

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	4
2	Background Information.....	4
3	Prerequisites.....	4
4	Step-by-Step Procedure.....	4
4.1	Install the SAP Cryptographic Libraries.....	4
4.2	Add Required Profile Parameters.....	6
4.3	Configure SSL Server PSE for Incoming Request	7
4.4	Create Trust Center in Database to Import Root CA Certificate.....	8
4.5	Generate Certificate Request for SSL Server PS.....	11
4.6	Import Certificate Request Response.....	13
4.7	Configure SSL Client PSE for Outgoing Requests	14
4.8	Import certificate request response	18
4.9	Test Connection.....	19

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

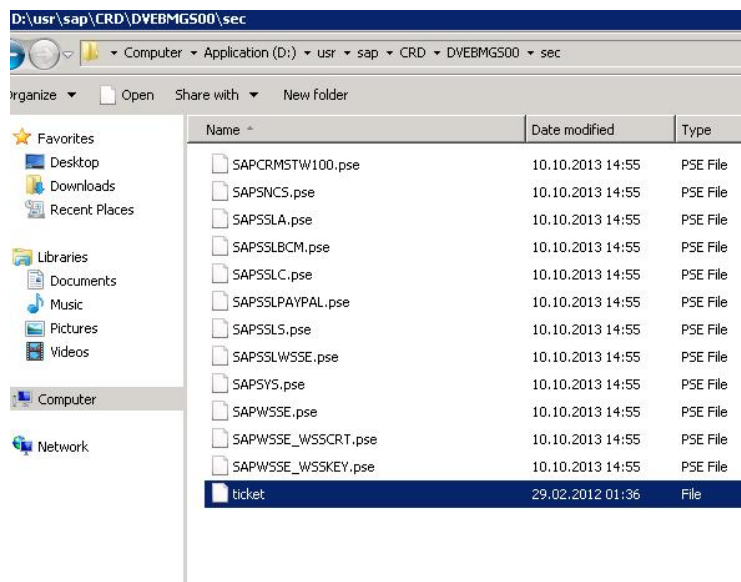
1. Download the latest SAP Crypto Libraries from the SAP Marketplace. Access URL <http://service.sap.com/swdc>, and follow path Support Packages and Patches → Browse our Download Catalog → SAP Cryptographic Software → SAPCryptolib for Installations → SAPCryptoLibs<version>
2. Select the desired platform,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

```
D:\software>D:\usr\sap\CRD\SYS\exe\uc\NTAMD64\sapcar -xvf SAPCRYPTOLIB_36-1001008
00.SAR
SAPCAR: processing archive SAPCRYPTOLIB_36-10010088.SAR (version 2.00)
x ChangeLog.txt
x LEGAL.TXT
x LICENSE.TXT
x Uer555.pl36
x WHICH.TXT
x nt-x86_64
x nt-x86_64/sapcrypto.lst
x nt-x86_64/sapcrypto.pdb
x nt-x86_64/sapgenpse.pdb
x nt-x86_64/sapgenpse.exe
x nt-x86_64/sapcrypto.dll
x nti64
x nti64/sapcrypto.lst
x nti64/sapcrypto.pdb
x nti64/sapgenpse.pdb
x nti64/sapgenpse.exe
x nti64/sapcrypto.dll
x ntintel
x ntintel/sapcrypto.lst
x ntintel/sapcrypto.pdb
x ntintel/sapgenpse.pdb
x ntintel/sapgenpse.exe
x ntintel/sapcrypto.dll
x ticket
x SIGNATURE.SMF
SAPCAR: 25 file(s) extracted
D:\software>
```

