Dr. Shibblelove: How I Learned to Stop Worrying and Implement Single-Sign On

11-1-2015

Athena Hoeppner
University of Central Florida, athena@ucf.edu

Adam Traub

Find similar works at: https://stars.library.ucf.edu/ucfscholar

University of Central Florida Libraries http://library.ucf.edu

Part of the Library and Information Science Commons

STARS Citation

Hoeppner, Athena and Traub, Adam, "Dr. Shibblelove: How I Learned to Stop Worrying and Implement Single-Sign On" (2015). Faculty Scholarship and Creative Works. 810.
https://stars.library.ucf.edu/ucfscholar/810

This Conference Presentation is brought to you for free and open access by STARS. It has been accepted for inclusion in Faculty Scholarship and Creative Works by an authorized administrator of STARS. For more information, please contact lee.dotson@ucf.edu.
How I Learned to Stop Worrying and Implement Single-Sign On

LITA Forum | Minneapolis, MN | 12-15 November 2015

Athena Hoeppner
University of Central Florida

Adam Traub
University of Rochester
Login: A User’s Perspective

Researcher → Credentials

Federated ID
User ID: John
Password: ****

Shibboleth

Access

Canvas
Authentication Part I

Hey UCF Shibboleth, check this guy for me.

Hi Canvas. I'll check his credentials.

Service Provider

Answer this or you shall not pass!
Do you know a guy with these credentials?

I can authenticate him.

Here is his NameID and some assertions.

SAML
Security Assertion Markup Language

https://www.samltool.com/generic_sso_res.php
Authorization

About that guy...

These assertions tell you some of his attributes.

His NameId is Johnd, an authenticated UCF EduPerson with PrimaryAffiliation Faculty.

Okay. Users with those attributes are authorized access for and faculty get extra permissions.
Here’s your page.

...and have a cookie

He gets an IDP cookie, too.

UCF Canvas
Hello John D

Your courses: LIT321 Mythologies in Genre Fiction...
One Login; Many Services

UCF

Single Sign On (SSO)

Credentials
InCommon Federation

UCF Entity

ProQuest Entity

UR Entity

EBSCO Entity

Federated ID
Entity and Service Examples

Service Providers (SPs)
- UCF Canvas
- UCF HR
- Subcription Database

ID Providers (IdPs)
- UCF LDAP
- UCF Active Directory

EntityIDs: Unique Identifiers
- https://auth.yale.edu/idp/shibb
- http://qapub1.imodules.com/sp
In theory, any of these SPs could authorize based on attributes from any of these IdPs.
Tales of Three Shibboleth Service Providers
Lynda’s Tale

• Previously logged in via IP
• Couldn’t tell who was using it
• Shibboleth already used for other campus services
• Shibb login allows users to track progress
HathiTrust’s Tale

• Membership requirements:
  • Academic and research Institution
  • Paid fee
  • Shibboleth for authentication

• Benefits:
  • Complete PDF download
  • Access to in-copyright material if owned by university
Ezproxy’s Prologue

- IP authentication widely used by vendors
- Existed separately from campus federated ID and single sign on
- Familiar to users
- Extend campus single sign-on experience for database and journal access
Relationship Building

Identity Management
Access!
Data!
Functional Anecdote

E-Res Librarian
Role: Cheerleader; Project Manager; Requirements Co-Creator

Library IT
Role: Facilitator; Co-Creator; Internal Advisor

Central IT
Role: Shibboleth Admin; Attribute Mapper

Vendor IT
Role: Service Provider; External Advisor
An attribute is simply a name-value pair providing single piece of information. Some subset of all attributes defines a unique individual.
Shibboleth and EduPerson

“Shibboleth is a standards based, open source software package for web single sign-on across or within organizational boundaries.”

EduPerson Schema

• Supports LDAP Environments
• Familiar Attributes
  ✓ CommonName
  ✓ Surname/Family Name
  ✓ Email
  ✓ UserID

I have one of each of those attributes!
EduPerson Schema - Affiliations

**eduPersonAffiliation**

“broad category affiliations”

Examples:

- Faculty
- Staff
- Student
- Alum
- Employee
- Member
- Affiliate
- Library-Walk-in

I graduated from this place AND I work here as Faculty!
eduPersonPrimaryAffiliation

“Think of this as the affiliation one might put on the name tag if this person were to attend a general institutional social gathering.”

