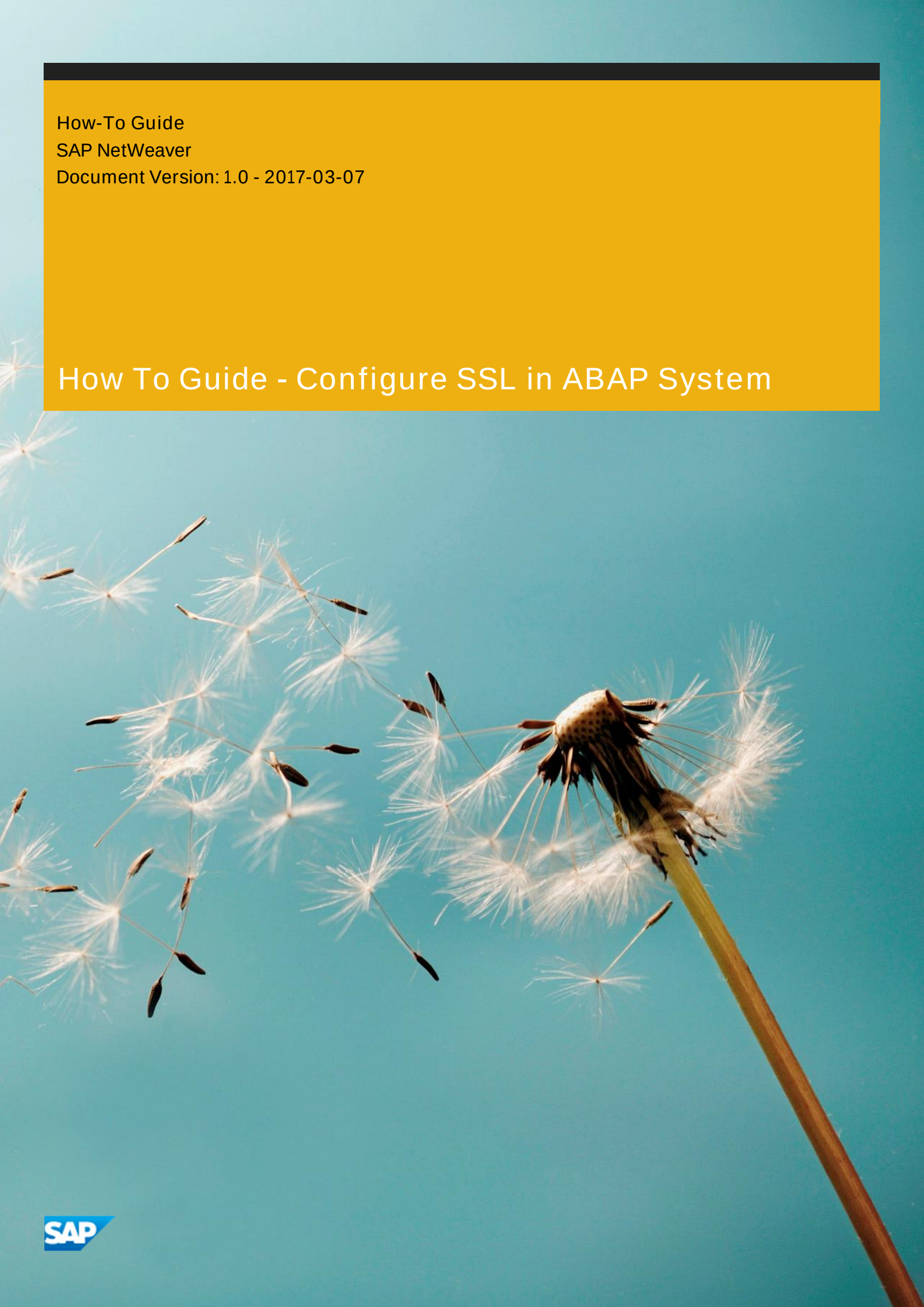
How-To Guide
SAP NetWeaver
Document Version: 1.0 - 2017-03-07

How To Guide - Configure SSL in ABAP System



Document History

Document Version	Description
1.0	First official release of this guide

Table of Contents

1 Business Scenario

As part of a system implementation, there is a requirement to establish SSL (Secure Sockets Layer) security for an ABAP-based system that requires secure, encrypted communications.

2 Background Information

SSL (Secure Sockets Layer) is a communication method whereby secure communication between system entities is accomplished by the use of encryption facilitated by X.509 certificates published by Certificate Authorities (CA) in tandem with public and private decryption keys.

3 Prerequisites

These tasks should be performed by a qualified SAP Basis Administrator, with a solid conceptual understanding of SSL and certificate-based encryption concepts.

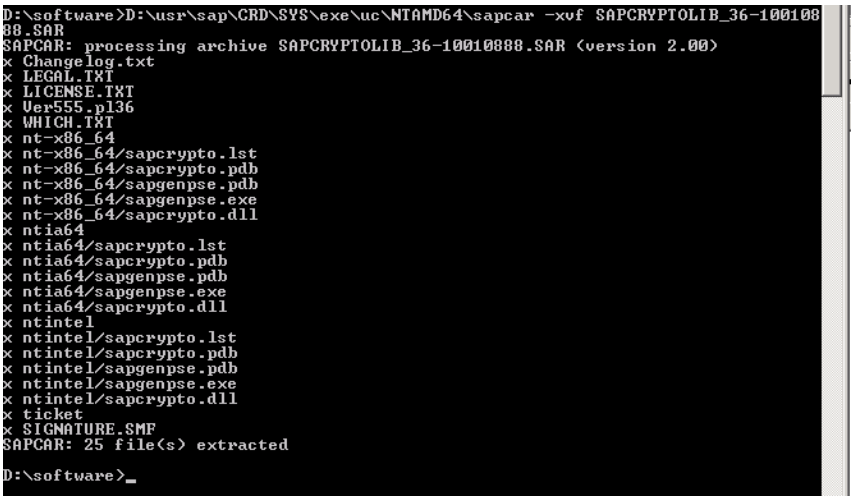
4 Step-by-Step Procedure

4.1 Install the SAP Cryptographic Libraries

1. Download the latest SAP Crypto Libraries from the SAP Marketplace. Access URL http://service.sap.com/swdc, and follow path Support Packages and Patches → Browse our Download Catalog → SAP Cryptographic Software → SAPCryptolib for Installations → SAPCryptoLibs<version>