- 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\

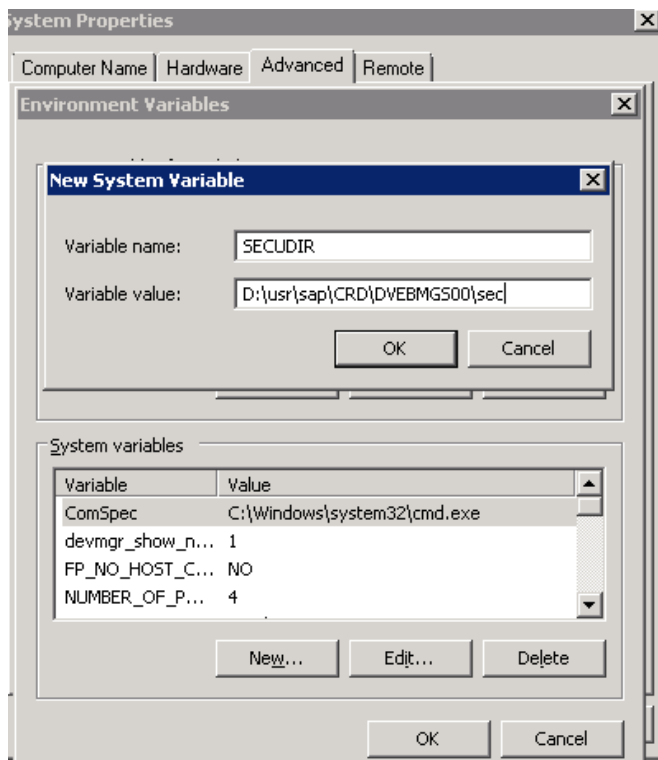


- Verify the files have the right permissions with execution permissions for <sid>adm and SAPService<SID>
- Copy the ticket file to the "sec" directory of the instance directory



- 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
```

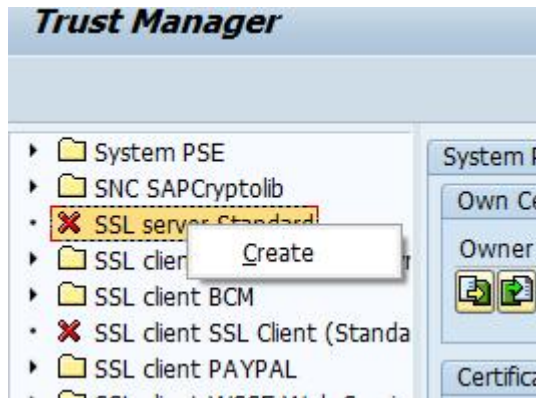
In case of dual stack add the following parameter

```
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.



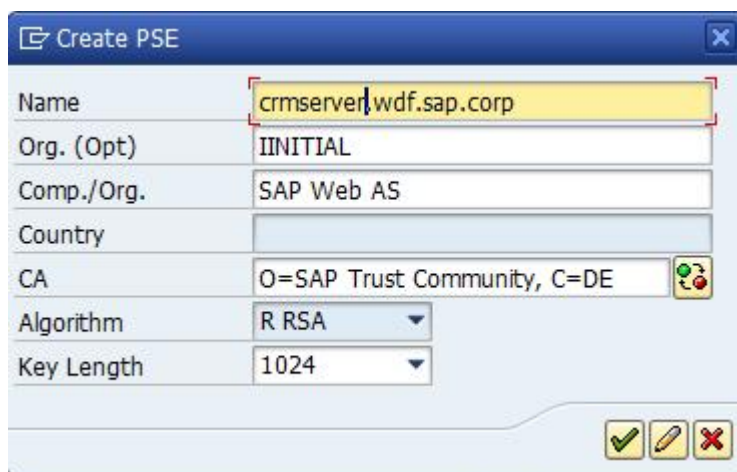
3. Enter the distinguished name, the name of the server on how it will be accessed over HTTPS protocol, by default the system assigns a wildcard for the hostname and the rest of by example :

Name= *.mycompany.com

Org. (opt.)= Test

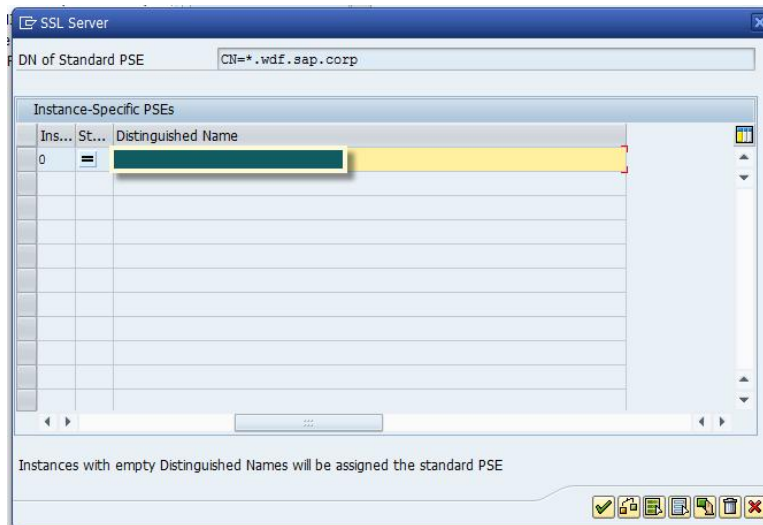
Comp./Org.= MyCompany

Country= US



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

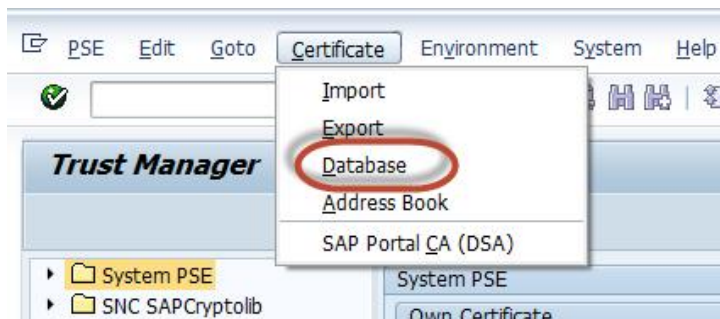
- Press enter and then Save the configuration.



