ONESOURCE™ INDIRECT TAX - SAP INTEGRATIONS

HTTPS Connection to Determination

THOMSON REUTERS®

Reference:

The most current version of the instructions provided in this document can be found in the ONESOURCE Support Network in Install Certificate for SAP Global Integration 6.x.x.x.. Please make sure you always download the most current version.

Table of Contents

Purpose:

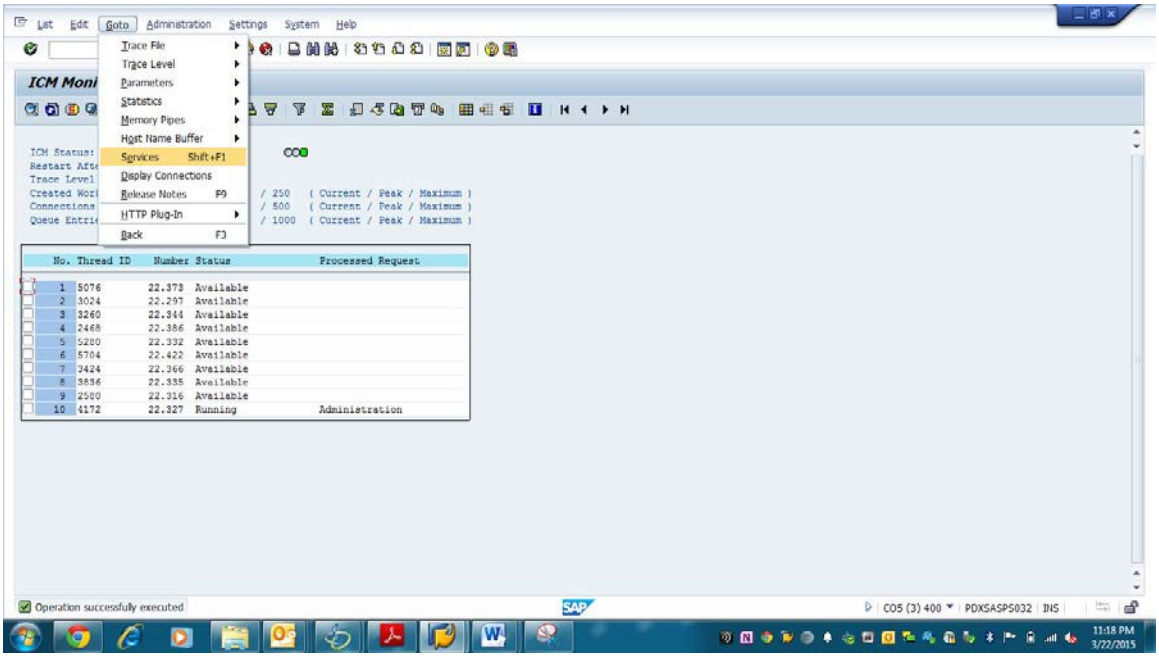
The main intend of this document is in assisting an experienced SAP Basis person in setting up a secure connection (HTTPS) between the SAP system and the ONESOURCE Indirect Tax Determination. This process isn't specific to the SAP Integration, but a common task for any SOAP based integration between an SAP and a non-SAP system. This document assumes that the person doing the setup has extensive experience in this task.

Prerequisites

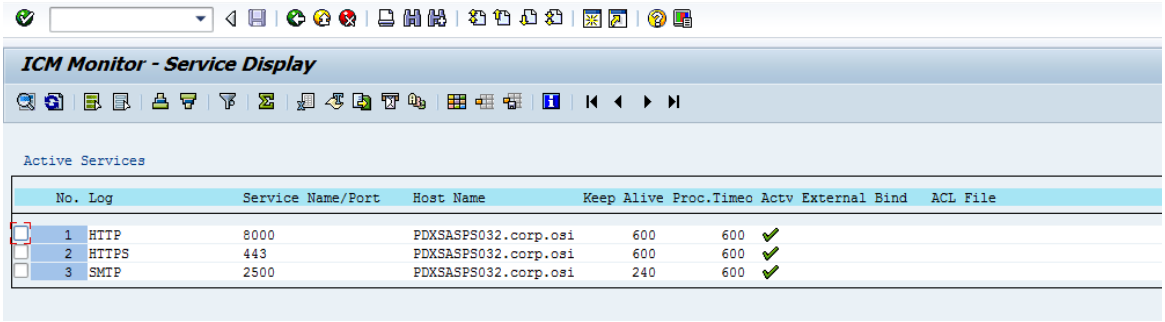
HTTPS Service

The HTTPS service must be running within your SAP system, make sure this is the case:

1) Check if the HTTPS service is running in transaction SMICM. Go to transaction SMICM. Click on GOTO->SERVICES



2) HTTPS service should be up and running.