2. Select the desired platform, and download the latest version of the software.

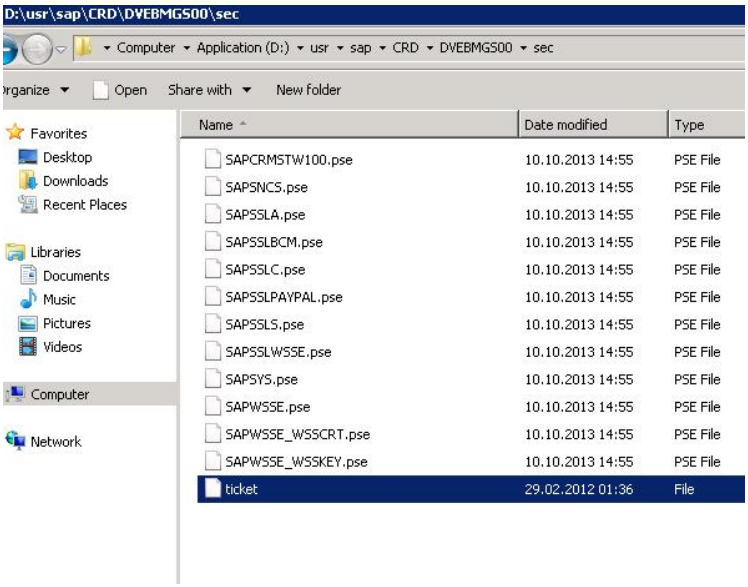
3. Login with <sid>adm into the server and extract the content of the downloaded SAR file containing the SAPCrypto libraries.



4. Copy the library file and the binary file sapgenpse to the DIR_EXECUTABLE directory, in unix is /usr/sap/<SID>/SYS/exe/run on windows is <DRIVE>:\usr\sap\<SID>\SYS\exe\run\

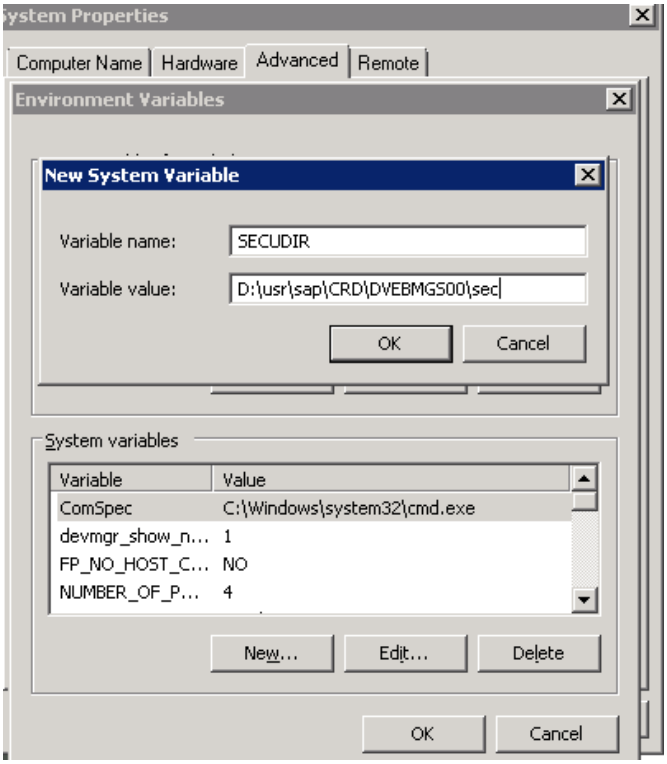
5. Verify the files have the right permissions with execution permissions for <sid>adm and SAPService<SID>

6. Copy the ticket file to the “sec” directory of the instance directory



7. Set the environment variable SECUDIR to the “sec” directory of the instance directory, this is used by the application server to find the ticket file and locate its credentials at runtime. By example in Windows:

Right click in my computer → Properties →Advance system settings →Environment Variables → set the variable under System variables



4.2 Add Required Profile Parameters

1. Set the following profile parameters:

   ssl/ssl_lib
   sec/libsapsecu
   ssf/ssfapi_lib
   ssf/name
   icm/HTTPS/verify_client

   For example:

   #SSL Configuration
   ssl/ssl_lib = D:\usr\sap\CRD\DVEBMGS00\exe\sapcrypto.dll
   sec/libsapsecu = D:\usr\sap\CRD\DVEBMGS00\exe\sapcrypto.dll
   ssf/ssfapi_lib = D:\usr\sap\CRD\DVEBMGS00\exe\sapcrypto.dll
   ssf/name = SAPSECULIB
   icm/HTTPS/verify_client=1

