1)create a self signed keystore

"%JAVA\_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA.

2)modify the connector tag in server.xml of tomcat installation directory.

a)<Connector SSLEnabled="true" acceptCount="100" clientAuth="false"

disableUploadTimeout="true" enableLookups="false" maxThreads="25"

port="8443" keystoreFile="/Users/loiane/.keystore" keystorePass="password"

protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"

secure="true" sslProtocol="TLS" />

b)if the tomcat is embedded inside the eclipse the above changes can be

done in /Servers/Tomcat v6.0 Server at localhost-config/server.xml file.

3)need to add a security constraint in web.xml of your project.

<security-constraint>

<web-resource-collection>

<web-resource-name>securedapp</web-resource-name>

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

</web-resource-collection>

<user-data-constraint>

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

</user-data-constraint>

</security-constraint>

If the transport guarantee tag is made to NONE then the https wont work.

4)download keystore explorer,export the certificate of keystore file which was Generated by us.

5)add the certificate to our keystore present in jre folder.

6)use below command to add the certificate

C:\Windows\system32>"%JAVA\_HOME%/bin/keytool" -import -alias mycertificate -keystore "C:/Program Files/Java/jdk1.7.0\_80/jre/lib/security/cacerts" -file "C:/Users/HCL/nithin\_chatra.cer"