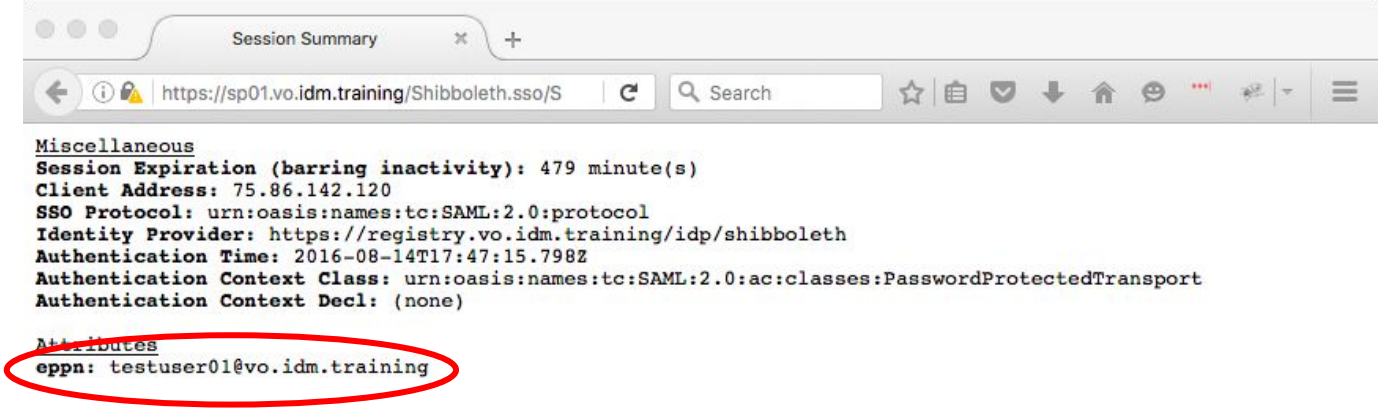
By default sessions stored in memory and are lost during shibd restart



Shibboleth SP: Hands-On Exercise

showAttributeValues="true" helpful in debugging

Point user having trouble to the /Shibboleth.sso/Session session and ask them to send the screen output



Shibboleth SP: Hands-On Exercise

Edit shibboleth2.xml and change

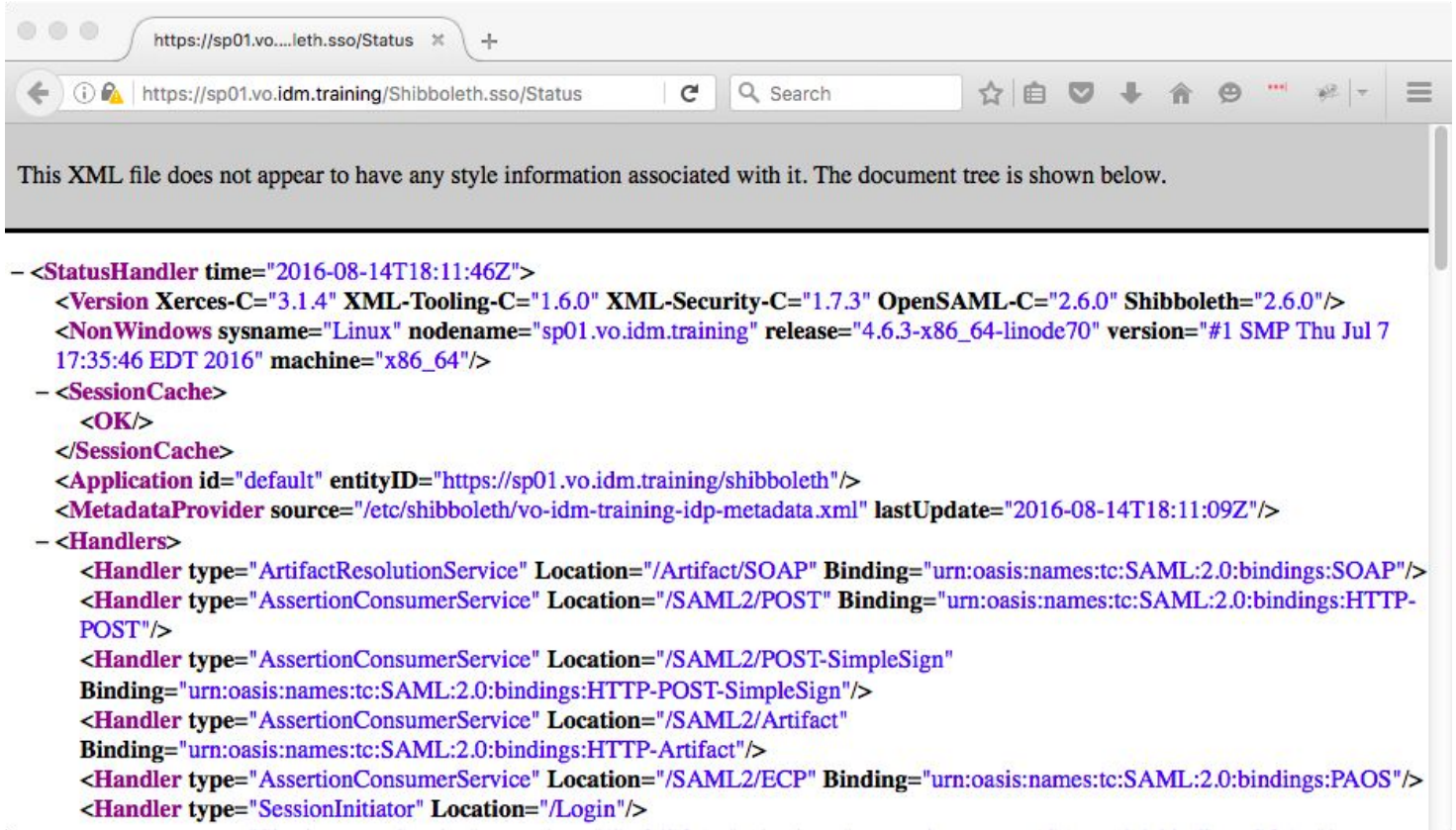
```
<Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>
```

to be instead

```
<Handler type="Status" Location="/Status" acl="0.0.0.0/0"/>
```

then restart shibd and httpd and browse
to
https://sp0N.vo.idm.training/Shibboleth.sso/Status

Shibboleth SP: Hands-On Exercise

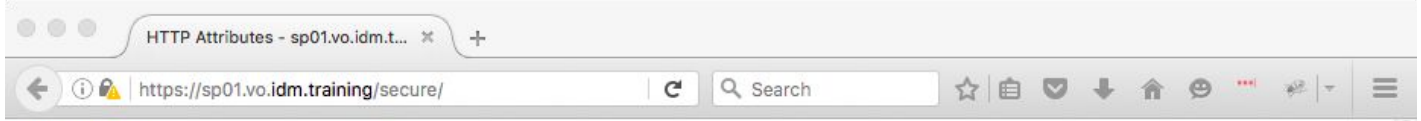


Shibboleth SP: Hands-On Exercise

Shib SP makes information available to applications

```
cd /var/www/html/secure
mv index.html index.html.old
cp index.php.template index.php
```

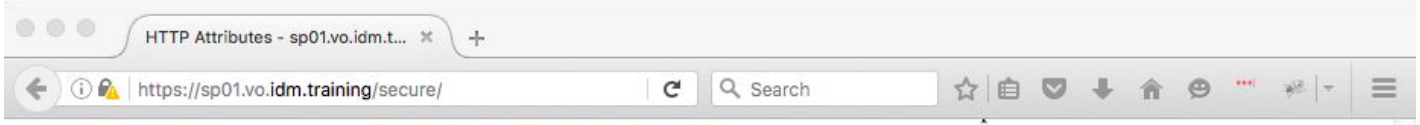
Browse again to https://sp0N.vo.idm.training/secure/



$_REQUEST

$_SERVER

Shib-Handler	https://sp01.vo.idm.training/Shibboleth.sso
Shib-Application-ID	default
Shib-Session-ID	_43e568ea588601e702640c55e5608d13
Shib-Identity-Provider	https://registry.vo.idm.training/idp/shibboleth
Shib-Authentication-Instant	2016-08-14T17:47:15.798Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-Session-Index	_12dfb3c8b9566448226565e5f3b17663
eppn	testuser01@vo.idm.training
HTTPS	on
SSL_TLS_SNI	sp01.vo.idm.training
HTTP_HOST	sp01.vo.idm.training
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate, br
HTTP_REFERER	https://registry.vo.idm.training/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZLRboIwFIZfhfReCgoK%2F%2F5fOkTd1y5LOVHIH7x2gsT6bWiI7X0Sk05IpjgKZ5A0gMwVLk4c1G9sOa7UyqlA1sRJE0EYouVRelayState=ss%3Amem%3Af0601813707d3070d8b8e0810d2d9a116dfd30ae747d311131493678772dab89
HTTP_COOKIE	_shibsession_64656661756c7468747470733a2f2f737030312e766f2e69646d2e747261696e696e672f736869
HTTP_CONNECTION	keep-alive
PATH	/sbin:/usr/sbin:/bin:/usr/bin
SERVER_SIGNATURE	*Apache/2.2.15 (CentOS) Server at sp01.vo.idm.training Port 443*



Shib-Session-Index	_12dfb3c8b9566448226565e5f3b17663
eppn	testuser01@vo.idm.training
HTTPS	on
SSL_TLS_SNI	sp01.vo.idm.training
HTTP_HOST	sp01.vo.idm.training
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate, br
HTTP_REFERER	https://registry.vo.idm.training/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZLRboIwFIZfhfReCgoK%2F%2F5fOkTd1y5LOVHIH7x2gsT6bWiI7X0Sk05IpjgKZ5A0gMwVLk4c1G9sOa7UyqlA1sRJE0EYouVRelayState=ss%3Amem%3Af0601813707d3070d8b8e0810d2d9a116dfd30ae747d311131493678772dab89
HTTP_COOKIE	_shibsession_64656661756c7468747470733a2f2f737030312e766f2e69646d2e747261696e696e672f736869
HTTP_CONNECTION	keep-alive
PATH	/sbin:/usr/sbin:/bin:/usr/bin
SERVER_SIGNATURE	*Apache/2.2.15 (CentOS) Server at sp01.vo.idm.training Port 443*
SERVER_SOFTWARE	Apache/2.2.15 (CentOS)
SERVER_NAME	sp01.vo.idm.training
SERVER_ADDR	45.79.169.109
SERVER_PORT	443
REMOTE_ADDR	75.86.142.120
DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	root@localhost
SCRIPT_FILENAME	/var/www/html/secure/index.php
REMOTE_PORT	51119
REMOTE_USER	testuser01@vo.idm.training
AUTH_TYPE	shibboleth

Shibboleth SP: Hands-On Exercise

The shibd configuration

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
     REMOTE_USER="eppn persistent-id targeted-id">
```

tells the SP which attributes from the IdP to search for in order and then populate into REMOTE_USER CGI environment variable

HTTP headers may also be populated by there is some security risk

- HTTP headers can be spoofed
- Shib SP includes protection but better to use CGI environment if you can
- Often see HTTP headers used with proxied Java servlets

Shibboleth SP: Attribute Mapping

- Any and all attributes asserted by IdP can be mapped and made available to applications in CGI environment variables and/or HTTP headers
- Attributes mapped from formal "on the wire" names (eg. OIDs) to more friendly applications names

  "urn:oid:1.3.6.1.4.1.5923.1.1.1.6" mapped to "eppn"

- attribute-map.xml controls the mapping
  - Default includes both older SAML1 and SAML2 names

Shibboleth SP: Attribute Mapping

- Unmapped attributes "dropped on the floor"
- Possible to set policy on which attributes and values allowed from which IdPs
- Some limited support for modifying attribute values
  - Transform via regex
  - Templates with substitution
  - Upper casing
  - Lower casing
  - Better handled by applications whenever possible
- Apps should be prepared to handle multiple values for multi-valued attributes!
  - Multiple asserted emails often break applications

Shibboleth SP: Hands-On Exercise

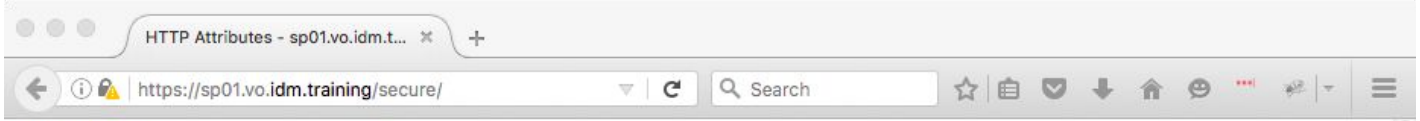
Edit attribute-map.xml to read:

```
<Attributes xmlns="urn:mace:shibboleth:2.0:attribute-map"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" id="eppn">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
  </Attribute>

  <Attribute name="urn:oid:2.5.4.4" id="sn"/>
  <Attribute name="urn:oid:2.5.4.42" id="givenName"/>
  <Attribute name="urn:oid:2.16.840.1.113730.3.1.241" id="displayName"/>
  <Attribute name="urn:oid:0.9.2342.19200300.100.1.3" id="mail"/>

</Attributes>
```

Restart shibd and httpd

Browse to https://sp0N.vo.idm.training/secure/

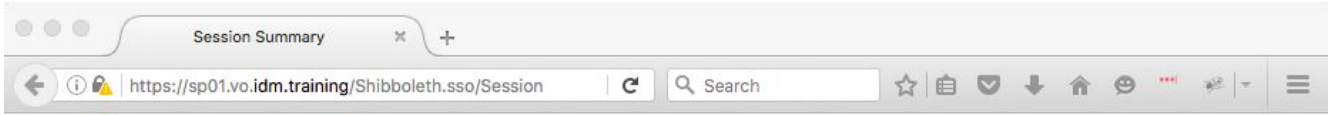
and then https://sp0N.vo.idm.training/Shibboleth.sso/Session



$_REQUEST

$_SERVER

Shib-Handler	https://sp01.vo.idm.training/Shibboleth.sso
Shib-Application-ID	default
Shib-Session-ID	_afa2ed68fec35b8d88098f143fb37aef
Shib-Identity-Provider	https://registry.vo.idm.training/idp/shibboleth
Shib-Authentication-Instant	2016-08-14T19:36:14.994Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-Session-Index	_fdb512e6a2c4b4d42921c3a27a57c751
displayName	Test User01
eppn	testuser01@vo.idm.training
givenName	Test
mail	testuser01@vo.idm.training
sn	User01
HTTPS	on
SSL_TLS_SNI	sp01.vo.idm.training
HTTP_HOST	sp01.vo.idm.training
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate, br
HTTP_REFERER	https://registry.vo.idm.training/idp/profile/SAML2/Redirect/SSO?execution=e1s1
HTTP_COOKIE	_shibsession_64656661756c7468747470733a2f2f737030312e766f2e69646d2e747261696e696e672f736869



Miscellaneous
Session Expiration (barring inactivity): 479 minute(s)
Client Address: 75.86.142.120
SSO Protocol: urn:oasis:names:tc:SAML:2.0:protocol
Identity Provider: https://registry.vo.idm.training/idp/shibboleth
Authentication Time: 2016-08-14T19:36:14.994Z
Authentication Context Class: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Authentication Context Decl: (none)

Attributes
displayName: Test User01
eppn: testuser01@vo.idm.training
givenName: Test
mail: testuser01@vo.idm.training
sn: User01

Shibboleth SP: Apache Access Control

- Significant differences from Apache 2.2 to 2.4
- Use 'ShibCompatWith24 On' with 2.2 to be forward-compatible
- General syntax:

```
require rule-type value1 value2
```

- Some rules support a regular expression mode:

```
require rule ~ exp1 exp2
```

- See https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPhtaccess

Shibboleth SP: Hands-On Exercise

Task:

- Edit /etc/httpd/conf.d/shib.conf and replace

  ```
  require shib-session
  ```

  with

  ```
  require shib-attr eppn testuser0N@vo.idm.training
  ```

  to only allow a single user
- You can reload httpd since only editing access control:
  ```
  service httpd reload
  ```

Shibboleth SP: Hands-On Exercise

Try specifying two allowed users, for example