   In case of dual stack add the following parameter

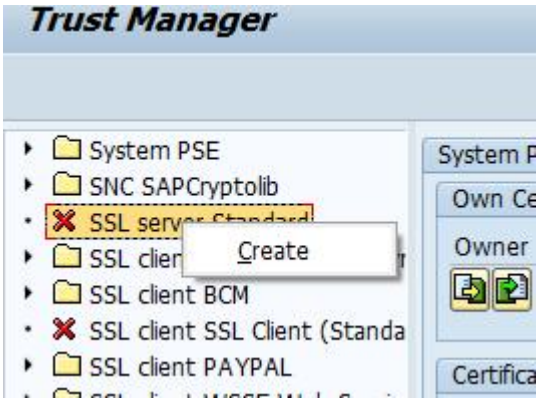
   ssl/pse_provider = ABAP

2. After the parameters are added, restart the ABAP system.

4.3 Configure SSL Server PSE for Incoming Request

1. Create SSL Server PSE by calling transaction STRUST.

2. Select the SSL Server Standard and right click and select Create.



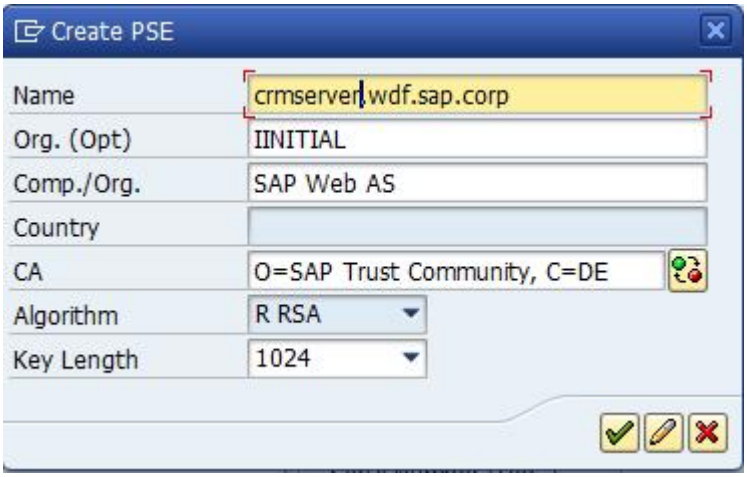
3. Enter the distinguished name, the name of the server on how it will be access over HTTPS protocol, by default the system assigns a wildcard for the hostname and the rest of by example :

   Name= *.mycompany.com

   Org. (opt.)= Test

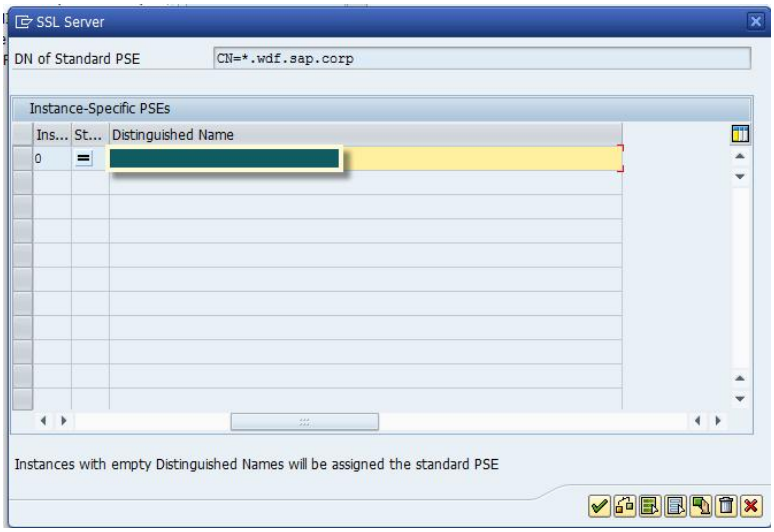
   Comp./Org.= MyCompany

   Country= US



4. If necessary, modify the distinguished name for the individual application servers. For example, <hostname>.companyname.com

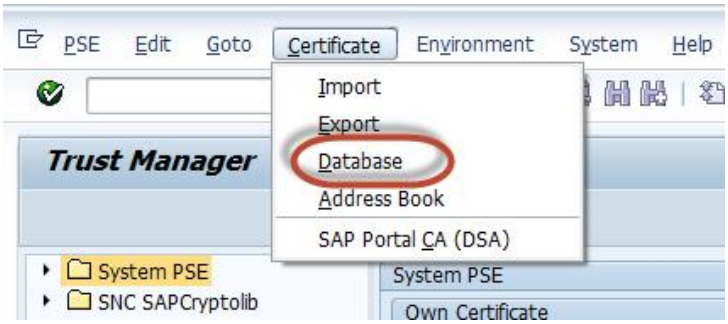
5. Press enter and then Save the configuration.



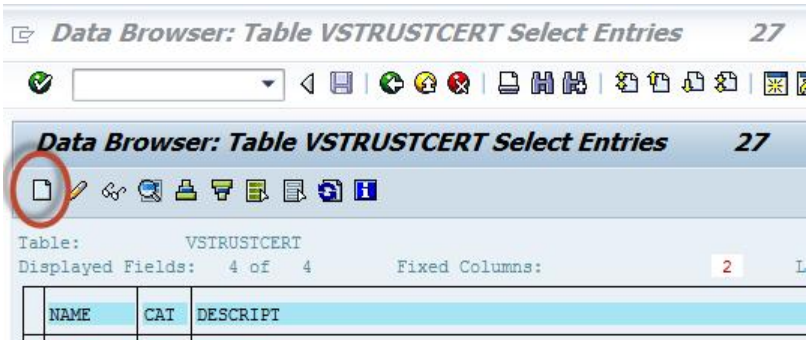
4.4 Create Trust Center in Database to Import Root CA Certificate

Create Trust center in database to import root CA certificate. In the case where the certificate authority that will be used to sign the SSL Server certificates is not available in the system, create a trust center and load the root certificate as follows:

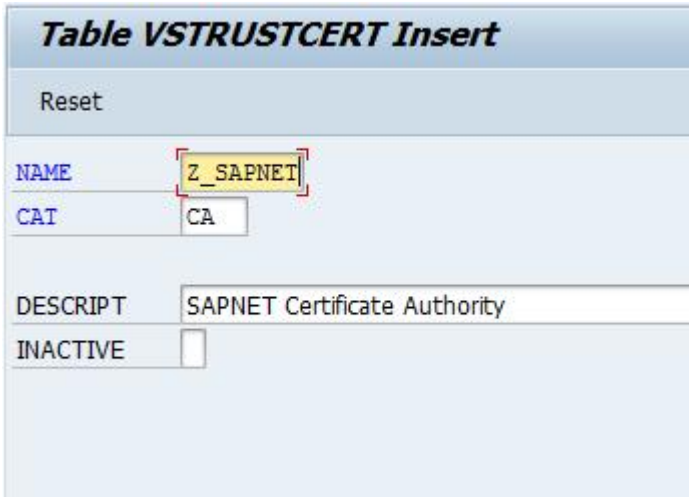
1. Within transaction STRUST, click on menu certificates → database.