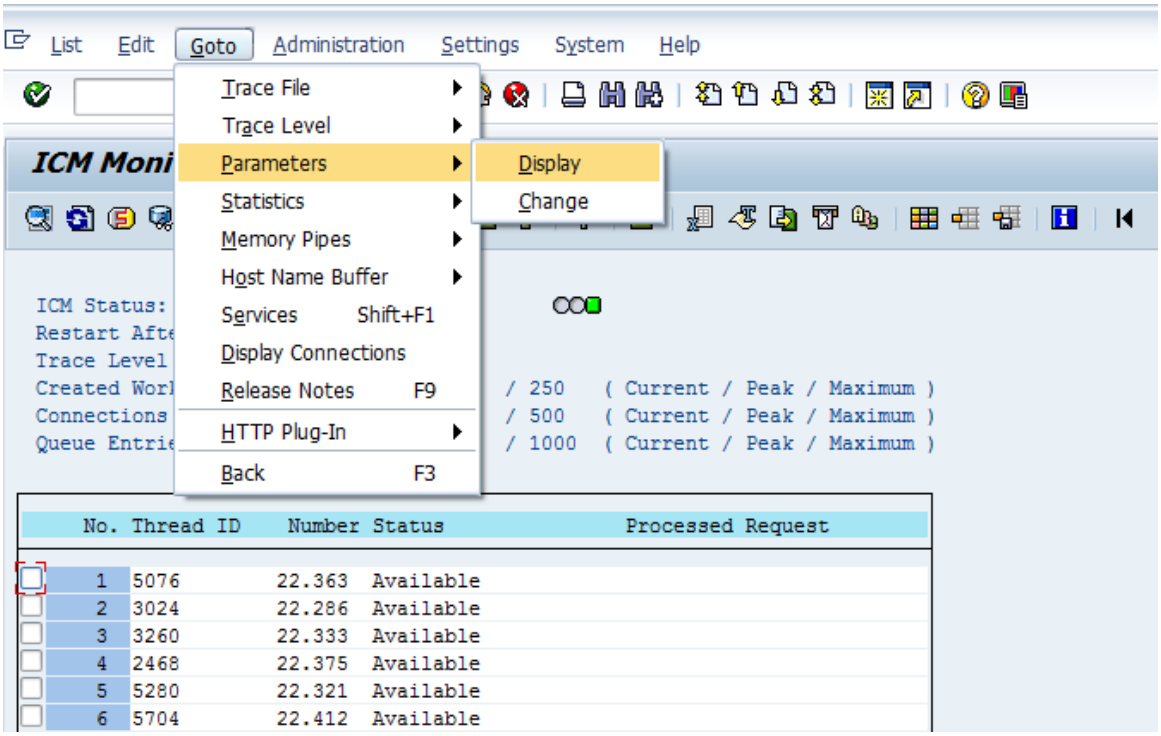


Note: If not create a https service by following steps in section Creating HTTPS service.

SAP Cryptographic Library

The SAP Cryptographic Library must be installed properly:

1) To check the installation of SAP Cryptographic Library, please go to transaction SMICM.
   Click on GOTO->PARAMTERS->DISPLAY



Cryptographic Library Parameters in SMICM:

The following parameters are the file path for SAP Cryptographic Library. Please remember the file name may be different based on version of the library whether it's COMMONCRYPTOLIB 8 or SAPCRYPTOLIB 5.5.5 and also depends on SAP OS.

HTTPS (SSL) settings
icm/HTTPS/verify_client = 1
ssf/name = SAPSECULIB
ssf/ssfapi_lib = E:\usr\sap\C05\SYS\exe\uc\NTAMD64\sapcrypto.dll
sec/libsapsecu = E:\usr\sap\C05\SYS\exe\uc\NTAMD64\sapcrypto.dll
ss1/ssl_lib = E:\usr\sap\C05\SYS\exe\uc\NTAMD64\sapcrypto.dll

Note: If the SAP Cryptographic Library is not installed properly then please move to section Installing the SAP Cryptographic Library of this document.

HTTPS Port Check

Verify whether HTTPS port parameter is present in the SMICM Parameters. To check the https parameter, navigate to Parameters page in the SMICM transaction as shown above. The HTTPS parameters are shown below. Please create the parameter if it did not exist.

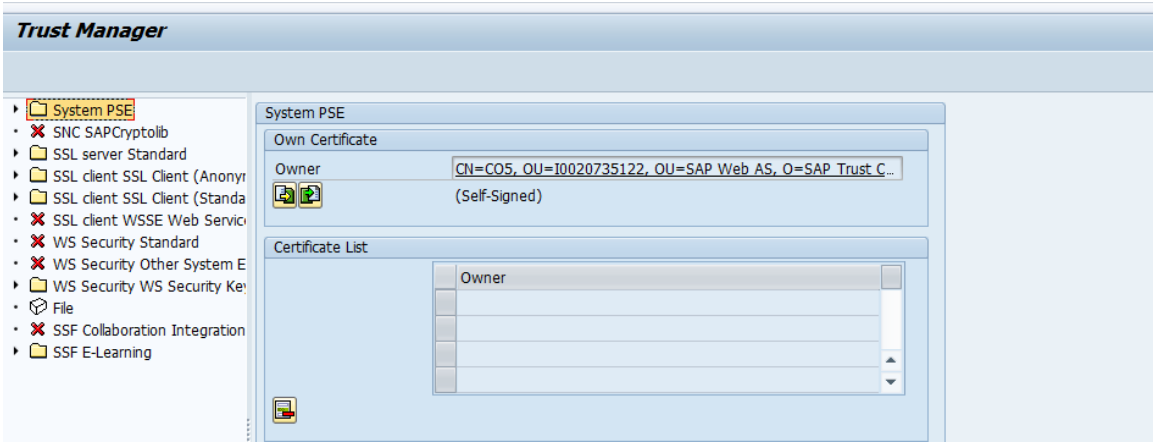
ICM Parameter
Services
icm/server_port_0 = PROT=HTTP, PORT=8000, TIMEOUT=600, PROCTIMEOUT=600
icm/server_port_1 = PROT=HTTPS, PORT=443, TIMEOUT=600, PROCTIMEOUT=600
icm/server_port_2 = PROT=SMTP, PORT=2500, TIMEOUT=240, PROCTIMEOUT=600