```
require shib-attr eppn testuser01@vo.idm.training testuser02@vo.idm.training
```

Shibboleth SP: Hands-On Exercise

Try specifying a regular expression, for example

```
require shib-attr eppn ~ ^testuser..@vo.idm.training
```

Shibboleth SP: Hands-On Exercise

Make sure you try a negative test to prove you can deny access

Shibboleth SP: Active Vs Passive Protection

- We have examined active protection of resources
  - User must have a valid SP session to access resource
  - Session may not be enough--some access control might also be in place
  - SP will start SAML Web SSO flow immediately if no session
- "Passive" protection is also possible
  - No valid session required
  - SP will not start SAML Web SSO flow if user access resource
  - If there is a valid session asserted attributes will be made available in usual ways
  - Also called "lazy sessions"

Shibboleth SP: Hands-On Exercise

Task:

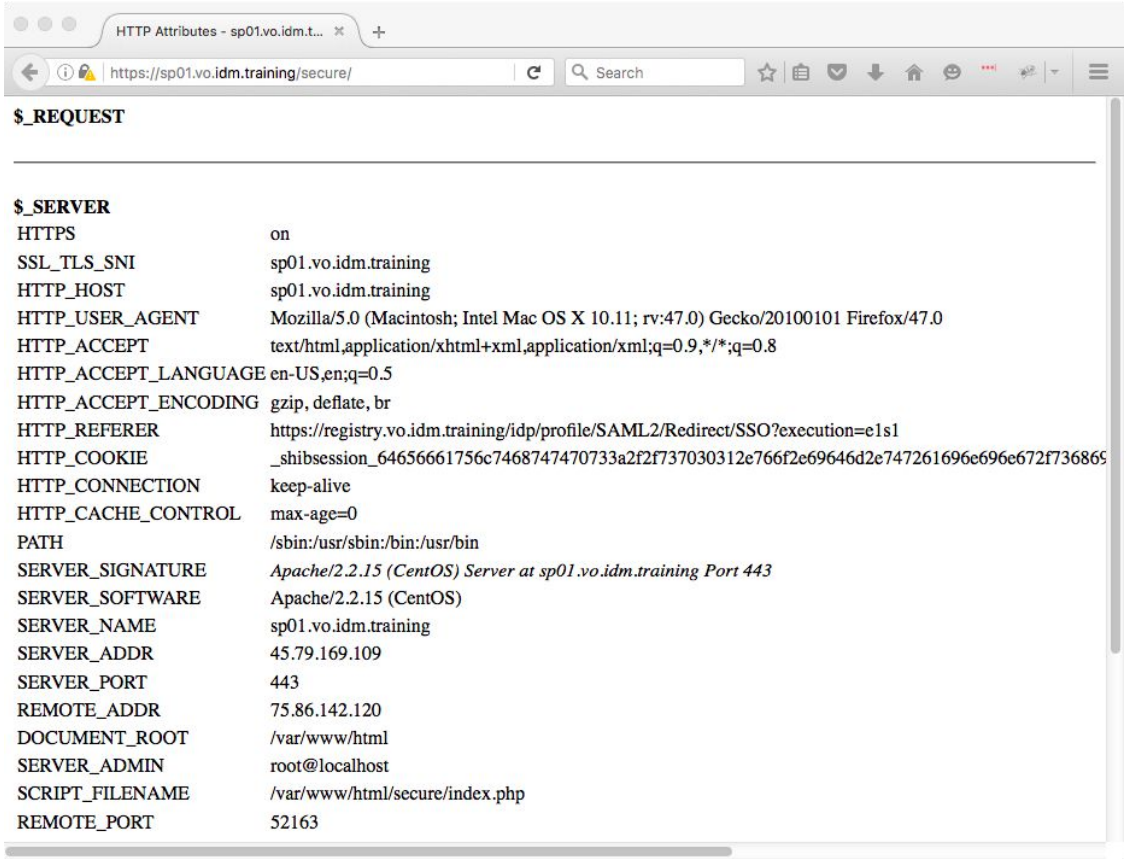
- Edit /etc/httpd/conf.d/shib.conf so that /secure access stanza is

```
<Location /secure>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession 0
  require shibboleth
</Location>
```

- Restart both shibd and httpd
- Browse to https://sp0N.vo.idm.training/secure/

Shibboleth SP: Hands-On Exercise

No CGI environment variables from Shibboleth SP and no start of the SAML Web SSO flow



Shibboleth SP: Hands-On Exercise

- To kick off a SAML Web SSO flow and initiate a SP session browse to

  https://sp0N.vo.idm.training/Shibboleth.sso/Login

- Then browse to

  https://sp0N.vo.idm.training/secure/

- You should see the attributes asserted by IdP again in the CGI environment variables
- If you did not use a "fresh" browser, you probably still had a session with IdP and did not have to authenticate again - SSO in effect

Shibboleth SP: Hands-On Exercise

- Use a "fresh" browser and/or restart shibd
  - Private-browsing window for example
  - Restarting shibd only throws away the session with the SP
  - To "throw away" the session with the IdP also try private browsing or clear cookies
- Browse to

  https://sp0N.vo.idm.training/Shibboleth.sso/Login?target=https%3A//sp0N.vo.idm.training/secure/

- target query parameter tells the SP to redirect the browser to that URL after the SAML Web SSO flow is complete
  - Must be URL-encoded so ":" becomes "%3A"

Shibboleth SP: Lazy Sessions

- Lazy sessions is a common application integration pattern
- Often used with semi-public wikis
  - Anyone can read
  - Write access requires authentication (a valid SP session)
  - Wiki is configured to send browser to the /Shibboleth.SSO/Login endpoint when either user clicks "Login" or chooses "Edit"
- Access control is fully delegated to the application

Shibboleth SP: Session Initiation Parameters

A number of additional session initiation parameters are available:

- entityID - specify which IdP to use for SAML Web SSO
- acsIndex - specify (by index) which SAML binding to use
- forceAuthn - ask the IdP for forced re-authentication
- authContextClassRef - ask the IdP for particular class of authentication

Shibboleth SP: Hands-On Exercise

Try the following:

`https://sp0N.vo.idm.training/Shibboleth.sso/Login?entityID=https%3A//idp.uwm.edu/idp/shibboleth`

- Should not work since your SP is not (yet) federated with UWM

`https://sp0N.vo.idm.training/Shibboleth.sso/Login?acsIndex=3`

- Use SAML tracer to see how the flow is different (hint: using artifact binding)

With a fresh browser go through a normal flow by visiting

`https://sp0N.vo.idm.training/Shibboleth.sso/Login`

then immediately browse to

Shibboleth SP: Ending SP Session

- After a SAML Web SSO flow there are (usually) TWO sessions
  a. Session with the login server or IdP, effectively providing SSO
  b. Session with the SP
- Lifetimes of these two sessions are completely independent
  a. Ending one has no bearing on ending the other
  b. Each may have its own lifetime AND inactivity timeout
  c. Caveat: SAML protocol includes ability for IdP to signal to SP to create a session only valid for a particular amount of time
     - This is rarely used--do NOT depend on it for any type of security calculation!
- Significant impact on the notion of "logout" in a Federated context
  a. Only when the same enterprise operates the IdP and the SP(s) can you realize the notion of "global logout" or single logout (SLO) that you might expect
  b. Example: why should an SP operated by LIGO be able to tell the University of Wisconsin-Madison IdP to end all sessions for the user?

SAML2 Logout

- "global logout" in a SAML2 Federated (large "F") context is not well defined
- Advanced topic not covered more here today
- Most people concerned about SSO sessions from "public" terminals
  - Need to assess your risks per-service
  - Forced re-authentication can help (but not all IdPs will respect the request)
  - Educate your users -- if your users routinely use "public" terminals not managed by an organization you trust you probably have larger issues than SAML2 SLO

Shibboleth SP: Hands-On Exercise

Terminate the Shibboleth SP session by browsing to

```
https://sp0N.vo.idm.training/Shibboleth.sso/Logout
```

You may include a 'return' parameter to send the browser to a location

- Often used to display a page reminding users about possible sessions still remaining with the IdP

```
https://sp0N.vo.idm.training/Shibboleth.sso/Logout?
     return=https%3A//registry.vo.idm.training/logout.html
```

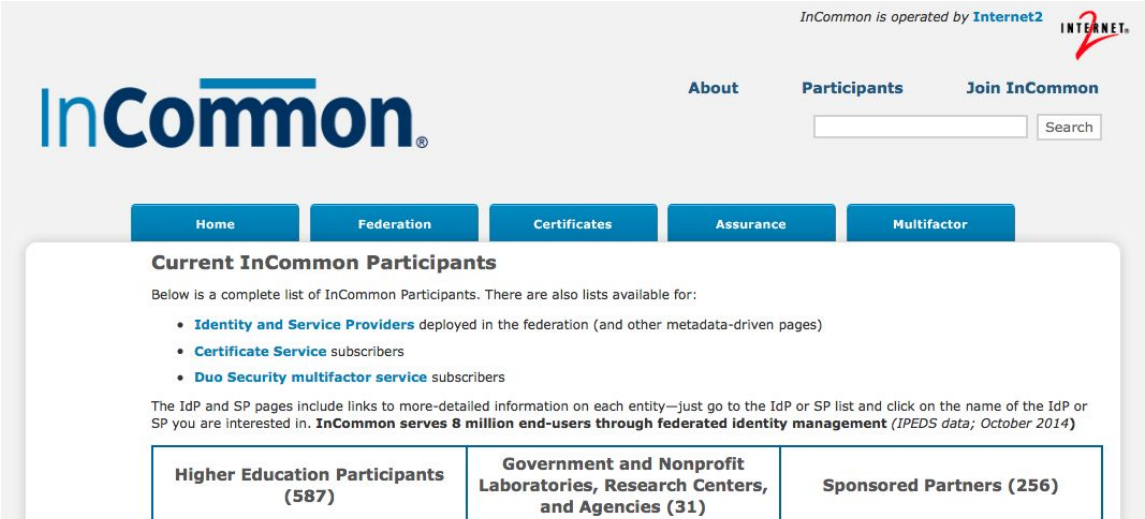
SAML Federation Deep Dive

The Role of Federations

- Enable us to scale up to 1000s of IdPs and SPs
- Publish digitally signed SAML metadata containing public keys, endpoint URLs, and other info about IdPs and SPs
- Set standards for SAML attributes, levels of assurance, etc.
- Provide support and training

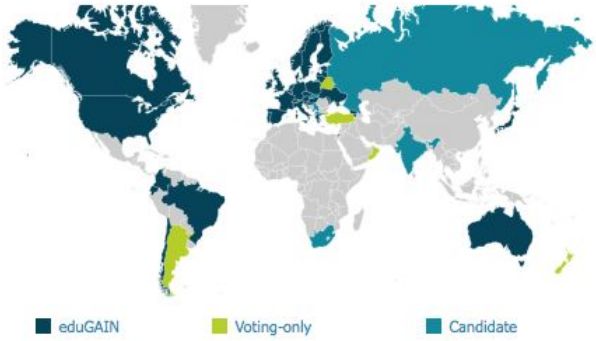
InCommon: The US R&E Federation

- https://www.incommon.org/
- Over 800 participants and growing: https://www.incommon.org/participants
- 400+ IdPs / 3000+ SPs: https://incommon.org/federation/info/all-entities
- Becoming an InCommon Member: https://www.incommon.org/join



eduGAIN: Global InterFederation

- InCommon joined eduGAIN in Feb 2016 https://www.incommon.org/edugain/
- Enables SAML metadata exchange across federations, with per-entity opt-in/opt-out
- eduGAIN Policy Framework requires members to:
  - Primarily serve the interests of the R&E sector.
  - Provide a point of contact for technical issues.
  - Provide processes for handling complaints and incidents.
  - Have a published Metadata registration practice statement.
- http://www.edugain.org
- https://technical.edugain.org/



eduGAIN numbers	
Federations:	38
All entities:	3419
IdPs:	2159
SPs:	1264
Standalone AAs:	3

SAML Metadata

- InCommon metadata includes US IdPs/SPs plus international IdPs/SPs from eduGAIN: https://incommon.org/federation/metadata.html
- SAML metadata interoperability enables secure, scalable federation between IdPs and SPs: http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.html
- SAML metadata is a digitally signed XML document that establishes trust in the federation: http://md.incommon.org/InCommon/InCommon-metadata.xml
    - https://spaces.internet2.edu/display/InCFederation/Metadata+Signing+Certificate

```
<EntityDescriptor entityID="https://idp.ncsa.illinois.edu/idp/shibboleth">
  <Extensions>...</Extensions>
  <IDPSSODescriptor errorURL="https://idp.ncsa.illinois.edu/error"
                    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>
      <shibmd:Scope regexp="false">ncsa.illinois.edu</shibmd:Scope>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="en">National Center for Supercomputing Applications</mdui:DisplayName>
        <mdui:Description xml:lang="en">National Center for Supercomputing Applications</mdui:Description>
        <mdui:PrivacyStatementURL xml:lang="en">...</mdui:PrivacyStatementURL>
        <mdui:Logo height="100" width="148" xml:lang="en">...</mdui:Logo>
      </mdui:UIInfo>
    </Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo><ds:X509Data><ds:X509Certificate>...</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
    </KeyDescriptor>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
                         Location="https://idp.ncsa.illinois.edu/idp/profile/SAML2/Redirect/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                         Location="https://idp.ncsa.illinois.edu/idp/profile/SAML2/POST/SSO"/>
  </IDPSSODescriptor>
  <Organization>...</Organization>
  <ContactPerson>...</ContactPerson>
</EntityDescriptor>
```

```
<EntityDescriptor entityID="https://cilogon.org/shibboleth">
  <Extensions>...</Extensions>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>...</Extensions>
    <KeyDescriptor>
      <ds:KeyInfo><ds:X509Data><ds:X509Certificate>...</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
    </KeyDescriptor>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                              Location="https://cilogon.org/Shibboleth.sso/SAML2/POST" index="1"/>
    <AttributeConsumingService index="1">
      <ServiceName xml:lang="en">CILogon</ServiceName>
      <ServiceDescription xml:lang="en">...</ServiceDescription>
      <RequestedAttribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
      <RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
      <RequestedAttribute FriendlyName="eduPersonTargetedID" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
      <RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    </AttributeConsumingService>
  </SPSSODescriptor>
  <Organization>...</Organization>
  <ContactPerson>...</ContactPerson>
</EntityDescriptor>
```

Federation Metadata: Hands-On Exercise

Task:

- Update SP to use InCommon metadata
- See http://sl.cilogon.org/vot

References:

- https://spaces.internet2.edu/display/InCFederation/Metadata+Client+Software
  - https://spaces.internet2.edu/display/InCFederation/Shibboleth+Metadata+Config

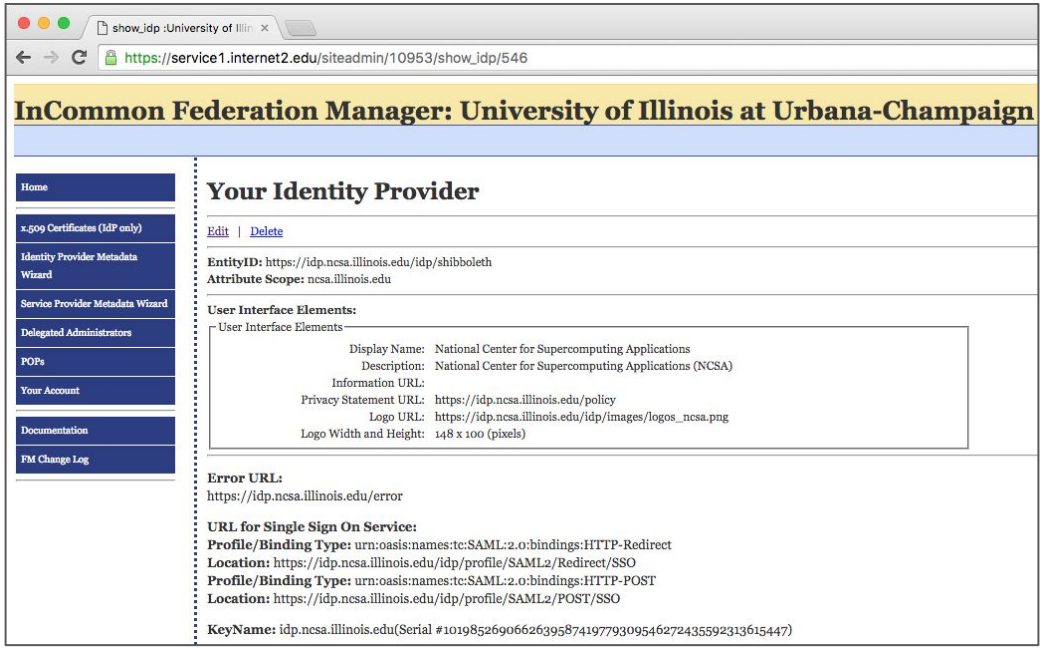
Federation Metadata: Hands-On Exercise

Edit /etc/shibboleth/shibboleth2.xml and add the following element after existing <MetadataProvider> element