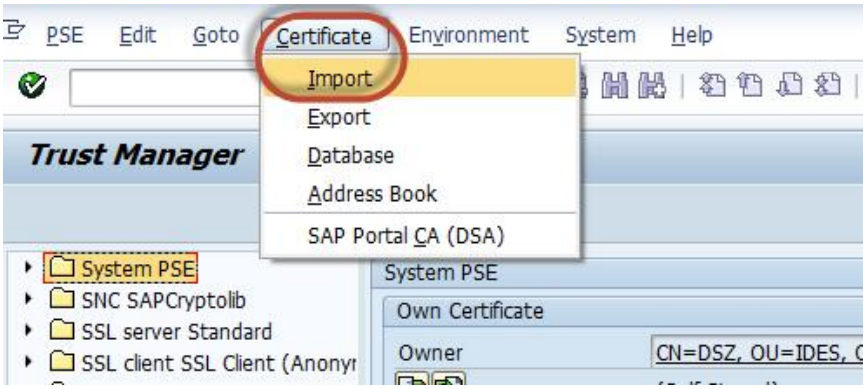
2. Create a new entry from the create icon.



3. Enter the name under the customer namespace, the category and a description.

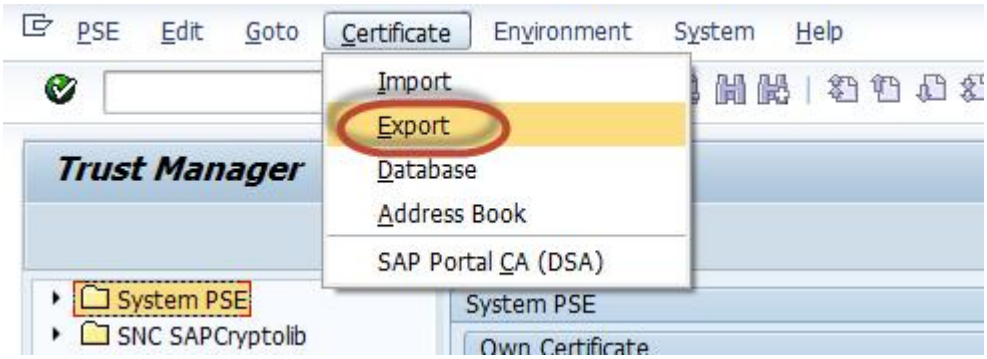


4. Import the CA root certificate from the file system in STRUST click in menu certificate → Import .

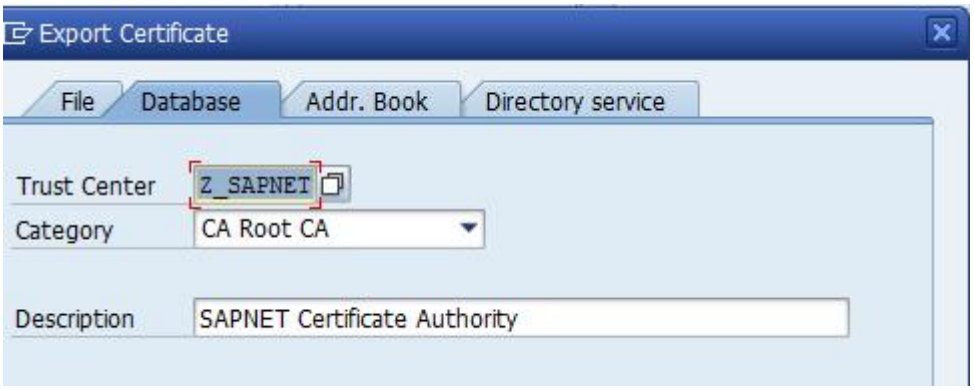


5. From the file system select the root certificate and hit Enter.

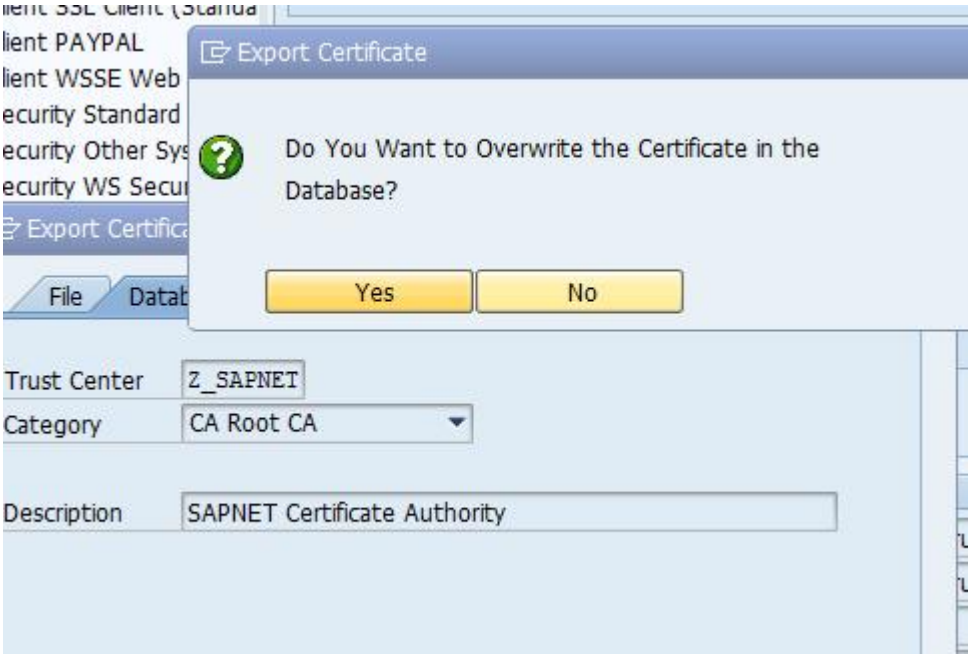
6. Click in the menu Certificate → Export.



