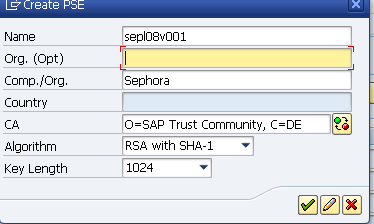
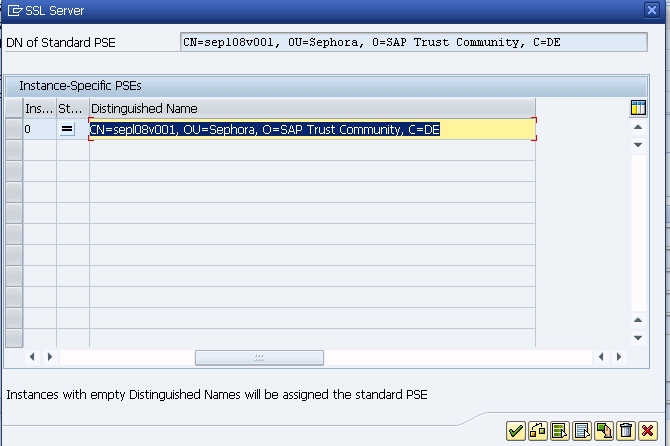
* 1. **SSL Setup**

