SAP NetWeaver
How-To Guide

How To Configure SSL for SAP NetWeaver Mobile 7.1

Applicable Releases:

SAP NetWeaver Mobile 7.1 and above

Topic Area:

User Productivity

Capability:

Mobile

Version 1.0

December 2009

HOW-TO GUIDE

THE BEST-RUN BUSINESSES RUN SAP™

© Copyright 2009 SAP AG. 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.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, 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 in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. 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.

These materials are provided “as is” without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

SAP NetWeaver “How-to” Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP’s Support Services and may not be modified or altered in any way.

Document History

Document Version	Description
1.00	First official release of this guide

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

Icons

Icon	Description
	Caution
	Note or Important
	Example
	Recommendation or Tip

Table of Contents

1. Scenario 1

2. Background Information 1

3. Prerequisites 1

4. Step-by-Step Procedure 2

4.1 Install SAP Cryptographic Library 2

4.2 Configure Profile Parameters 3

4.3 Generate the Server Certificate 6

4.4 Export the Server Certificate 12

4.5 Import the Certificate to the Client 14

5. Appendix 15

1. Scenario

You use SAP NetWeaver Mobile 7.1 or above. Data exchange between the Data Orchestration Engine (DOE) and clients need to be in a secured way.

2. Background Information

SAP NetWeaver Mobile 7.1 uses HTTP protocol as default data communications between the DOE and clients. Use of HTTP protocol may not meet your security requirement since the business data may be intercepted by unauthorized parties.

You can configure to use The SSL based HTTPS protocol, in which the data exchange is encrypted and requiring a certificate.

In this document, HTTPS connection configurations are explained.

3. Prerequisites

Software

- You have downloaded SAP Cryptographic Software from the SAP software distribution center, and you have unpacked the software.

  http://service.sap.com/swdc → *Download* → *SAP Cryptographic software*

- JDK 1.5 or above has been installed on your computer.
- SAP NetWeaver Mobile client has been installed on your computer for laptop.

Relevant SAP Notes

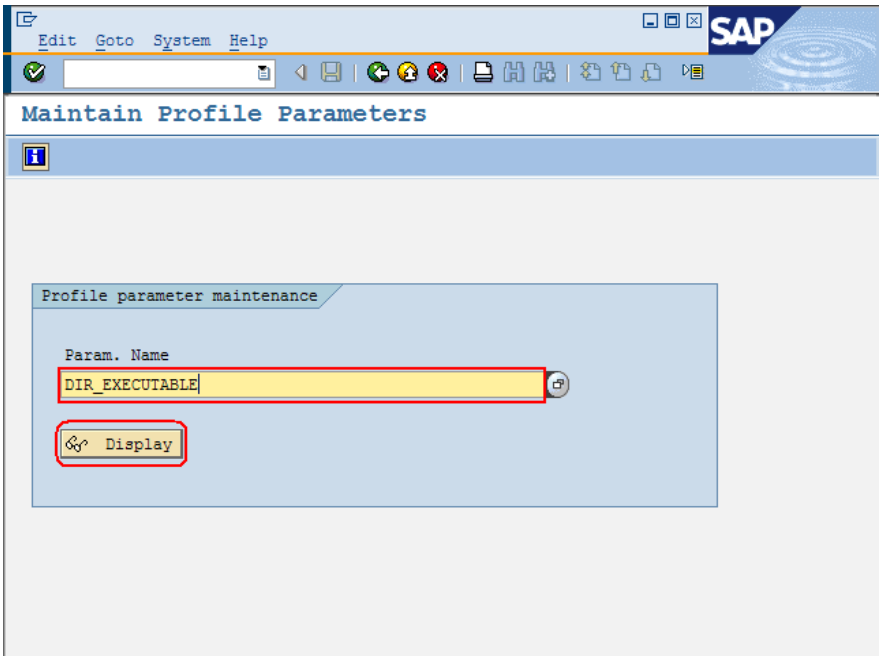
- Your country and company meets the export /import regulation of SAP Cryptographic Library. For more details, please refer to Note 397175 - SAP Cryptographic Software - Export control
- Note 510007 - Setting up SSL on Web Application Server ABAP
- Note 1312866 – Configuration Parameters for NetWeaver Mobile 7.1

4. Step-by-Step Procedure

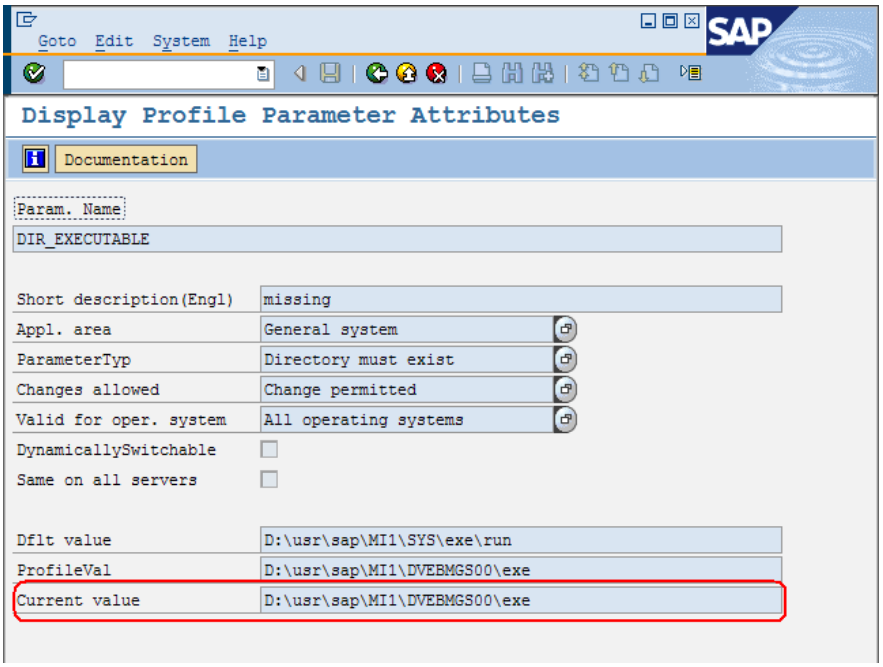
We first start with installation of the cryptographic library and setting server's parameters. Then import a server certificate to the saver. Finally, obtain and import the certificate into the client.

4.1 Install SAP Cryptographic Library

1. Check the server's profile parameter DIR_EXECUTABLE.
   a. Call the transaction, **`RZ11`**
   b. Enter **`DIR_EXECUTABLE`** in `Pram. Name` and press *Display*



   c. Make a note of the `Current value`.



d. Similarly, repeat the steps above for the parameter, DIR_INSTANCE

e. Copy the library file and the configuration tool to the directory specified in DIR_EXECUTABLE.

Note

Operating system	Library file name	Configuration tool
UNIX	libsapcrypto.<ext>	sapgenpse
Windows	sapcrypto.dll	sapgenpse.exe

Important

For UNIX, make sure to set the file permissions to be executable. For Windows, make sure that <sid>adm has the execution rights.

f. Copy the ticket file to the directory, $(DIR_INSTANCE)\sec.