7. Click in the tab Database and select the Trust Center that was created before, and hit enter.

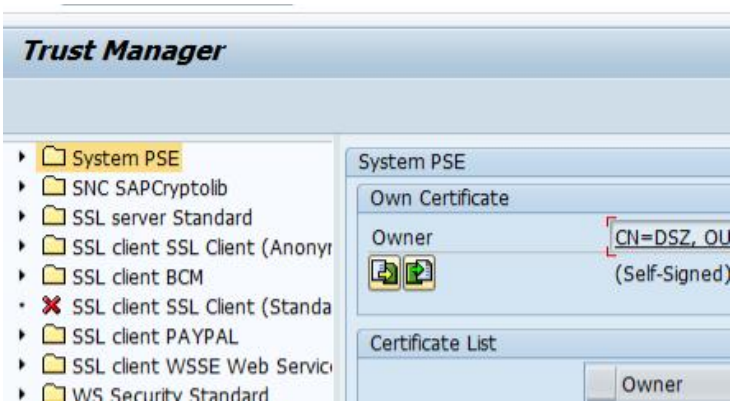


8. Click Yes during the question of overwrite in the database.



4.5 Generate Certificate Request for SSL Server PS

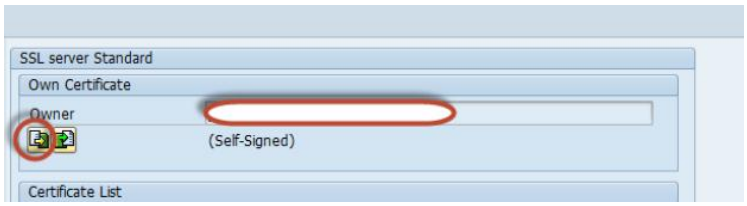
1. Open transaction STRUST



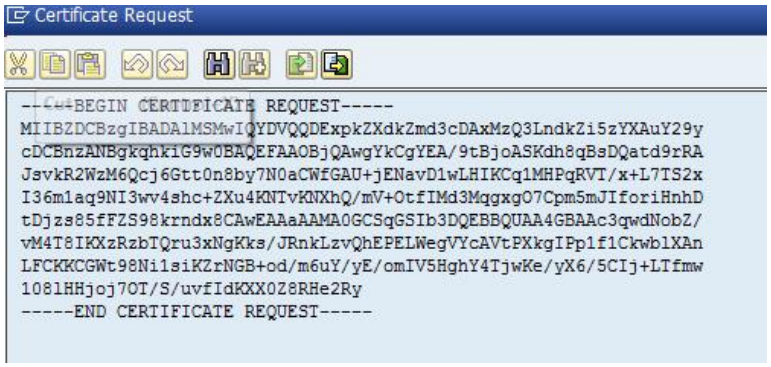
2. For each of the SSL Server PSE do the following:

   a. Select the application server

   b. In the maintenance section select the icon to create certificate request



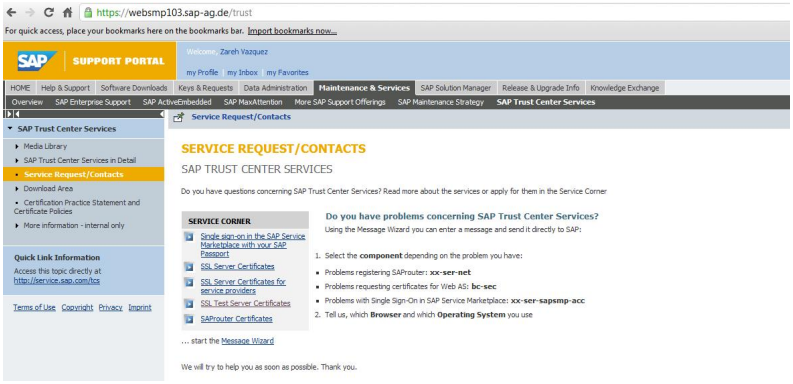
   c. Copy the output to the clipboard or save it as a P10 file



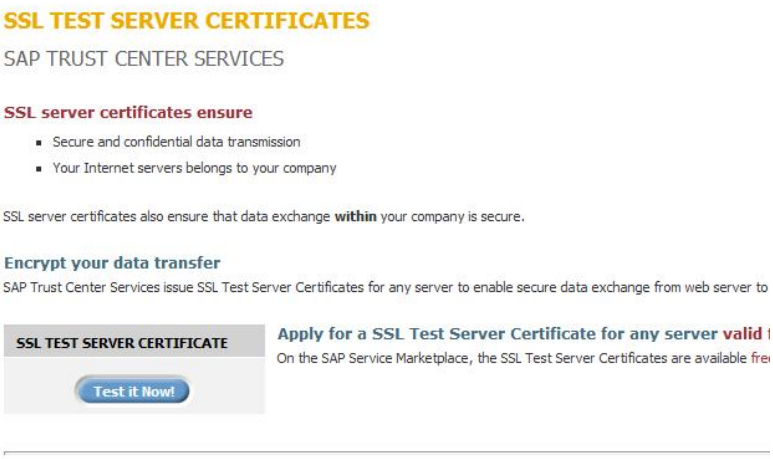
Example: How to sign certificate request with SAP CA

For testing purposes we can use the SSL Test Server Certificates trust center from the SAP Support Portal, this will provide a signed certificate that will last 8 weeks. For a permanent solution other certificate authority can be used.