***Creating the SSL Server PSE***

call transaction STRUST

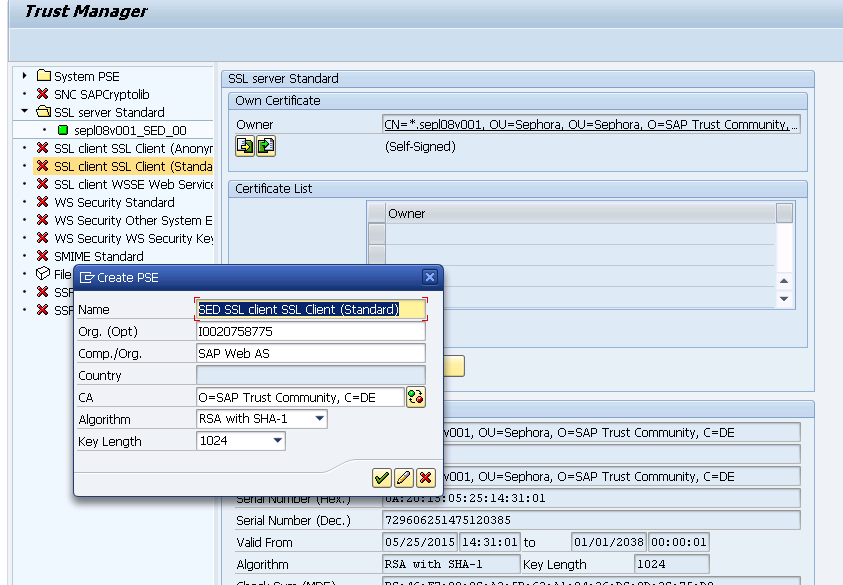
Select SSL server standard and create

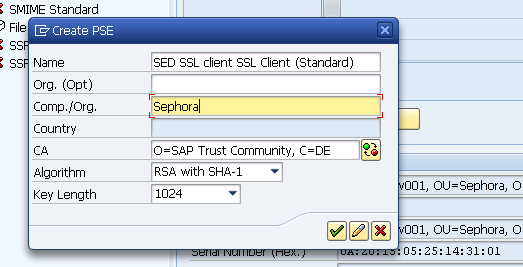




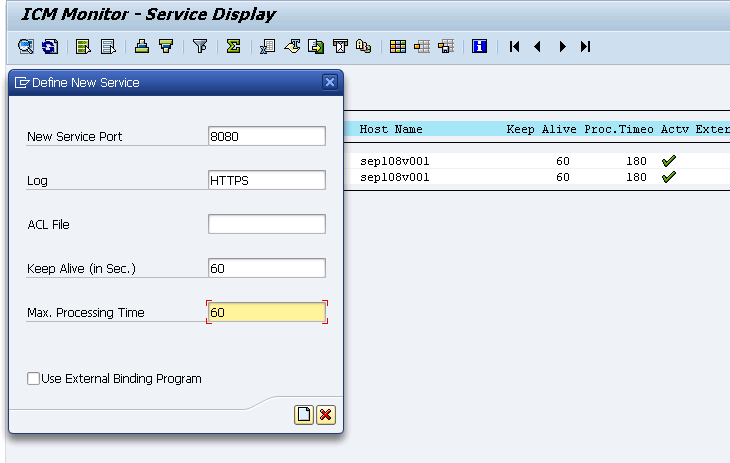


***Creating the SSL client PSE***





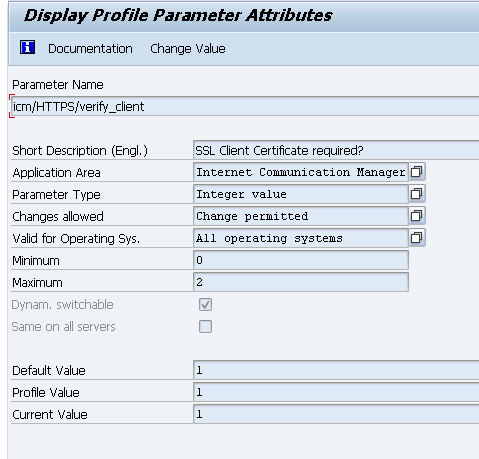
***HTTPS service creation in SMICM***

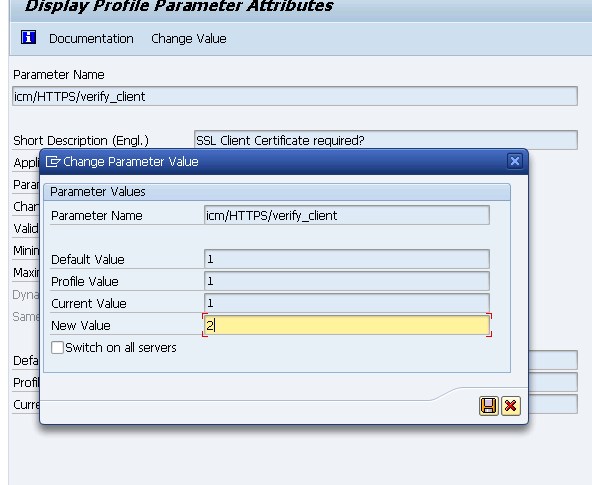


**1.2 Profile Parameters**

**Transaction code: RZ11**

**Profile Parameter:** icm/HTTPS/verify\_client = 2





***The ICM trusts the system certificate for principal propagation***

1.Transaction code: RZ10

2.Select the profile you like to edit, for example, the instance profile.

3.Select the radio button for Extended maintenance and choose the Change button.

4.Create the following two parameters:

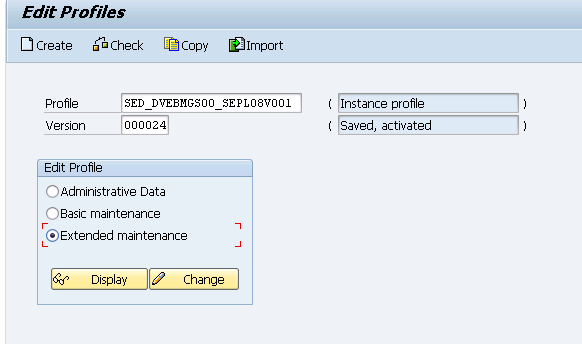
icm/HTTPS/trust\_client\_with\_issuer= \*

