SETUP GUIDE SHIBBOLETH AS IdP

STEP 1:

- In **conf/idp.properties**, uncomment and set 'idp.encryption.optional' to true. Eg.

```
idp.encryption.optional = true
```

- In conf/metadata-providers.xml, configure Wordpress as an SP like this

```
<MetadataProvider id="Wordpress"
      xsi:type="FileBackedHTTPMetadataProvider"
      backingFile="%{idp.home}/metadata/wp-metadata.xml"
      metadataURL="http://<YOUR_WP_DOMAIN>/wp-content/plugins/miniorange-saml-20-
single-sign-on/metadata.php"/>
```

- In **conf/saml-nameid.properties**, uncomment and set default NameID as EmailAddress like this

```
idp.nameid.saml2.default = urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
```

- In **conf/saml-nameid-xml**, search for *shibboleth.SAML2NameIDGenerators*. Uncomment the *shibboleth.SAML2AttributeSourcedGenerator* bean and comment all other ref beans. Eg.

```
<!-- SAML 2 NameID Generation -->
<util:list id="shibboleth.SAML2NameIDGenerators">
       <!-- <ref bean="shibboleth.SAML2TransientGenerator" /> -->
       <!-- <ref bean="shibboleth.SAML2PersistentGenerator" /> -->
       <bean parent="shibboleth.SAML2AttributeSourcedGenerator"
             p:format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
             p:attributeSourceIds="#{ {'email'} }" />
</util:list>
```

- Make sure you have defined AttributeDefinition in **conf/attribute-resolver.xml.** Eg.

```
<!-- Note: AttributeDefinition id must be same as what you provided in
     attributeSourceIds in conf/saml-nameid.xml -->
<resolver:AttributeDefinition xsi:type="ad:Simple" id="email" sourceAttributeID="mail">
      <resolver:Dependency ref="ldapConnector" />
      <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="email"
                                 friendlyName="email" />
</resolver:AttributeDefinition>

<resolver:DataConnector id="ldapConnector" xsi:type="dc:LDAPDirectory"
      ldapURL="%{idp.authn.LDAP.ldapURL}"
      baseDN="%{idp.authn.LDAP.baseDN}"
```

```
      principal="%{idp.authn.LDAP.bindDN}"
      principalCredential="%{idp.authn.LDAP.bindDNCredential}">
      <dc:FilterTemplate>
          <!-- Define you User Search Filter here -->
            <![CDATA[
            (&(objectclass=*)(cn=$requestContext.principalName))
            ]]>
      </dc:FilterTemplate>
      <dc:ReturnAttributes>*</dc:ReturnAttributes>
</resolver:DataConnector>
```

- Make sure you have AttributeFilterPolicy defined in **conf/attribute-filter.xml.** Eg.

```
<afp:AttributeFilterPolicy id="ldapAttributes">
      <afp:PolicyRequirementRule xsi:type="basic:ANY" />
      <afp:AttributeRule attributeID="email">
            <afp:PermitValueRule xsi:type="basic:ANY"/>
      </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

- Restart the Shibboleth Server.

STEP 2:

- Go to **Service provider** Tab in **miniOrange SAML Plugin** and enter the following details:

Identity Provider Name	Shibboleth
SAML Login URL	https://<your_domain>/idp/profile/SAML2/Redirect/SSO
IdP Entity ID or Issuer	https://<your_domain>/idp/shibboleth
X.509 Certificate	The public key certificate of your IdP
Response Signed	Checked
Assertion Signed	Checked