• Must also appear in eduPersonAffiliation

✓ Faculty (mostly)
EduPerson Schema - Affiliations

**eduPersonScopedAffiliation**

“Specifies the person's affiliation within a particular security domain in broad categories.”

HathiTrust requires Scoped Affiliation

Example:

What is Athena’s affiliation to UCF, as translated by HathiTrust?

faculty@ucf.edu
Gollum the Freshman

1. Precious wants your database.
2. Do you know this person?
3. I need you to login.
4. UN Precious; PW: Precious
5. That’s Gollum; he’s a student.
Frodo the Alumnus

1. I'd like to use your database.
2. Do you know this person?
3. I need you to login.
4. UN Fbaggins; PW: i<3Sam
5. That's Frodo; he's an alum.
6. Your license doesn't allow alum access.
Saurman the Forgetful (or Malicious)

1. I’d like to use your database.
2. Do you know this person?
3. I need you to login.
4. UN: SauronRules; PW: friend?
5. I have no idea who this is.
6. Not with that attitude (or login) you won’t.
WAYFless URL Authentication

Login as per usual...

WAYFless URL

IdP already identified

LDAP
Wraithless URLs

WAYFless
Chocolate and red wine—A comparison between flavonoids content

FA Pimentel, JA Nitzke, CB Klipel, EV de Jong - Food chemistry, 2010 - Elsevier

Cocoa has also been described as being a good source of flavonoids, such as catechins. ... Based on this, the present study was carried out to compare flavonoid content of different types of red wine and chocolate and to suggest a daily chocolate ingestion dose that could ...
You are a Guest.  Sign In

Chocolate and red wine—A comparison between flavonoids content

OH NO...
HAVE A...

BUT THE MORDOR UNIVERSITY LIBRARY SHOULD HAVE THIS...

EV de
I don’t even know where to begin checking his credentials. Better make small talk...

So... where are you from?
Choose your region or group and institution below to login.

Region or Federation: Mordor

Institution: Nazgul Group

This should get me access.
I demand the article on chocolate and wine!

Where are you from?

I'm with the Nazgul!

OK. Read up!

Do you know this person?

That's Nazgul King; he's Sauran's lieutenant.

UN: NazgulKing;
PW: Immort@l

Login.
Access to Everything Else...
Ezproxy as a Shibboleth Service Provider
Library Vendors in InCommon Federation:

- Hathi Trust
- EBSCOhost
- ProQuest
- EBL
- Elsevier
- JSTOR
- ...and many more

https://spaces.internet2.edu/display/inlibrary/targetresources
https://spaces.internet2.edu/display/inlibrary/registryofresources
InCommon Best Practices for Libraries

✔ Implement authorization via eduPerson attributes
✔ Shibboleth enable EZproxy
✔ Implement WAYFless URLs
✔ Implement authenticated direct links to resources.
  • Use Shibboleth-Ready Ezproxy Starting point URLs

https://spaces.internet2.edu/display/inclibrary/Best+Practices
EZproxy config.txt

#### Shibboleth Stuff

ShibbolethDisable 1.3
ShibbolethMetadata \n  -EntityID=LibraryEZProxy
  -File=ucf-prod-metadata.xml \n  -Cert=4 \n  -URL=https://idp-prod.cc.ucf.edu/idp/shibboleth

SP Entity name!

UCF's IdP Entity!
EZproxy Admins

if auth:urn:oid:1.3.6.1.4.1.5923.1.1.1.6 eq "LibITGuy@ucf.edu";
Admin

Deny Access to Problem Users

if auth:urn:oid:1.3.6.1.4.1.5923.1.1.1.6 eq "BadUser@ucf.edu";
Deny

Set EZproxy username to UCF ID

set login:loguser = urn:oid:1.3.6.1.4.1.5923.1.1.1.6
<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Formal Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>eduPersonScopedAffiliation</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.9</td>
</tr>
<tr>
<td>eduPersonPrincipalName</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.6</td>
</tr>
<tr>
<td>eduPersonEntitlement</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.7</td>
</tr>
<tr>
<td>eduPersonTargetedID</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.10</td>
</tr>
<tr>
<td>sn</td>
<td>urn:oid:2.5.4.4</td>
</tr>
<tr>
<td>givenName</td>
<td>urn:oid:2.5.4.42</td>
</tr>
<tr>
<td>displayName</td>
<td>urn:oid:2.16.840.1.113730.3.1.241</td>
</tr>
<tr>
<td>mail</td>
<td>urn:oid:0.9.2342.19200300.100.1.3</td>
</tr>
</tbody>
</table>