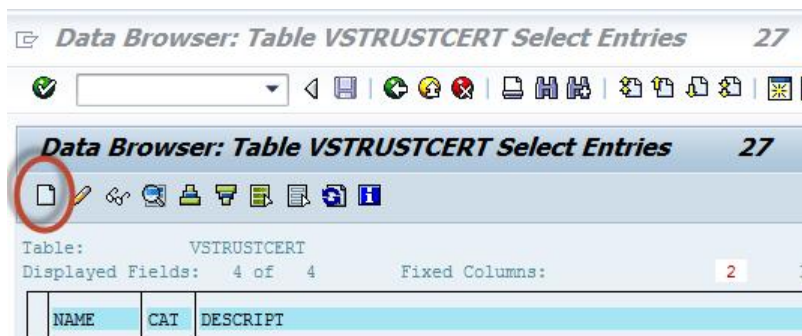
4.4 Create Trust Center in Database to Import Root CA Certificate

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:

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



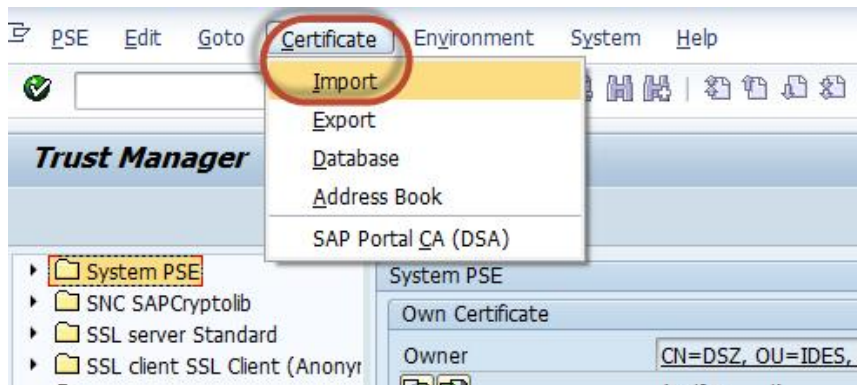
- Create a new entry from the create icon.



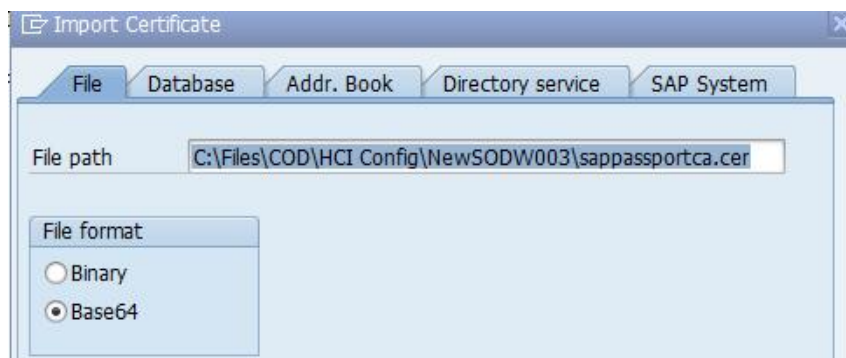
3. Enter the name under the customer namespace, the category and a description.

Table VSTRUSTCERT Insert	
Reset	
NAME	Z_SAPNET
CAT	CA
DESCRIPT	SAPNET Certificate Authority
INACTIVE	<input type="checkbox"/>

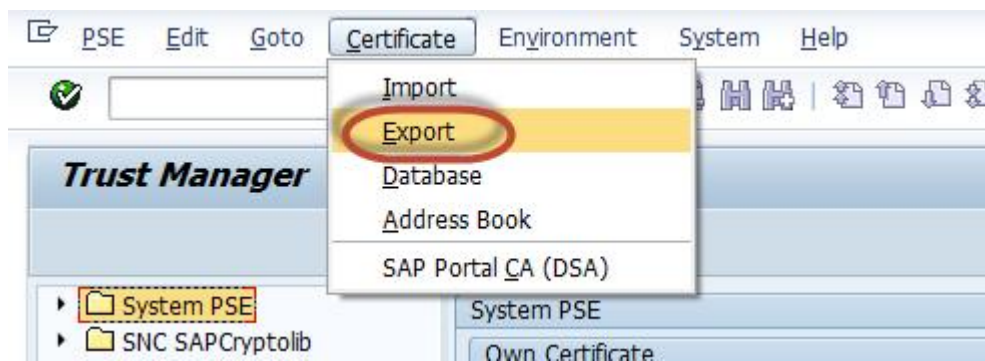
4. Import the CA root certificate from the file system in STRUST click in menu certificate → Import .