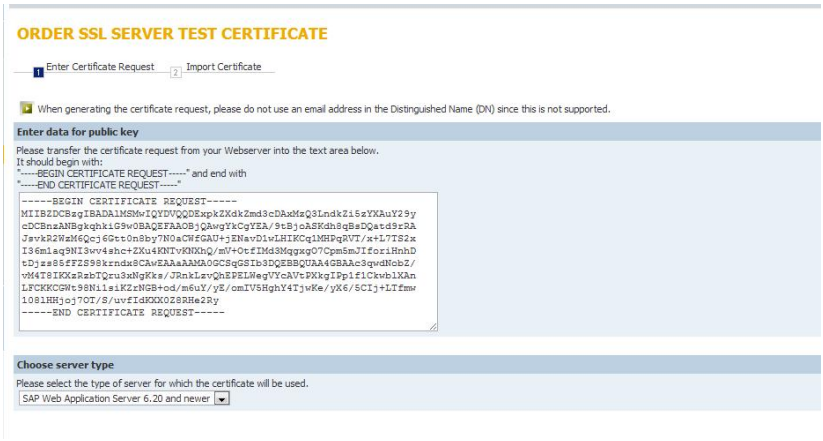
3. The trust manager requires that the certificate request response adheres to the PKCS#7 certificate chain format. Connect to the support portal in the following alias to access the SAP Trust Center Services http://service.sap.com/trust



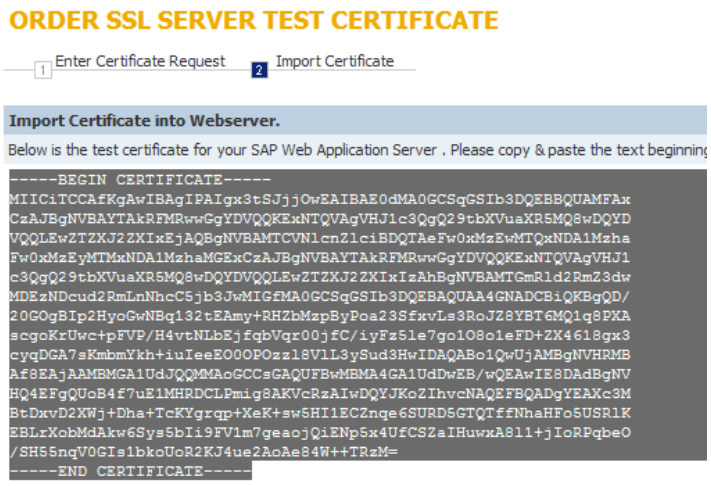
4. Clink in the link SSL Test Server Certificates.



5. Click in Test IT Now! And paste the output from the create certificate request from STRUST, select the server type “SAP Web Application Server 6.20 and newer” and click continue



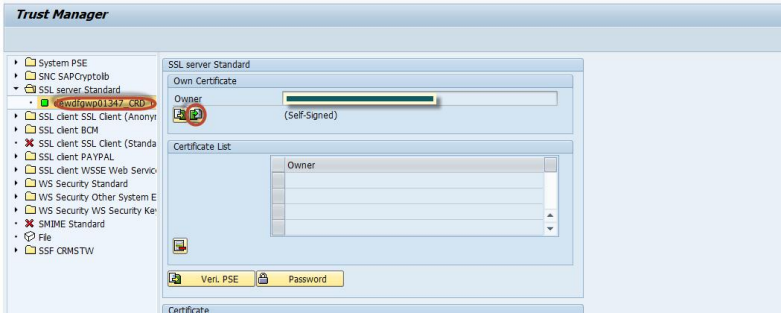
6. Select the output and save it to a file or in clipboard.



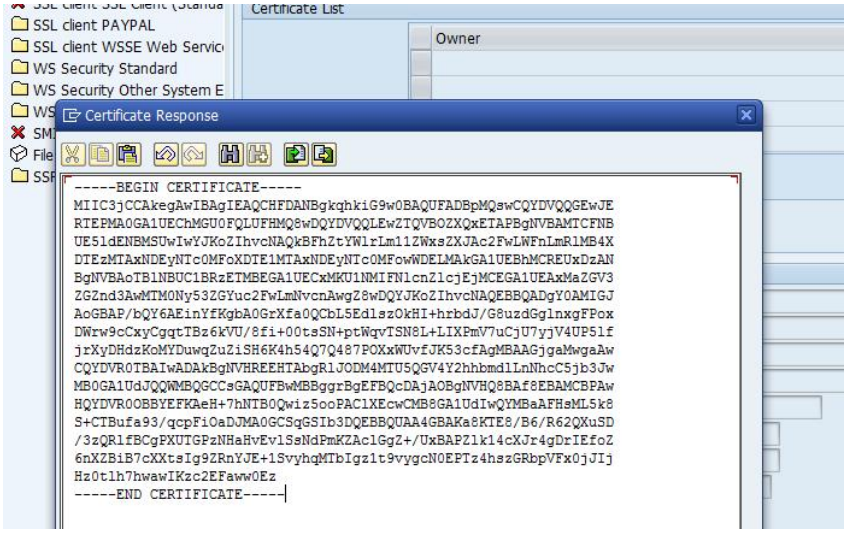
4.6 Import Certificate Request Response

The CA will send a certificate request response that contains the signed public key for the application server, we need to import this response into the corresponding PSE.

1. Expand the SSL server PSE. For each of the application servers, import the response by clicking the icon Import Certificate response.



2. Paste the entire content from the response that was signed by the certificate authority. In the previous example we used SAP Trust Center, and hit enter.

