Shibboleth @ LSU

General Information:

https://webauth.shib.lsu.edu/shibboleth

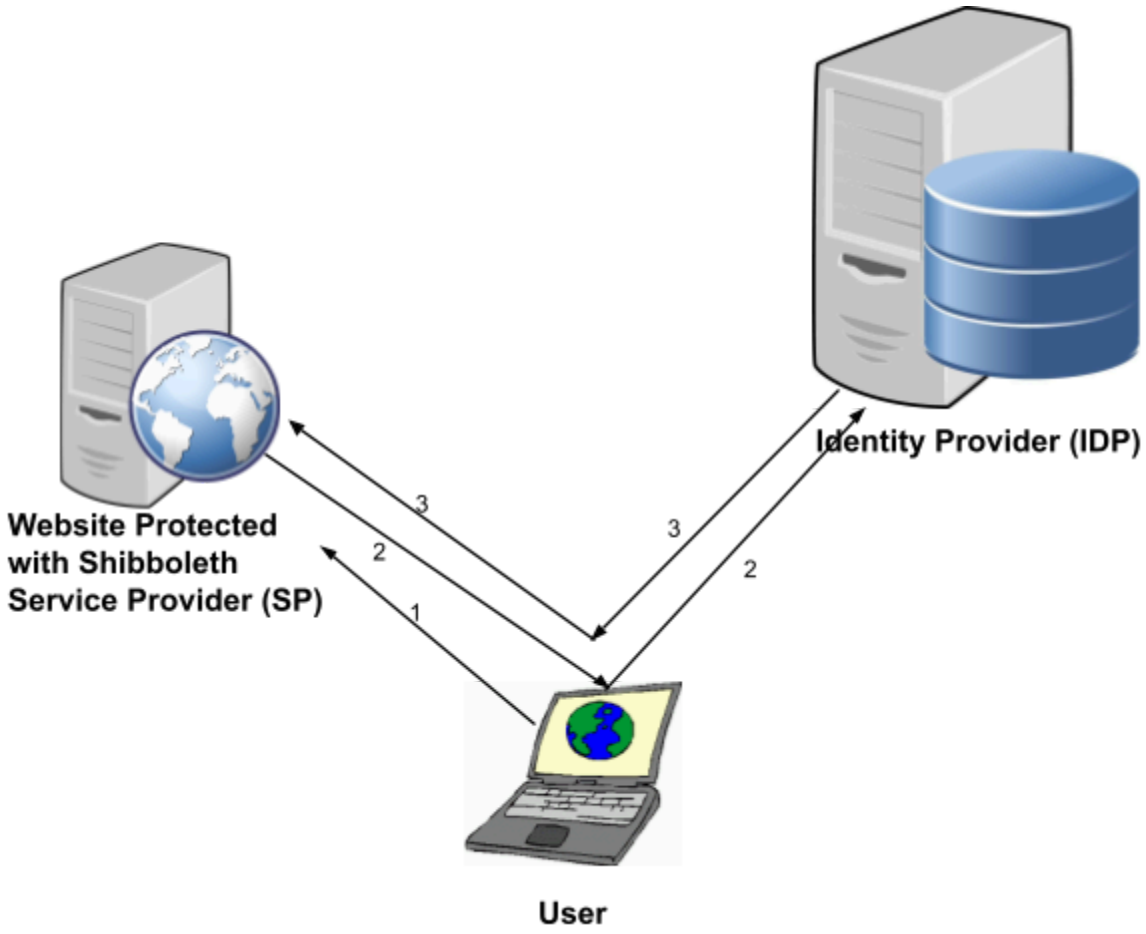
What is Shibboleth?

Open source, federated, web single sign-on software package.

Shibboleth contains two main pieces:

1. The Identity Provider (IDP). Think of it as the “server.”
2. The Service Provider (SP). Think of it as the “client.”

The Shibboleth Service Provider (SP) lives on the web application server. When an un-authenticated user visits a website protected by the SP, the SP redirects the user to the Identity Provider (IDP) for authentication. If the user successfully authenticates to the IDP, the IDP then redirects the user back to the SP along with attributes or “data” about the logged in user. The underlying protocol use by the IDP and SP is called OASIS Security Assertion Markup Language (SAML).



1. Unauthenticated user visits a Shibboleth Protected website.
2. The Service Provider (SP) redirects the user to the Identity Provider (IDP) for authentication.
3. After the user successfully authenticated to the IDP, the IDP then redirects the user back to the SP. The IDP also sends the SP attributes about the logged in user.

Attributes:

Attributes are information about the logged in users. Some examples of attributes are:

1. **givenName** - First name of the user
2. **sn** - User's "family" name or surname.
3. **eduPersonPrincipalName** - PAWS ID@lsu.edu. Usually same as user's e-mail address, but not always.
4. **eduPersonScopedAffiliation** - the affiliation of the user. Can be one of the following, and more:
    a. student
    b. faculty
    c. staff
    d. alum
    e. affiliate
5. Many, many other.

