Creating a certificate for Tomcat & OE Pas

Overview

Navigating the minefield of requesting and installing a certificate for a Tomcat instance is not easy, hopefully this guide makes it a bit easier and focuses on the Openedge pacific application server but would work for other Tomcat instances.

1. Create a CSR using the Java tool **keytool** this will generate a keystore file. **NB** Use the same keystore file throughout this process as we will use this keystore to replace the default keystore used in the PAS i.e. conf/*tomcat-keystore.p12*
   https://www.alphassl.com/support/create-csr/tomcat.html

2. Send the certificate request to the CA
3. When certificates received import root and intermediate certificates into your keystore file generated above e.g.
   a. https://www.alphassl.com/support/install-root/tomcat.html
   b. https://www.alphassl.com/support/install-ssl/tomcat.html
4. Copy your keystore file and replace the conf/*tomcat-keystore.p12*
   a. Edit the Catalina.properties file to reflect your keypass password and keyalias
   b. Change the trustpass password to use the password when you created the CSR

JSSE keystore used by server.xml for its server key & certificates
psc.as.https.keypass=password
psc.as.https.keyalias=test
psc.as.https.storeType=PKCS12

JSSE certificate store used by server.xml for validating client certificates
psc.as.https.trustpass=password
psc.as.https.trustType=JKS

Appendix

Keytool is in your java\bin folder