```
<MetadataProvider type="XML"
    url="http://md.incommon.org/InCommon/InCommon-metadata.xml"
    backingFilePath="InCommon-metadata.xml"
    maxRefreshDelay="3600"
    legacyOrgNames="true">
  <MetadataFilter type="Signature" certificate="inc-md-cert.pem" verifyBackup="false"/>
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="1209600"/>
  <MetadataFilter type="EntityRoleWhiteList">
    <RetainedRole>md:IDPSSODescriptor</RetainedRole>
    <RetainedRole>md:AttributeAuthorityDescriptor</RetainedRole>
  </MetadataFilter>
  <DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"
      attributeName="http://macedir.org/entity-category"
      attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      attributeValue="http://refeds.org/category/hide-from-discovery"/>
 </MetadataProvider>
```

InCommon Federation Manager

- https://spaces.internet2.edu/display/InCFederation/Federation+Manager



Attributes: eduPerson

The eduPerson specification defines the attributes used in InCommon/eduGAIN:

- eduPersonPrincipalName (user@example.edu)
- eduPersonTargetedID (https://example.edu/idp!https://example.org/sp!ChF3nEYtvG3a5G4Xv0g=)
- eduPersonUniqueId (28c5353b8bb34984a8bd4169ba94c606@example.edu)
- eduPersonOrcid (http://orcid.org/0000-0002-1825-0097)
- eduPersonAffiliation (faculty,student,staff,alum,member,affiliate)
- eduPersonScopedAffiliation (faculty@example.edu,member@example.edu)
- eduPersonEntitlement (http://example.com/contracts/HEd123)
- displayName (John Smith)
- givenName (John)
- sn (Smith)
- mail (jsmith@example.edu)

http://macedir.org/specs/eduperson/

The Reality of Attribute Release

The attributes an IdP is able/willing to release to your SP varies, due to:

- Privacy concerns (e.g., US FERPA, EU Data Protection)
- Federation boundaries (eduGAIN opt-in/opt-out)
- Technical limitations (e.g., no eduPersonTargetedID support)
- Lack of data (e.g., guest accounts, no email contact info)

Attribute release can vary across the IdP’s membership:

- Students / Faculty / Staff / Guests / Affiliates
- Emeritus / Retired / Pre-matriculated / Alumni
- Directory Opt-Out / FERPA Hold / Protective Order

The Reality of Attribute Release: IDs

IdP may provide ePPN and/or ePTID to your SP.

eduPersonPrincipalName (ePPN)

- May be re-assigned (usually after some hiatus period)
- Mitigate re-assignment through SP-side offboarding

eduPersonTargetedID (ePTID)

- Non-reassigned, targeted, opaque
- https://example.edu/idp!https://example.org/sp!ChF3nEYtvG0S3a5G4Xv0g=

The Reality of Attribute Release: Names

IdP may provide displayName or givenName and surname.

displayName

- Single valued
- Don't assume it contains spaces

givenName and surname

- Multi-valued

May contain arbitrary UTF-8 characters, not just ASCII.

REFEDS Research and Scholarship (R&S)

Defines an attribute bundle:

- personal identifiers: email address, person name, eduPersonPrincipalName
- pseudonymous identifier: eduPersonTargetedID
- affiliation: eduPersonScopedAffiliation

Federations tag R&S entities in metadata:

- Research and Scholarship SPs
- IdPs that release the attribute bundle to R&S SPs

https://refeds.org/category/research-and-scholarship

Metadata Tag for IdP R&S Support

```
<EntityDescriptor entityID="https://idp.ncsa.illinois.edu/idp/shibboleth">
  <Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="https://incommon.org"/>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      Name="http://macedir.org/entity-category-support"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      Name="http://macedir.org/entity-category"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>http://id.incommon.org/category/registered-by-incommon</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

Metadata Tag for R&S SP

```
<EntityDescriptor entityID="https://cilogon.org/shibboleth">
  <Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="https://incommon.org"/>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      Name="http://macedir.org/entity-category"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>http://id.incommon.org/category/research-and-scholarship</saml:AttributeValue>
        <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
        <saml:AttributeValue>http://id.incommon.org/category/registered-by-incommon</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

The IdP of Last Resort

The user may not be able to log in with their “home campus” identity:

- University not a federation member
- University doesn’t operate an IdP
- International IdP did not opt-in to eduGAIN
- IdP does not release eduPersonPrincipalName/eduPersonTargetedID

Approaches:

- External Guest IdP: Google, GitHub, UnitedID, NCSA, etc.
- Local Guest IdP: On-premises or cloud

https://wiki.refeds.org/display/GROUPS/IoLR

SAML Federations: Review

- Enable us to scale up to 1000s of IdPs and SPs
- Publish digitally signed SAML metadata containing public keys, endpoint URLs, and other info about IdPs and SPs
- Set standards for SAML attributes, levels of assurance, etc.
- Provide support and training

Questions? Comments?

Application Integration

Application Integration

- Writing a SAML consumer is hard
  - Don't do it
  - Even the best SAML libraries have significant limitations
    - Large part of why commercial vendor implementations so limited
  - As a ***LAST RESORT***:
    - OpenSAML from Shibboleth team (used to build Shibboleth IdP implementation)
      - Java
      - Documentation, if it exists, aimed at internal use by Shibboleth team
    - Spring Security SAML Extension - Java
    - pySAML2 - Python
    - Python-SAML by OneLogin
    - .NET SAML by Microsoft

- We will focus on application integration using Shibboleth SP

Integration Strategy: Choose Integrated Apps

A number of applications, especially collaborative tools, already integrated

- Look for SAML or "Shibboleth" "authentication"
- Confluence, WordPress, Dokuwiki, ...
- Ask on the Shibboleth users email list

Issues:

- Often donated modules that may not be maintained or used heavily
- Uneven documentation
- Varying levels of sophistication
- Terminology and vocabulary not always accurate

Integration Strategy: Choose Primary Identifier

Most often one identifier is the primary key for the application

- Choose identifier (if you can) asserted by IdPs and usable by application
- ePPN is usually the best choice but...
  - Some applications have issues with the scoping (@some.org)
  - See previous caveats about ePPN sometimes being re-assigned
    - Some applications have character limits on identifiers!
- Common to have the "bootstrapping issue"
  - Application requires deployment WITHOUT SAML/Shibboleth
  - Choose "admin" account before SAML/Shibboleth
  - The "admin" account becomes inaccessible later when adding SAML/Shibboleth
  - Try to provision the "admin" account with identifier (ePPN) you expect after federating

Application Integration: Broken Applications

Some applications are "broken" in ways that make federation hard

- Limitations on characters in identifiers (no '@' or '.' or '+')
- Length restrictions on identifiers, names, other attributes asserted by IdPs
- Assumptions about CGI environment variables
  - Single valued versus multi-valued

Not uncommon to have to hack the application code

- Most developers still assume their code will be creating/provisioning accounts and group memberships and take short cuts
- Trend is improving with more adoption of federated identity

Application Integration: Hands-On Exercise

Task: Use Dokuwiki as an example

- Configure Apache/Shib for passive or "lazy sessions"
- Browse to https://sp0N.vo.idm.training/dokuwiki/install.php
- Bootstrap

Application Integration: Hands-On Exercise

Edit /etc/httpd/conf.d/shib.conf and add

```
<Directory /var/www/html/dokuwiki>
  AuthType shibboleth
  ShibCompatWith24 On
  require shibboleth
</Directory>
```

to use "lazy sessions" for Dokuwiki

Reload httpd

Enter any name you like

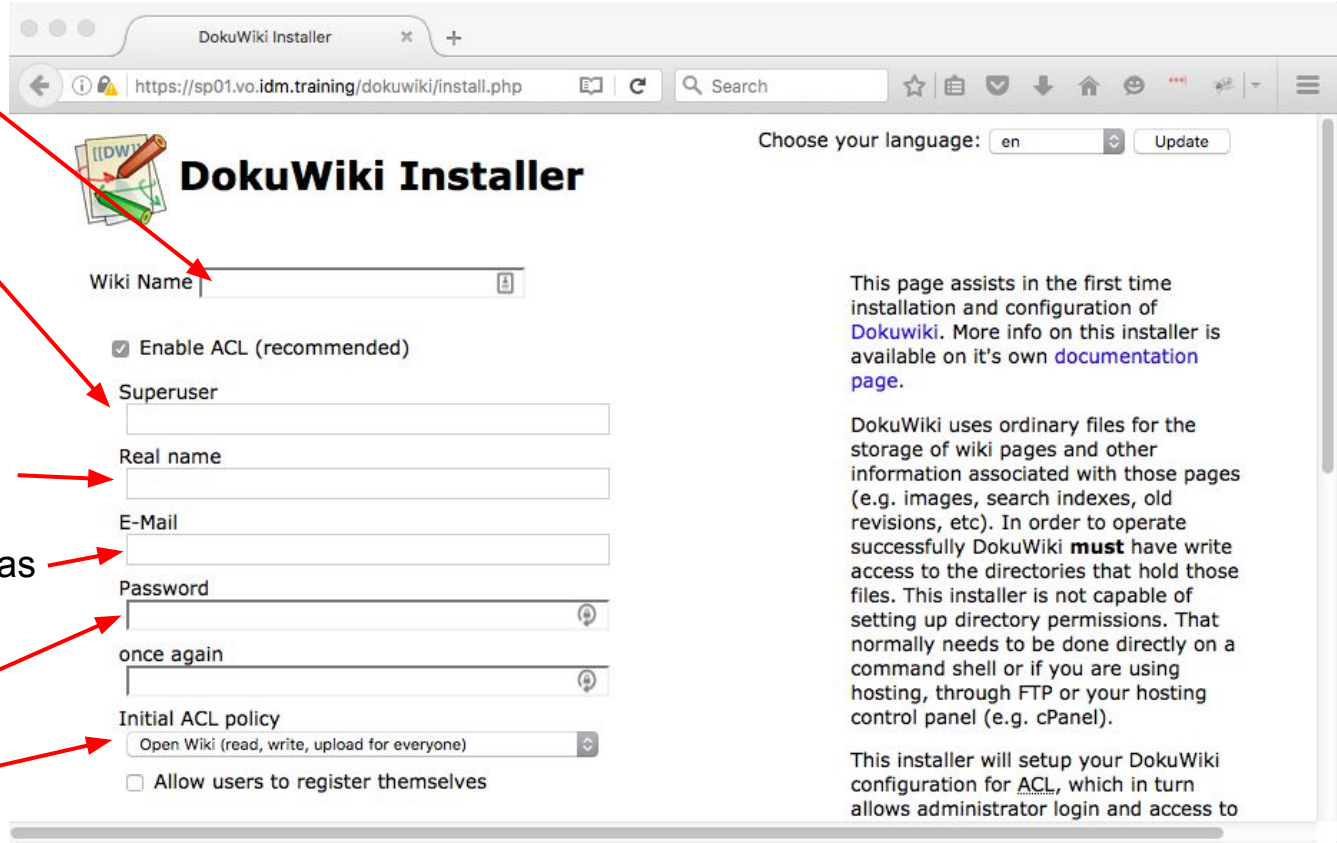
Try ePPN "testuser0N@vo.idm.training" as the Superuser identifier

Enter any "Real name" you like

Try "testuser0N@vo.idm.training" as the email

Use a "dummy" password

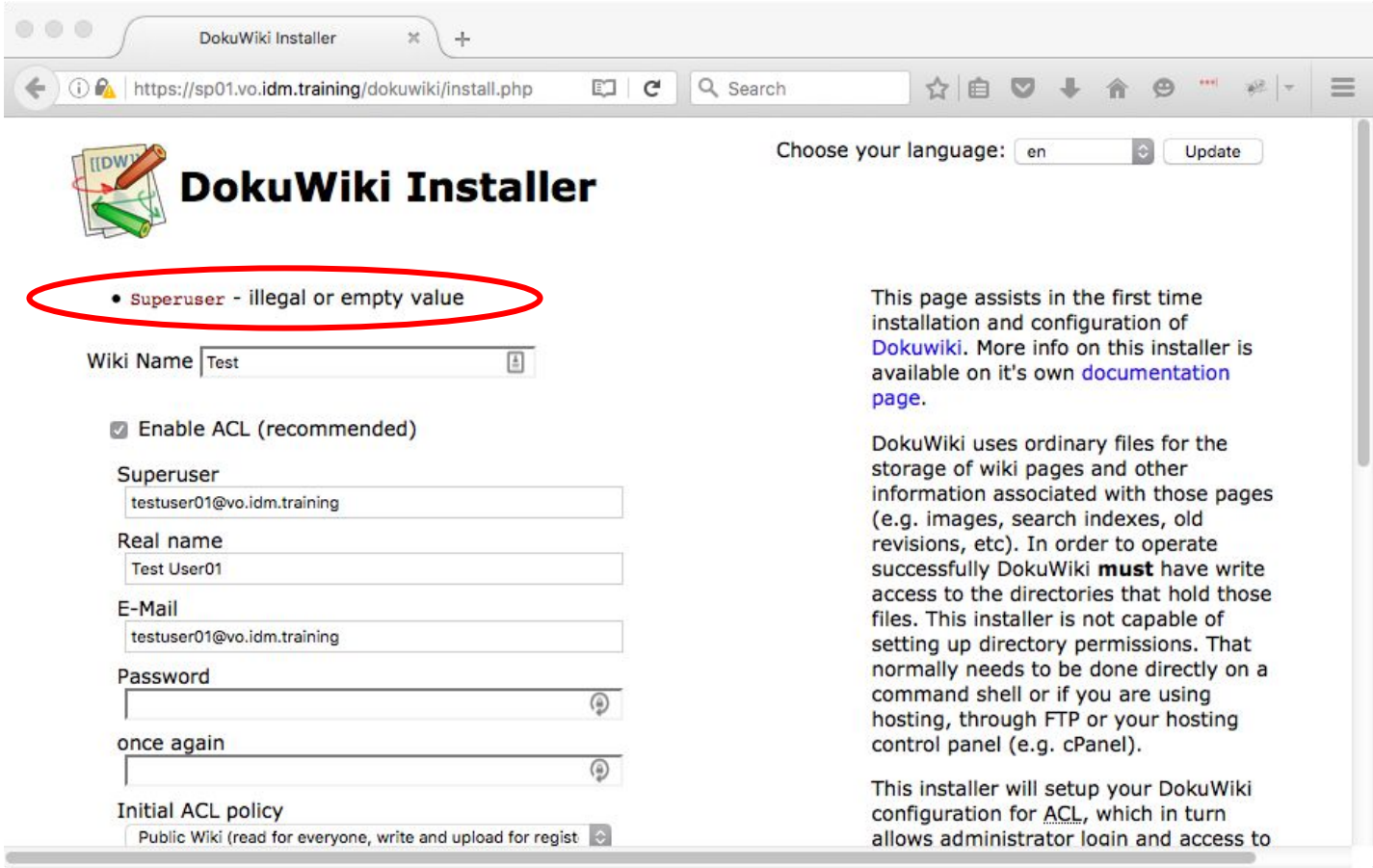
Select "Public wiki"



Hmmmm....

Is the '@' sign a problem?

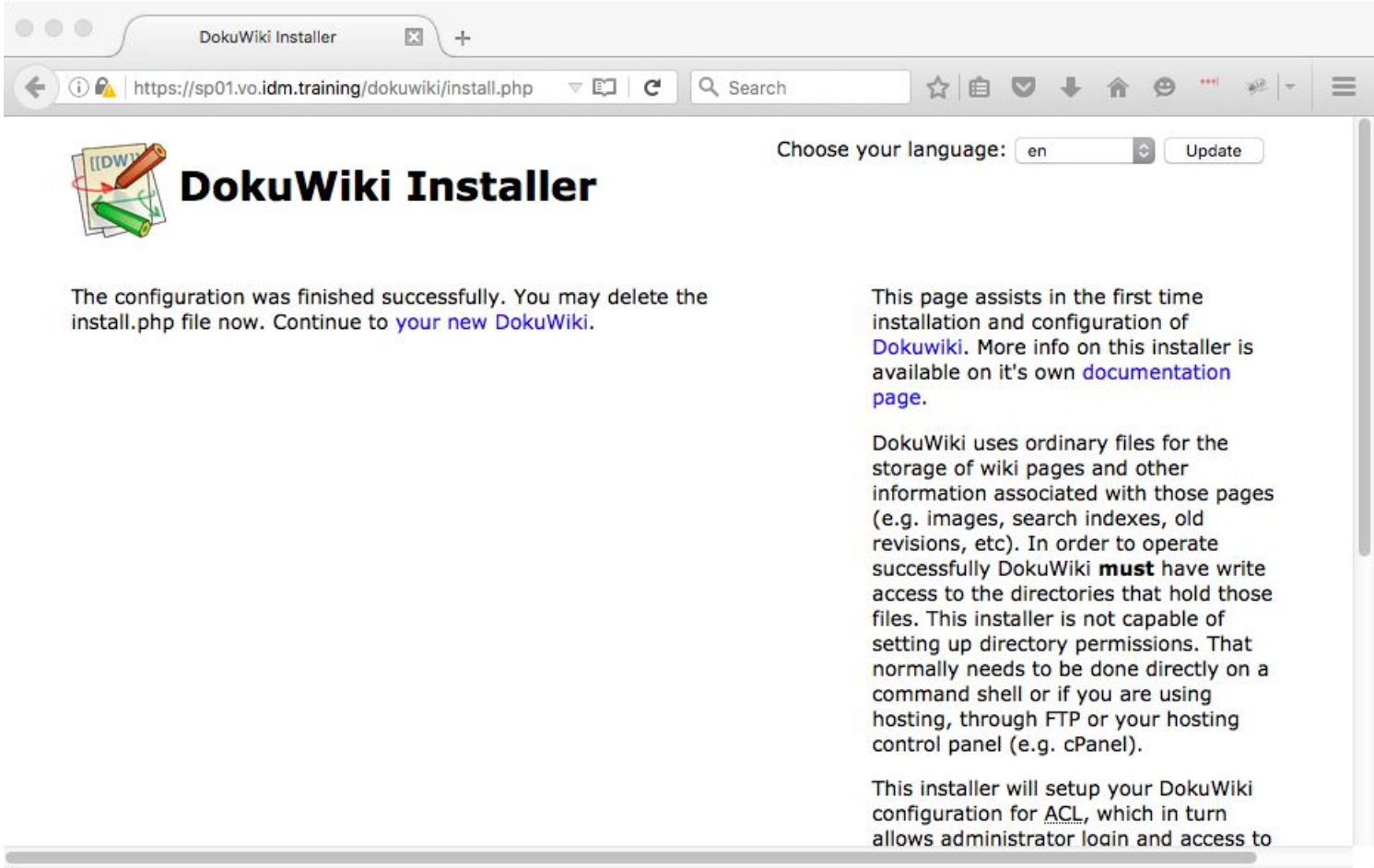
Try again with just plain "admin"



So can DokuWiki consume ePPN as identifier?

It turns out, yes...

Limitation just in the install form.



Application Integration: Hands-On Exercise

Edit /var/www/html/dokuwiki/conf/local.php and change