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



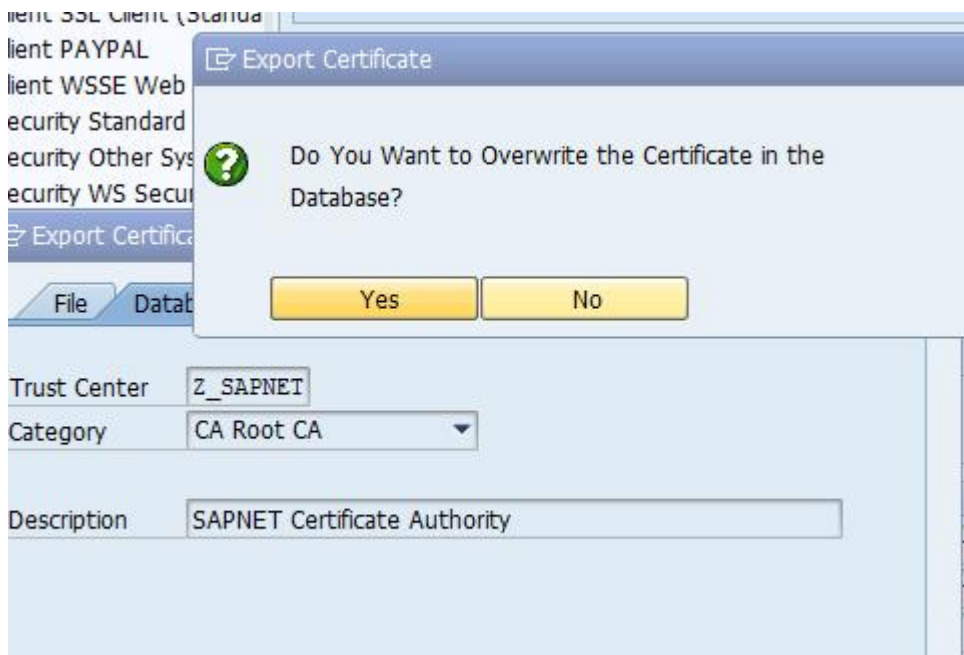
6. Click in the menu Certificate → Export.



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

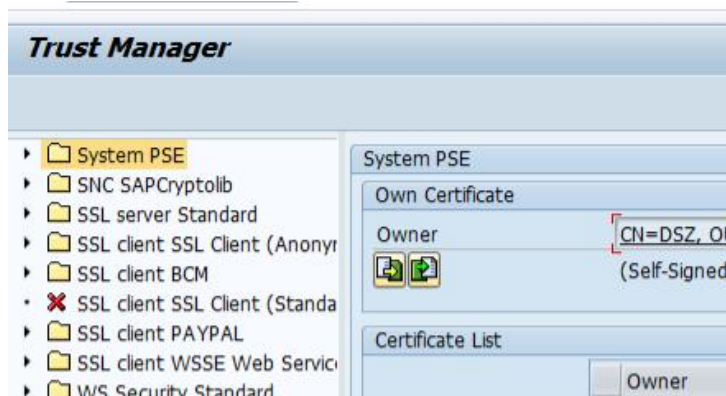


8. Click Yes during the question of overwrite in the database.



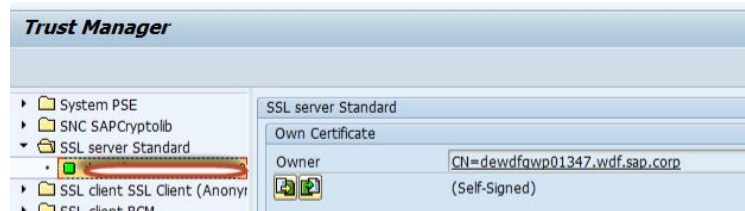
4.5 Generate Certificate Request for SSL Server PS