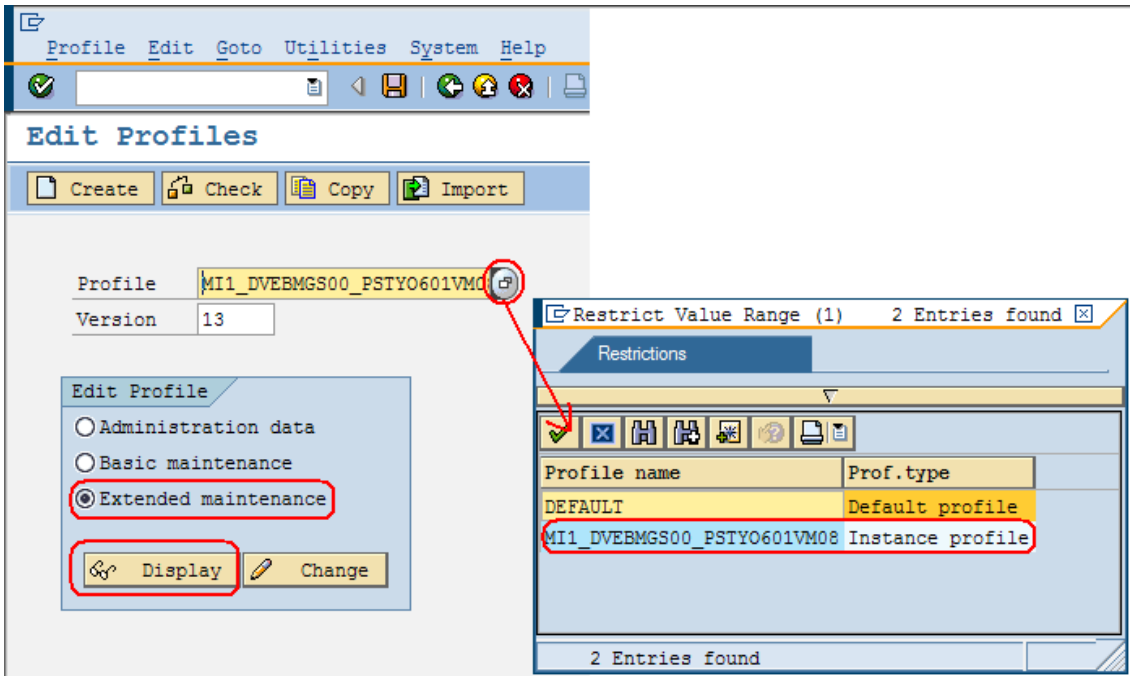
Note

If there is no directory named sec under $(DIR_INSTANCE), create it

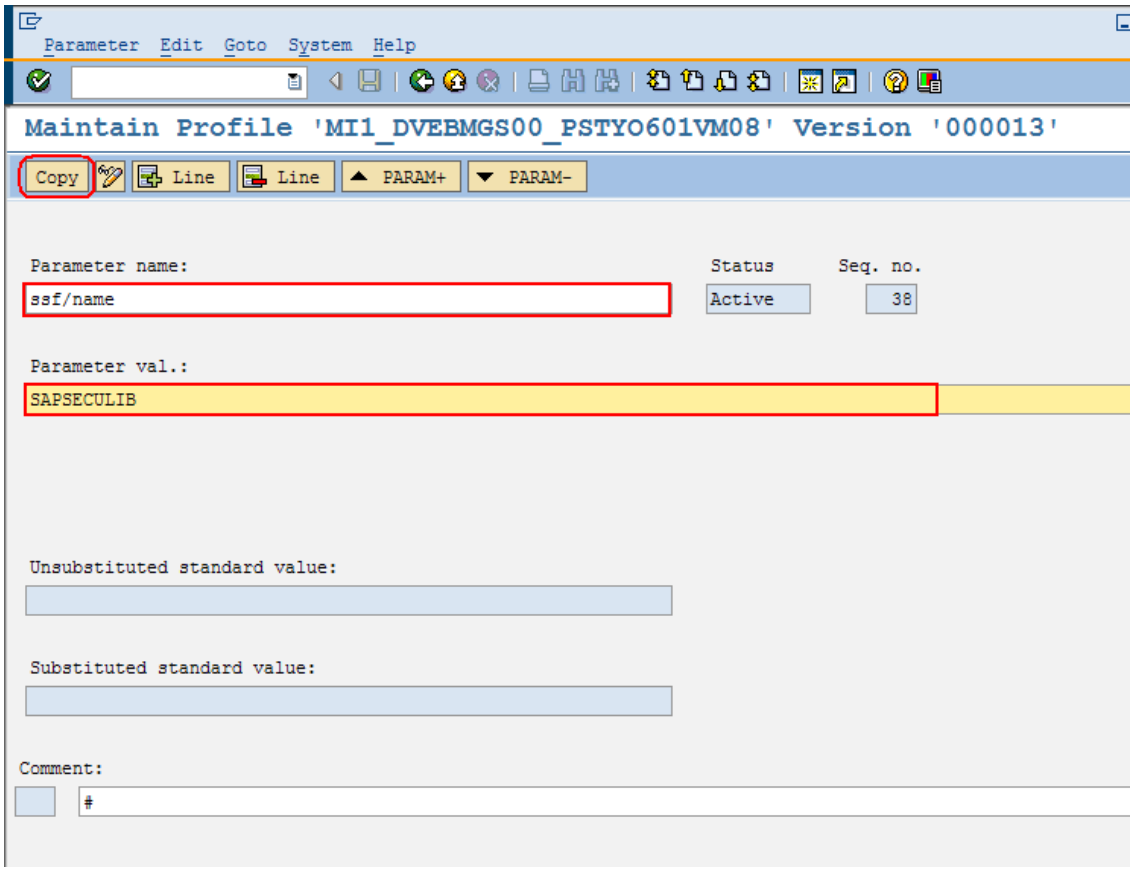
g. Create an environment variable SECUDIR that refers to the ticket's file path from the previous step. This environment variable needs to be accessible to the user account that is used to execute the Dispatcher process for the SAP system.

4.2 Configure Profile Parameters

1. Call the transaction, **`RZ10`**.
2. Select the instance profile and check `Extended maintenance`, then press *Change* button.

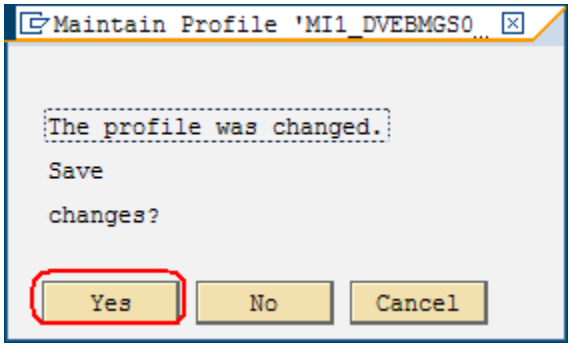


3. Press Parameter
4. Enter each of the following parameter name and value and press Copy button twice. Then press button