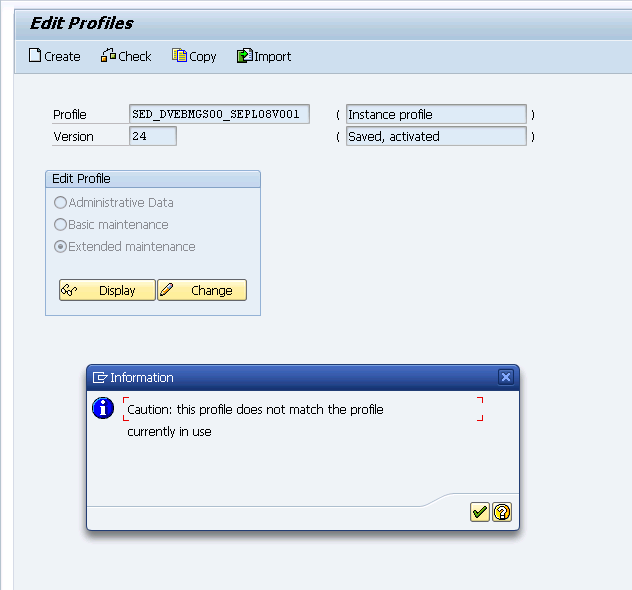
icm/HTTPS/trust\_client\_with\_subject= \*

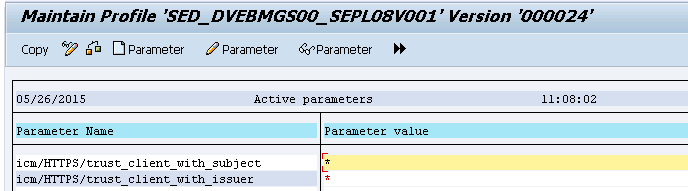
5.Save the profile.

6.Open the ICM Monitor (transaction code: SMICM) and restart the ICM. To do so, choose  Administration --> ICM--> Exit Hard--> Global .

7.Verify that the two profile parameters have been taken over by ICM as desired. To do so, choose  Goto -->Parameter--> Display  .







Save

**1.4 Providing Logon Data**

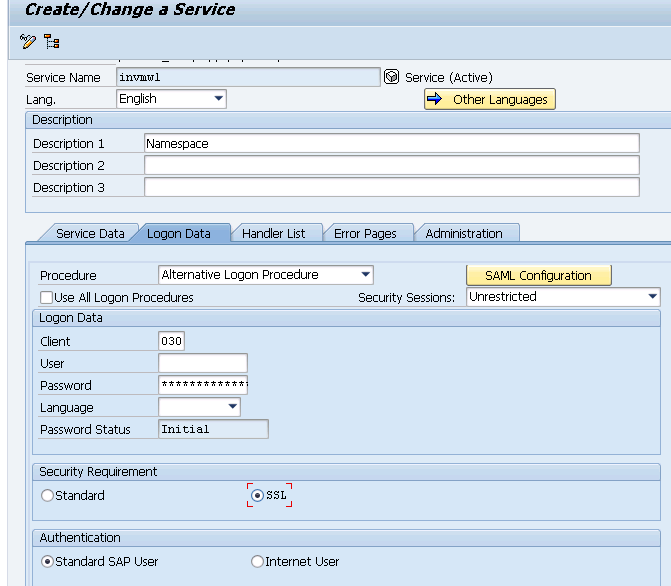
Transaction code: Sicf

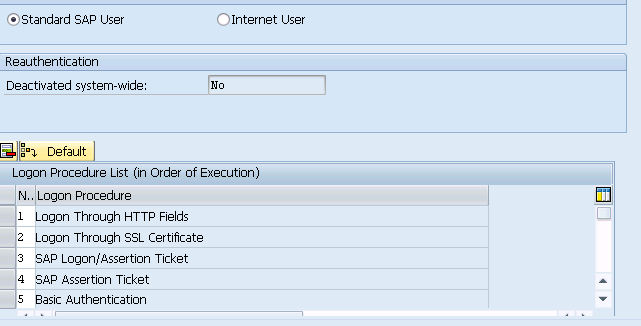
Goto /default\_host/sap/opu/odata

Click on invmwl

Change the procedure to Alternative Logon Procedure.