1. Open transaction STRUST



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

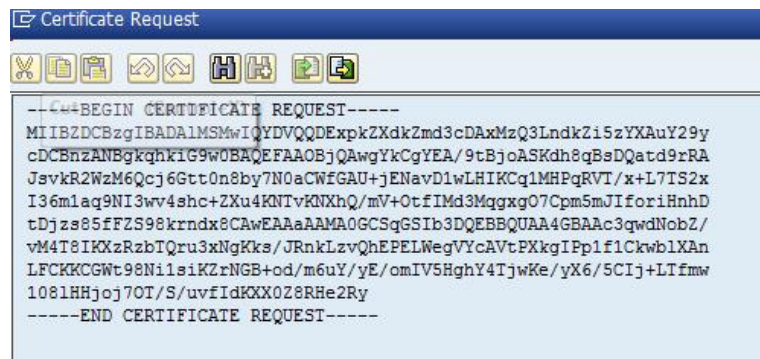
- a. Select the application server



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



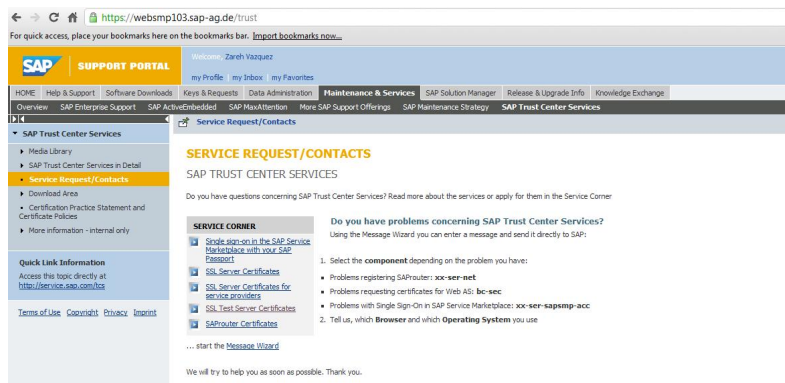
- c. Copy the output to the clipboard or save it as a P10 file



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. Click in the link SSL Test Server Certificates.

SSL TEST SERVER CERTIFICATES

SAP TRUST CENTER SERVICES

SSL server certificates ensure

- Secure and confidential data transmission
- Your Internet servers belongs to your company

SSL server certificates also ensure that data exchange **within** your company is secure.

Encrypt your data transfer

SAP Trust Center Services issue SSL Test Server Certificates for any server to enable secure data exchange from web server to

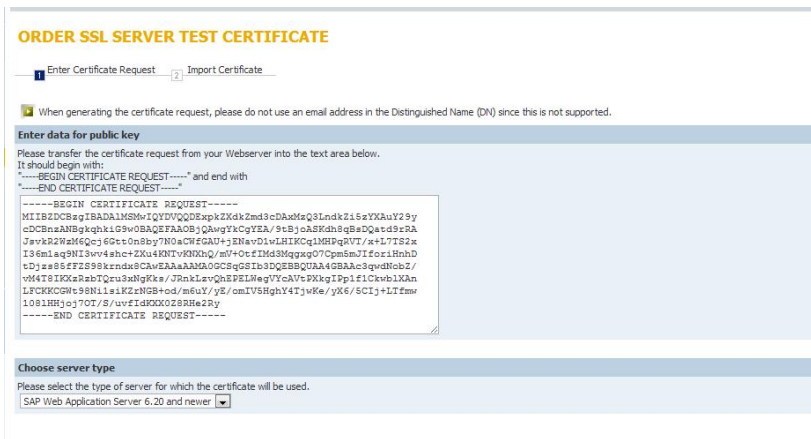
SSL TEST SERVER CERTIFICATE

Apply for a SSL Test Server Certificate for any server valid 1

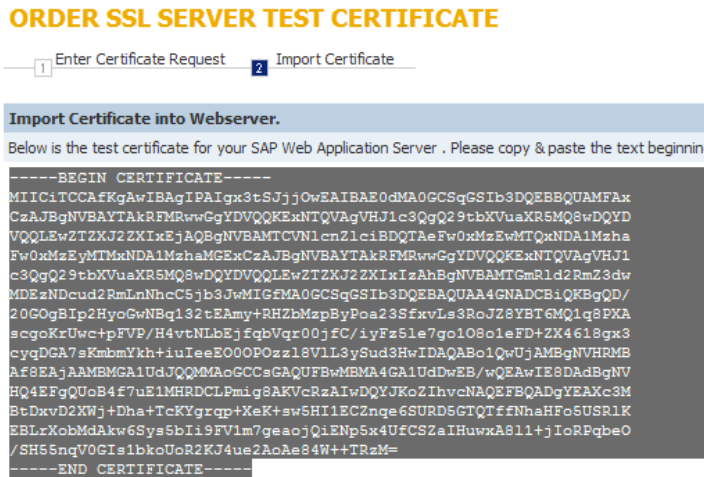
On the SAP Service Marketplace, the SSL Test Server Certificates are available **fre**