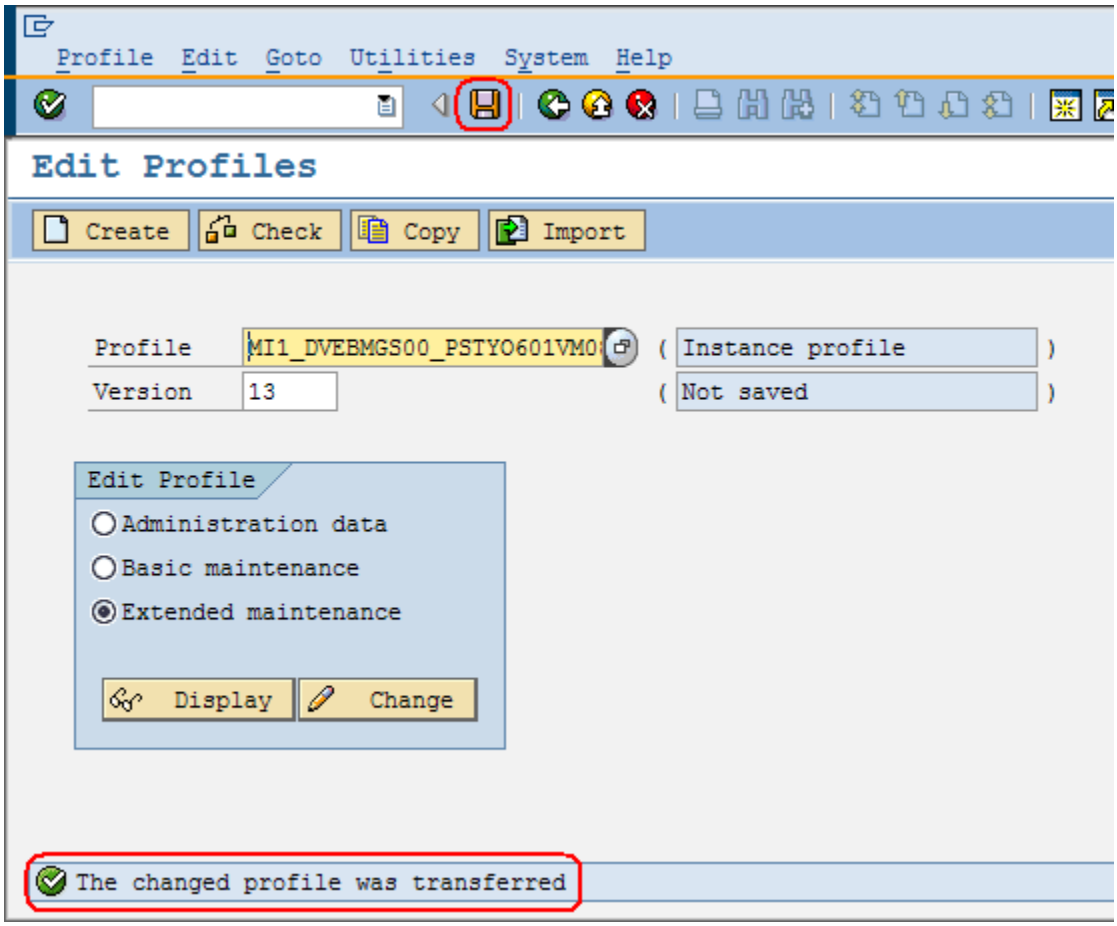


Parameter name	Parameter Value (Windows)	Parameter Value (UNIX)
Ssl/ssl_lib	$(DIR_EXECUTABLE)\ sapcrypto.dll	$(DIR_EXECUTABLE)/ libsapcrypto.<ext>
Sec/libsapsecu	$(DIR_EXECUTABLE)\ sapcrypto.dll	$(DIR_EXECUTABLE)/ libsapcrypto.<ext>
Ssf/ssfapi_lib	$(DIR_EXECUTABLE)\ sapcrypto.dll	$(DIR_EXECUTABLE)/ libsapcrypto.<ext>
Ssf/name	SAPSECULIB	
Icm/ssl_config_<xx>	CRED=<credential> [, CASHESIZE=<cashe size>, LIFETIME=<max lifetime>,VCLIENT=<SSL client verification>, CIPHERS=<Cipher Suites>]	
Icm/server_port_<xx>	PROT=HTTPS, PORT=<port number> [,TIMEOUT=<timeout in seconds>, PROCTIMEOUT=<proctimeout in seconds>, EXTBIND=1, HOST=<host name>. VCLIENT=<SSL Client Verification>, SSLCONFIG=ssl_config_<xx>]	
Icm/HTTPS/verify_client	0: Do not use certificate 1: Allow certificates (default) 2: Require certificate	

5. Press *Yes* to save changes.



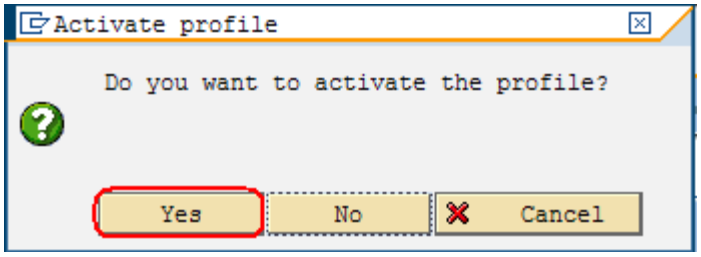
6. Press Save button.



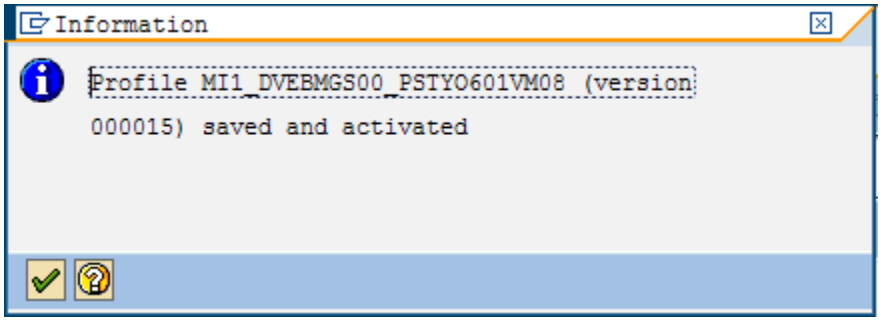
Note

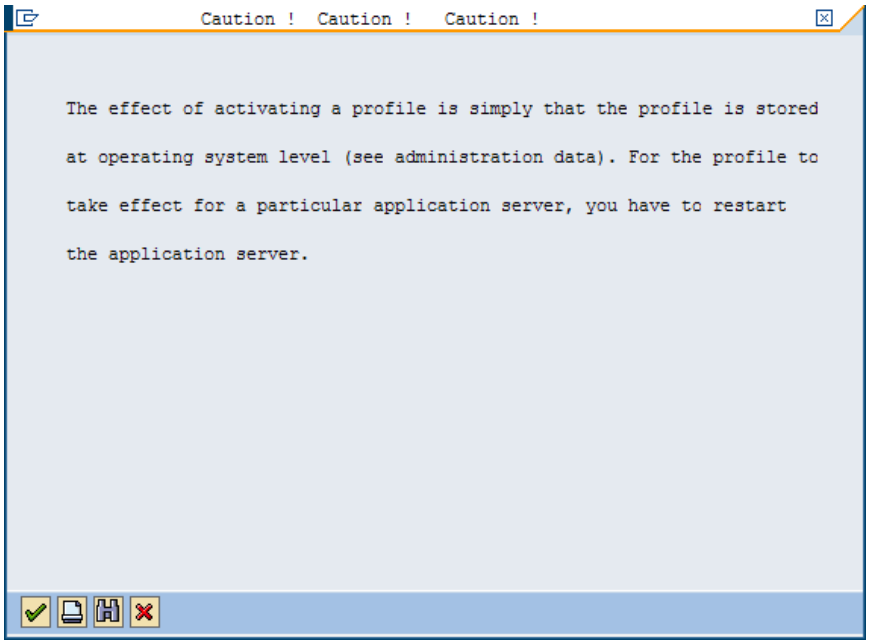
You can ignore the warning of unknown parameter.

