javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

Are you getting this error? This simply means that the web server or the URL you are connecting to does not have a valid certificate from an authorized CA. But however, being a programmer you would want to find out the alternative way to solve this issue.

What you need to do is to import the server certificate and install it in your JDK's keystore. If I am talking greek, its ok. I too just leant this. Just follow these steps and you will be able to get rid of that error.

1. First of all you copy the URL that you are connecting to and paste it in your browser. Let us say you are using IE. Just paste the url in the address bar and press enter.

2. You will now probably see a dialog box warning you about the certificate. Now click on the 'View Certificate' and install the certificate. Ignore any warning messages.

3. Now that the server certificate is installed in your computer, your browser will not warn you when you visit the same site again. But however your JRE dumb as it is does not yet know about this certificate's existence until you add it to its keystore. Usually you will use the keytool to manage certificates. Keytool is a command-line utility with numerous arguments that allow you to create and manage keystores for housing digital certificates. For the complete documentation of keytool,<http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html>

4. You can list the current certificates contained within a keystore using they **keytool -list** command. The initial password for the cacerts keystore is **changeit**. For example:

C:\Program Files\Citrix\Citrix Extranet Server\SGJC\jre\bin>**keytool -list** **-keystore ..\lib\security\cacerts**

Enter keystore password: **changeit**

**You will then see the something like this:**

Keystore type: jks

Keystore provider: SUN

Your keystore contains 11 entries:

engweb, Wed Apr 11 16:22:49 EDT 2001, trustedCertEntry,

Certificate fingerprint (MD5): 8C:24:DA:52:7A:4A:16:4B:8E:FB:67:44:C9:D2:E4:16

thawtepersonalfreemailca, Fri Feb 12 15:12:16 EST 1999, trustedCertEntry,

Certificate fingerprint (MD5): 1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9

thawtepersonalbasicca, Fri Feb 12 15:11:01 EST 1999, trustedCertEntry,

Certificate fingerprint (MD5): E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41

verisignclass3ca, Mon Jun 29 13:05:51 EDT 1998, trustedCertEntry,

Certificate fingerprint (MD5): 78:2A:02:DF:DB:2E:14:D5:A7:5F:0A:DF:B6:8E:9C:5D

thawteserverca, Fri Feb 12 15:14:33 EST 1999, trustedCertEntry,

Certificate fingerprint (MD5): C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D

thawtepersonalpremiumca, Fri Feb 12 15:13:21 EST 1999, trustedCertEntry,

Certificate fingerprint (MD5): 3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D

verisignclass4ca, Mon Jun 29 13:06:57 EDT 1998, trustedCertEntry,

Certificate fingerprint (MD5): 1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10

verisignclass1ca, Mon Jun 29 13:06:17 EDT 1998, trustedCertEntry,

Certificate fingerprint (MD5): 51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20

verisignserverca, Mon Jun 29 13:07:34 EDT 1998, trustedCertEntry,

Certificate fingerprint (MD5): 74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93

thawtepremiumserverca, Fri Feb 12 15:15:26 EST 1999, trustedCertEntry,

Certificate fingerprint (MD5): 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A

verisignclass2ca, Mon Jun 29 13:06:39 EDT 1998, trustedCertEntry,

Certificate fingerprint (MD5): EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8

5. Now you have to add the previosly installed certificate to this keystore. To add, begin by exporting your CA Root certificate as a DER-encoded binary file and save it as **C:\root.cer**. (you can view the installed certificates under Tools->'Internet Options' ->Content->Certificates. Once you open the certificates, locate the one you just installed under 'Trusted Root Certification Authorities". Select the right one and click on 'export'. You can now save it (DER encoded binary) under your c: drive.

6. Then use the **keytool -import** command to import the file into your cacerts keystore.

    For example:-alias myprivateroot -keystore ..\lib\security\cacerts -file c:\root.cer

Enter keystore password: **changeit**

Owner: CN=Division name, OU=Department, O=Your Company, L=Anytown,

ST=NC, C=US, EmailAddress=you@company.com

Issuer: CN=Division name, OU=Department, O=Your Company, L=Anytown,

ST=NC, C=US, EmailAddress=you@company.com

Serial number: 79805d77eecfadb147e84f8cc2a22106

Valid from: Wed Sep 19 14:15:10 EDT 2001 until: Mon Sep 19 14:23:20 EDT 2101

Certificate fingerprints:

MD5: B6:30:03:DC:6D:73:57:9B:F4:EE:13:16:C7:68:85:09

SHA1: B5:C3:BB:CA:34:DF:54:85:2A:E9:B2:05:E0:F7:84:1E:6E:E3:E7:68

Trust this certificate? [no]: **yes**

Certificate was added to keystore

7. Now run **keytool -list** again to verify that your private root certificate was added:

C:\Program Files\Citrix\Citrix Extranet Server\SGJC\jre\bin>**keytool -list -keystore ..\lib\security\cacerts**

You will now see a list of all the certificates including the one you just added.

This confirms that your private root certificate has been added to the Extranet server cacerts keystore as a trusted certificate authority.