Personal Security Environment (PSE)

Verify whether the required PSE's have self-signed certificates in transaction STUST. The required PSE's for HTTPS connections are

i) System PSE
ii) SSL Server Standard PSE
iii) SSL Client Standard PSE
iv) SSL Client Anonymous PSE

Make sure you check each one of them.



Note: If the above mentioned PSE's did not have self-signed certificate, create it by following steps in section Creating Self-Signed Certificates in the PSE.

Installing the Certificates

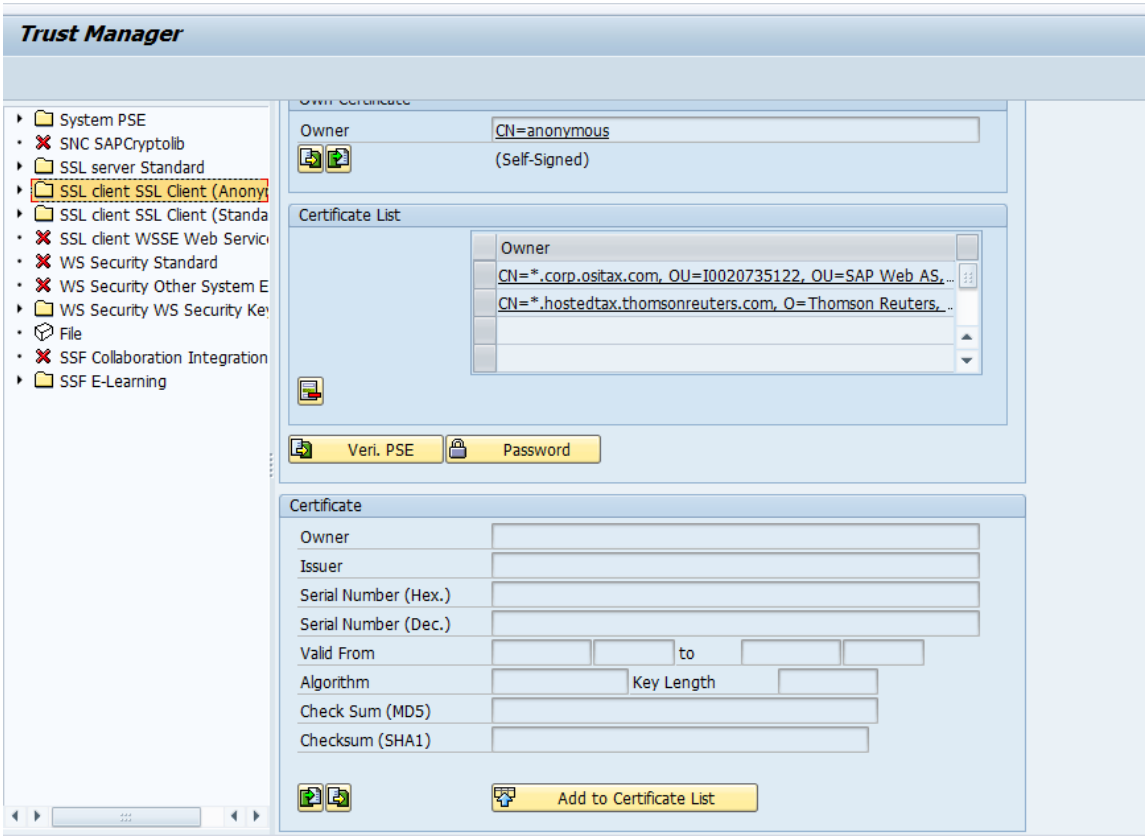
Downloading Security Certificates

Please follow the instructions provided via the Download Security Certificate.pdf document.