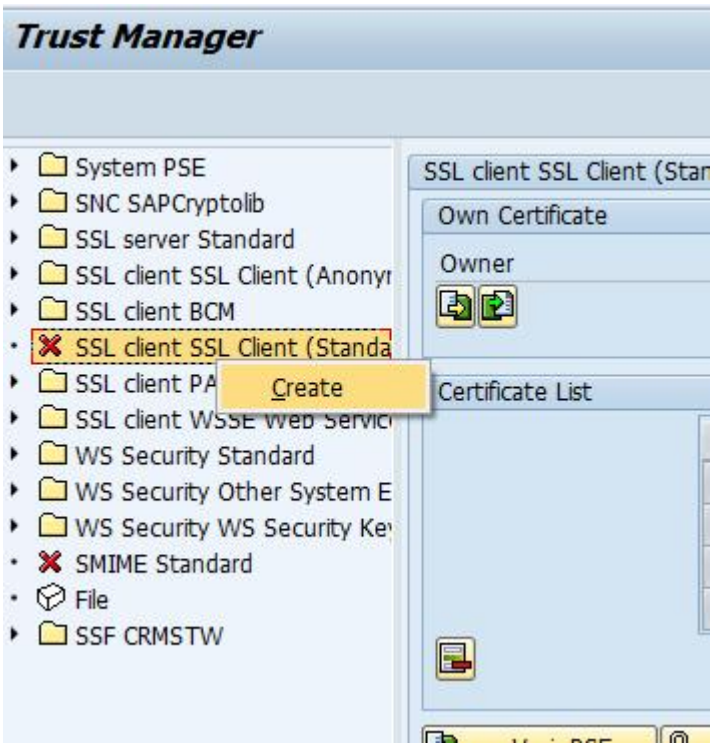


3. Click Save

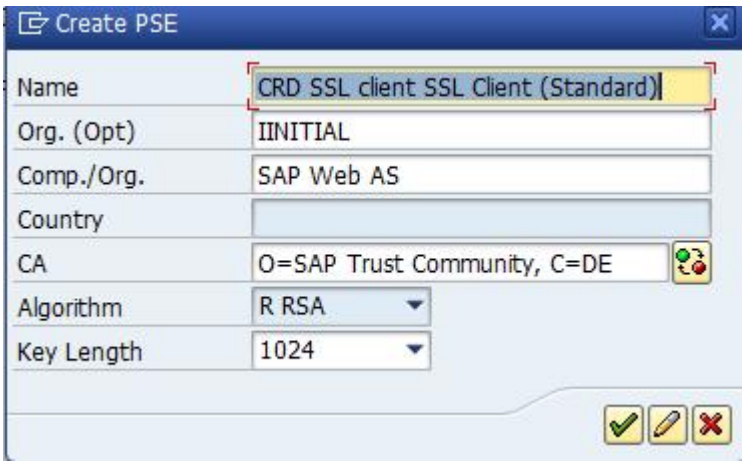
4.7 Configure SSL Client PSE for Outgoing Requests

1. Create SSL Client PSE by calling transaction STRUST.

2. Select the SSL Client Standard and right click and select Create.

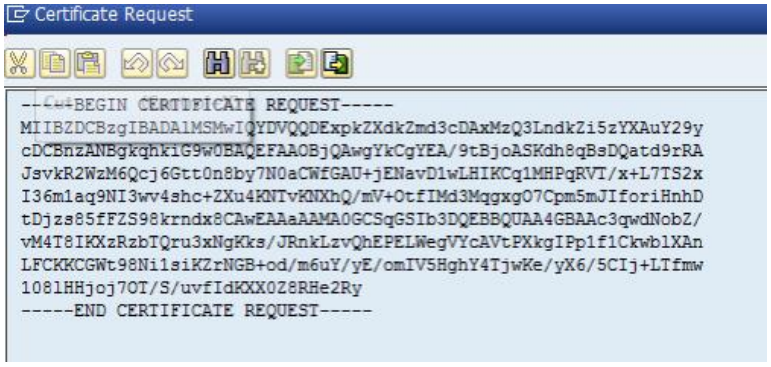


3. Enter the distinguished name for the system, something unique that identifies the system as client to access other systems:



4. Select SSL Client Standard PSE do the following:
   a. In the maintenance section select the icon to create certificate request.

   b. Copy the output to the clipboard or save it as a file P10

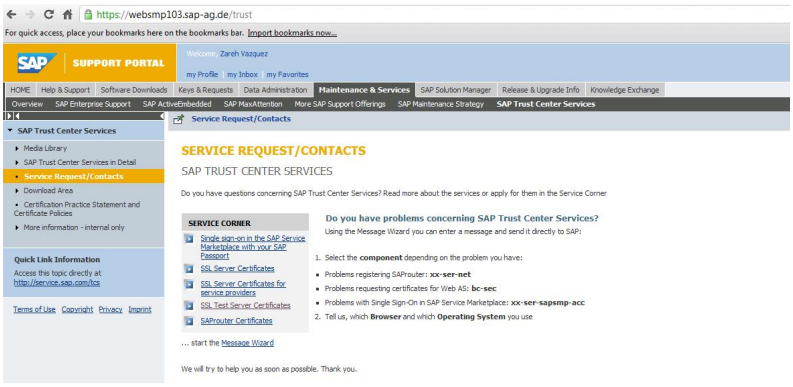


Example: how to sign certificate request with SAP CA.

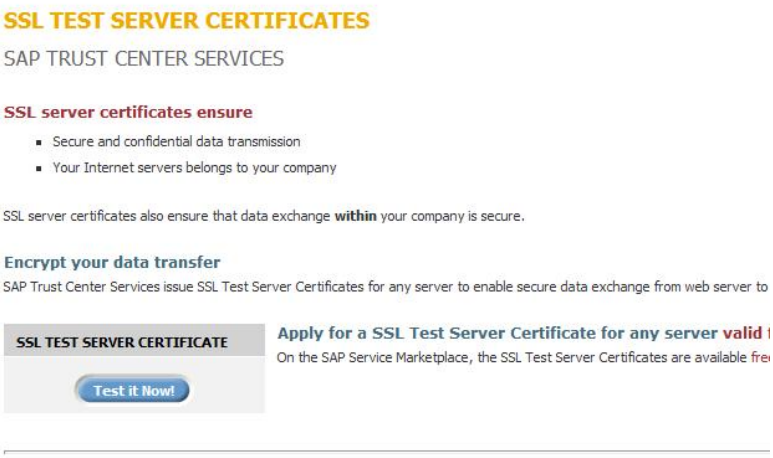
For testing purposes we can use the SSL Test Server Certificates trust center from the SAP Support Portal, this will provide a signed certificate that will last 8 week. For a permanent solution other certificate authority can be used.