7. Press *Yes* to activate the profile



8. The information pop up followed by caution pop up will be displayed.

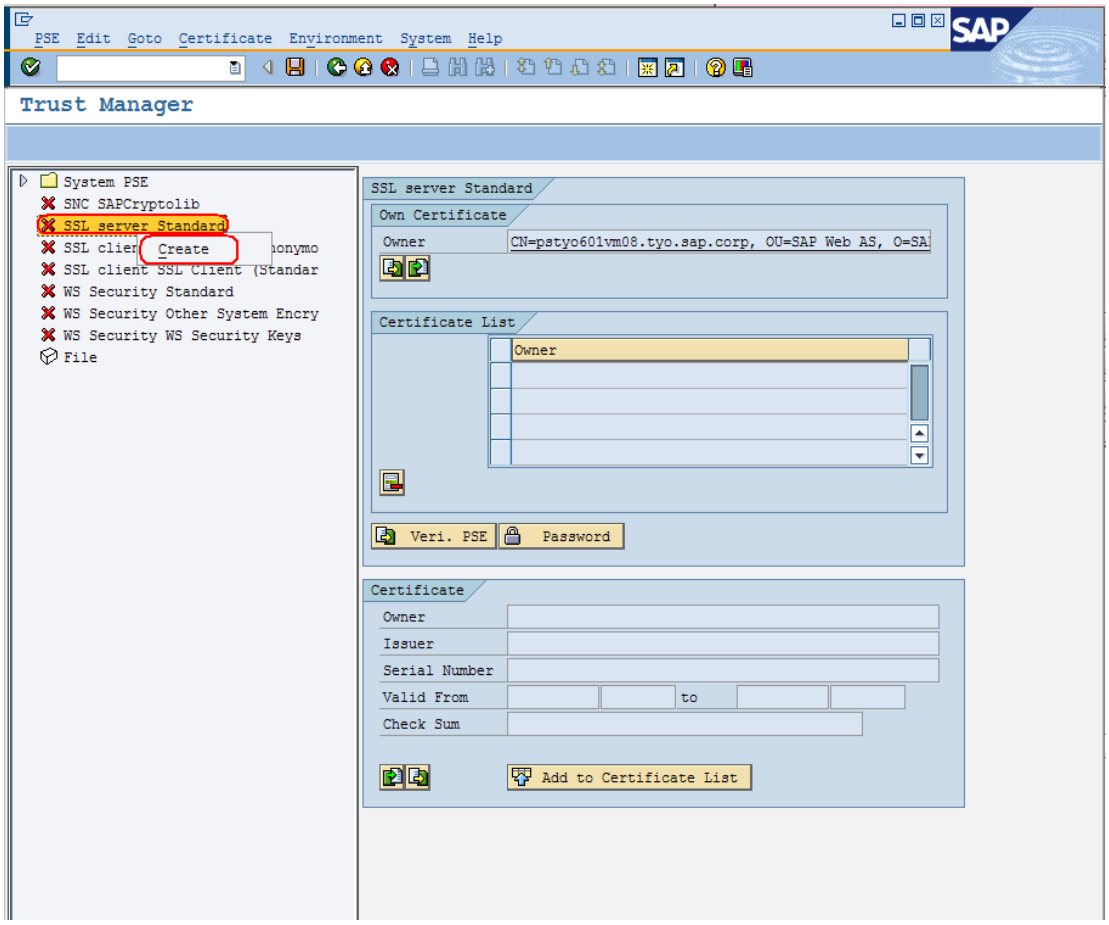




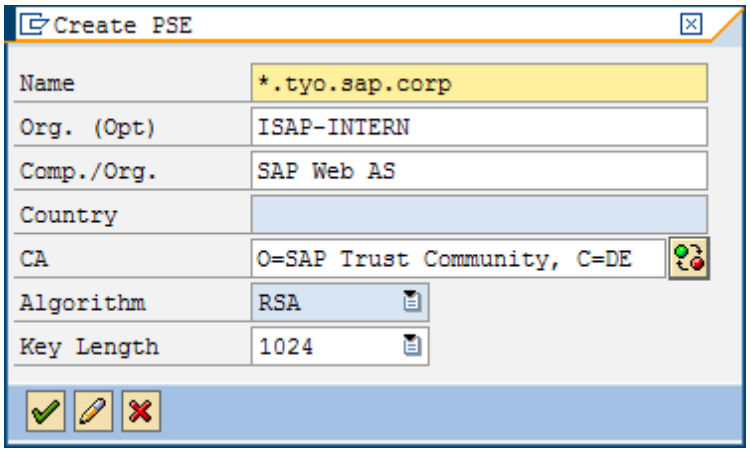
9. Restart the application server to take effect of the profile change.

4.3 Generate the Server Certificate

1. Call the transaction code, **STRUST**.
2. Select SSL server Standard right click to display the context menu. Then select Create, or Replace if the PSE already exists.



3. Edit the certificate attributes.



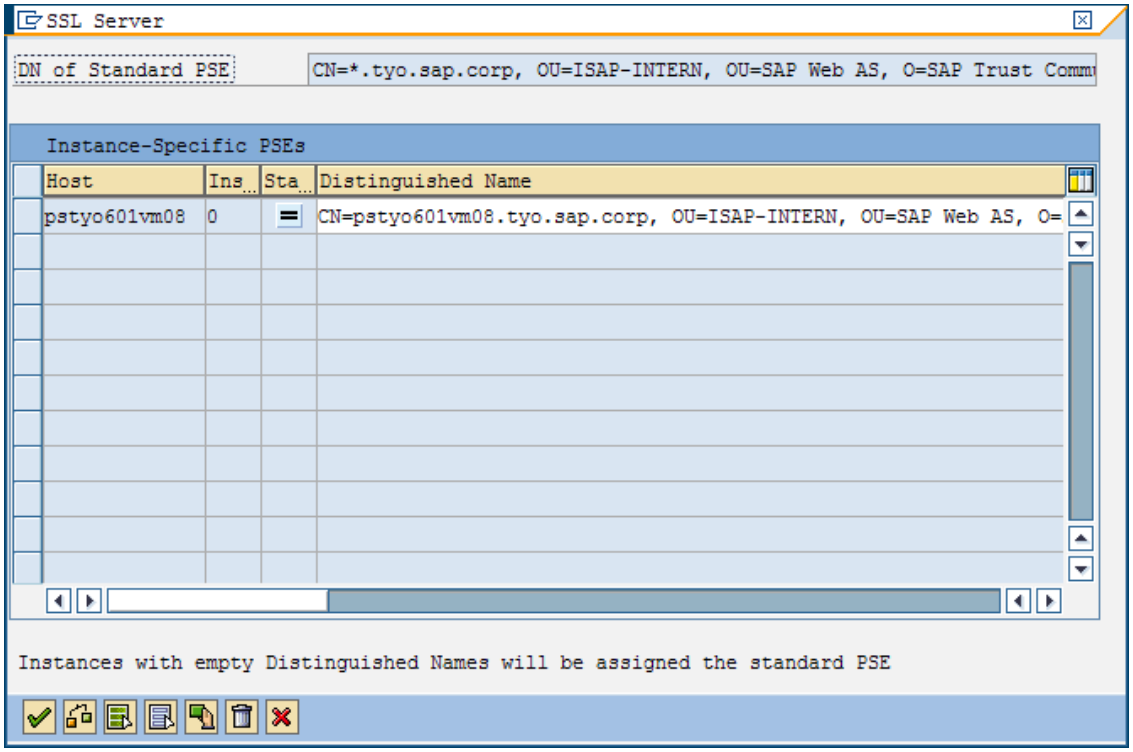
Important

The name must match the client's synchronization host name. You can leave the default value (*.<domain>) here, and the trust manager automatically switch to the right name.