```
$conf['superuser'] = '@admin';
```

to

```
$conf['superuser'] = 'testuser0N@vo.idm.training';
```

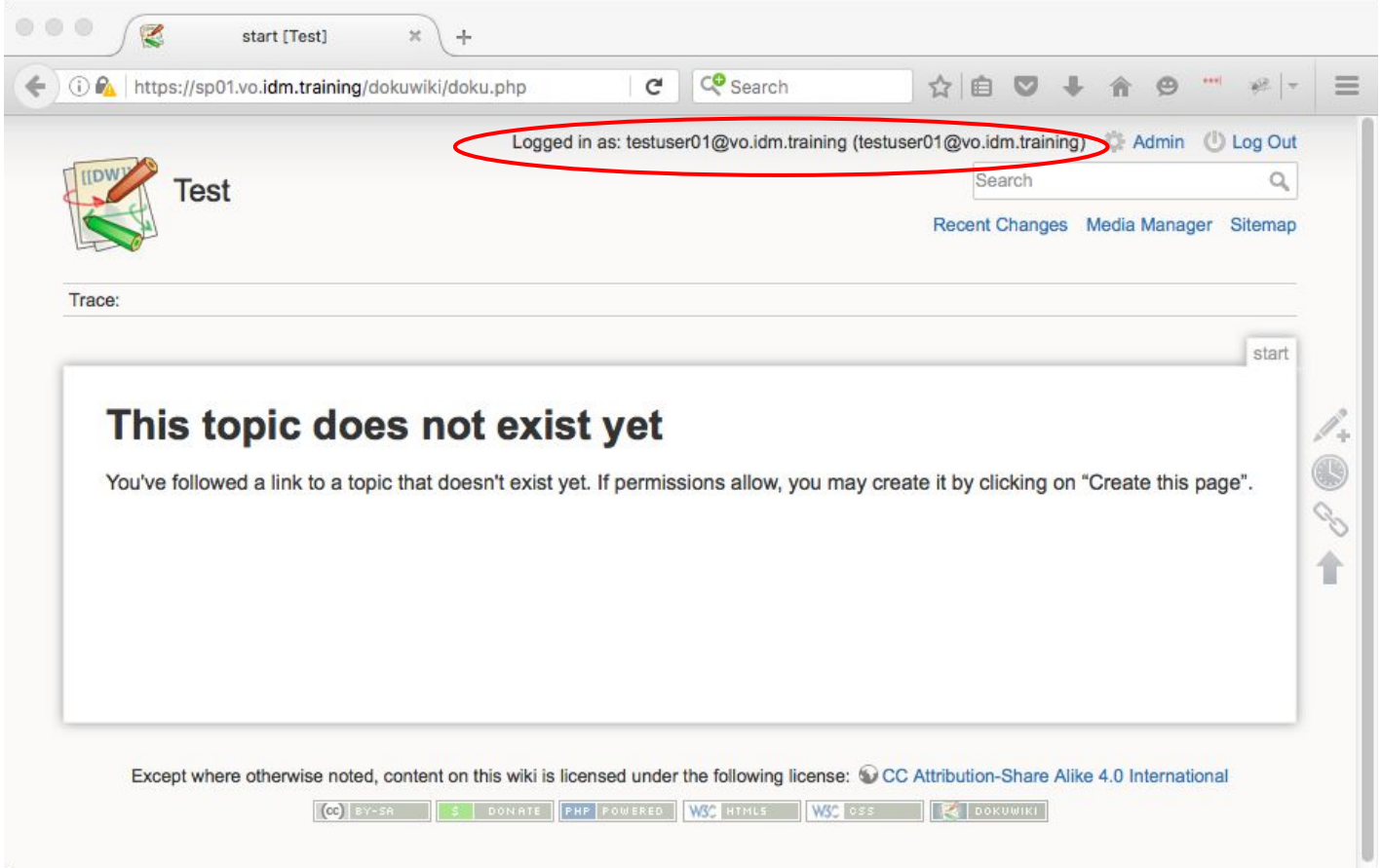
and add the line