The trust manager requires that the certificate request response adheres to the PKCS#7 certificate chain format.

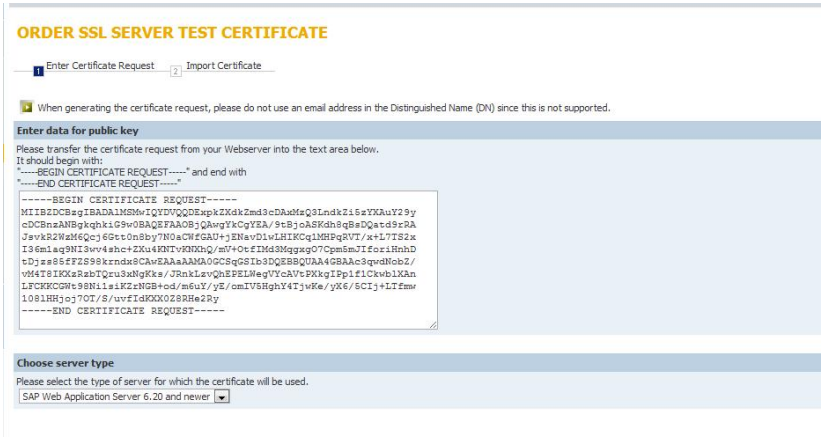
5. Connect to the support portal in the following alias to access the SAP Trust Center Services http://service.sap.com/trust



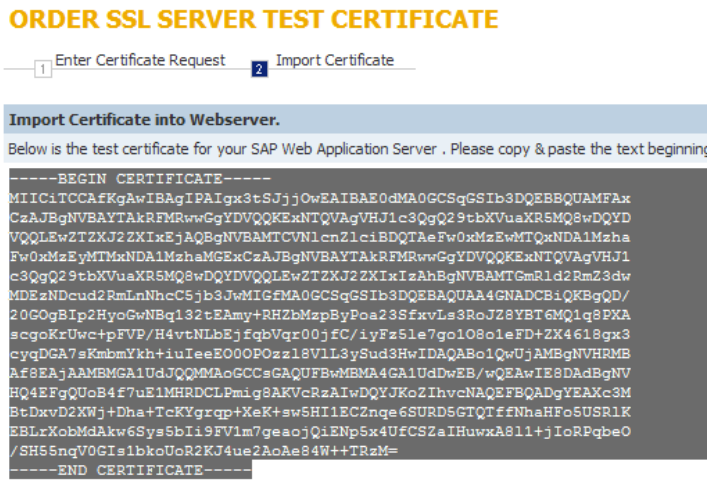
6. Clink in the link SSL Test Server Certificates



7. Click in Test IT Now! And paste the output from the create certificate request from STRUST, select the server type “SAP Web Application Server 6.20 and newer” and click continue.



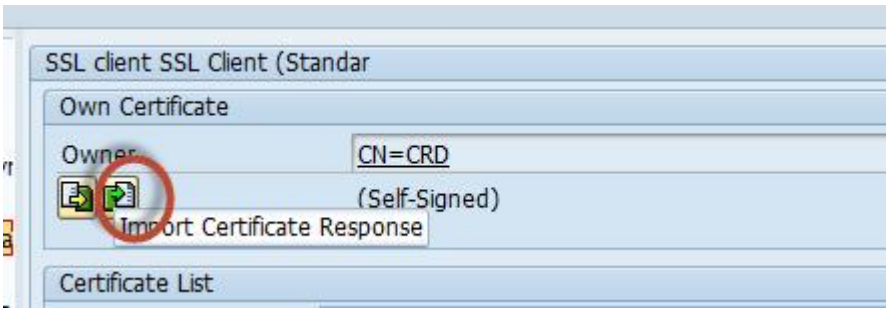
8. Select the output and save it to a file or in clipboard.



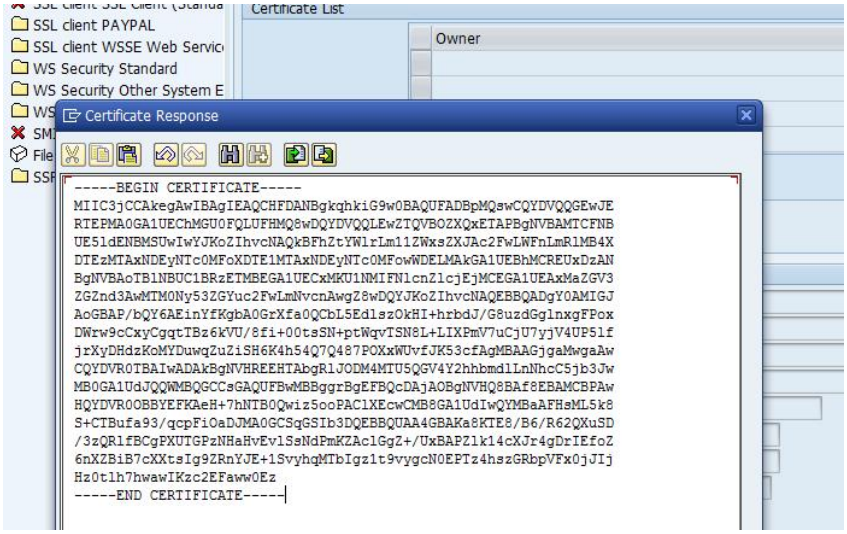
4.8 Import certificate request response

The CA will send a certificate request response that contains the signed public key for the application server, we need to import this response into the corresponding PSE.

1. Expand the SSL Client PSE



2. Paste the entire content from the response that was signed by the certificate authority in our previous example we use SAP Trust Center and hit enter.



3. Click Save

4.9 Test Connection

Test the SSL connection by example hitting the following URL on your SAP ABAP system from an internet browser.

https://<FQHN>:<SSLport>/sap(bD1lbiZjPTgwMA==)/bc/bsp/sap/it00/default.htm

www.sap.com/contactsap