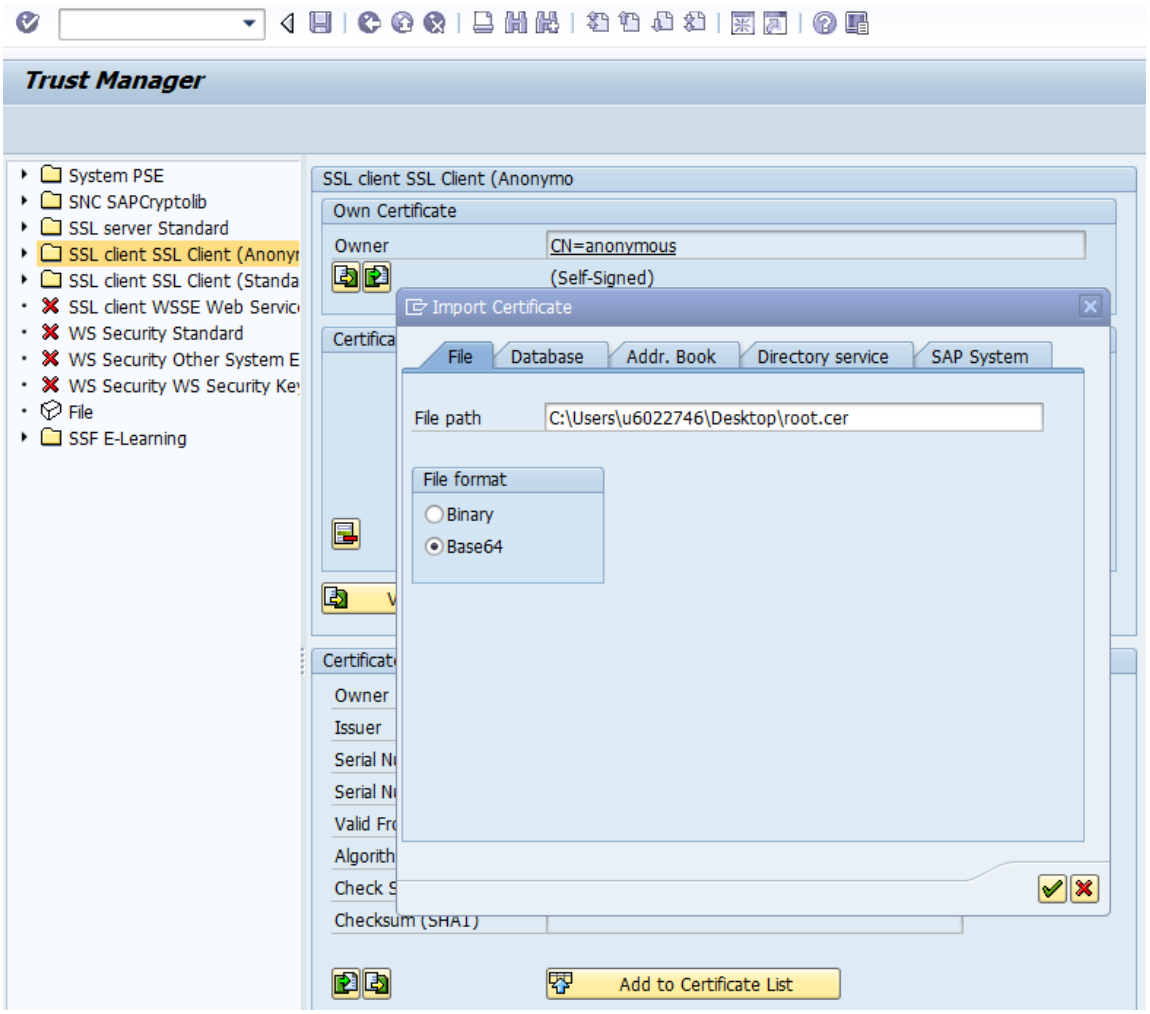
Certificate Install

Once you have downloaded the relevant certificates you need to install them in SAP following these steps:

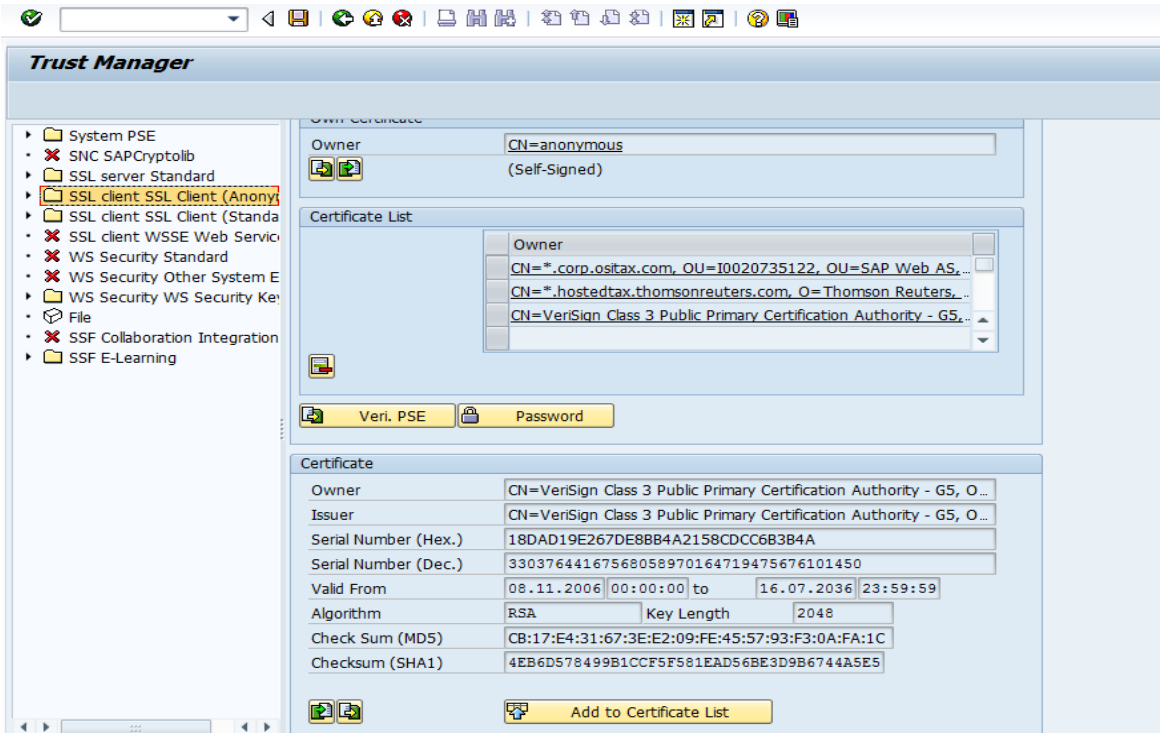
1) Go to transaction STRUST, double click on the **SSL client (Anonymous) PSE**:



2) Go to menu **Certificate -> Import**. In the pop-up browse to the certificate file at the location you downloaded it in the prior step and select that file. Make sure the file format matches the one you used for the download, then **Enter**.



3) Click **Add to Certificate List** button at the end of the screen and finally click on **Save**



NOTE: In some older version of SAP, the Internet Communication Manager (ICM) has to be restarted if you install new certificates. In those cases please restart the ICM in transaction SMICM.

Configure Integration for SAP

Follow the instructions provided in the *Integration for SAP Install Guide* in chapter *Connecting SAP and Determination*.

Supporting Documentation

Installing the SAP Cryptographic Library

Download SAP Cryptographic Library from SAP Market Place in the Installations and Upgrades section, and follow the below steps to deploy the library:

As user <sid>adm:

1) Extract the contents of the SAP Cryptographic Library installation package.

2) Copy the library file and the configuration tool sapgenpse.exe to the directory specified by the application server's profile parameter DIR_EXECUTABLE. In the following, we represent this directory with the notation$(DIR_EXECUTABLE).

   UNIX:

   DIR_EXECUTABLE: /usr/sap/<SID>/SYS/exe/run/
   Location of SAP Cryptographic Library: /usr/sap/<SID>/SYS/exe/run/libsapcrypto.so

   Windows NT:

   DIR_EXECUTABLE: <DRIVE>:\usr\sap\<SID>\SYS\exe\run
   Location of SAP Cryptographic Library: <DRIVE>:\usr\sap\<SID>\SYS\exe\run\sapcrypto.dll

3) Check the file permissions for the SAP Cryptographic Library. If, for example, you copied the library to its location using ftp on UNIX, then the file permissions may not be set correctly. Make sure that <sid>adm (or SAPService<SID> under Windows NT) is able to execute the library's functions.

4) Copy the ticket file to the sub-directory sec in the instance directory $(DIR_INSTANCE).

   Examples

   UNIX:

   DIR_INSTANCE: /usr/sap/<SID>/<instance>
   Location of the ticket: /usr/sap/<SID>/<instance>/sec/ticket

   Windows NT:

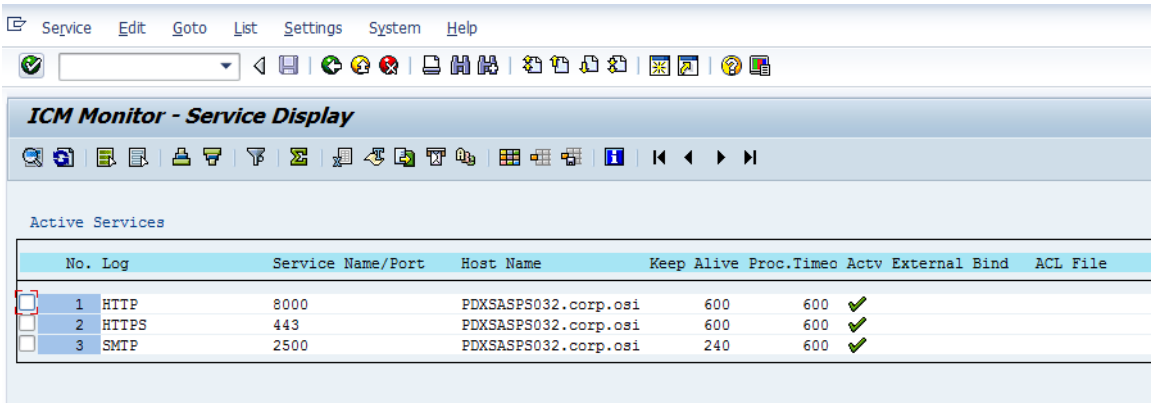
   DIR_INSTANCE: <DRIVE>:\usr\sap\<SID>\<instance>
   Location of the ticket: <DRIVE>:\usr\sap\<SID>\<instance>\sec\ticket

5) Set the environment variable SECUDIR to the sec sub-directory. The application server uses this variable to locate the ticket and its credentials at run-time.