```
$conf['authtype'] = 'authshibboleth';
```

Application Integration: Hands-On Exercise

Browse to https://sp0N.vo.idm.training/dokuwiki/

Click "Log In"


start [Test]
https://sp01.vo.idm.training/dokuwiki/doku.php
Search
Logged in as: testuser01@vo.idm.training (testuser01@vo.idm.training)
Admin
Log Out
Test
Search
Recent Changes
Media Manager
Sitemap
Trace:
start
This topic does not exist yet
You've followed a link to a topic that doesn't exist yet. If permissions allow, you may create it by clicking on “Create this page”.
Except where otherwise noted, content on this wiki is licensed under the following license:
CC Attribution-Share Alike 4.0 International
DONATE
POWERED
HTML5
CSS
DOKUWIKI

Application Integration: Hands-On Exercise

Examine /var/www/html/dokuwiki/conf/authshibboleth.conf.php to see all options for the "DokuWiki Shibboleth Authentication Plugin"

- Better than average flexibility and customization
- Logging option is helpful for troubleshooting

Application Integration: DokuWiki Example

DokuWiki integration experience is fairly typical

- SAML/Shibboleth integration is not streamlined but doable
- "Bootstrap problem" presents a learning curve
- Best practice is to "learn the application" without SAML/Shibboleth in a test tier and later "bolt on" the SAML/Shibboleth functionality
- Similar experiences with WordPress, Confluence, JIRA, Foswiki,...

Application Integration: "Greenfield" Approaches

When it is necessary to "domesticate" an application yourself

- Avoid any constraints on the characters in identifiers
- Avoid any length constraints on identifiers
- Use a primary key for each user but do not display it
  - Use the notion of a "display name" instead
  - Mapping from IdP-asserted identifier to an application internal primary key is good practice
  - Consider sensible default when no display name available
- Plan for and expect multiple values in CGI env variables and HTTP headers

Application Integration: "Greenfield" Approaches

When it is necessary to "domesticate" an application yourself

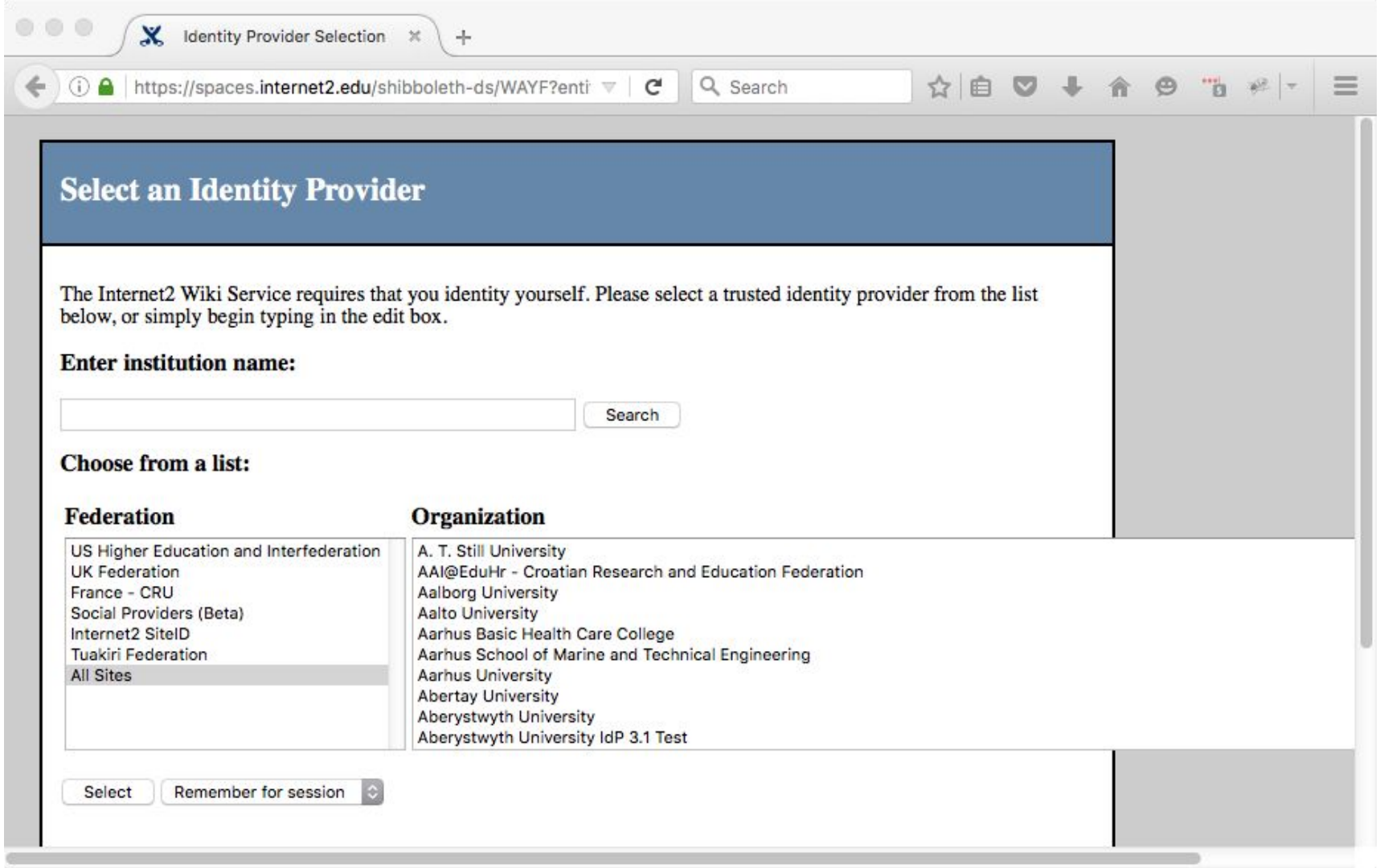
- Prepare to consume both identity and group membership information from external sources
- Consider application-level session management
  - Consume information from IdP assertion then abandon the Shibboleth SP session
- Consider "just in time" provisioning
- Fail gracefully
  - Expect some IdPs to assert nothing or assert garbage

IdP Discovery

IdP Discovery

- SP federated with more than one IdP?
- How does the SP decide to which IdP to send the browser?
- Many bad ideas proven through experience to not work:
  - IP address of the browser
  - Different "applications" or URLs as gateways to different IdPs
  - Referring pages
- Usually these approaches trying to prevent the actual best solution
  - Prevent one or a few extra "clicks"
  - Cost is higher and results in more user confusion in the long term

Ask the user to choose!


Identity Provider Selection
https://spaces.internet2.edu/shibboleth-ds/WAYF?enti
Search
Select an Identity Provider
The Internet2 Wiki Service requires that you identity yourself. Please select a trusted identity provider from the list below, or simply begin typing in the edit box.
Enter institution name:
Search
Choose from a list:
Federation
US Higher Education and Interfederation
UK Federation
France - CRU
Social Providers (Beta)
Internet2 SiteID
Tuakiri Federation
All Sites
Organization
A. T. Still University
AAI@EduHr - Croatian Research and Education Federation
Aalborg University
Aalto University
Aarhus Basic Health Care College
Aarhus School of Marine and Technical Engineering
Aarhus University
Abertay University
Aberystwyth University
Aberystwyth University IdP 3.1 Test
Select
Remember for session

Select your identity provider

GÉANT Association (NL) | https://login.terena.org/wayf/module.php/disco

Search

SELECT YOUR IDENTITY PROVIDER

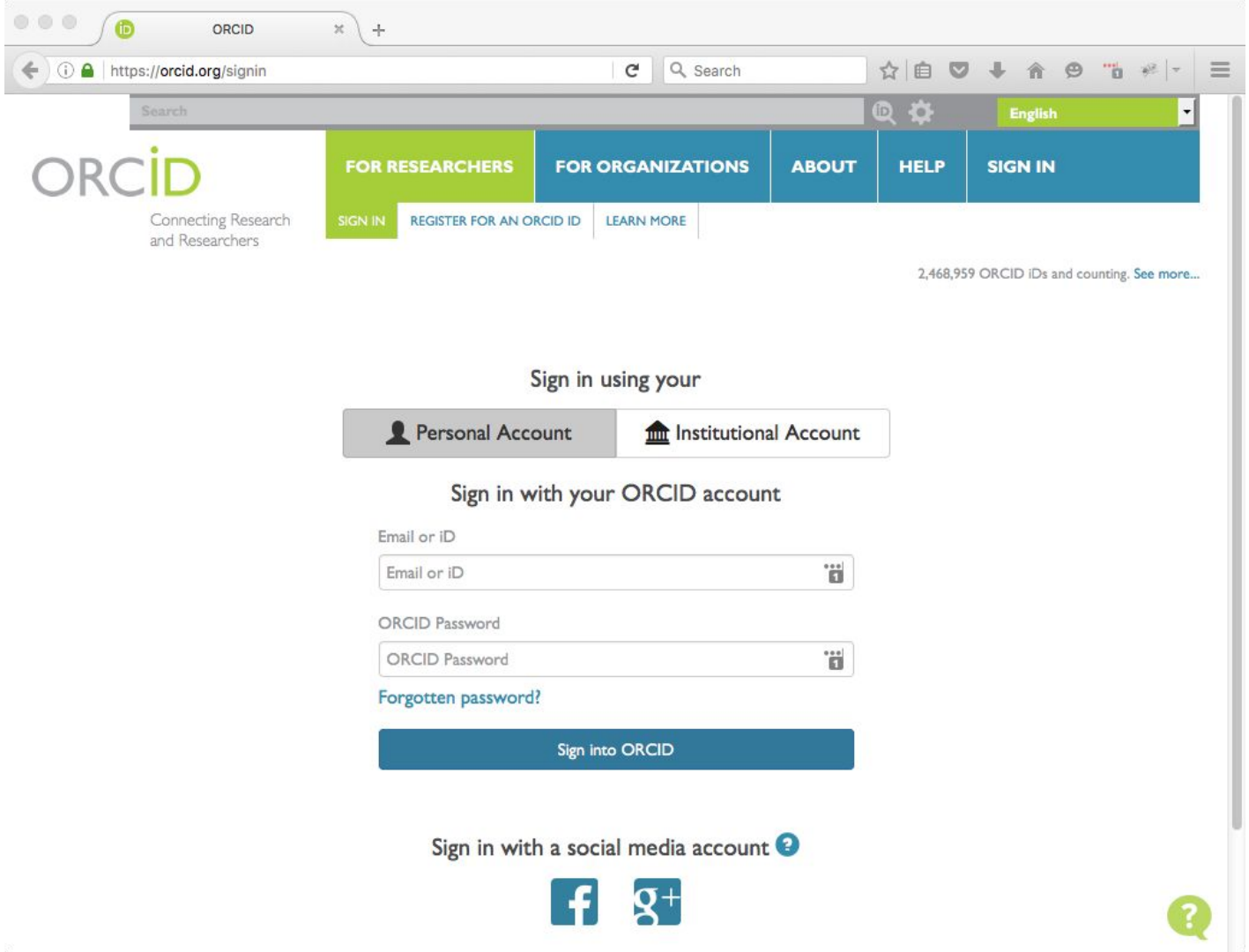
English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Español | Svenska | Suomeksi | Français | Italiano | Nederlands | Luxembourgish | Czech | Slovenščina | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 中文 | ελληνικά | Lietuvių kalba | Åarjelh-saemien giele | русский язык

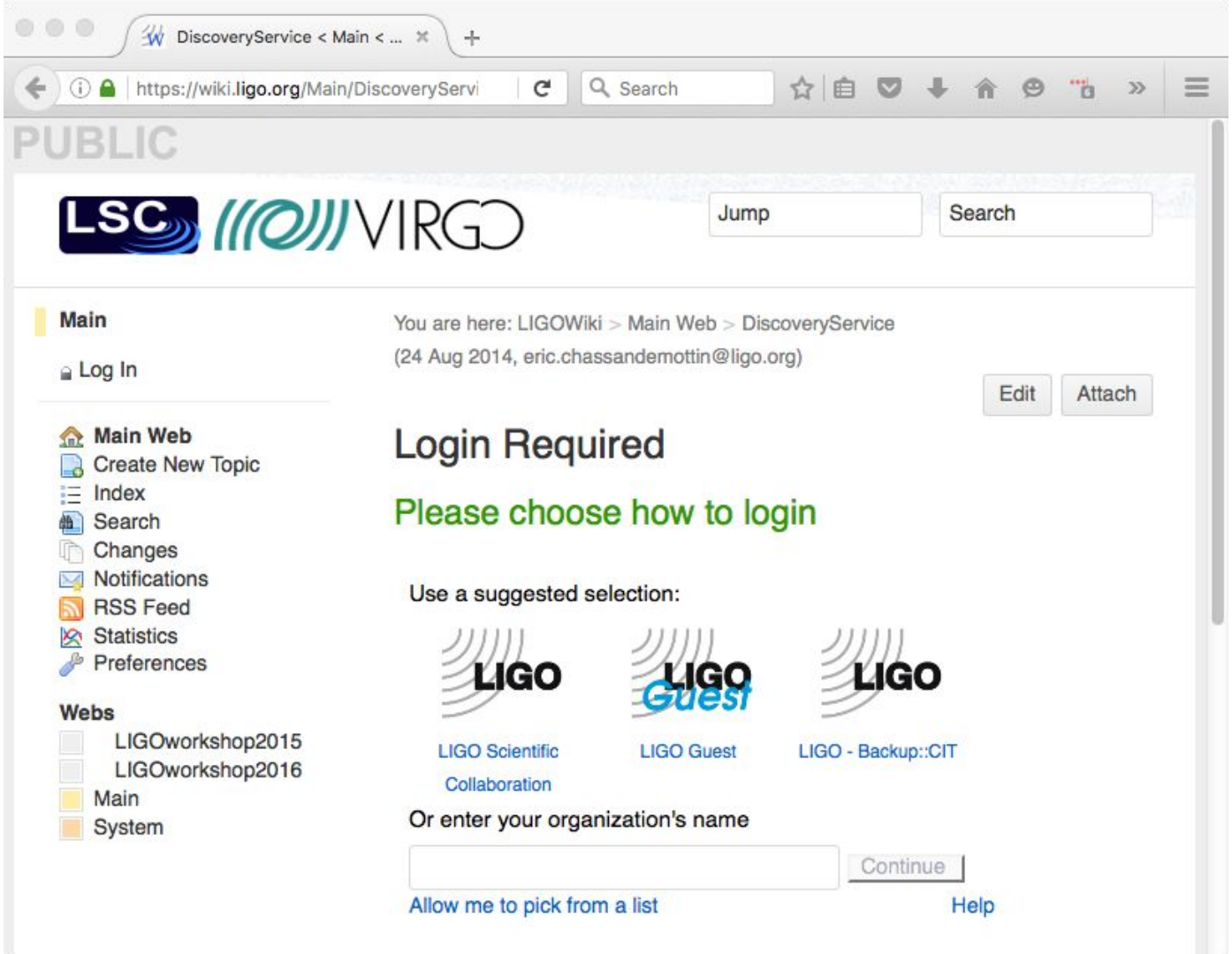
All | eduGAIN | ϕEDUrus | Chile | Nordic countries | Spain | UKfederation | US | Italy | NZ | AU | NL | SAFIRE | Social networks | Guest providers | Miscellaneous

2423 entries

Incremental search...

A. T. Still University
AAF Virtual Home
AAI@EduHr Single Sign-On Service
Aalborg University
Aalto University
Aarhus Basic Health Care College
Aarhus School of Marine and Technical Engineering


ORCID
https://orcid.org/signin
Search
Search
English
ORCID
Connecting Research and Researchers
FOR RESEARCHERS
FOR ORGANIZATIONS
ABOUT
HELP
SIGN IN
SIGN IN
REGISTER FOR AN ORCID ID
LEARN MORE
2,468,959 ORCID iDs and counting. See more...
Sign in using your
Personal Account
Institutional Account
Sign in with your ORCID account
Email or iD
Email or iD
ORCID Password
ORCID Password
Forgotten password?
Sign into ORCID
Sign in with a social media account


DiscoveryService < Main < ...
https://wiki.ligo.org/Main/DiscoveryServi
Search
PUBLIC
LSC
VIRGO
Jump
Search
Main
Log In
Main Web
Create New Topic
Index
Search
Changes
Notifications
RSS Feed
Statistics
Preferences
Webs
LIGOworkshop2015
LIGOworkshop2016
Main
System
You are here: LIGOWiki > Main Web > DiscoveryService
(24 Aug 2014, eric.chassandemottin@ligo.org)
Edit
Attach
Login Required
Please choose how to login
Use a suggested selection:
LIGO
LIGO Guest
LIGO
LIGO Scientific Collaboration
LIGO Guest
LIGO - Backup::CIT
Or enter your organization's name
Continue
Allow me to pick from a list
Help

REFEDS

GÉANT Association (NL) | https://discovery.refeds.org

Search

REFEDS

HOME BEST PRACTICE GUIDE DEMO ABOUT

REFEDS DISCOVERY GUIDE

REFEDS demonstrates the most effective way to present federated identity to users of your site, with best practice and examples of how to provide the best experience.

BEST PRACTICE GUIDE

In just 4 simple steps you can learn the key recommendations from the NISO ESPRESSO report and find out

DISCOVERY DEMO

See a guided demo of how to implement the best practice guide with visual demonstrations of how to, and how not to, use federated login effectively.

IdP Discovery: Research Organizations

Primary question: whether to use a centralized or embedded (per-SP) approach?

Centralized:

- One discovery service leveraged by multiple SPs
- Less operational overhead
- Easier to manage user state
  - "Use a previous choice..."
- Single point of failure
- Can lead to a jarring user experience
  - Switching between the UIs of the application, discovery service, and IdP

IdP Discovery: Research Organizations

Primary question: whether to use a centralized or embedded (per-SP) approach?

Embedded (per-SP):

- Easier to preserve "look and feel" of the application
- Less jarring visual experience for user
- No single point of failure
- More operational overhead
- Harder to manage consistent user experience across organization

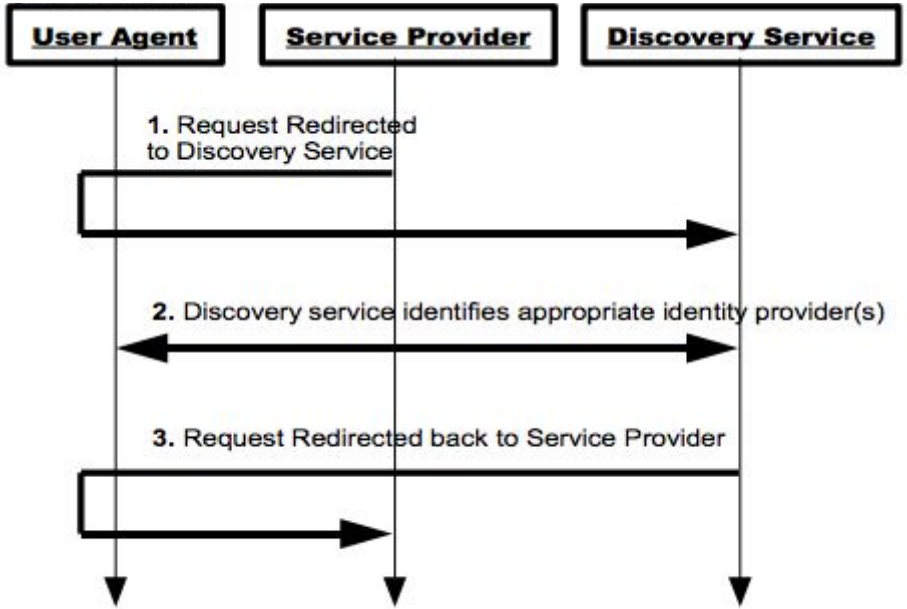
IdP Discovery: SAML Protocol

SP directs browser to discovery service and includes its own entityID

Discovery service may use whatever means it wants to "discover" which IdP to be used

Discovery service redirects back to the SP and includes entityID of the IdP to be used

SP then begins usual SAML Web SSO flow



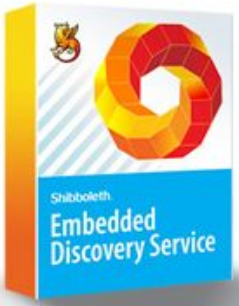
IdP Discovery: Shibboleth EDS

Pairs well with the Shibboleth SP

"Embedded" but often deployed with an un-federated Shibboleth SP and used as a centralized discovery service

Shibboleth

Embedded Discovery Service

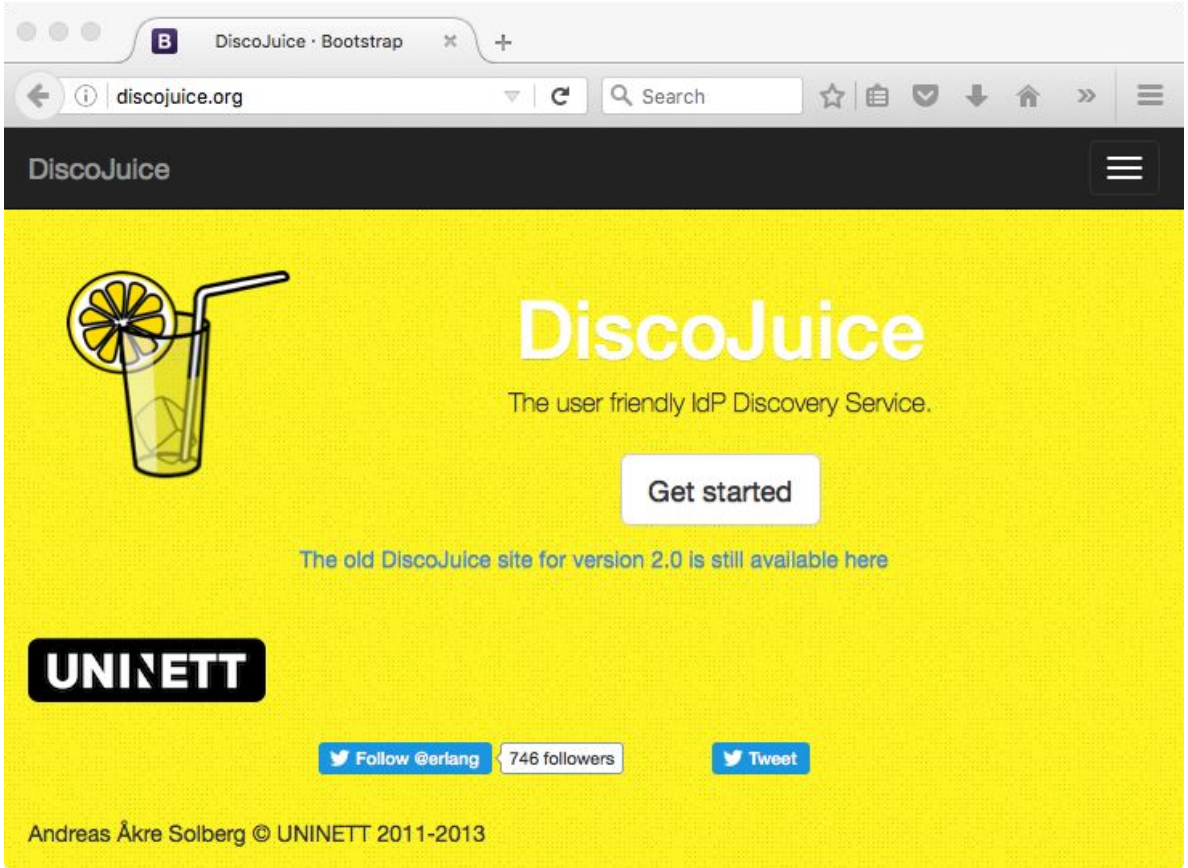


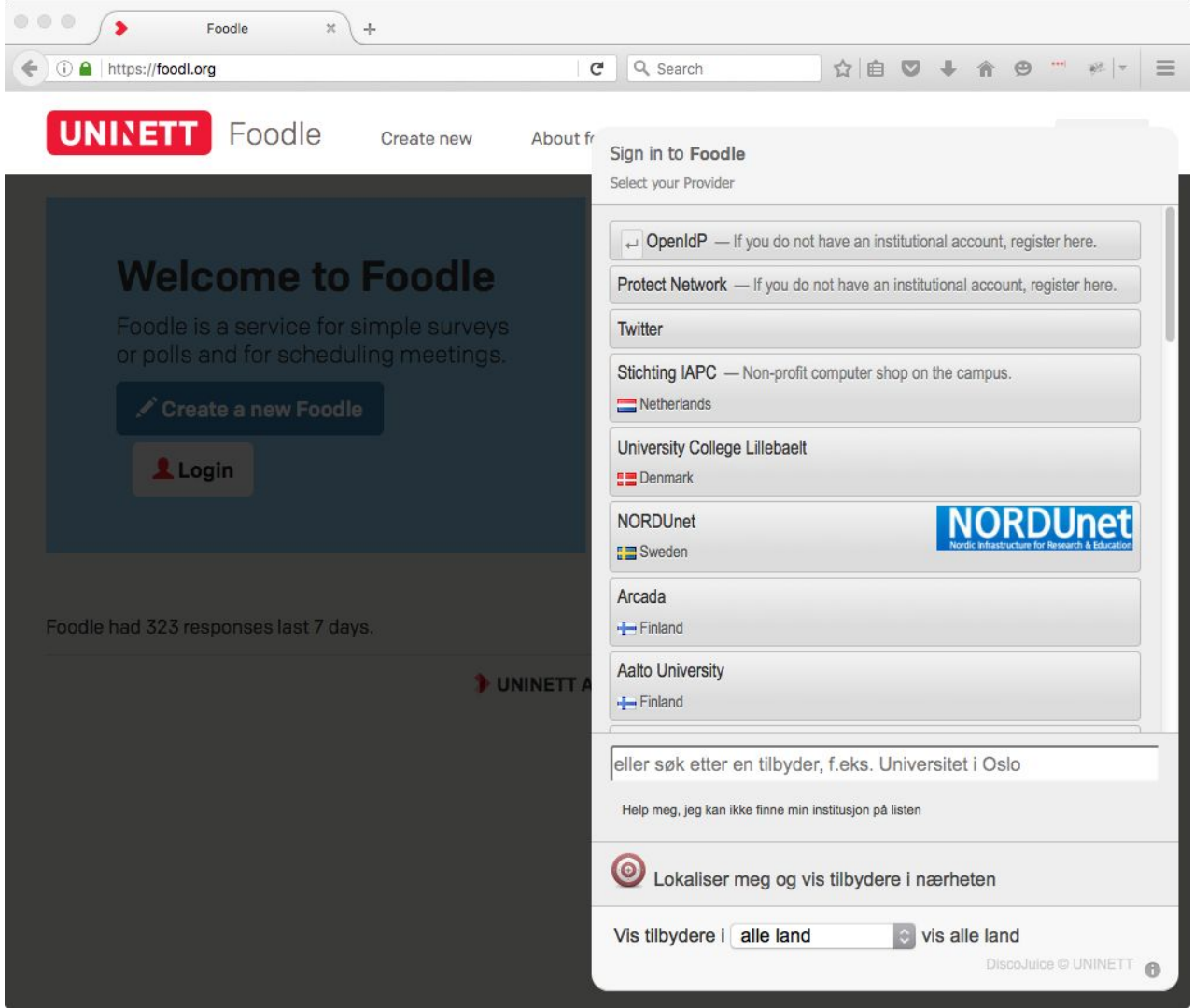
The **Embedded Discovery Service** provides a web interface allowing a user to select which Identity Provider they will use when accessing a Service Provider. This product is co-installed with a Service Provider and allows the discovery service to carry the same UI and branding.

Key Features

- Simple installation and configuration as HTML, Javascript and CSS files are deployed in the same manner as for any given web page on your site.
- Provides a smaller, easier to navigate list of Identity Providers by only presenting those known by your Service Provider.
- Supports assistive technologies such as screen readers.

IdP Discovery: DiscoJuice




Foodle
https://foodl.org
Search
UNINETT
Foodle
Create new
About f
Welcome to Foodle
Foodle is a service for simple surveys or polls and for scheduling meetings.
Create a new Foodle
Login
Foodle had 323 responses last 7 days.
UNINETT A
Sign in to Foodle
Select your Provider
OpenIdP — If you do not have an institutional account, register here.
Protect Network — If you do not have an institutional account, register here.
Twitter
Stichting IAPC — Non-profit computer shop on the campus.
Netherlands
University College Lillebaelt
Denmark
NORDUnet
Sweden
NORDUnet
Nordic Infrastructure for Research & Education
Arcada
Finland
Aalto University
Finland
eller søk etter en tilbyder, f.eks. Universitet i Oslo
Help meg, jeg kan ikke finne min institusjon på listen
Lokaliser meg og vis tilbydere i nærheten
Vis tilbydere i
alle land
vis alle land
DiscoJuice © UNINETT

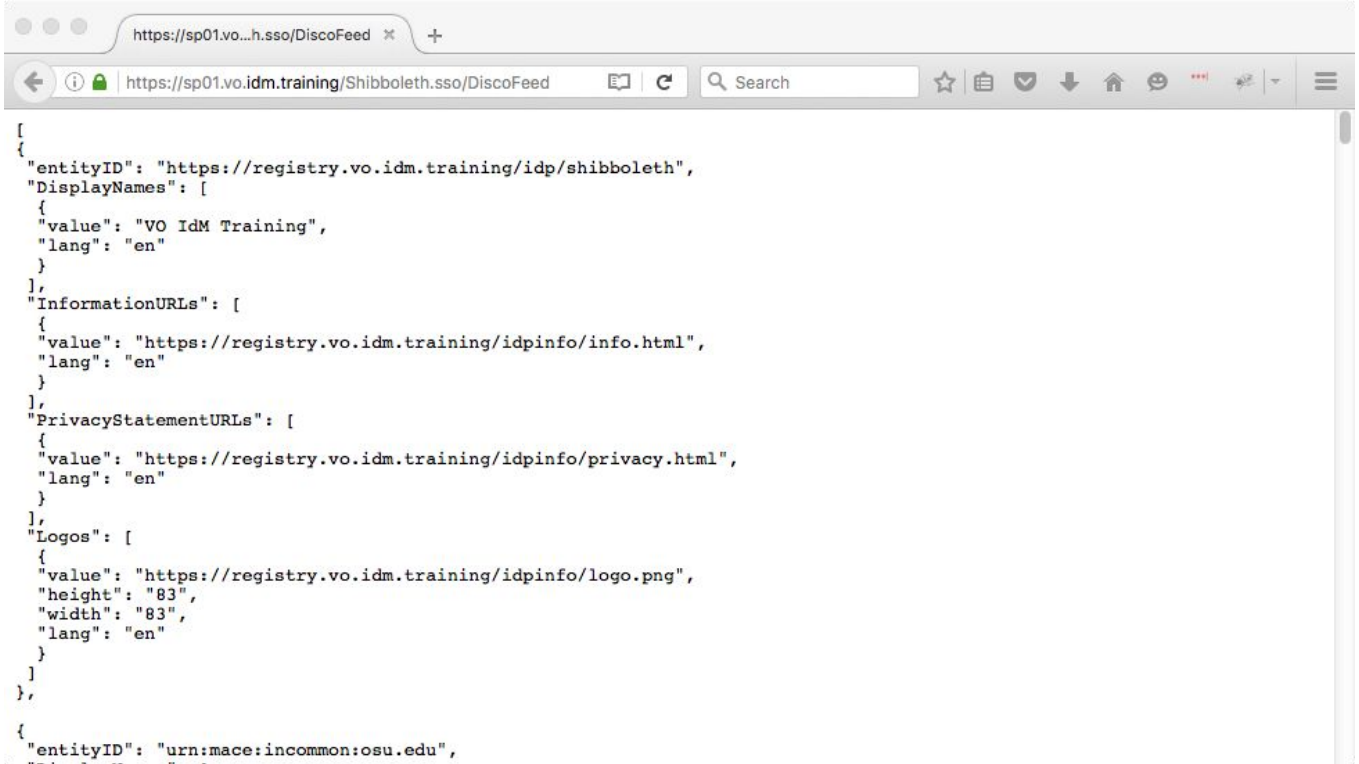
IdP Discovery: Hands-On Exercise

Task

- Verify Shibboleth SP is "federated" with InCommon
- Install the Shibboleth EDS
- Embed the Shibboleth EDS into DokuWiki
- Configure Shibboleth SP to use the discovery service

IdP Discovery: Hands-On Exercise

Browse to https://sp0N.vo.idm.training/Shibboleth.sso/DiscoFeed