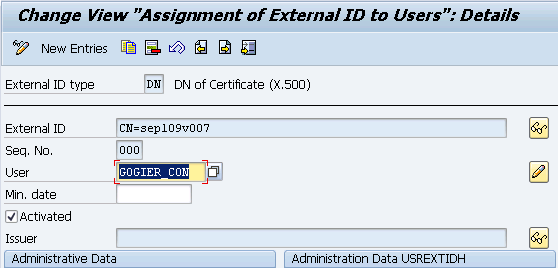
Security Requirements --> select SSL

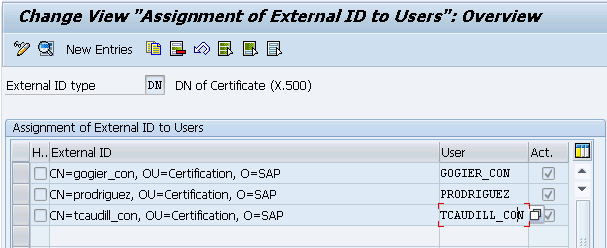




**1.5.Mapping Certificates to Corresponding Users**

1. Transaction code: EXTID\_DN
2. Switch to edit mode.
3. Create a new entry.
4. Save the mapping.





Note : Please make sure the value for **CN** in External ID field is maintained in lower case. This value for CN is actually the login id user enters on device.

To avoid any authentication failures because of this, we can choose to maintain 2 entries with both lower and upper case user IDs

Example : For user gogier\_con, we cn maintain below entries.

CN=gogier\_con, OU=Certification, O=SAP

CN=GOGIER\_CON, OU=Certification, O=SAP

**1.6. Export Gateway Certificates for SMP**

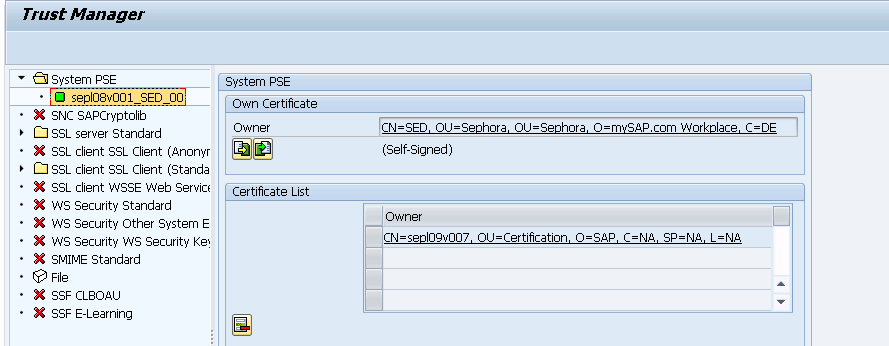
**Export System PSE Certificate**

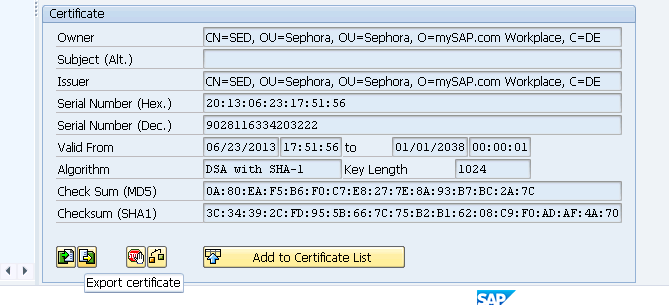
1.Transaction code: STRUST

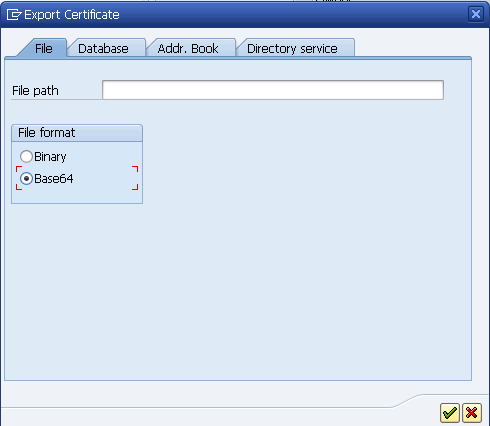
2.Open System PSE group and double click on the certificate node.