[Test it Now!](#)

- 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



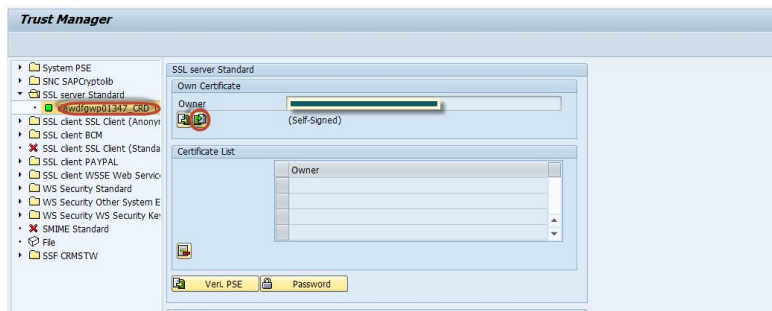
- Select the output and save it to a file or in clipboard.



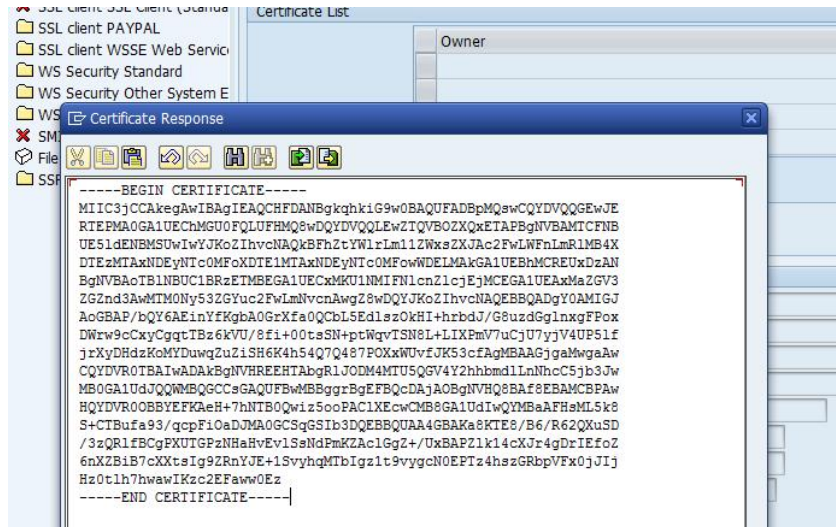
4.6 Import Certificate Request Response

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.

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



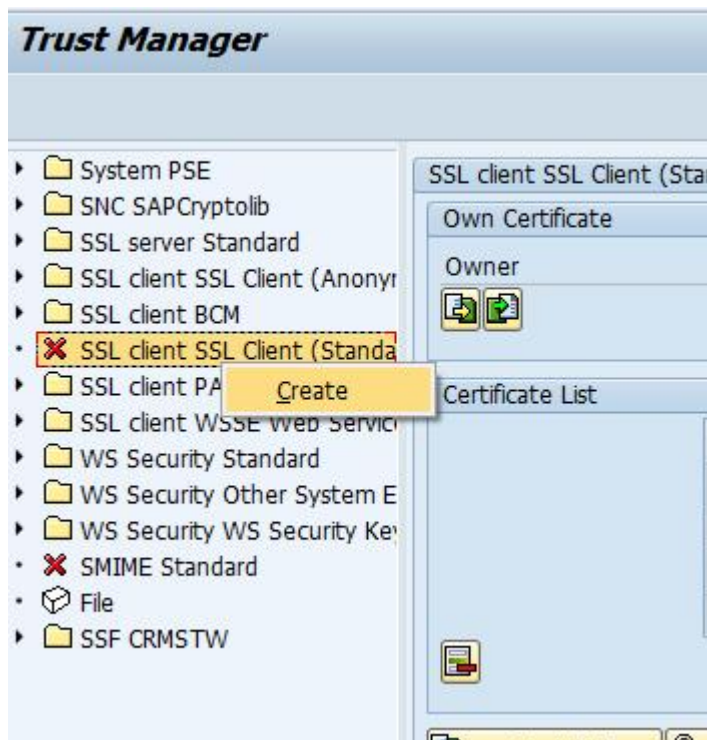
- Paste the entire content from the response that was signed by the certificate authority. In the previous example we used SAP Trust Center, and hit enter.