NOTE: If you set the environment variable using the command line, then the value may not be applied to the server's processes. Therefore, we recommend setting SECUDIR in the startup profile for the server's user or in the registry (Windows NT). Also, please refer to SAP Note 0000510007 for more details.

Creating HTTPS service

1) In SMICM->GOTO->SERVICES



2) Click on Service->Create

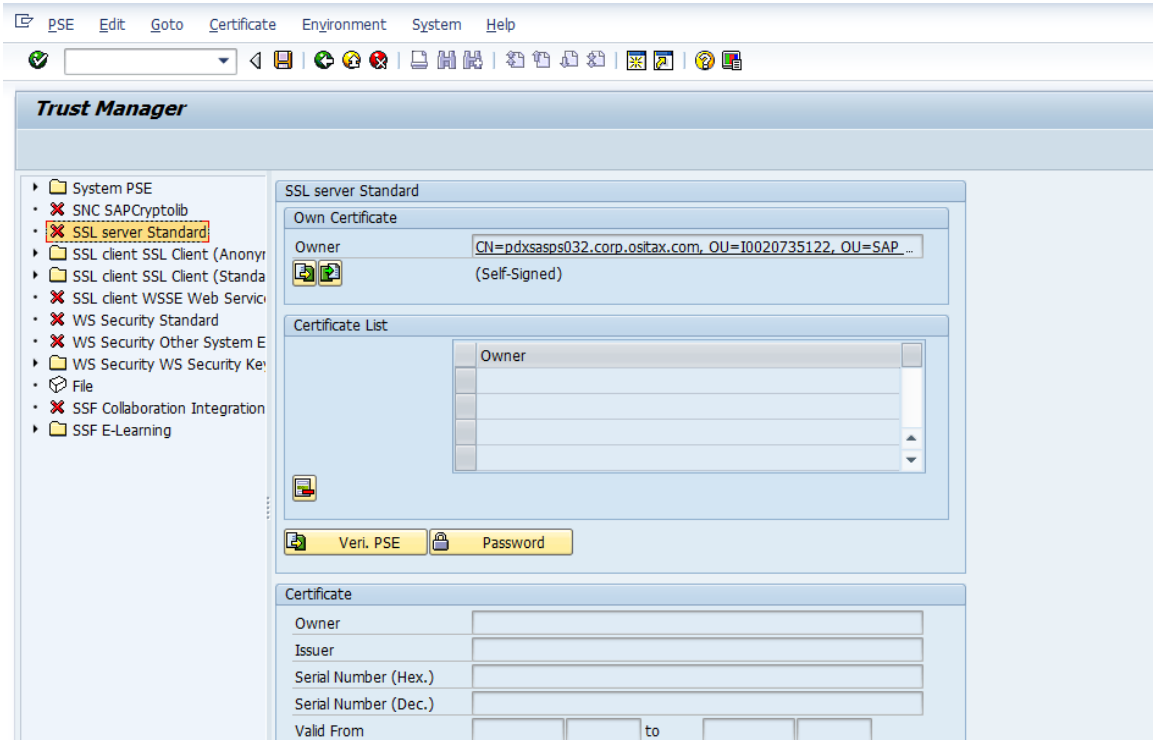
Enter the following parameters as shown below. However, please use the *Port Number* according to your configuration:

New Service Port: 44301
Log: HTTPS
ACL File: Blank
Keep Alive (in Sec.): 600
Max. Processing Time: 600
SSL Client Verification: 1 Optional

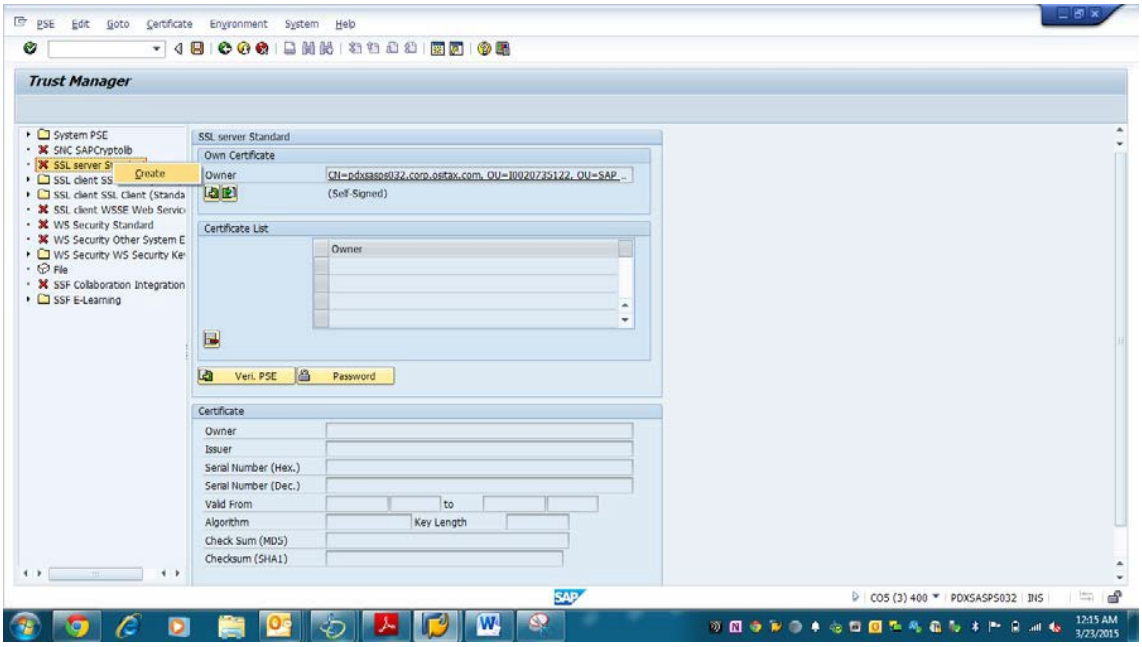
3) Finally click the **Create** icon. The new service will be created.