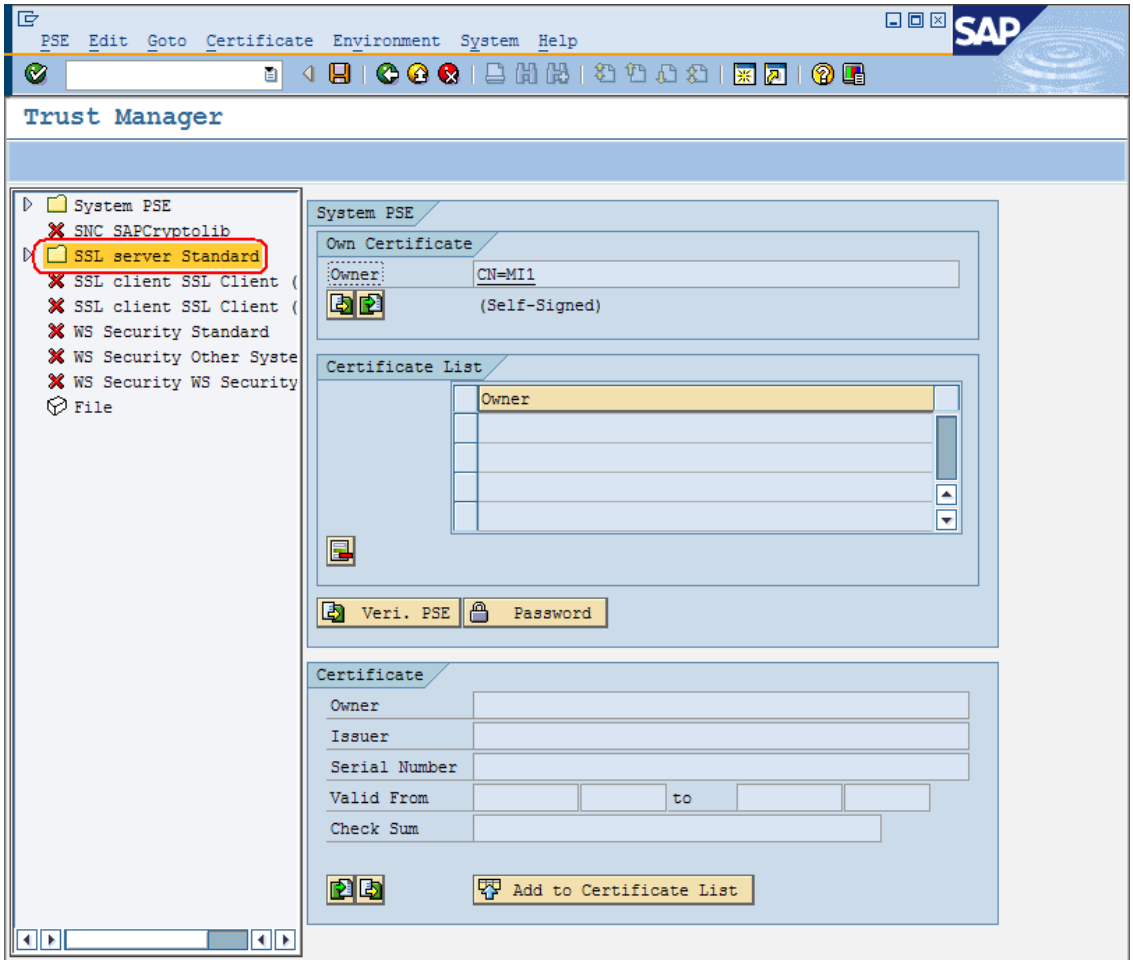
Note

Your CA may require additional attributes, for example, State or Province(S) and Locality or City(L). Contact your Certification Authority for the requirements. If this is the case, enter those attributes in the CA field.

