Shibbolized EZproxy

Model Name :

Shibbolized EZProxy

Description of the Assumed Model:

A library is running a combination of EZProxy and Shibboleth with a flow for interaction between library patron and EZproxy.

EZP has three distinct phases of processing:

1. Is the site Shib-enabled? If yes, always redirect directly to the site, bypassing the next two phases.
2. EZP triggers the locally configured authentication mechanism
    a. EZP access control (based on groups, etc configured into EZP; grant/deny access)
3. The traditional proxy.

Assumption is that the local Shib IdP has optionally been configured to allow authN by both

- people managed by the campus IdM system, and
- people who only appear in the campus ILS system.

The browser user has a variety of possible "launch points" that may take them to the external resource provider. For Shib-enabled sites, the flow will vary, depending on the user's starting point. The list of possible starting points includes: go directly to the site, use a campus maintained navigation page (ex. http://dl.lib.brown.edu/eresources/index.php?task=alpha&ltr=S); a campus maintained gateway of some sort (ex. metalib); a course home page in an LMS; a google search.

Note: The walk-in case is ignored in all of the use case models listed below because it is described in greater detail as part of an assumed model type.

Model Use Cases (Basic) :

1. Use Case Name :

- EZProxy Access with No Shibboleth, No physical location restrictions

Use Case Description :

- Library website contains a directory of the various services which uses an EzProxy login link for external users which proxies the entire library site, allowing users to use resources through the proxy. This leverages the default EzProxy login.
- access to an SSO protected resource from
  -- on campus
  -- off campus (ie. from home, while travelling)

Primary actor(s) :

- Member of the community (sometimes referred to as a Library Patron, but that term sometimes has a narrower meaning).

User Type :

- Administrator, Editor, End User (Primary actor)

Technology Type :

- N/A

Vendor Type :

- N/A

Precondition :

Trigger :

- Patron attempts to access restricted resource

Basic flow :

- Via web browser, patron attempts to access resource. Access to resource is granted.

2. Use Case Name:

- EZProxy Access with Shibboleth, No physical location restrictions

Use Case Description:

- access to a resource protected by EZP (and not by Shibboleth) from
  -- on campus
  -- off campus (ie. from home, while travelling)

Primary actor(s):

- Member of the community (sometimes referred to as a Library Patron, but that term sometimes has a narrower meaning).

User Type:

- Administrator, Editor, End User (Primary actor)

Technology Type:

- N/A

Vendor Type :

- N/A

Precondition :

Trigger :

- Patron attempts to access restricted resource

Basic flow :

- Via web browser, patron attempts to access proxy-protected resource. By virtue of AuthZ authentication process, access to resource is either granted or denied. Ultimately, services would be affiliated with a federation [InCommon] and we could bypass the proxy login entirely.

3. Use Case Name :

- EZProxy Access with No Shibboleth, physical location restrictions

Use Case Description :

- access to an SSO protected resource from
  -- on campus
  -- off campus (ie. from home, while travelling)

Primary actor(s) :

- Member of the community (sometimes referred to as a Library Patron, but that term sometimes has a narrower meaning).

User Type :

- Administrator, Editor, End User (Primary actor)

Technology Type :

- N/A

Vendor Type :

- N/A

Precondition :

Trigger :

- Patron attempts to access restricted resource

Basic flow :

- Via web browser, patron attempts to access proxy-protected resource. Access to resource is either granted or denied based the users IP address.

4. Use Case Name:

- EZProxy Access with Shibboleth, physical location restrictions

Use Case Description:

- access to a resource protected by EZP (and not by Shibboleth) from
  -- on campus
  -- off campus (ie. from home, while travelling)

Primary actor(s):

- Member of the community (sometimes referred to as a Library Patron, but that term sometimes has a narrower meaning).

User Type:

- Administrator, Editor, End User (Primary actor)

Technology Type:

- N/A

Vendor Type :

- N/A

Precondition :

Trigger :

- Patron attempts to access restricted resource

Basic flow :

- Via web browser, patron attempts to access proxy-protected resource. Access to resource is either granted or denied based the users IP address or by virtue of AuthZ authentication process which inspect attributes returned in AuthN assertion.

Model Use Cases (Advanced) :

1. Use Case Name :

- Federated Search User Viewable

Use Case Description :

- Federated Search which returns results that a user is allowed to view.

Primary actor(s) :

- Library patron. Patron Types - Walk-in, Student, Faculty, Staff, Person Outside the Institute (POI)

User Type :

Technology Type :

Vendor Type :

Precondition :

Trigger :

Basic flow :

2. Use Case Name :

- Federated Search Group Viewable

Use Case Description :

- Federated Search which returns results that are based on facets related to a group (or other shibb attribute)

Primary actor(s) :

User Type :

Technology Type :

Vendor Type :

Precondition :

Trigger :

Basic flow :

3. Use Case Name :

- OpenURI Redirects

Use Case Description :

- OpenURl based redirects in the middle of the sequence

Primary actor(s) :

User Type :

Technology Type :

Vendor Type :

Precondition :

Trigger :

Basic flow :

4. Use Case Name :

- Federated Search AuthN Viewable

Use Case Description :

- various weird local authN sequences

Primary actor(s) :

User Type :

Technology Type :

Vendor Type :

Precondition :

Trigger :

Basic flow :

5. Use Case Name :

- VPN Access

Use Case Description :

- Off-campus users relying on VPN access to the campus network

Primary actor(s) :

User Type :

Technology Type :

Vendor Type :

Precondition :

Trigger :

Basic flow :

5. Use Case Name :

- uApprove Access

Use Case Description :

- The campus uses uApprove, an extension to the IdP develop by the Swiss National network that allows user control over attribute release.

Primary actor(s) :

User Type :

Technology Type :

Vendor Type :

Precondition :

Trigger :

Basic flow :

6. Use Case Name :

- Library hosts IdP as part of a campus Federation

Use Case Description :

- Library has a need to authenticate a separate group of individuals, Friends of the Library members, or other group and installs a local IdP to join to a campus federation.

Primary actor(s) :

- Member of the community

User Type :

- Individual who is not a member of the Institution, but has privileges within the library system to access electronic resources remotely. Also sometimes referred to as the POI (person outside the institute).

Technology Type :

Vendor Type :

Precondition :

- Links to individual resources have been created.
- EZProxy configured to use an institutional federation WAYF.
- Library IdP has been incorporated into institutional federation.
- EZProxy configured to recognize authorized shibboleth attributes

Trigger :

- User clicks a "proxied" link to a Library resource. E.g.https://proxy.domain.edu/login?auth=shibboleth&url=http://www.sciencedirect.com

Basic flow :

- User routed to Institutional WAYF where they will select the Library IdP as their affiliation
- The Library IdP is configured to use secondary LDAP, or possibly a RDBMS lookup for authentication
- Shibboleth attributes are assigned and user is directed to resource.