**Shibboleth Authentication Notes**

**Service Provider Installation on RedHat Systems**

These instructions assume familiarity with Red Hat Enterprise Linux and Apache 2.4.

**Setup**

1. First install Shibboleth Service Provider on the operating system. You’ll need to add a repository and use yum to install. Follow instructions for “Installing via Yum” here: <https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLinuxRPMInstall>
	1. To add the repo, create a file called /etc/yum.repos.d/security\_shibboleth.repo. The file should contain text generated at this link, which is mentioned in the link above: <https://shibboleth.net/downloads/service-provider/latest/RPMS/>
2. Add name directives and Location sections to Apache virtual server configuration (/etc/httpd/conf.d/yourwebsite.conf)

ServerName yourserver.uta.edu

CanonicalName On

<Location />

 # Configure Shibboleth for "lazy" authentication

 AuthType shibboleth

 ShibUseHeaders on

 Require shibboleth

</Location>

<Location /Shibboleth.sso>

 # Suggested by DSpace docs

 ProxyPass !

 SetHandler shib

</Location>

1. Restart Apache: **service httpd restart**
2. Edit /etc/shibboleth2.xml:
	1. entityID= "https://yourserver.uta.edu/shibboleth"
	2. SSO entityID= <https://idp.uta.edu/idp/shibboleth>
	3. Use local IdP metadata file (optional).
		1. Download from IdP: <https://idp.uta.edu/idp/shibboleth>
		2. Save as /etc/shibboleth/partner-metadata.xml.
		3. Uncomment reference in /etc/shibboleth/shibboleth2.xml:

<MetadataProvider type="XML" validate="true" file="partner-metadata.xml"/>

1. Edit /etc/attribute-map.xml
	1. Uncomment “LDAP-based attributes”
2. Start the shibd service: **service start shibd**
3. Enable start at boot time: **systemctl enable shibd**
4. Make sure /etc/shibboleth/sp-key.pem and ./sp-cert.pem are owned by shibd:shibd:
	1. **ls -l /etc/shibboleth/\*.pem**
	2. If not owned by shibd:shibd, change ownership:
		1. **chown shibd:shibd /etc/shibboleth/\*.pem**
5. Download metadata file from <https://yourserver.uta.edu/Shibboleth.sso/Metadata> and send to OIT with ticket requesting authentication be enabled. Also ask OIT to send required attributes on login. Depending on the requirements of your application, these might include: NetID, first name, last name, and email address.

**Troubleshooting**

**Error Message: No peer endpoint available to which to send SAML response**

Probably your Apache configuration does not have the correct ServerName directive. You also need to have UseCanonicalName On. And if you’ve configured a reverse proxy in Apache, you might need to add a ProxyPreserveHost On. Restart Apache whenever you make changes in its configuration.

**Error Message: Unable to encrypt assertion**

This means the public key for the SP is not available to the IdP, probably because you forgot to change ownership of /etc/shibboleth/sp-key.pem and ./sp-cert.pem to shibd before you donwloaded the metadata.

**Show attributes sent by IdP**

If there’s any doubt what attributes are being returned by the IdP after the user logs in, you can view them using the following steps:

* In /etc/shibboleth/shibboleth2.xml, change session handler showAttributeValues to true:
	+ <Handler type="Session" Location="/Session" showAttributeValues="true"/>
* Restart shibd **service shibd restart**
* Attempt to log into your site with Shibboleth.
* In another window, browse to https://yourserver.uta.edu/Shibboleth.sso/Session
	+ The returned attributes will be displayed.
* Change back when finished testing (for security).
* Attributes not listed in /etc/shibboleth/attribute-map.xml will not be displayed in session page.

**utaEmplID**

If you want to use the numerical employee ID (e.g., 6001155882), you need to add these lines to /etc/shibboleth/attribute-map.xml:

<Attribute name="urn:oid:1.3.6.1.4.1.19638.1.1.109" id="utaEmpID"/>

<Attribute name="urn:mace:dir:attribute-def:utaEmpID" id="utaEmpID"/>

The attribute ID can be renamed in the Service Provider if desired. That is, you can map the OID to a different name than on the IdP. The SP identifies the attribute based on its OID, not on the attribute name.