SHRINE 4.0.0 Appendix A.2 - Quick Configuration

The following instructions are meant to get you going as quickly as possible. If you want a better understanding of what's going on, go to the "More Details" sections of this document.

Configuration Directories

In summary, the directories containing configuration files which need to be modified are:

`/opt/shrine/tomcat/conf/` Tomcat configuration files

`/opt/shrine/tomcat/lib/` Shrine config files

`/etc/shibboleth/` Shibboleth configuration files

`/etc/httpd/**` Apache configuration files

`/var/www/html/` Apache static content as set in, for instance, `/etc/httpd/conf/httpd.conf`

Configuration files to create from scratch or to import

	Location on SP	Description

key pair	`/etc/shibboleth/sp-key.pem`
	
	`/etc/shibboleth/sp-cert.pem`
		If the Shibboleth installer has not already done so, create a key pair; include the content of the public key certificate (**`sp-cert.pem`**) in **`sp-metadata.xml`** (see below), and the paths of the **key** and **certificate** as xml attributes of the **`<CredentialResolver>`** element of **`shibboleth2.xml`** (see below)
		
		To create a key pair, use **`/etc/shibboleth/keygen.sh`**; as per https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2067398706/keygen and also https://docs.shib.ncsu.edu/docs/configure/index.html.
		
		You don't need to create separate key pairs for signing and for encryption.

`idp-metadata.xml`	`/etc/shibboleth/idp-metadata.xml`	A copy of your idP's metadata. You'll need to ask the admin(s) of your idP for a copy of it, most likely over a secure channel. Rename it to **`idp-metadata.xml`** and put it in **`/etc/shibboleth`**

Configuration files based on samples in Git

Sample configuration files can be found in the nightly shrine-setup zip file located at https://repo.open.catalyst.harvard.edu/nexus/content/groups/public/net/shrine/shrine-setup/4.0.0/shrine-setup-4.0.0-dist.zip

- `sso/apache/sp.conf-sample`
- `sso/apache/sp-metadata.xml-sample`
- `sso/shibboleth/attribute-map.xml-sample`
- `sso/shibboleth/shibboleth2.xml-sample`
- `sso/tomcat/server.xml-sample`
- `sso/shrine/shrine.conf-sample`
- `sso/shrine/override.conf-sample`

Copy these files to the location on the SP (i.e. your server) indicated in the table below. Remove the "`-sample`" from the file names. Overwrite the existing config files.

Then search for the marker: '**`ADJUST_FOR_YOUR_SITE`**' in each of these files for indications of what / where you need to edit them.

Location in zip file	Location on SP	Description
`sso/apache/sp-metadata.xml-sample`	`/var/www/html/sp-metadata.xml` – as long as your Apache configuration sets `DocumentRoot` to `/var/www/html` (for instance in `/etc/httpd/conf/httpd.conf`)	To be shared dynamically with your site's IdP (i.e. make it available as a document at the document root and share that URL with your IdP's maintainers/admins); or omit from the SP's (i.e. your) web server, and instead share it securely with the IdP admins whenever it changes (if it does) In either case, populate the **entityID**, public key **certificate**, and consumer service **location** with yours.

sso/shibboleth/shibboleth2.xml-sample	/etc/shibboleth/shibboleth2.xml	Populate the **entityID** attribute in **<ApplicationDefaults>** to match your **entityID** in **sp-metadata.xml**. Populate the **entityID** attribute in **<SSO>** to match the idP's **entityID** in **idp-metadata.xml**. Populate the **supportContact** attribute of the **<Errors>** element with an email address. The **<CredentialResolver>** element specifies the private+public key to use for encryption and signing while communicating with the idP. If you put the keys in the location specified above and the private key is not password-protected, then there is no need to modify this element. Otherwise edit this file to reflect the location of the keys and optionally the private key password. The private key should be stored in a "safe" location. If it is password-protected, that should be reflected in the **<CredentialResolver>**'s **password** attribute.
sso/shibboleth/attribute-map.xml-sample	/etc/shibboleth/attribute-map.xml	Populate the idP's attribute name for the user; to be mapped to the attribute id "**userId**"
sso/apache/sp.conf-sample	/etc/httpd/conf.d/sp.conf	Populate the **ServerName**, **ProxyPass** and **Header set Access-Control-Allow-Origin** directives with your hostname.
sso/tomcat/server.xml-sample	/opt/shrine/tomcat/conf/server.xml	Most likely the following 3 attributes of **<Connector port="6443" ... />** are already populated, but if not then populate **certificateKeystoreFile**, **certificateKeystorePassword**, **certificateKeyAlias**. You will need to populate **proxyName** in the **AjpNio2Protocol** connector. Once done, **Merge** the contents of **server.xml-sample** into the existing **/opt/shrine/tomcat/conf/server.xml**.
sso/shrine/shrine.conf-sample or sso/shrine/override.conf-sample	/opt/shrine/tomcat/lib/shrine.conf or /opt/shrine/tomcat/lib/override.conf	Set Shrine configuration options for using SSO for login/logout. In **override.conf** it would look like: • Specify that we are using SSO: **shrine.queryEntryPoint.authenticationType = "sso"** • Specify the logout URL (**shrine.webclient.ssoLogoutUrl**) = (see override.conf-sample) • Specify Shrine's session timeout as such: **shrine.webclient.sessionTimeout = "30 minutes"**. You should use either file and **merge it** into the existing **shrine.conf** or **override.conf** in **/opt/shrine/tomcat/lib**

Next Steps:

Fast forward to SHRINE 4.0.0 Appendix A.8 - Starting and Stopping the Software

or

Read the "More Details" pages that follow, starting with SHRINE 4.0.0 Appendix A.3 - More Details : Shibboleth Configuration