3.Double click on the Owner entry under “Own certificate” section and scroll to the bottom of the screen.

4. Choose to export certificate, and save the certificate as sed\_system\_pse.crt.







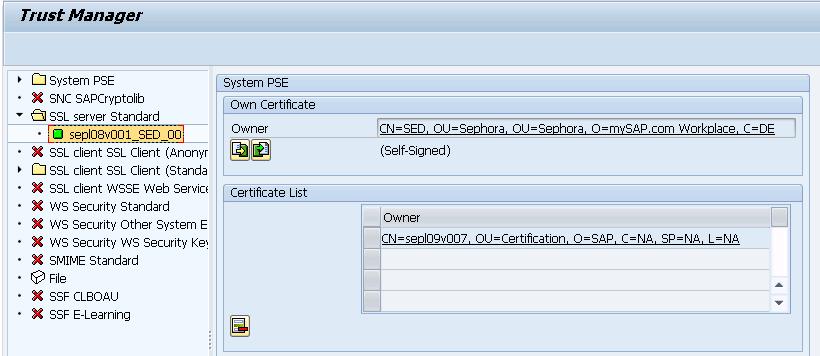
**Export SSL Server certificate**

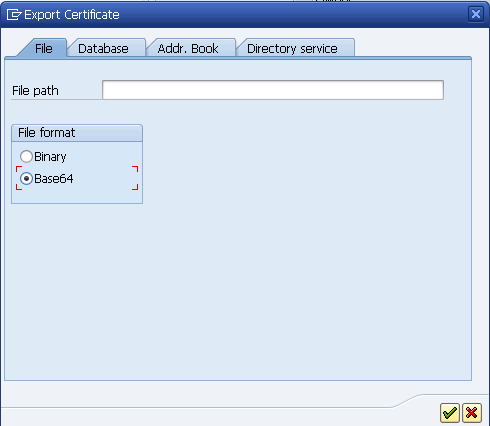
1.Transaction code: STRUST

2.Open SSL Server Standard group and double click on the certificate node.

3.Double click on the Owner entry under “Own certificate” section and scroll to the bottom of the screen.

4. Choose to export certificate, and save the certificate as sed\_ssl\_server.crt.





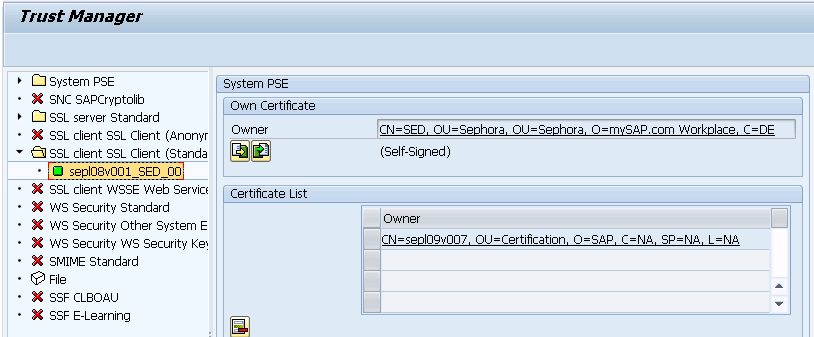
**Export SSL Client Certificate**

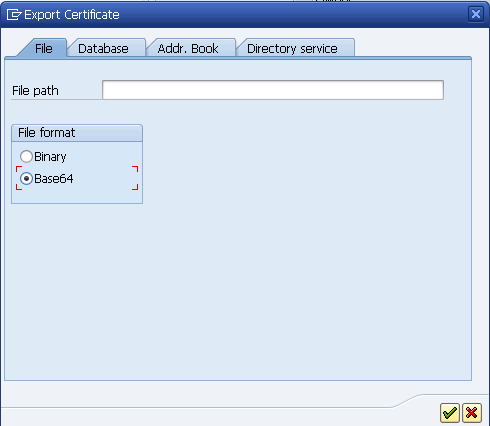
1.Transaction code: STRUST

2.Open SSL Client SSL Client(Standard) group and double click on the certificate node.