Creating Self-Signed Certificates in the PSE

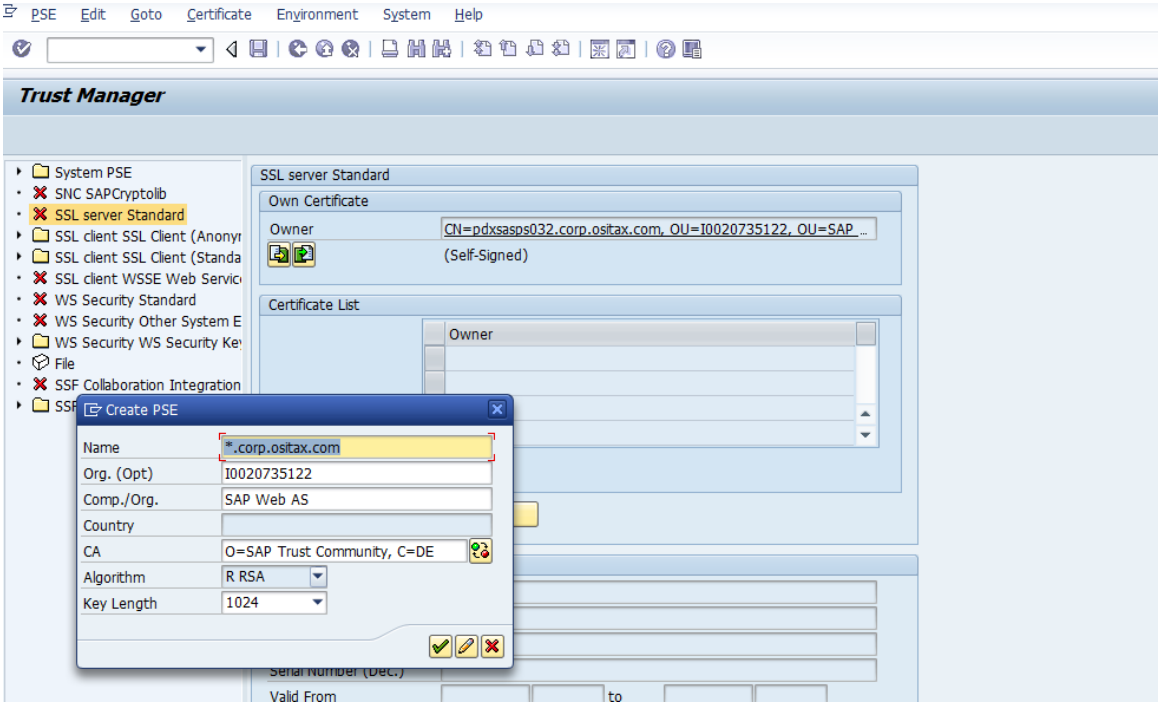
1) In transaction STRUST
   Select the PSE node in which you are going to create the self-signed certificate. For example for SSL Server Standard.