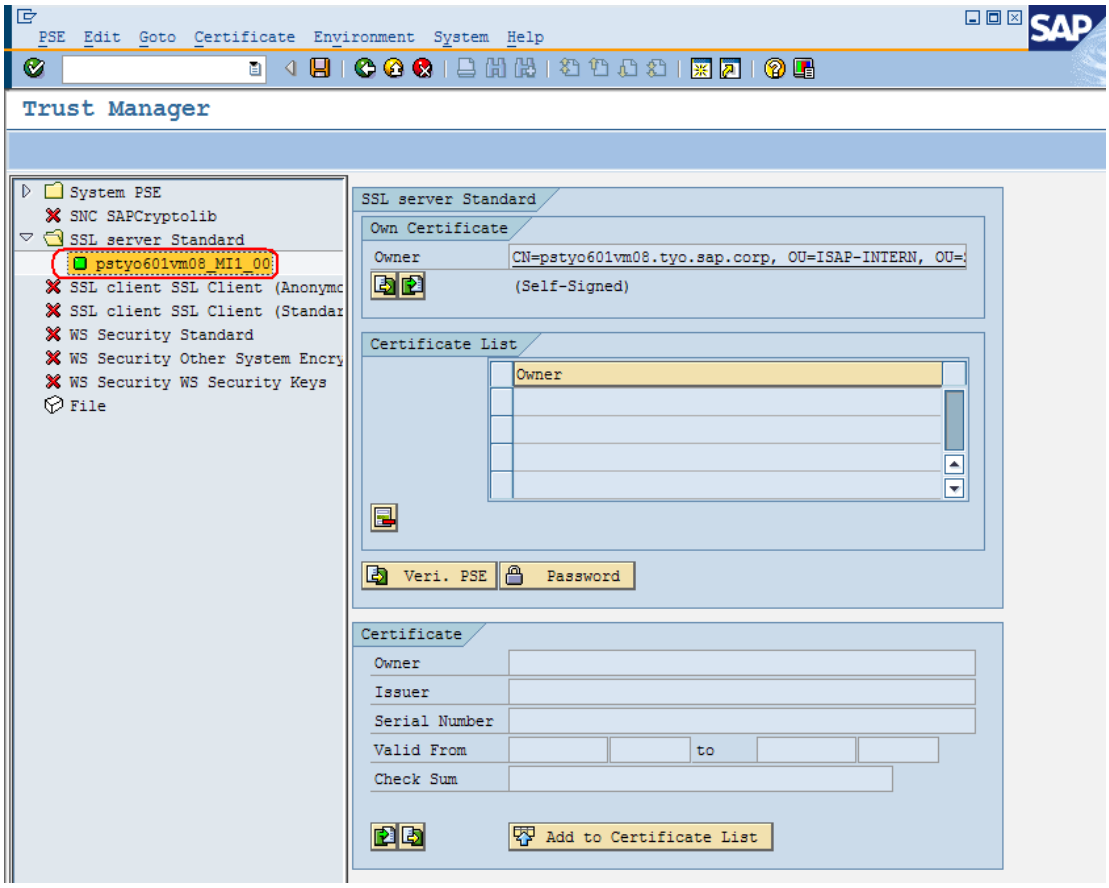
4. Press <Enter>



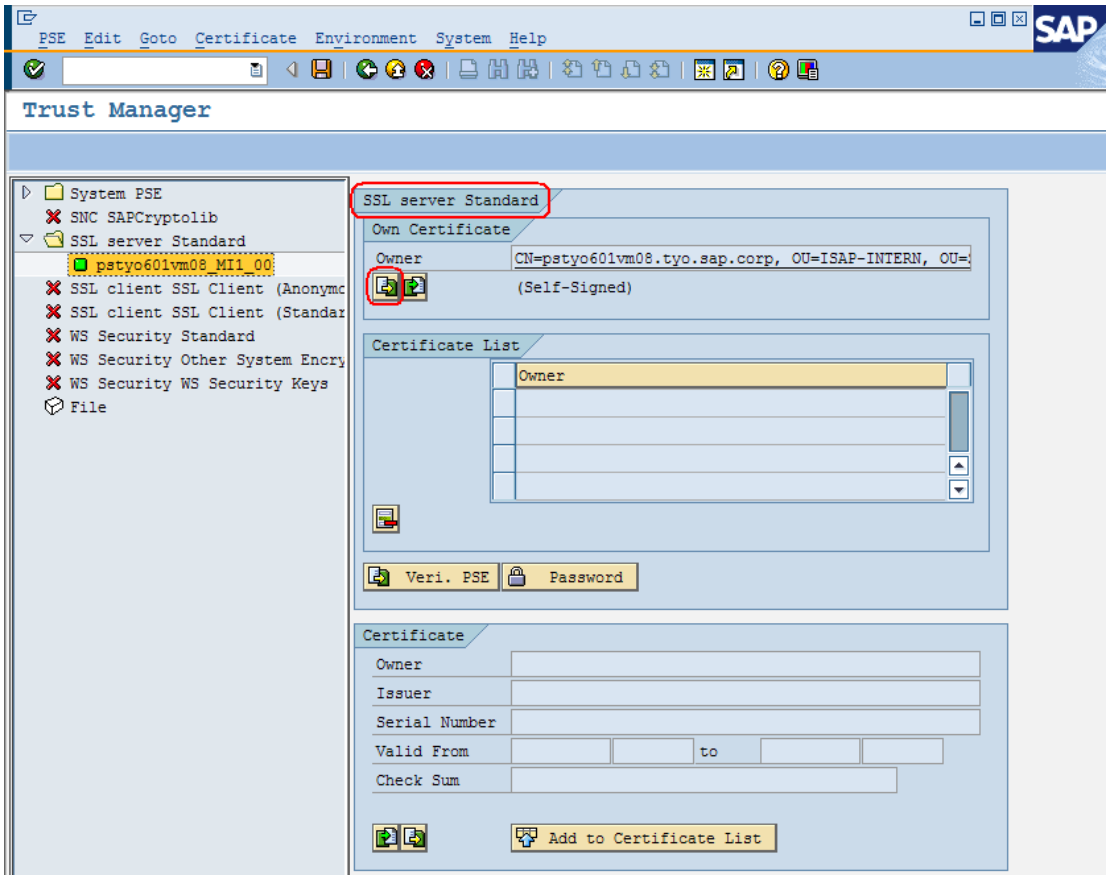
You have created the server certificate.



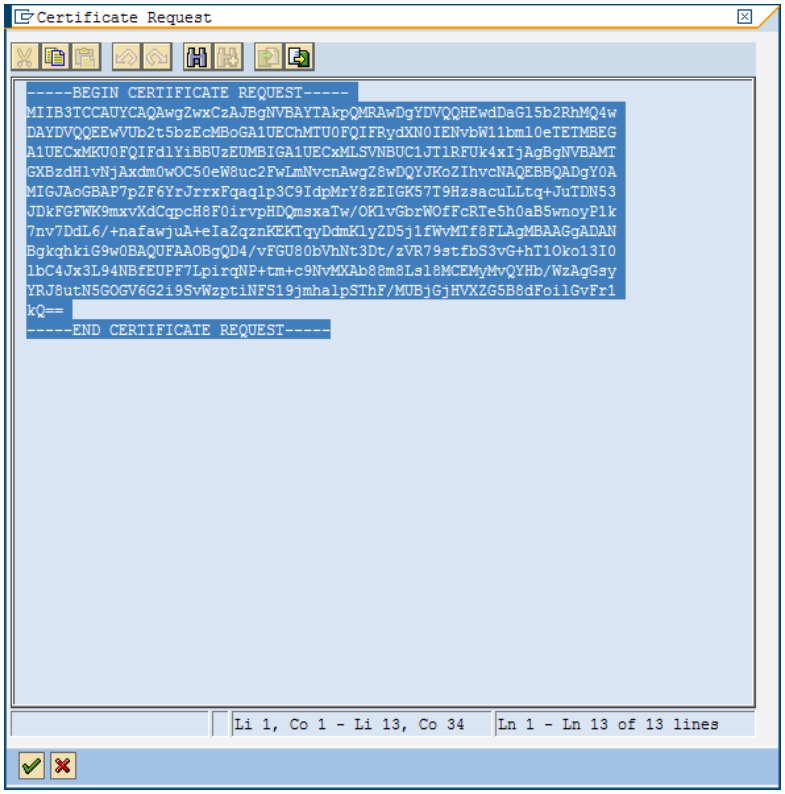
5. Expand the *SSL server Standard* node and double click on the server certificate you just created.