```
[
{
 "entityID": "https://registry.vo.idm.training/idp/shibboleth",
 "DisplayNames": [
  {
  "value": "VO IdM Training",
  "lang": "en"
  }
 ],
 "InformationURLs": [
  {
  "value": "https://registry.vo.idm.training/idpinfo/info.html",
  "lang": "en"
  }
 ],
 "PrivacyStatementURLs": [
  {
  "value": "https://registry.vo.idm.training/idpinfo/privacy.html",
  "lang": "en"
  }
 ],
 "Logos": [
  {
  "value": "https://registry.vo.idm.training/idpinfo/logo.png",
  "height": "83",
  "width": "83",
  "lang": "en"
  }
 ]
},

{
 "entityID": "urn:mace:incommon:osu.edu",
```

IdP Discovery: Hands-On Exercise

Install the Shibboleth EDS RPM:

```
yum install shibboleth-embedded-ds
```

Examine the Apache configuration made by the RPM install:

```
less /etc/httpd/conf.d/shibboleth-ds.conf
```

Reload Apache configuration:

```
service httpd reload
```

IdP Discovery: Hands-On Exercise

Examine the EDS deployment directory:

```
ls /etc/shibboleth-ds/
```

Edit idpselect_config.js and set

```
this.testGUI = true;
```

to enable a "testing mode" useful during initial deployment and configuration

IdP Discovery: Hands-On Exercise

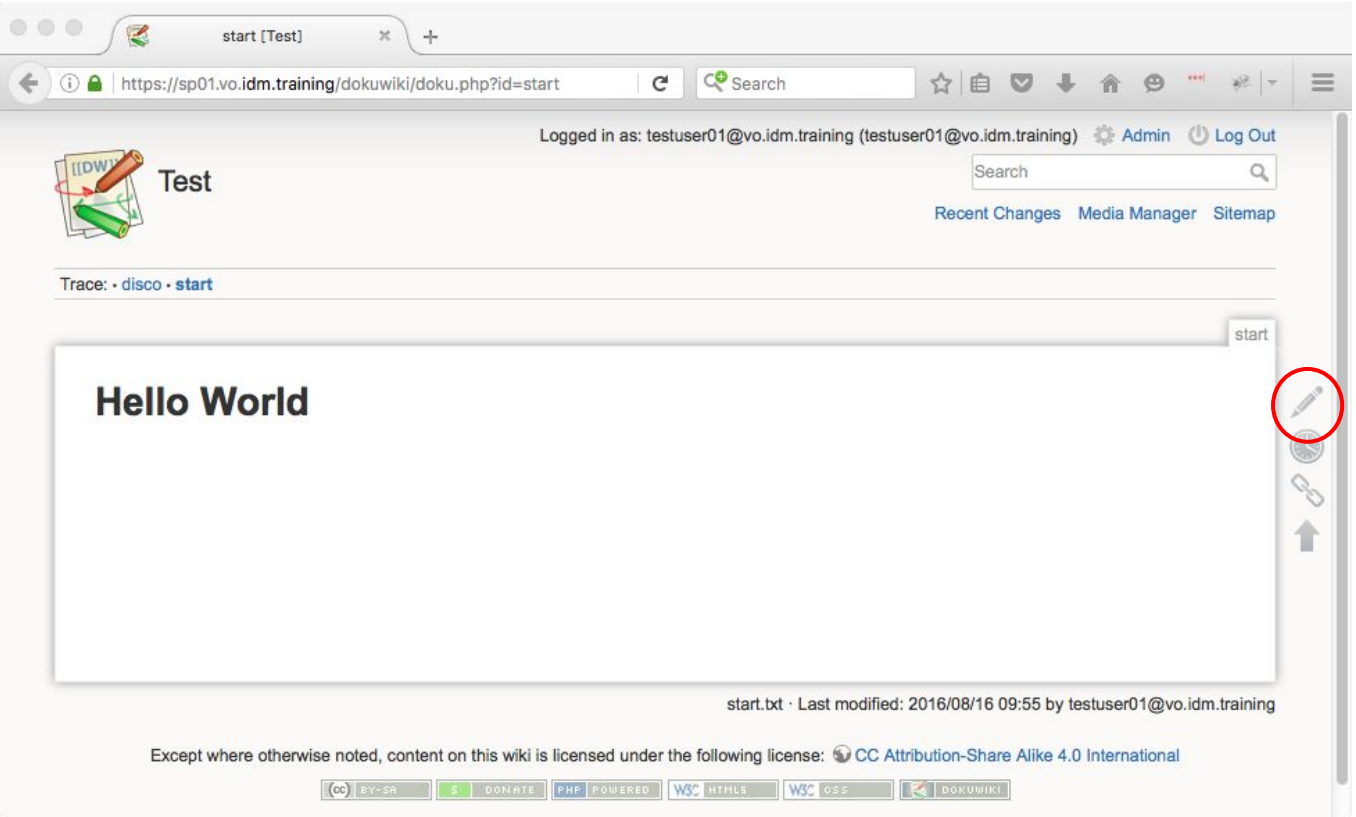
Edit /var/www/html/dokuwiki/conf/local.php and add the line

