How is a Keystore and Certificate Signing Request (CSR) generated using the Keytool utility?

NOTE: These instructions apply to the following server types:

Apache Tomcat
Java (Generic) Web Servers

During the online enrollment process you will be required to provide Entrust Certificate Services with a Certificate Signing Request (CSR).

This encrypted data is generated from your server, and contains information about your company and Web server.

Part 1 – Create a Certificate Keystore

keytool -genkey -alias <tomcat> -keyalg RSA –keysize 2048 -keystore <yourdomain.keystore>
Important:
! Always specify your keystore location when it is being created.
! If you are renewing your certificate, you must create a new key pair and keystore.
! Please use the same alias when creating your CSR and installing your certificate that you use to create your self-signed keystore.
As an example:

C:\> keytool -genkey -alias myalias -keysize 2048 -keyalg RSA -keystore c:\.mykeystore

Enter keystore password: password
What is your first and last name?
[Unknown]: www.testcertificates.com
What is the name of your organizational unit?
[Unknown]: Entrust CS
What is the name of your organization?
[Unknown]: Entrust
What is the name of your City or Locality?
[Unknown]: Ottawa
What is the name of your State or Province?
[Unknown]: Ontario
What is the two-letter country code for this unit?
[Unknown]: CA
Is CN=www.testcertificates.com, OU=Entrust CS, O=Entrust, L=Ottawa, ST=Ontario, C=CA correct?
[no]: yes

Enter key password for
(RETURN if same as keystore password):

Ensure that you take note of the password that is entered and use it when generating the CSR in Part 2.

Part 2 – Generating the Certificate Signing Request

1. *keytool -certreq -keyalg RSA -alias <tomcat> -file certreq.csr -keystore <yourdomain.keystore>*
   Important:
   ! Please use the same alias when creating your CSR and installing your certificate that you use to create your self-signed keystore.
   As an example:
   C:\>keytool -certreq -keyalg RSA -alias myalias -file certreq.txt -keystore c:\.mykeystore
   Enter keystore password:

2. Paste this CSR into your Entrust enrollment submittal page. The CSR should look similar to this:

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBujCCASMCAQAwejELMAkGA1UEBhMCQ0ExEDAOBgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90
dGF3YTEQMA4GA1UEChMHRW50cnVzdDETMBEGA1UECxMKRW50cnVzdCBDUzEhMB8GA1UEAxMYd3d3
.
.
.
5w6T+q/f+wIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAF+0hqAqXumz/vGrzGVhKHlnxd7HW3ezS
GIbIUcOy1YdDc/1ZCqRpu3utYIZ6welK++l+QjlbL6p5RJJETkkLKXjb/WVFajNuPl7Yob9pbwA7
JBrCCKbFj+kzDNbGhCR1RgFA9vQj5vob41Vj+k+TQchliuTLL9rFXNDHrtgTMtA=
-----END NEW CERTIFICATE REQUEST-----

How is the Server Certificate installed on using Keytool?

To install the Server Certificate, complete the following steps:

1. Copy and paste the server certificate from the pickup page (including the BEGIN and END tags) into a text editor such as Notepad. Save the file with a .cer extension (for example, server.cer).

2. Using the keytool utility, enter the following:

keytool -import -alias <*alias*> -keystore <*your_keystore_filename*> -trustcacerts -file <*filename_of_the_chain*>

As an example:

C:\>keytool -import -alias myalias -keystore c:\.mykeystore -trustcacerts -file c:\server.cer
Enter keystore password:
Certificate was added to keystore.
Note – You must install the supplied chain certificates before installing the server certificate or you will not be able to install the certificate.