6. Double click on the certificate and press .

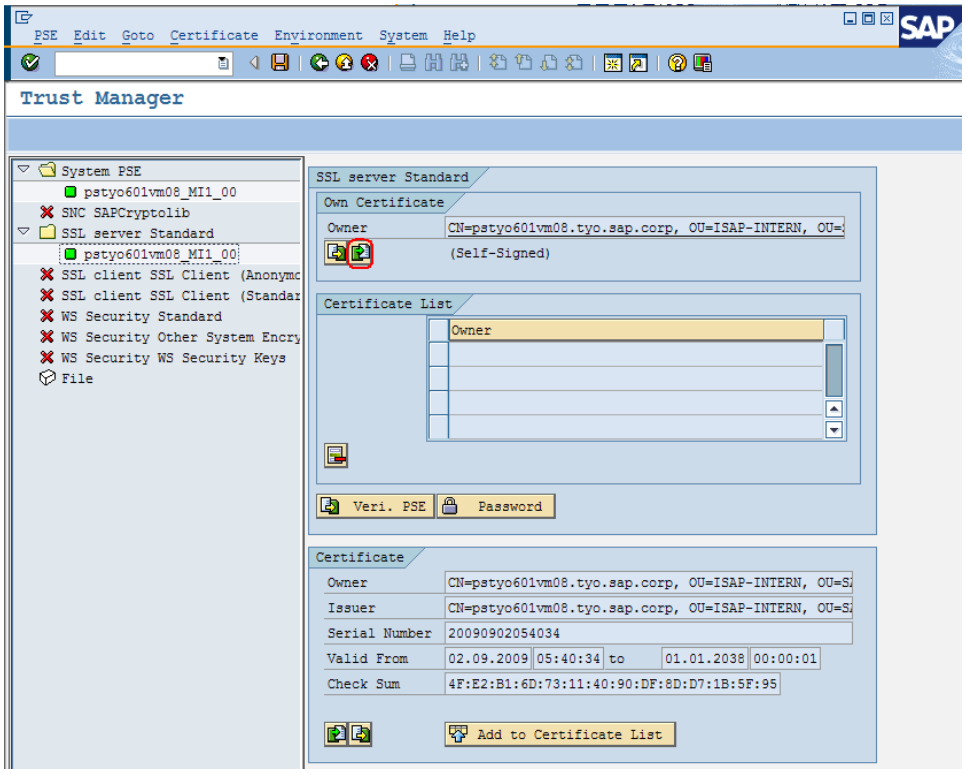


7. Save it to a file by pressing .



8. Send this request to your Certification Authority.

9. Once you receive the response, press .

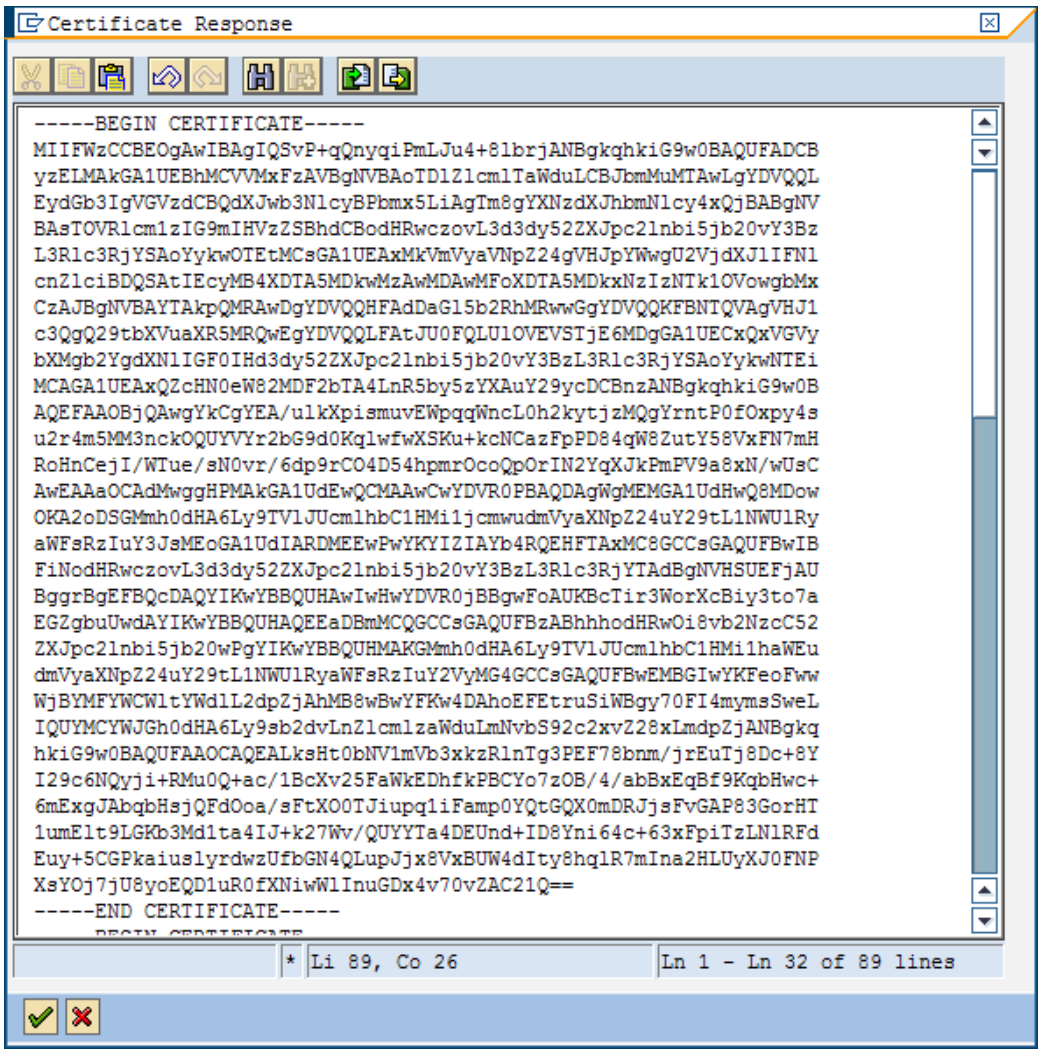


10. Copy and paste or import from a local file

Note

If the response is not in PKCS#7 certificate chain format, and your Certification Authority uses intermediate certificates, then each certificate must be combined before importing to the server.

-----BEGIN CERTIFICATE-----
<contents of the re-issued certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<contents of the certificate of the intermediate CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<contents of the certificate of the root CA>
-----END CERTIFICATE-----