```
$conf['htmlok'] = 1;
```

to allow embedding HTML into pages

IdP Discovery: Hands-On Exercise

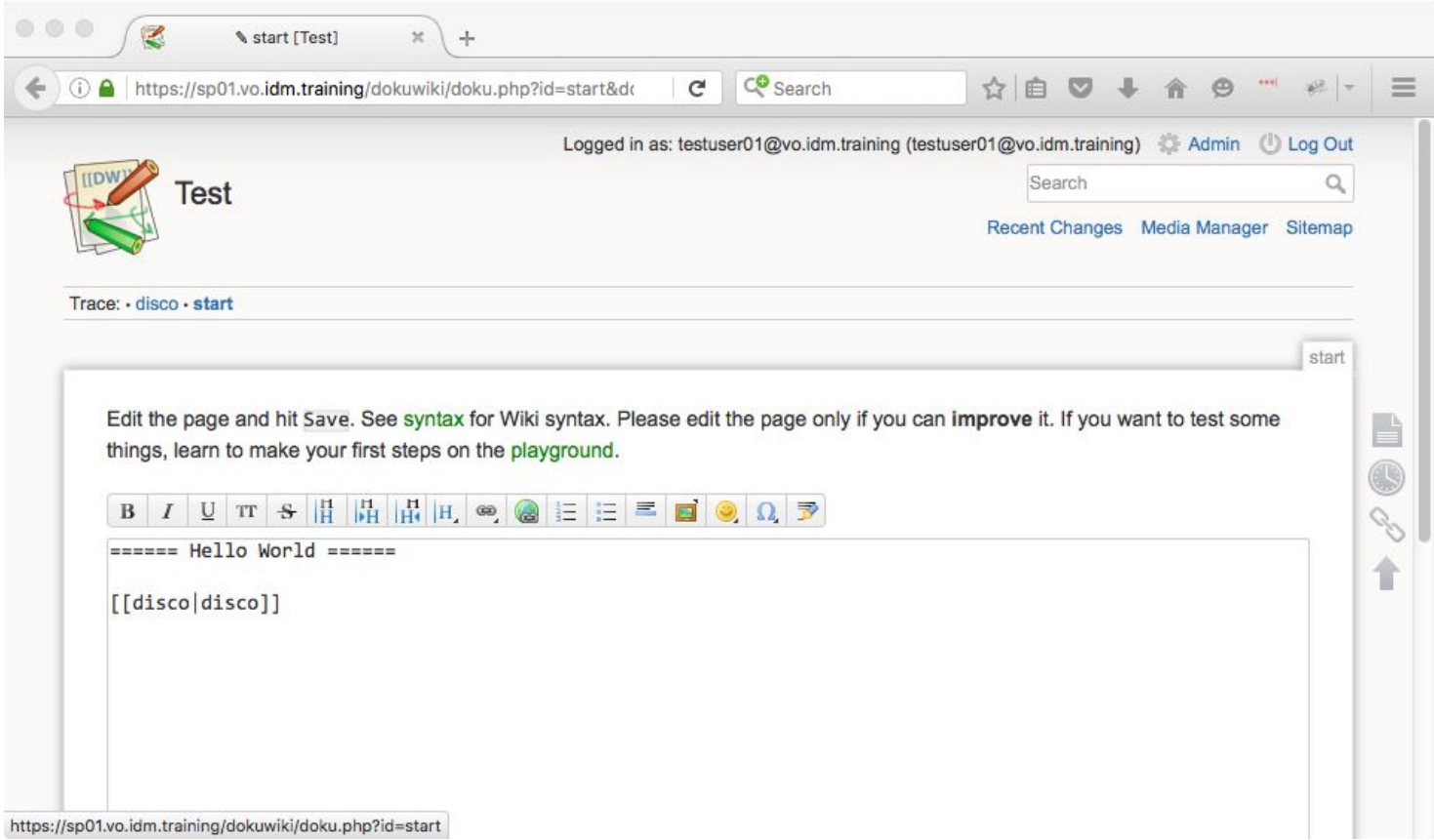
Browse to https://sp0N.vo.idm.training/dokuwiki/ and click "Log In" to log in



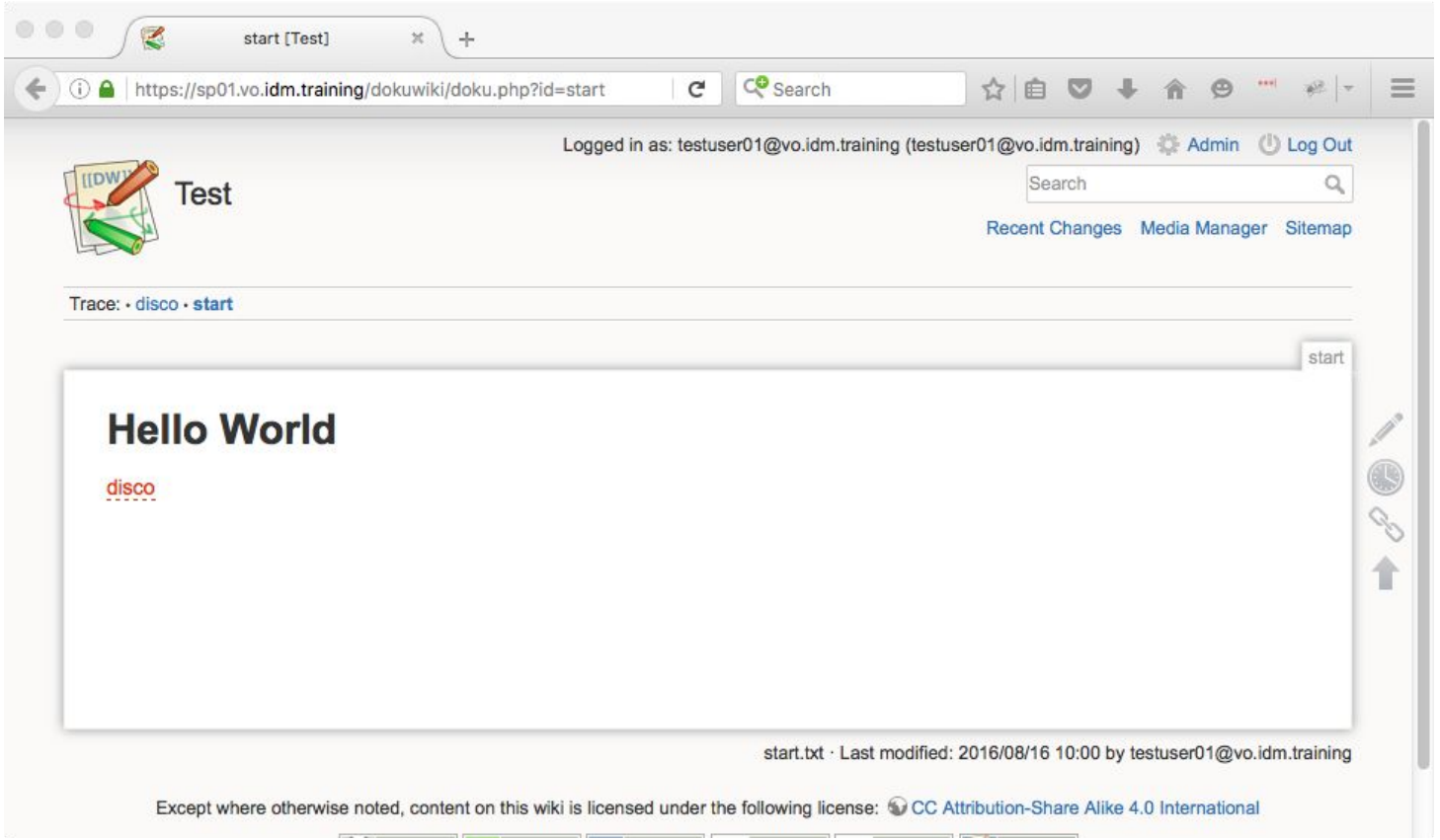
Click the pencil icon and choose "Edit this page"

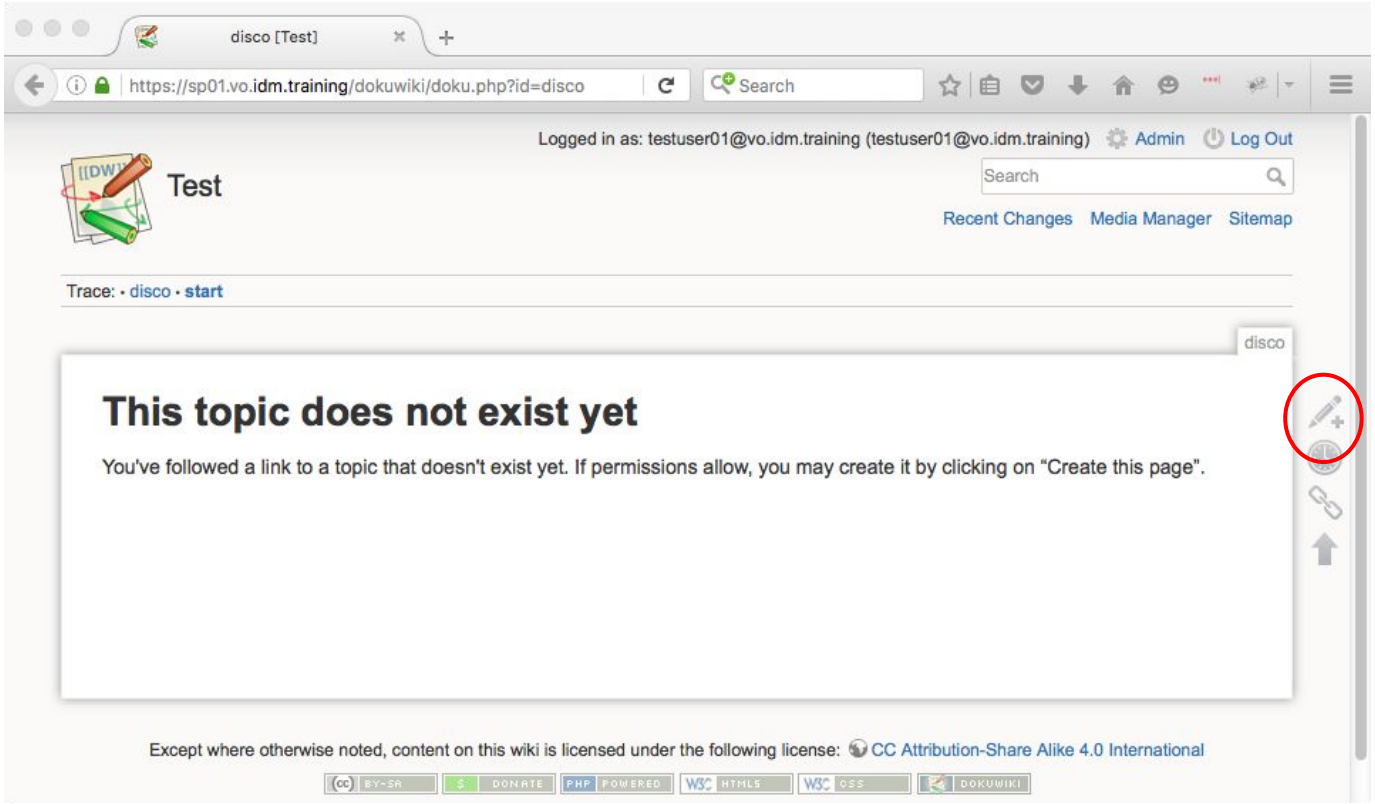
Add a "link" to a new page that does not exist yet to create the new page.

Scroll down and click "Save"



Click on the link just created.



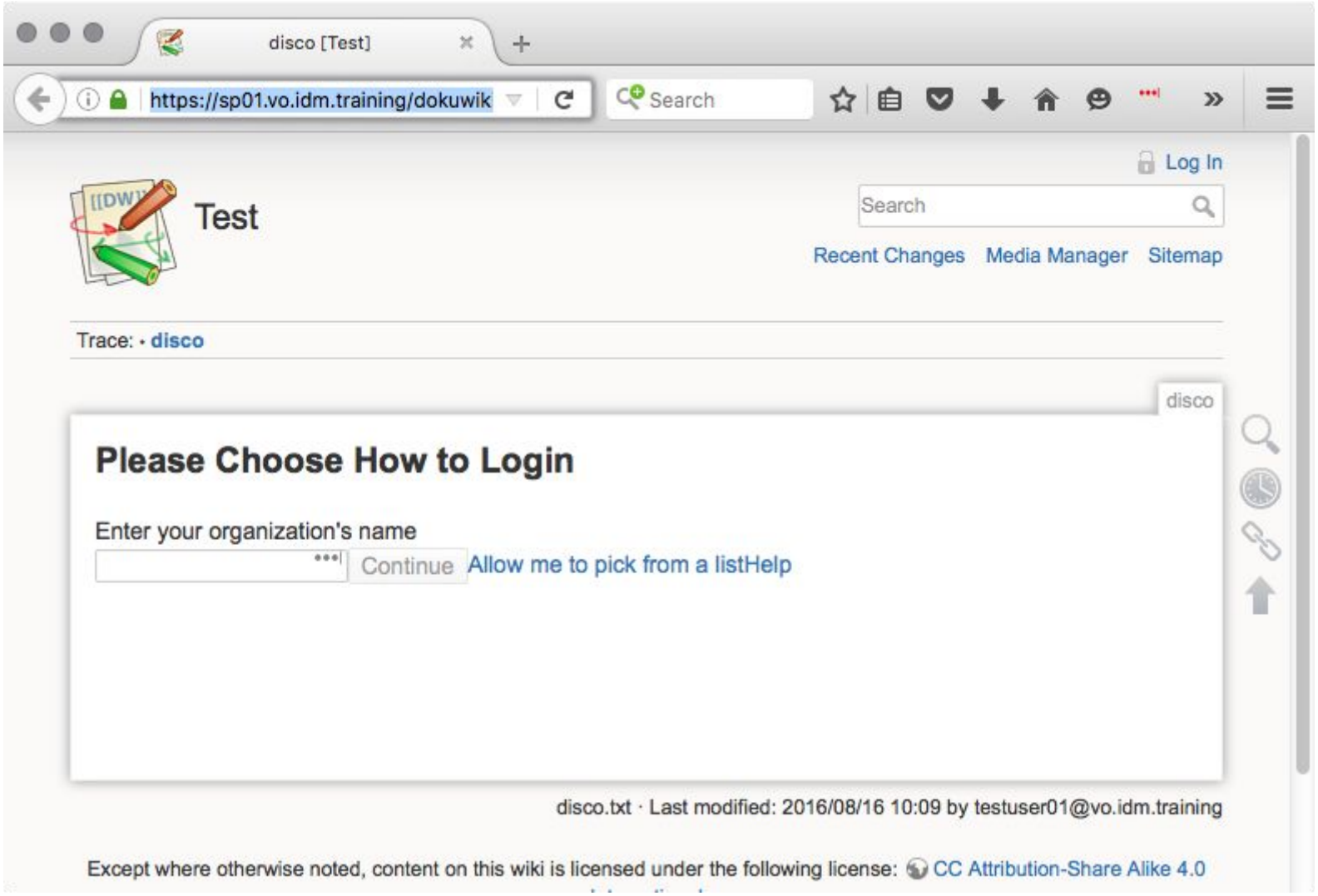


Click on the pencil icon and choose "Create this page".

IdP Discovery: Hands-On Exercise

Add the following wiki text to the page and save:

```
===== Please Choose How to Login =====
<html>
<div id="idpSelect"></div>
<script src="/shibboleth-ds/idpselect_config.js" type="text/javascript" language="javascript"></script>
<script src="/shibboleth-ds/idpselect.js" type="text/javascript" language="javascript"></script>
</html>
```


disco [Test]
https://sp01.vo.idm.training/dokuwik
Search
Log In
Test
Search
Recent Changes
Media Manager
Sitemap
Trace: • disco
disco
Please Choose How to Login
Enter your organization's name
Continue
Allow me to pick from a listHelp
disco.txt · Last modified: 2016/08/16 10:09 by testuser01@vo.idm.training
Except where otherwise noted, content on this wiki is licensed under the following license: CC Attribution-Share Alike 4.0

IdP Discovery: Hands-On Exercise

Edit /etc/shibboleth-ds/idpselect_config.js and set

```
this.testGUI = false;
```

to take EDS out of "testing mode"

IdP Discovery: Hands-On Exercise

Edit /etc/shibboleth/shibboleth2.xml and change

```
<SSO entityID="https://registry.vo.idm.training/idp/shibboleth">
  SAML2
</SSO>
```

to

```
<SSO discoveryProtocol="SAMLDS"
  discoveryURL="https://sp01.vo.idm.training/dokuwiki/doku.php?id=disco">
  SAML2
</SSO>
```

Restart both shibd and httpd

IdP Discovery:Hands-On Exercise

With a fresh browser (no state) browse to

https://sp0N.vo.idm.training/dokuwiki/

and click "Log In" and hoose the IdP to use for authentication

Note that only the "VO IdM Training" IdP will actually work since the other IdPs have no metadata about your SP.

OpenID Connect (OIDC)

OpenID Connect: Introduction

- The third generation of OpenID (after OpenID 1.0 and OpenID 2.0)
- Adopted by Amazon, Google, IBM, Microsoft, and many others
- Authentication layer on top of OAuth 2.0 authorization framework (RFC 6749)
- Adds new token type: ID Token
- Adds new OAuth resource: UserInfo
- Defines standard claims included in ID Token and UserInfo response
- Defines scope values for requesting claims
- Specifications: https://openid.net/connect/

SAML or OIDC?

Gateways mean you don't need to support both in each application.

- OIDC to SAML (e.g., Cirrus)
- SAML to OIDC (e.g., CILogon)

Choose based on application/platform/language support.

SAML and OIDC: Terminology

SAML	**OIDC**
Identity Provider (IdP)	OpenID Provider (OP)
Service Provider (SP)	Relying Party (RP)
Attributes	Claims
Attribute Bundle	Scope
Authentication Assertion	ID Token

OpenID Connect: Standard Claims

- sub

scope: openid

- email
- email_verified

scope: email

- phone_number
- phone_number_verified

scope: phone

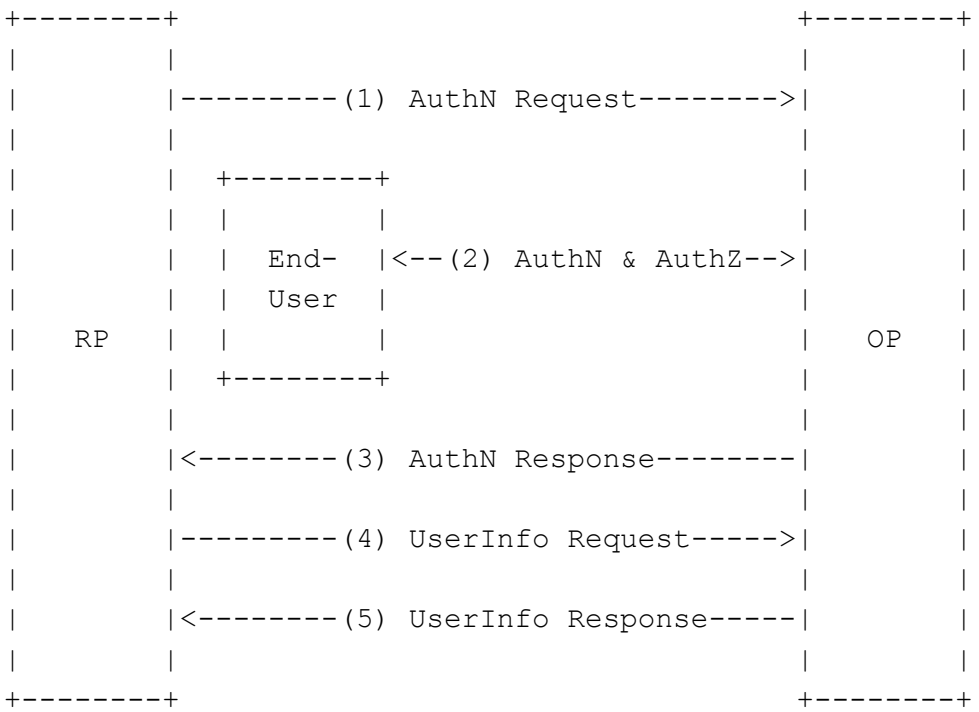
- address

scope: address

- name
- given_name
- family_name
- middle_name
- nickname
- preferred_username
- profile / picture
- website
- gender / birthdate
- zoneinfo / locale
- updated_at

scope: profile

OpenID Connect: Protocol Overview



1. The RP (Client) sends a request to the OpenID Provider (OP).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP can send a request with the Access Token to the UserInfo Endpoint.
5. The UserInfo Endpoint returns Claims about the End-User.

Source:
https://openid.net/specs/openid-connect-core-1_0.html

OpenID Connect: Hands-On Exercise

Task:

- Update SP to use Google OIDC instead of Shibboleth
- See http://sl.cilogon.org/vot

Background:

- We've already registered an OIDC client at https://console.developers.google.com/apis/credentials
- Google OIDC documentation is at https://developers.google.com/identity/protocols/OpenIDConnect
- See also Google OAuth playground at https://developers.google.com/oauthplayground/

OpenID Connect: Hands-On Exercise

Task:

- Demonstrate OIDC claim-based authorization using .htaccess files

Background:

- https://github.com/pingidentity/mod_auth_openidc/wiki/Authorization

OpenID Connect: Protocol Deep Dive

What did mod_auth_openidc do? Let’s reproduce it using curl.

- Initial browser-based AuthN/AuthZ request/response
- Get Access Token and ID Token
- Look inside ID Token
- Use Access Token to get UserInfo

OpenID Connect: Get Access Token and ID Token