3.Double click on the Owner entry under “Own certificate” section and scroll to the bottom of the screen.

4. Choose to export certificate, and save the certificate as sed\_client\_server.crt.





**1.7. Import SMP self-signed certificate to Gateway trust store**

Copy smp\_crt.cer certificate file from the location <SMP3\_HOME>\Server\configuration on SMP server to the SAP Gateway system.

**Import SMP Cert to System PSE**

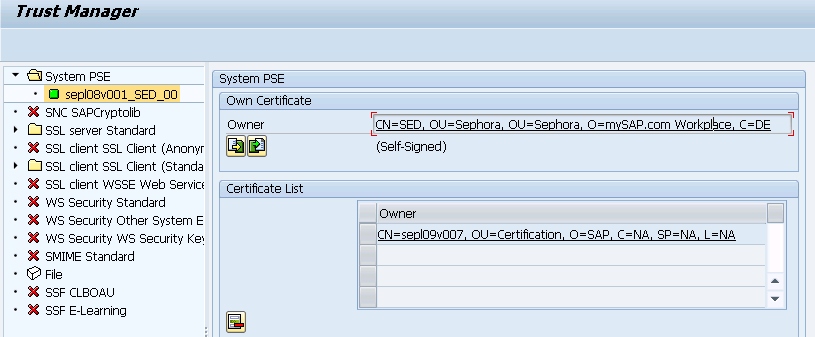
1.Transaction code: STRUST

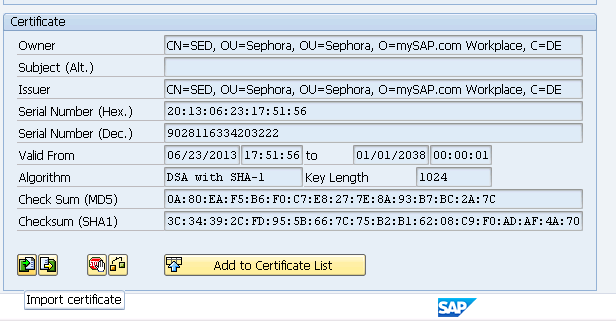
2.Open System PSE group and double click on the certificate node.

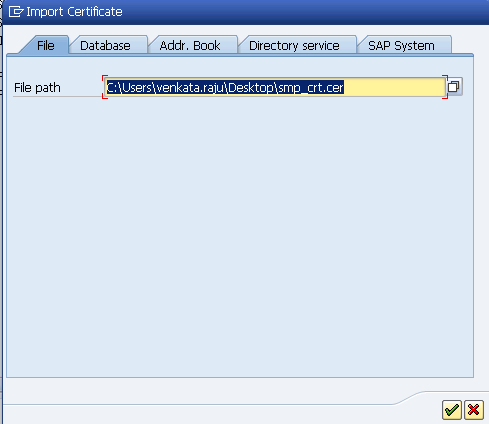
3.Double click on the Owner entry under “Own certificate” section and scroll to the bottom of the screen.

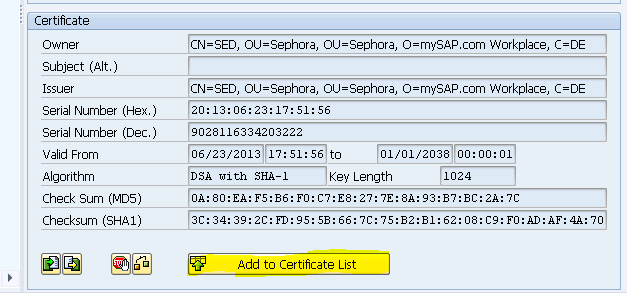
4. Choose to import certificate, and browse for smp\_crt.cer file and choose to import.