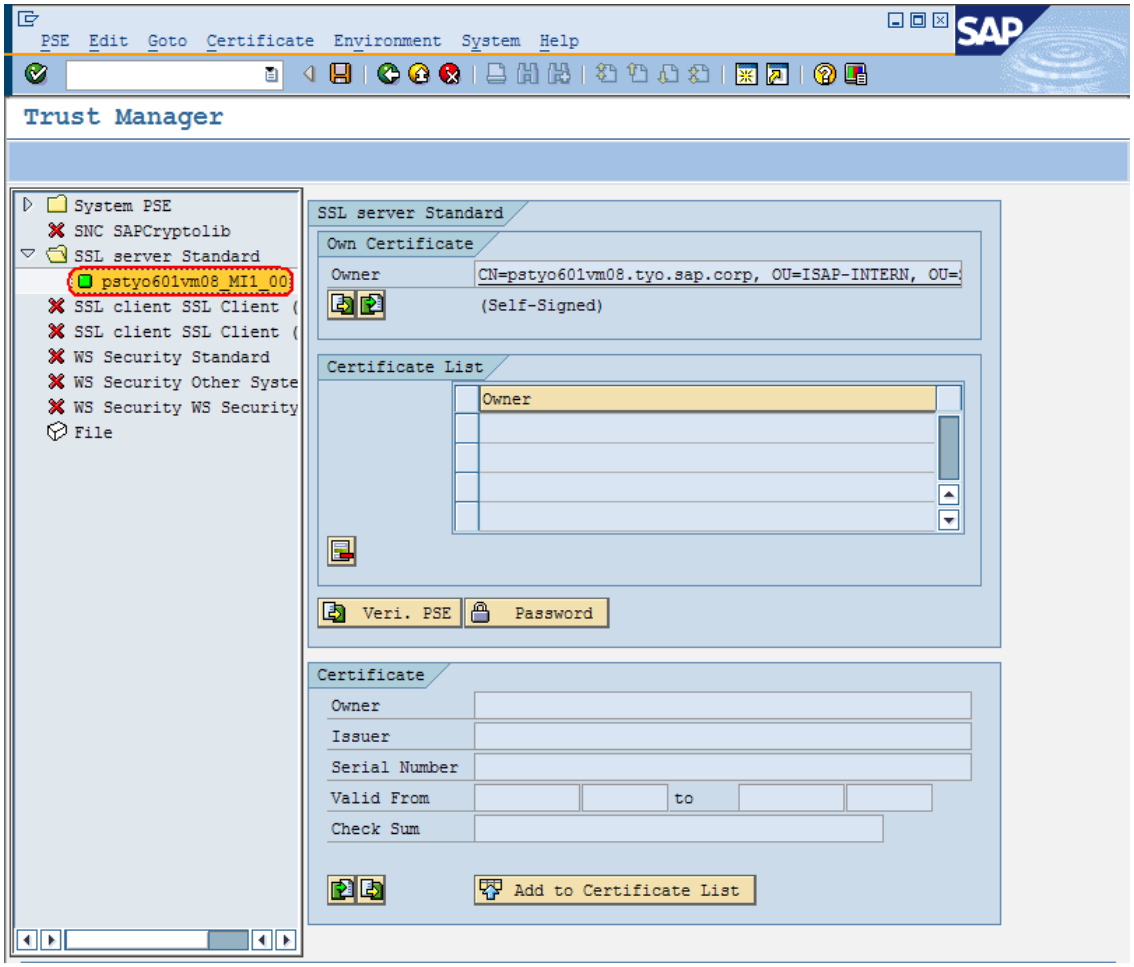


11. Press <Enter>.

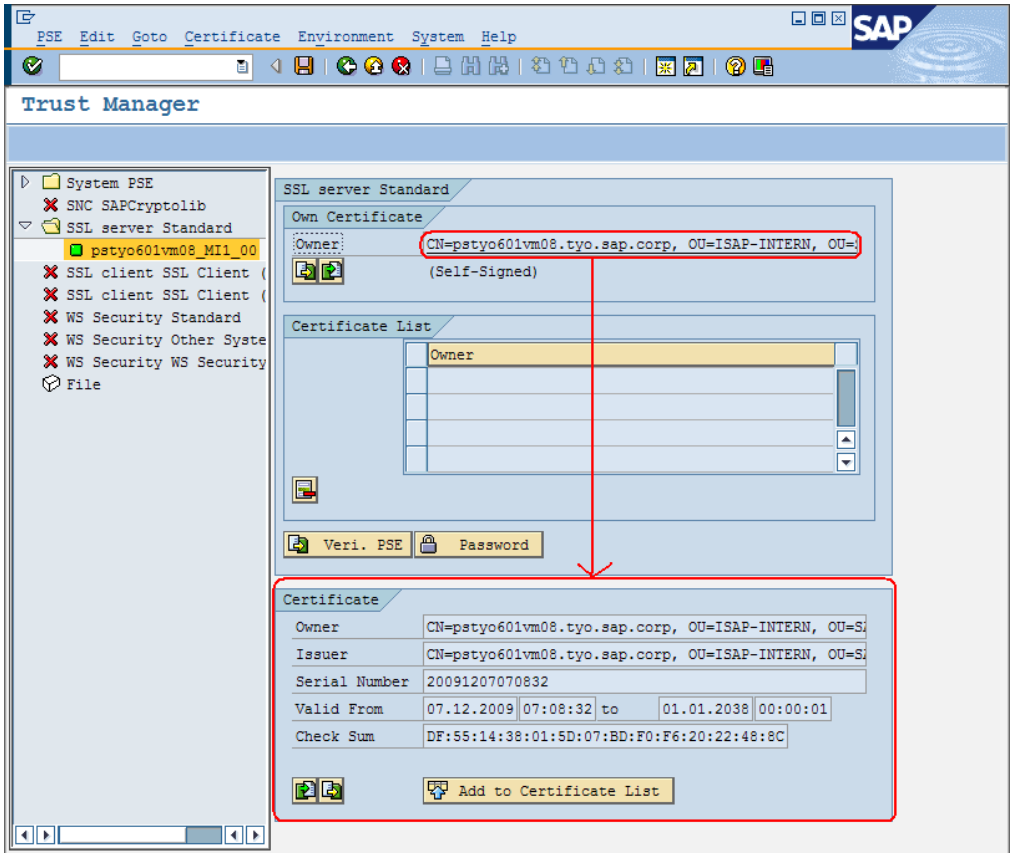
12. The certificate response is imported successfully.

4.4 Export the Server Certificate

1. Call the transaction code, **STRUST**.
2. Expand *SSL server Standard* and double click the certificate.

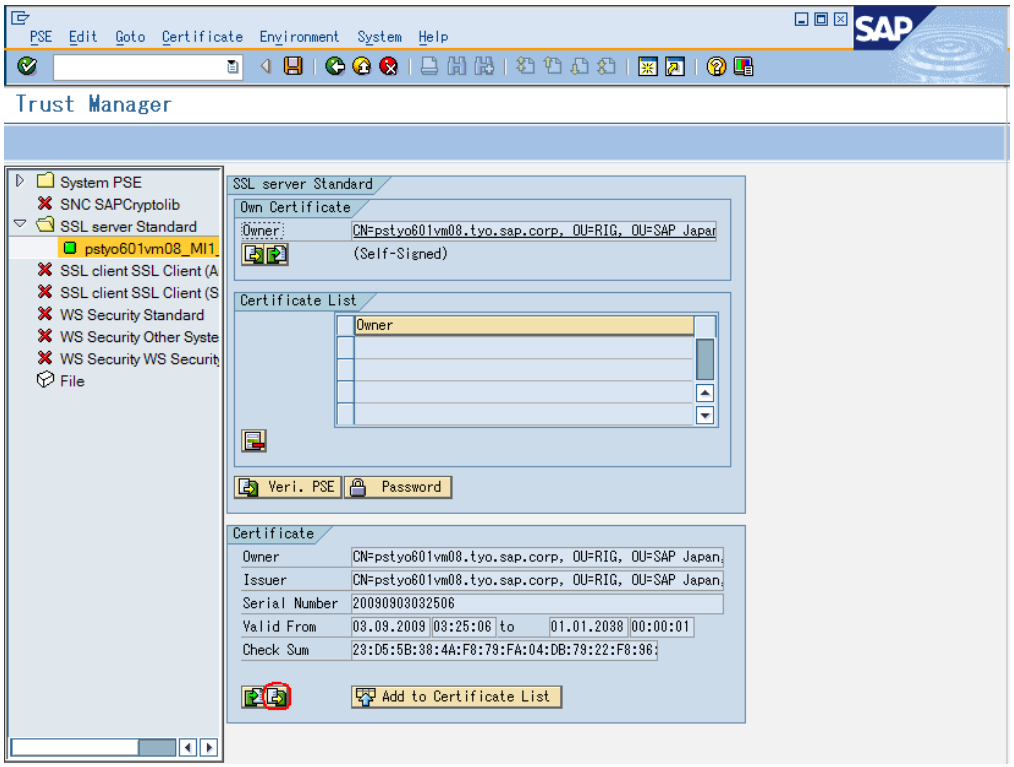


3. Double click the Owner in the SSL server Standard – Own Certificate section.

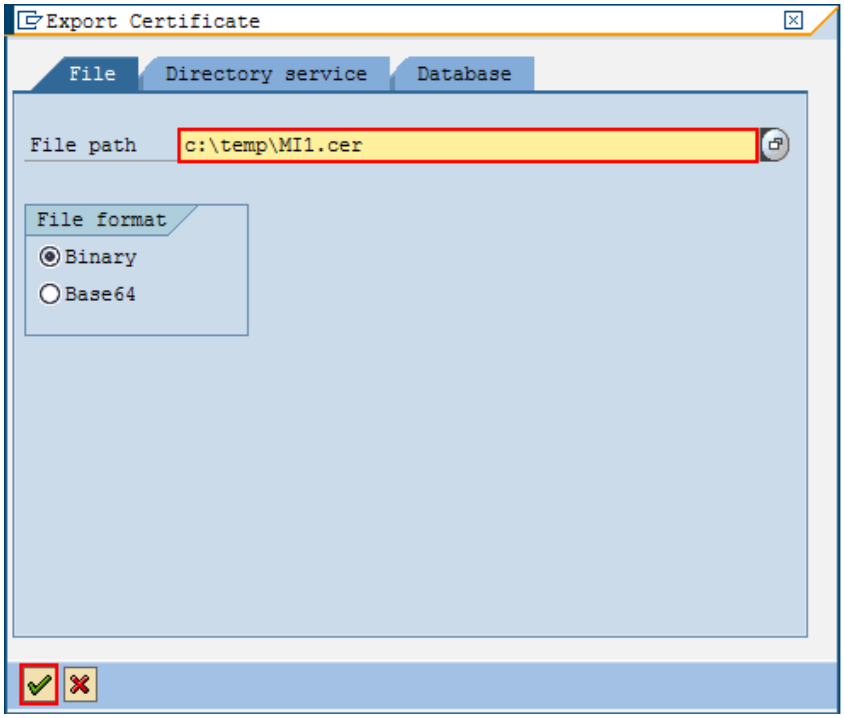


You will see the information of the certificate in the Certificate section.

4. Press in the **Certificate** section.



5. Enter the file path with the file name being **<System ID>.cer** for the certificate and press <Enter>



4.5 Import the Certificate to the Client

1. Open the command prompt on your pc.
2. Go to <SAP NetWeaver Mobile client installed directory>\settings.

   Note

   For the non-laptop client, copy the truststore file located under <SAP NetWeaver Mobile client installed directory>\settings to your pc and work on this copied file. Once it is done, put it back to the original location.

3. Execute the following command.

   <JAVA_HOME>\bin\keytool –import –alias <certificate file name> -file <full path of certificate file> -keystore truststore –storepass access

   Example

   System ID is MI1

   Certificate file was saved as "C:\TEMP\MI1.cer

   ```
   "C:\Program Files\Java\jdk1.5.0_12\bin\keytool" -import -alias
   MI1.cer -file C:\TEMP\MI1.cer -keystore truststore -storepass
   access
   ```

4. Enter **yes** for the prompt "`Trust this certificate? [no]`".
5. `Certificate was added to keystore` message appears.
6. Restart SAP NetWeaver Mobile client.

5. Appendix

Appendix A - Troubleshooting

Note 508307 - Trust Manager: Problems importing certificate responses

www.sdn.sap.com/irj/sdn/howtoguides

THE BEST-RUN BUSINESSES RUN SAP™