- Click Save

4.7 Configure SSL Client PSE for Outgoing Requests

- Create SSL Client PSE by calling transaction STRUST.
- 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

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBZDCBzgIBADA1MSMwIQYDVQQDEExpkZXdkZmd3cDxMzQ3LndkZ15zYXAuY29y
cDRCbnZANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA/9tBjcASKdh8qBsDQatd9rRA
JsvkR2WzM6Qcj6Gtt0n8by7N0aCWFGAU+jENavD1wLHIKCq1MHPqRVT/x+L7TS2x
I36m1aq9NI3wv4shc+2Xu4KNTvKXhQ/mV+OtfIMd3MggxgO7Cpm5mJIforiHnhD
tDjz885fFZS98krndx8CAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAAc3gwdNobZ/
vM4T8IKXzRzbTQru3xNgKks/JRnkLzvQhEPELWegVYcAVtPXkgIPp1f1CkwblXAn
LFCKKCGwt98Ni1siKZrNGB+od/m6uY/yE/omIV5HghY4TjwKe/yX6/5CIj+LTfwm
1081HHjoj7OT/S/uvfIdKXX0Z8RHe2Ry
-----END CERTIFICATE REQUEST-----

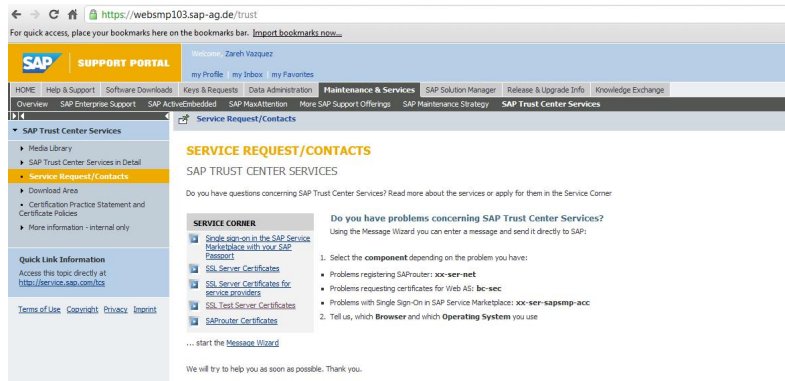
```

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. Click in the link **SSL Test Server Certificates**

SSL TEST SERVER CERTIFICATES

SAP TRUST CENTER SERVICES

SSL server certificates ensure

- Secure and confidential data transmission
- Your Internet servers belongs to your company

SSL server certificates also ensure that data exchange **within** your company is secure.

Encrypt your data transfer

SAP Trust Center Services issue SSL Test Server Certificates for any server to enable secure data exchange from web server to

SSL TEST SERVER CERTIFICATE

Apply for a SSL Test Server Certificate for any server valid !

On the SAP Service Marketplace, the SSL Test Server Certificates are available **free**

[Test it Now!](#)

- 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.

ORDER SSL SERVER TEST CERTIFICATE

1 Enter Certificate Request 2 Import Certificate

When generating the certificate request, please do not use an email address in the Distinguished Name (DN) since this is not supported.

Enter data for public key

Please transfer the certificate request from your Webserver into the text area below.
It should begin with:
-----BEGIN CERTIFICATE REQUEST----- and end with
-----END CERTIFICATE REQUEST-----

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBDCCBgiBADA1MS0wIqYDVQQGEpKXdkZmd3cDAsMzQ3LmduZ216eYXN0Y29y
cDQ3MmRlZm9kaXkiS99vBkQEFM0BjQkVjY2E/9t3jcaSfhdq8dQtc89PA
JsvkR2WzH6Qccj6Gtt0n8By7NOaCHfGAU+jENavD1wLHIKq1MHPqRVt/x+17TSzX
I36m1a9N13vv4shc+2Ku4KNTvKXKhQ/nV+0eFI6d3Mqpxg07Cpm5mJIfoziRnhD
tDjz885FZ899krnd88CwEAA4AAAMA0GCSqSIB3DQEBBQUAA4GBAAc3qu8Nobz/
VW4TfIKz8ab7Qcna3n8Ks/J3nLrVq8FELMwYCaVeFXMgJlPp1f1Cwb13An
LFCKKCNz88N1i1K2zNGB+od/m6uY/yE/cmlV5HghY4TjwRe/yK6/SCIj1LIEmw
1081HH5oj70T/SuvfIdKXX028R8e2Ry
-----END CERTIFICATE REQUEST-----
```

Choose server type

Please select the type of server for which the certificate will be used.
SAP Web Application Server 6.20 and newer

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

ORDER SSL SERVER TEST CERTIFICATE

1 Enter Certificate Request 2 Import Certificate

Import Certificate into Webserver.