5. After import, click on ‘Add to certificate list’ to add the certificate to System PSE certificates list.









**Import SMP Cert to SSL Server Standard**

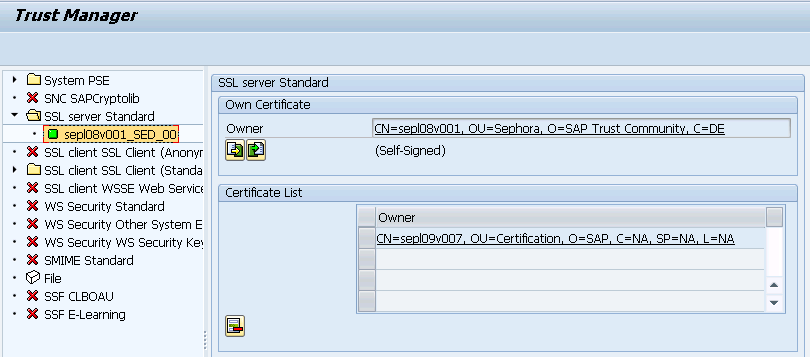
1.Transaction code: STRUST

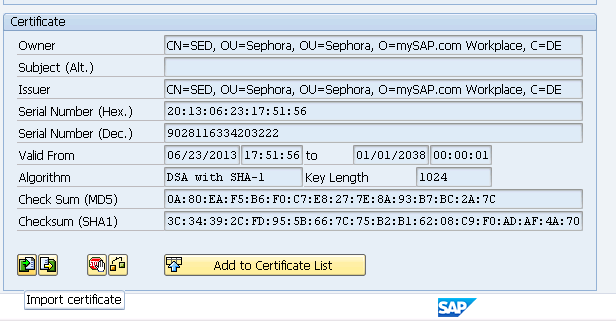
2.Open SSL Server Standard group and double click on the certificate node.

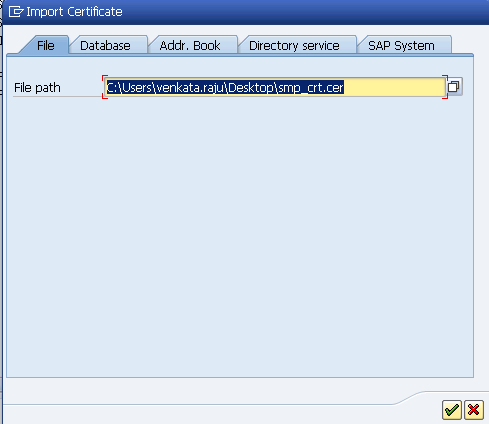
3.Double click on the Owner entry under “Own certificate” section and scroll to the bottom of the screen.

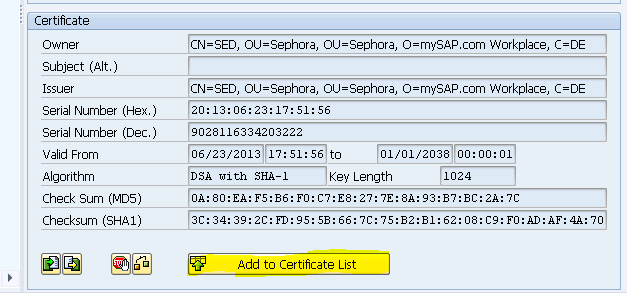
4. Choose to import certificate, and browse for smp\_crt.cer file and choose to import.

