**Certificates:**

**SSO certificate**: */tmp/saml.pem*

**Server self-certificate:** */etc/tomcat8/selfcert.keystore*

**Jars:**

**Semarchy**: com.semarchy.tool.jee.tomcat-8.5.4-alpha-20190404-1050.jar

**Fediz**: fediz-tomcat8-1.4.6-20190401.115514-14-zip-with-dependencies.zip

**Generate server cert:**

*keytool -genkey -noprompt -alias tomcatSSO -keyalg RSA -keystore /etc/tomcat8/selfcert.keystore -keypass changeit -storepass changeit -dname "CN=sanofi.com, OU=sanofi.com, O=Sanofi, L=France, S=Lion, C=FR"*

**Edit server.xml to enable SSL:**

*<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"*

*port="8443"*

*maxThreads="150"*

*SSLEnabled="true"*

*scheme="https"*

*secure="true"*

*keystoreFile="/etc/tomcat8/selfcert.keystore"*

*type="JKS"*

*keystorePass="changeit"*

*sslProtocol="TLS"*

*clientAuth="false"*

*/>*

**Edit Semarchy.xml:**

*<Valve className="com.semarchy.tool.jee.tomcat.FederationAuthenticator"*

*configFile="conf/fediz\_config.xml"*

*keepMappedRoles ="false"*

*keepUnmappedRoles ="false"*

*regexEnabled="true"*

*rolesMappingPathName="/usr/share/tomcat8/conf/roles-mapping.properties"*

*/>*

**Edit catalina.properties (/etc/tomcat8/catalina.properties):**

common.loader=${catalina.base}/lib,${catalina.base}/lib/\*.jar,${catalina.home}/lib,${catalina.home}/lib/\*.jar,"${catalina.home}/lib/fediz/\*.jar"

**Edit logging.properties (/etc/tomcat8/logging.properties):**

############################################################

# Semarchy Configuration

# Fedis for SSO

############################################################

org.apache.catalina.core.ContainerBase.[Catalina].[localhost].[/semarchy].level = ALL

org.apache.catalina.realm.level = ALL

org.apache.catalina.realm.useParentHandlers = true

org.apache.catalina.authenticator.level = ALL

org.apache.catalina.authenticator.useParentHandlers = true

# Turn on Fediz logging - add this row at the end

org.apache.catalina.authenticator.FormAuthenticator.level = FINE

org.apache.cxf.fediz.level = ALL

org.apache.wss4j.level = ALL

**Create fediz\_config.xml(/etc/tomcat8/fediz\_config.xml) :**

*<?xml version="1.0" encoding="UTF-8" standalone="yes"?>*

*<FedizConfig>*

*<contextConfig name="/semarchy">*

*<audienceUris>*

*<audienceItem>http://emea-aws-mdm-xdmhttp-sbx-a-01.service.cloud.local:3036/semarchy/</audienceItem>*

*</audienceUris>*

*<certificateStores>*

*<trustManager>*

*<!-- note that certificate is in file directly, not imported in keystore, as this is supported by fediz -->*

*<keyStore file="/tmp/saml.pem" type="PEM" />*

*</trustManager>*

*</certificateStores>*

*<trustedIssuers>*

*<issuer certificateValidation="PeerTrust" />*

*</trustedIssuers>*

*<!-- SAML protocol: -->*

*<protocol xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="samlProtocolType" version="2.0">*

*<authnRequestBuilder>com.semarchy.tool.jee.tomcat.fediz.PingFederateSamlRequestBuilder</authnRequestBuilder>*

*<doNotEnforceKnownIssuer>true</doNotEnforceKnownIssuer>*

*<disableDeflateEncoding>true</disableDeflateEncoding>*

*<issuer>https://idfedstaging.sanofi.com/idp/SSO.saml2</issuer>*

*<roleURI>Group</roleURI>*

*</protocol>*

*</contextConfig>*

*</FedizConfig>*

**Copy jars:**

mkdir /usr/share/java/tomcat8/fediz

cp /tmp/com.semarchy.tool.jee.tomcat-8.5.4-alpha-20190404-1050.jar /usr/share/java/tomcat8/

cp /tmp/fediz/\*.jar /usr/share/java/tomcat8/fediz/

**SSO PingFederation considerations:**

Send keyInfo in response

Sign the assertion URL