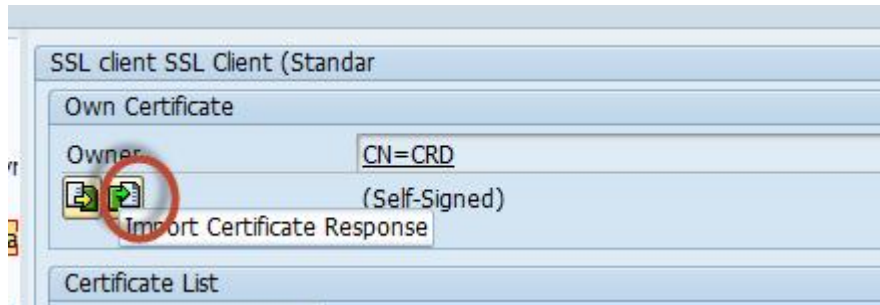
Below is the test certificate for your SAP Web Application Server . Please copy & paste the text beginning

```
-----BEGIN CERTIFICATE-----
MIICiTOCAfKgAwIBAgIPAIGx3tSjJjOwEAIBAB0dMA0GCSqGSIb3DQEBBQUAMFAx
CzAJBgNVBAYTAkRFRmRwGgYDVQQKEzNTQVAgVHJ1c3QgQ29tbXVuaXR5MzQ3LmduZ216eYXN0Y29y
cDQ3MmRlZm9kaXkiS99vBkQEFM0BjQkVjY2E/9t3jcaSfhdq8dQtc89PA
JsvkR2WzH6Qccj6Gtt0n8By7NOaCHfGAU+jENavD1wLHIKq1MHPqRVt/x+17TSzX
I36m1a9N13vv4shc+2Ku4KNTvKXKhQ/nV+0eFI6d3Mqpxg07Cpm5mJIfoziRnhD
tDjz885FZ899krnd88CwEAA4AAAMA0GCSqGSIb3DQEBBQUAA4GNADCBiQKBggQD/
20G0gBIp2HyoGwNBq132tEAmy+RHZbMzPByPoa23SfzvLs3RoJZ8YBT6MQ1q8PXA
scg0KrtWc+tpVVP/H4vtNLbEjfqBvqr00jfc/iyFz51e7go108o1eFD+ZX4618gx3
cyqG47sKmbmYkh+iuIeeE000P0zz18V1L3ySud3HwIDAQABo1QwUjAMBgNVHRMB
Af8EAjAAMBGA1UdJQQMMAoGCCeGAQUFwMBMA4GA1UdDwEB/wQEAWIE8DADBgNV
HQ4EFgQUoB4f7uE1MHRDCLPmiG8AKVcRzAIwDQYJKoZIhvcNAQEFBQADgYEAxc3M
BtdxvD2XWj+Dha+TcKYgrqp+XeK+sw5HI1ECZnge6SURD5GTfTffNhaHFo5USRLK
EBLrXobMdAkW6Ssys5bIi9FV1m7geaojQiENp5x4UfCSzaIHuwkA811+jIoRpqbeO
/SH56nqV0GIslbkoUoR2KJ4ue2AoAe84W++IRzM=
-----END CERTIFICATE-----
```

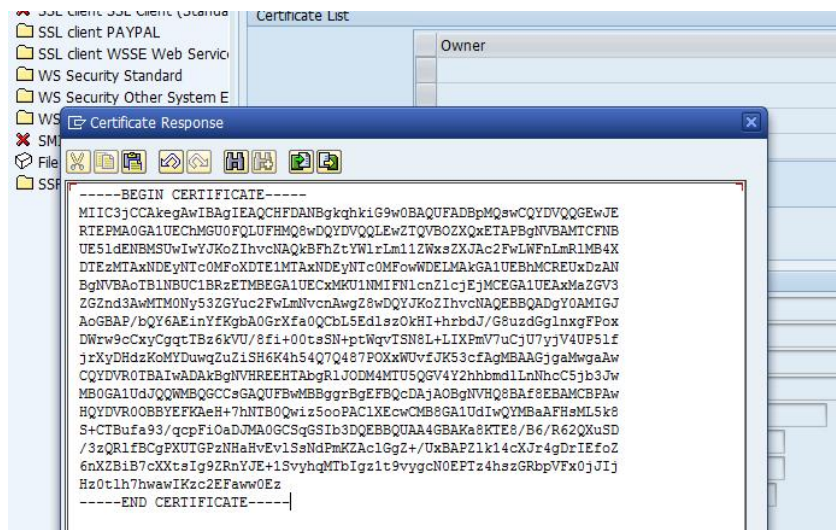
4.8 Import certificate request response

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

© 2017 SAP AG or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such

products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

The SAP logo, consisting of the letters "SAP" in white on a blue rectangular background.