```
curl -d grant_type=authorization_code \
     -d client_id=$CLIENT_ID \
     -d client_secret=$CLIENT_SECRET \
     -d code=$CODE \
     -d redirect_uri=$REDIRECT_URI \
  https://www.googleapis.com/oauth2/v4/token

{
 "access_token": "...",
 "token_type": "Bearer",
 "expires_in": 3600,
 "id_token": "..."
}
```

OpenID Connect: Decode ID Token


```
{
  "alg": "RS256",
  "kid": "104625465f6d4c7d214e3326913c5a5e4505699c"
}
{
  "iss": "https://accounts.google.com",
  "at_hash": "rWL5-6yzA1MSqUJ2i15jhw",
  "aud": "...bbqoqbgek8udgtiso3.apps.googleusercontent.com",
  "sub": "118227816977175824694",
  "email_verified": true,
  "azp": "...bbqoqbgek8udgtiso3.apps.googleusercontent.com",
  "email": "jbasney@illinois.edu",
  "iat": 1470926198,
  "exp": 1470929798
}
```


Header

Payload

Source: https://jwt.io/

OpenID Connect: Get UserInfo

```
curl -H "Authorization: Bearer $ACCESS_TOKEN" \
  https://www.googleapis.com/oauth2/v3/userinfo

{
 "sub": "118227816977175824694",
 "name": "John Smith",
 "given_name": "John",
 "family_name": "Smith",
 "profile": "https://plus.google.com/118227816977175824694",
 "email": "jsmith@example.edu",
 "email_verified": true
}
```

OpenID Connect: Hands-On Exercise

Task:

- Update SP to use CILogon (a SAML to OIDC gateway)

Background:

- CILogon (https://cilogon.org/) provides a SAML-OIDC gateway
- Enables use of InCommon identity providers with OIDC applications

OpenID Connect: Federation

- Apply Federation Trust Model to OpenID Connect
  - Provide integrity for exchange of OP and RP security parameters
  - Independent of TLS trust
  - https://lists.geant.org/sympa/info/oidc
- REFEDS OpenID Connect for Research and Education (OIDCre) WG
  - Mapping between eduPerson and OIDC claims
  - https://wiki.refeds.org/display/GROUPS/OIDCre

OpenID Connect: Review

- The third generation of OpenID (after OpenID 1.0 and OpenID 2.0)
- Adopted by Amazon, Google, IBM, Microsoft, and many others
- Authentication layer on top of OAuth 2.0 authorization framework (RFC 6749)
- Adds new token type: ID Token
- Adds new OAuth resource: UserInfo
- Defines standard claims included in ID Token and UserInfo response
- Defines scope values for requesting claims
- Specifications: https://openid.net/connect/
- SAML-OIDC / OIDC-SAML gateways provide interoperability

Questions? Comments?

Introduction to Collaboration Management

Collaboration Management: Introduction

How does the VO collect IdP asserted identifiers/attributes and associate that with a group structure the VO manages and cares about?

- Enrollment
- Identity Linking
- VO-specific attributes
- Group memberships
- Role assignments
- Application Authorization

A collaboration-management platform can fill this need.

Collaboration Management: Enrollment

Challenge: You don’t know the user’s federated identifier.

- Email-based invitation
- Web-based “petition” for enrollment

Collect additional VO-specific attributes at enrollment time.

- Policy acknowledgements
- Attributes not provided by IdP (e.g., research affiliations)

Implement VO-specific review/approval workflows.

Collaboration Management: Identity Linking

VO members may have multiple identities:

- Campus identities (may change over time)
- Cloud identities (Google, GitHub, etc.)
- Scholarly identities (e.g., ORCID)

An identity linking workflow prompts users to authenticate with multiple identities so they can access VO systems with either those identities.

Collaboration Management: Scalable Access Control

Per-application access control lists have scalability limits.

VO applications can leverage centrally-managed VO groups/roles:

- Exported via LDAP, SAML, OIDC, etc.

Management of groups/roles can be distributed according to VO responsibilities.

Collaboration Management with COmanage

COmanage

- Developed by InCommon/Internet2
- Initial support from National Science Foundation grant
- Use cases and input from research organizations

https://spaces.internet2.edu/display/COmanage/Home

COmanage Registry

Focused on managing federated identities:

- Enrollment (onboarding and offboarding)
- Group management
- Identifier management
- Identity linking
- Provisioning

Support for the entire lifecycle of federated identity management challenges faced by collaborative organizations like research organizations.

(CO = Collaborative Organization)

COmanage Registry People Types

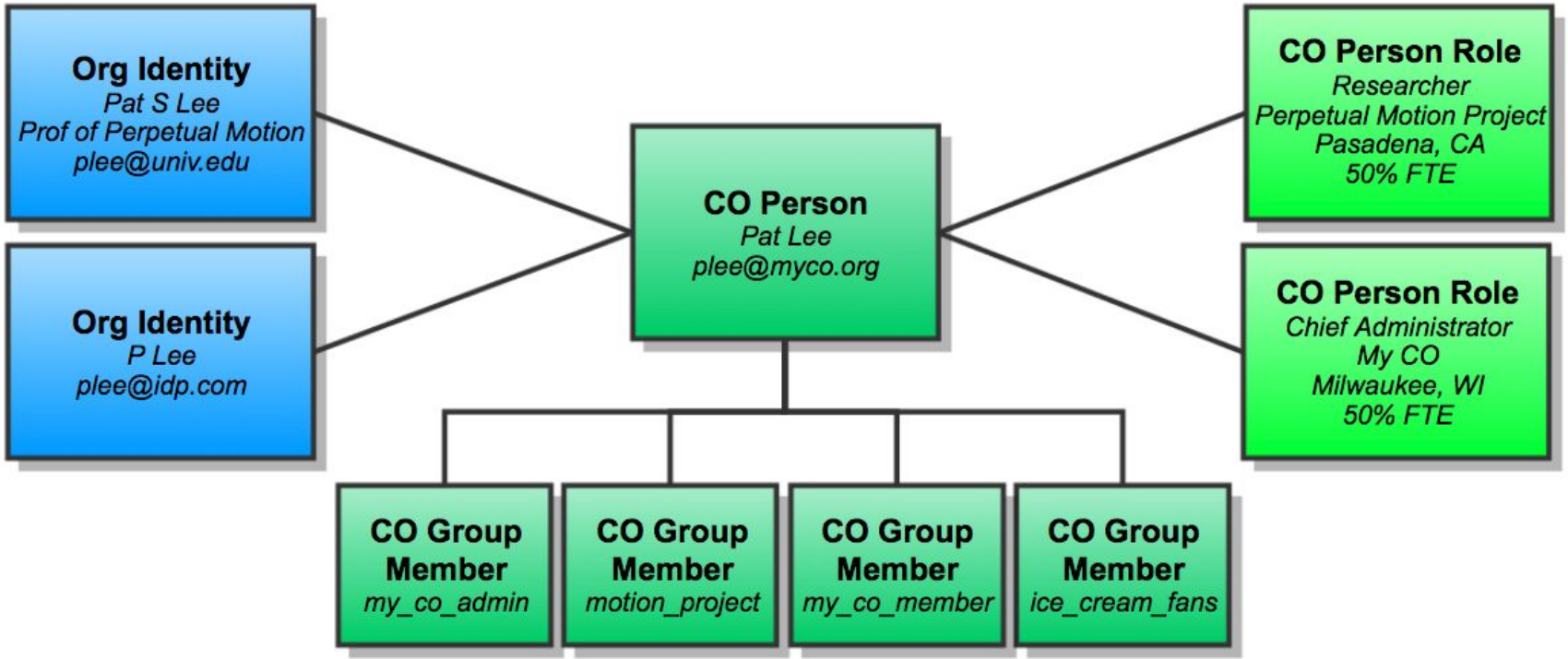
- COs are "virtual" collections of people
- These people authoritatively come from "real" institutions
- Registry tracks these identities using two different types of records:
  - Organizational Identity describes a person's relationship with their "real" institution
    - such as their home university
  - CO Person describes the person's relationship with their CO (i.e., their virtual organization)
- Person can have more than one relationship with their CO
  - Each of these relationships is referred to as a CO Person Role
- Organizational Identity is associated with a credential
  - usually described via an Identifier such as an ePPN from a University
  - When logging into COmanage the authenticated identifier used to find Organizational Identity records, which in turn are used to find CO Person records

COmanage Registry People Types

Example:

Organizational Identity	Pat Lee Central University Professor
CO Person	Pat Lee Earth Research Collaborative
CO Person Role #1	ERC Senior Researcher
CO Person Role #2	ERC Council Member

COmanage Registry People Types

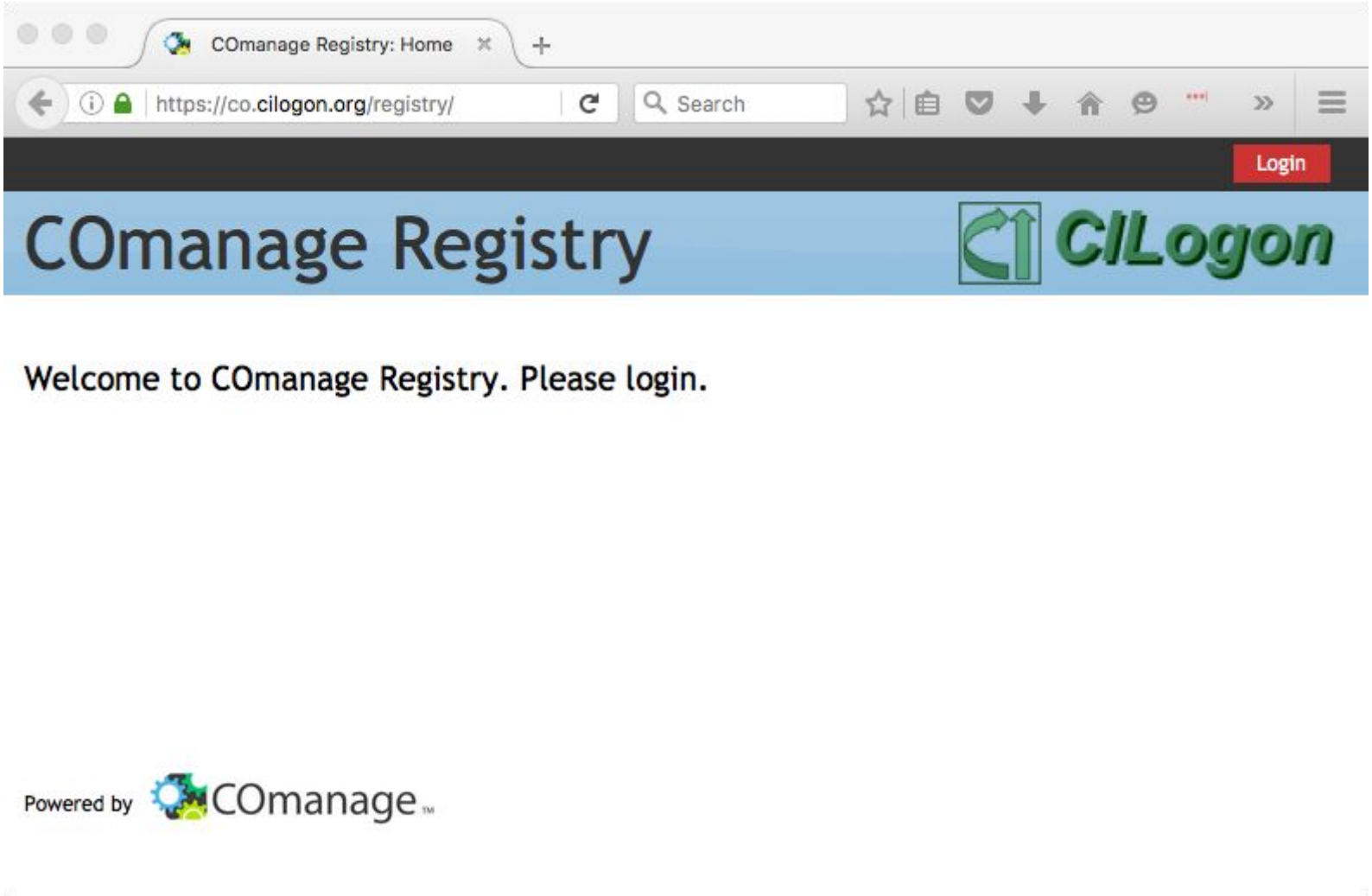


COmanage Registry Administrators

1. Platform (CMP) Administrators
    - Effectively super users
    - Perform almost all operations on the platform
    - Configured by adding the appropriate Organizational Identity to the COmanage CO, and then adding the corresponding person to the admin group within the COmanage CO
    - First user added as part of the Registry Setup Script is automatically configured to be a Platform Administrator
2. Collaboration (CO) Administrators
    - Super users within a CO
    - Collaboration Administrators configured by adding the appropriate Organizational Identity to the CO (if not already done), and then adding the corresponding person to the admin group within the CO

COmanage Registry Administrators

3. Unit (COU) Administrators
    - Collaboration Administrators with sophisticated administrative requirements may optionally define Unit Administrators
    - Unit Administrators have limited privileges within the CO, generally related to the ability to enroll and manage populations within the CO Unit (COU)
    - Configured by adding the appropriate Organizational Identity to the CO (if not already done), and then adding the corresponding person to the admin:COU-Name group within the CO
4. Enrolled users
    - Members of a CO (and possibly a COU)
    - No special privileges


COmanage Registry: Home
https://co.cilogon.org/registry/
Search
Login
COmanage Registry
CILogon
Welcome to COmanage Registry. Please login.
Powered by COmanage