The Service Provider (SP) takes the attributes returned by the IDP and sets them as server variables. Accessing these variables depends on the server-side programming language used for the website:

1. PHP: $_SERVER["Shib-Attribute-Key"]
2. ASP: Request("HTTP_SHIB_ATTRIB_KEY")
3. ASP.NET: Request.Headers("Shib-Attrib-Key")

Replace "Shib-Attribute-Key" with the name of the attribute(s) release by the IDP.

Metadata:

Metadata is an XML file used by both the IDP and the SP to store configuration data that allows both to communicate. As such, both SP and IDP must exchange metadata ahead of time. The SP automatically generates its own metadata based on the configuration file in **/etc/shibboleth2.xml**. For most cases, this metadata will work just fine and requires no further modification. For SP, the metadata can be assessed by going to: **https://yourshibsite.lsu.edu/Shibboleth.sso/Metadata**. The Shibboleth.sso and Metadata are case-sensitive.

https://webauth.shib.lsu.edu/shibboleth/lsu.php
https://wiki.shibboleth.net/confluence/display/SHIB2/MetadataForSP

How do I get Shibboleth?:

Because LSU ITS runs the Identity Provider (IDP) servers, admins only need to deploy the Service Provider (SP) component and tie it to the IDP. Below is just a brief summary of the steps involved. Please see the Deployment section of the official LSU documentation for more details:

https://webauth.shib.lsu.edu/shibboleth/

1. Get an SSL certificate and protect your site with TLS

2. Send an email to **security@lsu.edu** with a subject of "Shibboleth - LSU Service Provider Registration" with the following information
    1. Name of service (if multiple, just summarize)
    2. Brief description of service
    3. Technical, administrative, and/or support contact information for your service (names, e-mail addresses, phone, etc.)
    4. Summary of platform (operating system version, web server version, etc.)
    5. A verifiable phone number at which you can be reached for verification of the information
    6. User attributes required by service. Be specific as you can. Don't use words like anything or everything.
3. Disable SELinux
4. Install the Shibboleth Service Provider (SP):
    a. **https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLinuxInstall**
5. Download the following files to **/etc/shibboleth** (rename original files to save them):
    a. https://webauth.shib.lsu.edu/shibboleth/config/lsu-attribute-policy.xml
    b. https://webauth.shib.lsu.edu/shibboleth/config/lsu-metadata.pem
    c. https://webauth.shib.lsu.edu/shibboleth/config/shibboleth2.xml
    d. https://webauth.shib.lsu.edu/shibboleth/config/attribute-map.xml
6. Edit **shibboleth2.xml** to suit your environment
    a. Hint: Change anything with changeme
7. Exchange metadata with the IDP
    a. Remember, your SP metadata can be found at:
    b. https://sphostname.lsu.edu/Shibboleth.sso/Metadata
8. Be patient. Adding an SP requires the IDP service to be restarted, which is service affecting and must be scheduled.

Protecting your site with Shibboleth:

In **/etc/shibboleth/shibboleth2.xml:**

```
 <RequestMapper type="Native">
        <RequestMap>
        <!--
        The example requires a session for documents in /secure on the containing host with http and
        https on the default ports. Note that the name and port in the <Host> elements MUST match
        Apache's ServerName and Port directives or the IIS Site name in the <ISAPI> element above.
        -->
        <Host name="shibboleth-sp.lsu.edu">
                <Path name="secure" authType="shibboleth" requireSession="true"/>
```

```
            <Path name="secure2" authType="shibboleth" requireSession="true"/>
        </Host>
        <!-- Example of a second vhost mapped to a different applicationId. -->
        <!--
        <Host name="admin.example.org" applicationId="admin" authType="shibboleth"
requireSession="true"/>
        -->
        </RequestMap>
</RequestMapper>
```

The "**<Path name=**" specifies the folder under **/var/www/html** directory to secure with Shibboleth.

In **/etc/httpd/conf.d/shib.conf:**

```
<Location /secure>
        AuthType shibboleth
        ShibCompatWith24 On
        ShibRequestSetting requireSession 1
         require shib-attr some_attribute 'some_attribute's_value'
</Location>

<Location /secure2>
        AuthType shibboleth
        ShibRequestSetting requireSession 1
        require valid-user
</Location>
```

shib.conf is where we specify to apache how to lock down the shibboleth protected directories.

Because shibboleth returns the login user's attributes to the web applications, the web developer can leverage the attributes for further, more granular authorizations, as well as a more enhanced web experience. The limit is the imagination of the web developer.

Changes to files in **/etc/shibboleth** requires a restart of the shibd service:

service shibd restart
systemctl restart shibd

Changes to **/etc/httpd/conf.d/shib.conf** requires apache restart:

service httpd restart
systemctl restart httpd

Set shibd to start on system startup:

chkconfig shibd on
systemctl enable shibd

Logout:

Direct your visitor (via logout link) to:

https://yourshibsite.lsu.edu/Shibboleth.sso/Logout?return=https://webauth.shib.lsu.edu/idp/logout.jsp

Coming soon! Redirect user to a site after logging out:

https://yourshibsite.lsu.edu/Shibboleth.sso/Logout?return=https://webauth.shib.lsu.edu/idp/logout.jsp?url=https://somesite.lsu.edu

It is still highly recommended that user completely close their web browser to clear out any remaining sessions.