|  |
| --- |
| Invoking C3PRWeb Services |
|  |
| **Ramakrishna Gundala, Denis Krylov** |
| **3/24/2011** |

|  |
| --- |
| This document outlines the software versions, steps used to create, deploy and use an STS service for securely hitting the C3PR web services. |

Software versions Used:

Java : 1.6,Netbeans 6.9,Glassfish Server 3

Install GlassFish and Netbeans bundle from here, <http://netbeans.org/downloads/start.html?platform=windows&lang=en&option=java>

Deploy the STS service on Glassfish as outlined here, <http://metro.java.net/guide/Configuring_A_Secure_Token_Service__STS_.html#gfrig>

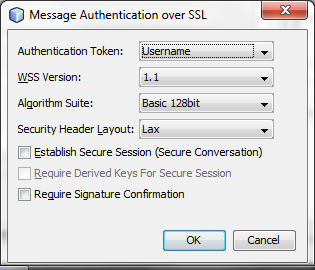
Most of the configuration follows the steps listed in the above URL except for few exceptions listed here,

In the Web Service Properties,

Select ‘ Message Authentication over SSL’ as the security mechanism.

Don’t load Alias for either TrustStore or KeyStore.

Click on the configure button and the settings should be like this.



Deploy the STS Service and start the glass fish server. This would create a unsecured service i.e. in non-SSL mode. You can verify this by looking at the wsdl from the browser.

**Making the STS server SSL enabled:**

STOP the running Glassfish server

For SSL enabling, we have to update the Glassfish server certificates first.

 Download the zip file that contains the certificates and the Ant scripts (copyv3.zip) by going to this URL: <https://xwss.dev.java.net/servlets/ProjectDocumentList?folderID=6645&expandFolder=6645&folderID=6645>.

 Unzip this file and change into its directory, copyv3.

 Verify that an environment variable named AS\_HOME is created, and that it specifies the full path to the location of your GlassFish installation, for example, C:\Sun\GlassFish.

**NOTE:** Some releases of GlassFish may have different default passwords for the keystores. If you are using a different version of GlassFish than the one recommended at wsit.dev.java.net, edit the file build.xml and specify the correct default password in the AS\_KEYSTORE\_PASSWORD field.

 From the copyv3 directory, execute the Ant command that will copy the keystore and truststore files to the appropriate location, and import the appropriate certificates into the GlassFish keystore and truststore. This Ant command is simply: <AS\_HOME>/lib/ant/bin/ant

Configure GlassFish project to add SSL.

Open web.xml of the STS project in Netbeans IDE and add this security constratint where MySTSService should be replaced by your service name.

<security-constraint>

<display-name>Constraint1</display-name>

<web-resource-collection>

<web-resource-name>MySTSService</web-resource-name>

<description/>

<url-pattern>/\*</url-pattern>

</web-resource-collection>

<user-data-constraint>

<description/>

<transport-guarantee>CONFIDENTIAL</transport-guarantee>

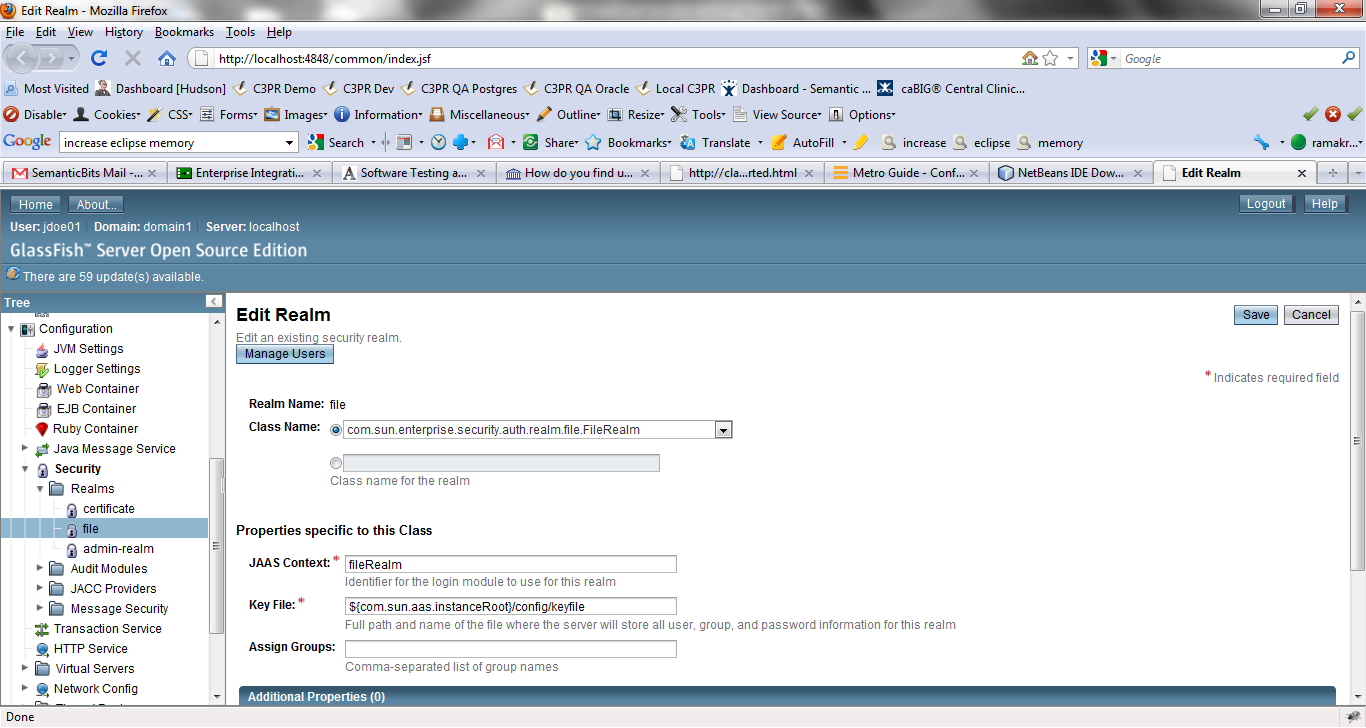
</user-data-constraint>

</security-constraint>

Restart the Glassfish server. Now the SSL should be enabled. The glassfish server would automatically redirect the http request at port 8080 (default) to the 8181 unless a different port is configured by the user.

**Glassfish Server user creation**

From the browser go the Glassfish admin page, navigate to the security node, and select file realm. Click on manage users, click on add user and create a user. The user group is not required. The user name should match the user name of the authorized user (who has access privileges to do the necessary operation) in the C3PR webservice.



**Running the Client:**

After checking out the STS client g the STS client from here, <https://ncisvn.nci.nih.gov/svn/c3pr/trunk/c3prv2/codebase/projects/ws-client>.

Update the applicationContext.xml to change the STS service location, wsdl name and the username and the password for the created Glassfish server user appropriately. Also update the endpointName.

Similarly in the ADFS\_STS.wsdl, change the location of the service in the wsdl:port.

Start the C3PR web service and STS Service.

Last step is to make sure the STS client has the certificates used by STS Service and the C3PR web service (one used by tomcat). For this, simply copy the certificates presented by the browsers by hitting the C3PR wsdl and the STS service wsdl.

Makesure the CU (user name) of the issuer for the above certificates is localhost if the URL of the STS service starts with localhost.