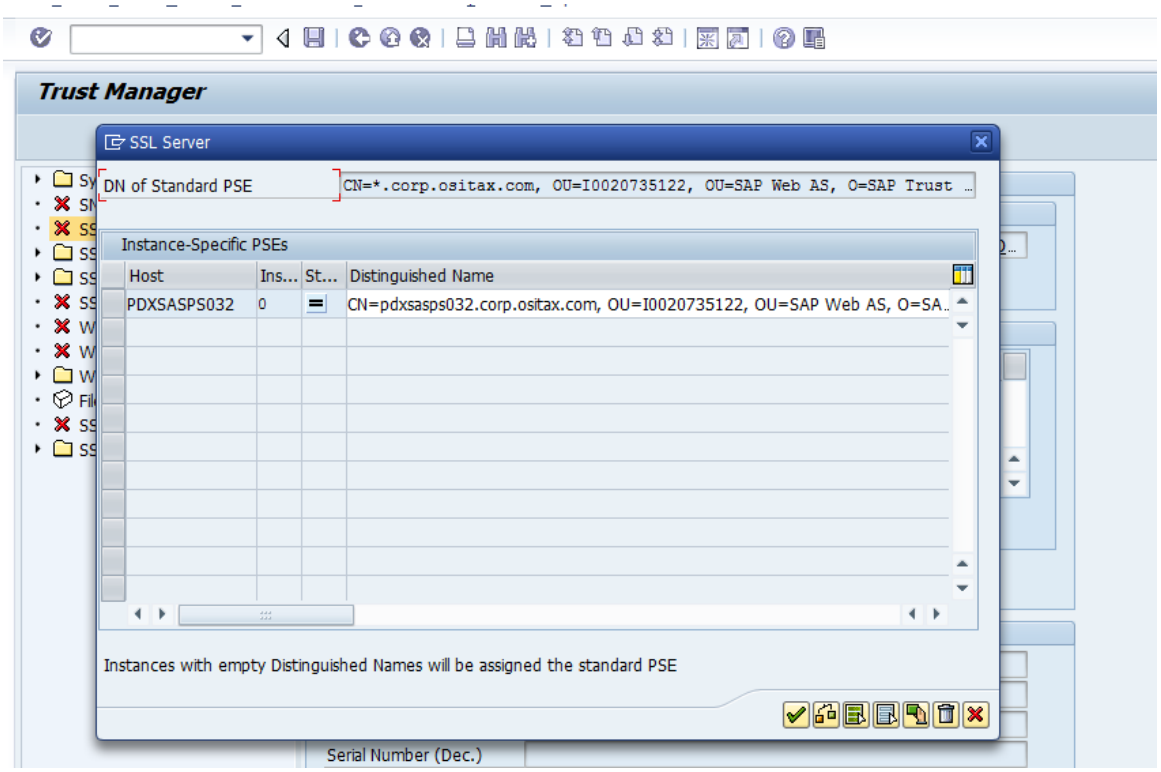


2) Right click on the node and select **Create**

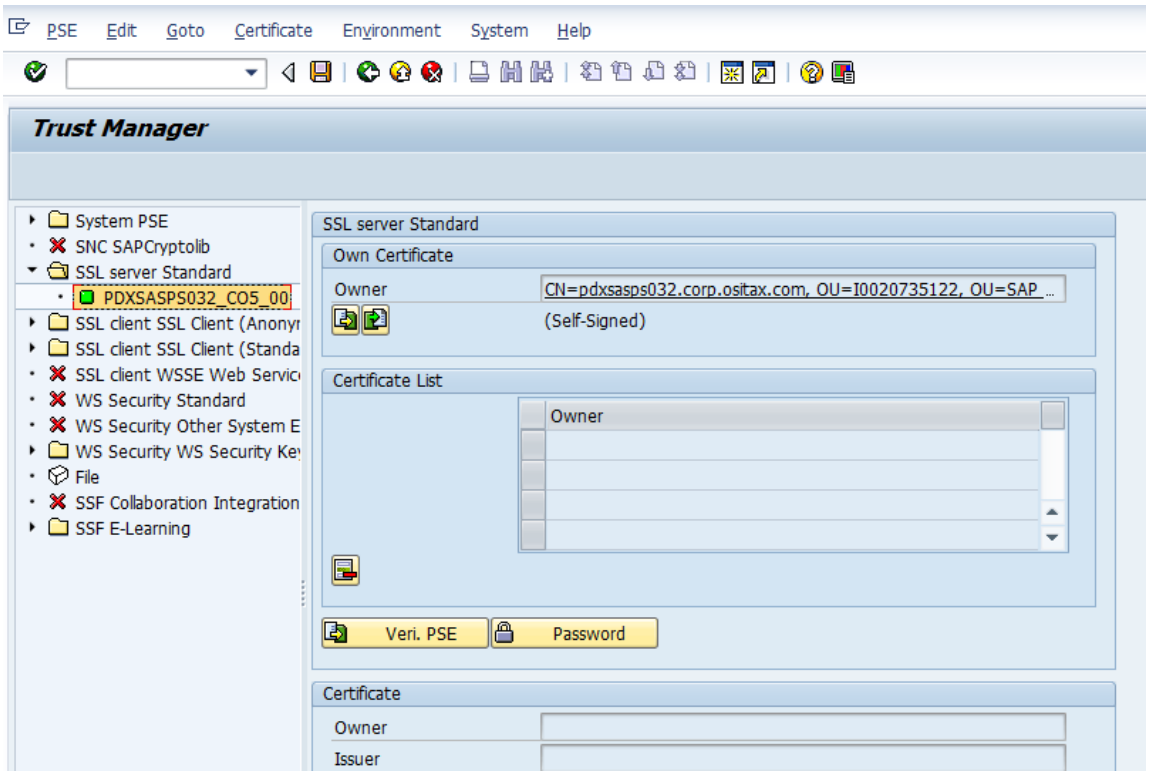


3) Press **Enter** in the next two screens.





4) A new self-signed certificate is create under the PSE you selected.


PSE
Edit
Goto
Certificate
Environment
System
Help
Trust Manager
System PSE
SNC SAPCryptolib
SSL server Standard
PDXSASPS032_CO5_00
SSL client SSL Client (Anonyr
SSL client SSL Client (Standa
SSL client WSSE Web Servic
WS Security Standard
WS Security Other System E
WS Security WS Security Ke
File
SSF Collaboration Integration
SSF E-Learning
SSL server Standard
Own Certificate
Owner
CN=pdxsasps032.corp.ositax.com, OU=I0020735122, OU=SAP
(Self-Signed)
Certificate List
Owner
Veri. PSE
Password
Certificate
Owner
Issuer