InCommon Federation Attribute Summary
https://www.incommon.org/federation/attributesummary.html
Shibuser.txt Revisited

if `eduPersonPrincipalName` equals `thisperson` then give them admin rights

if auth:urn:oid:1.3.6.1.4.1.5923.1.1.1.6 eq "LiblTGuy@ucf.edu";

Admin

if `eduPersonPrincipalName` equals `thisperson` then deny them access

if auth:urn:oid:1.3.6.1.4.1.5923.1.1.1.6 eq "BadUser@ucf.edu";

Deny

Set login to user’s `eduPersonPrincipalName`

set login:loguser = urn:oid:1.3.6.1.4.1.5923.1.1.1.6
EZproxy Shibb URLs

- EZproxy Starting Point URLs
  https://login.ezproxy.net.ucf.edu/login?url=

- Shibbbolized

- UCF Deployed in:
  - SFX
  - EBSCOhost Discovery
  - LibGuides and Database list
Too Permissive!

Everyone I know is an EduPerson!

- Current students
- Faculty
- Employees
- Alumni
- Previous students
- Department network accounts...

YIKES!!!

That's good enough for me.

LDAP

EZproxy
Based on this doc, Implementing the Shibboleth - EZproxy Hybrid - InCommon, I think we need to add this to our shibuser.txt:

If
!

I assume that our IdP is set up with the standard **common-lib-terms entitlements**. If not, then we should ask Matt and his crew to add it.
The **common-lib-terms** entitlement value represents the members of an institution that are included in the terms of a typical library contract with a library resource provider.
Getting EZProxy Out of the Way

• Challenges
  • Out-dated EZProxy links
  • Leverage service provider Shibb support

• SPUEdit
  • “Rarely used directive”
  • Best Practice

Summary

- Shibboleth enables
  - Single sign on across institution and federation services
  - Seamless user experience
  - Customized services based on attributes,
  - Personalized services for individuals,
  - Anonymity

Requires collaboration:
- Campus IT
- Library IT
- eResources Librarians

- Works with and expands on Ezproxy, IP-based, authentication
<table>
<thead>
<tr>
<th>Additional Resources</th>
<th>Implementation Info</th>
<th>Vendor Specific Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• InCommon Library Collaboration</td>
<td>• EZProxy</td>
</tr>
<tr>
<td></td>
<td>• Registry of Resources</td>
<td>• EBSCO</td>
</tr>
<tr>
<td></td>
<td>• Shibb Training</td>
<td>• ProQuest</td>
</tr>
<tr>
<td></td>
<td>• Shibb – EzProxy Hybrid</td>
<td>• JSTOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ACM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Elsevier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ovid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Project Muse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Thomson</td>
</tr>
</tbody>
</table>
Glossary

- **Assertion** - The identity information provided by an Identity Provider to a Service Provider.
- **Attribute** - A single piece of information. Some attributes are general; others are personal. Some subset of all attributes defines a unique individual. Examples of an attribute are name and enrollment.
- **Attribute statement** - asserts that a subject is associated with certain attributes. An attribute is simply a name-value pair. Relying parties use attributes to make access-control decisions.
- **Authentication statements** - statement that the principal did indeed authenticate with the identity provider at a particular time using a particular method of authentication.
- **Authorization decision statement** - asserts that a subject is permitted to perform action A on resource R given evidence E.
- **eduPerson** - An LDAP object class to facilitate inter-institutional applications
- **Provider url, and the network administrator.**
- **EntityID** - ID that identifies an enterprise in a federation. Usually a URL that points to an XML file of info about the entity, such as the ID
- **Federated identity** - management of identity information between members of a federation.
- **Identity Provider (IDp)** - The system that authenticates an entity
- **Security Assertion Markup Language (SAML, pronounced sam-el)** is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. (Wikipedia)
- **Service Provider (Sp)** - makes online resources available to users based in part on information about them that it receives from other InCommon participants.
- **Where Are You From (WAYF)** - A server used by the Shibboleth software to determine what a user's home organization is.

Questions?
Thank you!

Athena Hoeppner, UCF
Adam Traub, UR