5. After import, click on ‘Add to certificate list’ to add the certificate to System PSE certificates list.









**Import SMP Certificate SSL Client Standard**

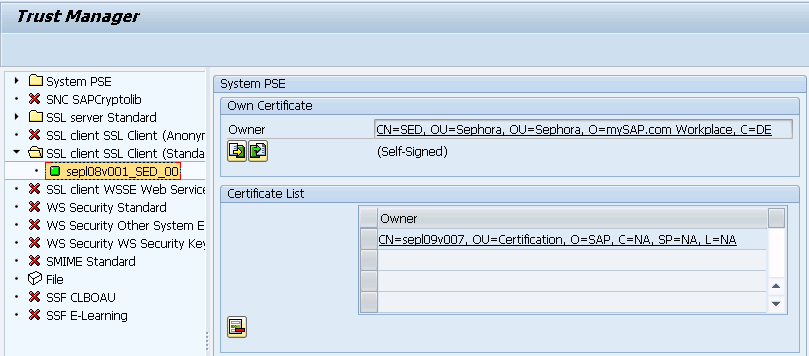
1.Transaction code: STRUST

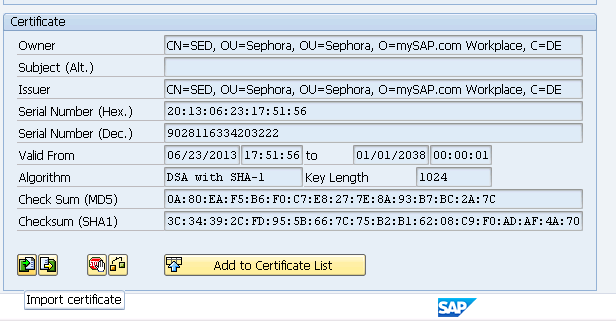
2.Open SSL Client SSL Client(Standard) group and double click on the certificate node.

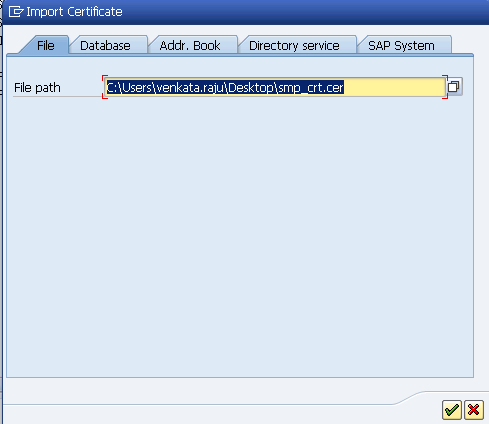
3.Double click on the Owner entry under “Own certificate” section and scroll to the bottom of the screen.

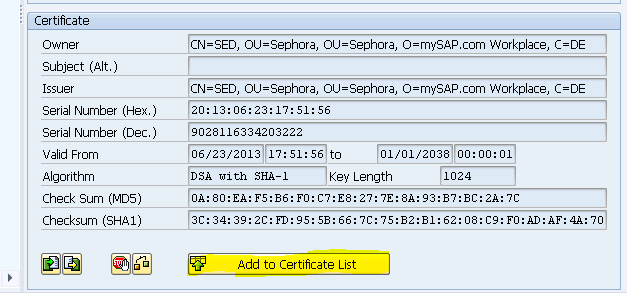
4. Choose to import certificate, and browse for smp\_crt.cer file and choose to import.

5. After import, click on ‘Add to certificate list’ to add the certificate to System PSE certificates list.









**1.8. Import NetWeaver Gateway Certificates to SMP Keystore on SMP Server**

Please follow below procedure to import the certificate into SMP keystore.

1. Take a backup of below files from the location <SMP3\_HOME>\Server\configuration before proceeding with cert import.

sapag.cer

smp\_crt.cer

smp\_keystore.jks

2. Copy the certificates generated from Gateway system to the folder <SMP3\_HOME>\\_smpjvm\bin.

3. Run the following commands for the certificates to be imported to SMP keystore

keytool -import -trustcacerts -alias sed\_pse -file sed\_system\_pse.crt -keystore <SMP3\_HOME>\Server\configuration\smp\_keystore.jks

keytool -import -trustcacerts -alias sed\_ssl\_server -file sed\_ssl\_server.crt -keystore <SMP3\_HOME>\Server\configuration\smp\_keystore.jks

keytool -import -trustcacerts -alias sed\_ssl\_client -file sed\_client\_server.crt -keystore <SMP3\_HOME>\Server\configuration\smp\_keystore.jks

you have to enter the keystore password to proceed, and enter 'yes' to confirm updating the keystore. Refer below screenshot.

