SAP Custom Development

SAP Corporate Connectivity for Banking

Security Configuration information

Version	Status	Date
1.0	Customer	January 25, 2013

Customer

The Best-Run Businesses Run SAP™

Dietmar-Hopp-Allee 16
D-69190 Walldorf

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	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes 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`	Exact user entry. 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	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library.*

Contents

1 Organization 4

1.1 Document Administration 4
1.1.1 Authors 4
1.1.2 History 4
1.1.3 Intended Audience 4
1.1.4 Related Documentation 4
1.2 Purpose and Scope 4
1.3 Glossary 5

2 User Administration and Authorization 5

2.1 Authorization Object for the *Payment Cockpit* 5

3 Certificate Implementation 6

3.1 Overview 6
3.2 Security Mechanisms 6
3.3 Step-by-Step Instructions 6
3.3.1 Transaction *STRUST* 6
3.3.2 Certificates Used – Scenario Information 8
3.3.3 Security Configurations in the Customer's ERP 9
3.3.4 Steps after Certificate-Installation in SAP ERP 15
3.4 Generic Steps – Creating a PSE (If required) 16
3.5 Installing a Root Certificate – Generic Procedure 20

4 Security Issues 23

1 Organization

1.1 Document Administration

1.1.1 Authors

Name	Company	Project Role or Comment
Vivek Vishal	SAP Custom Development	Author
Viswanath Natesan	SAP Custom Development	Reviewer

1.1.2 History

Date	Version	Chapter	Name	Change/Enhancement	Agreed with
07/12/2012	0.1.0	All	Vivek Vishal	Document Created	Viswanath Natesan

1.1.3 Intended Audience

This document is intended for persons in the following roles:

- Primary audience:
  - System administrators
  - Technology and security consultants
- Secondary audience:
  - Support consultants
  - Functional consultants
  - Partners and customers

1.1.4 Related Documentation

- Configuration Guide
- Corporate ERP Connectivity Guide
- SAP Solution Manager

1.2 Purpose and Scope

The purpose of this document is to describe the security configurations that are required for enabling a reliable and secure certificate-based asynchronous communication between *Westpac Bank's (the bank')* landscape and the customer's landscape. Integration between standard programs or components on the ERP side on the one hand, and, the bank's PI system, and further, to the bank's system on the other, is channeled through this secure communication path across the communicating landscape.

This security information document provides a central starting point for the technical implementation of the security standards and configurations as a part of *SAP Corporate Connectivity for Banking Westpac* solution (the solution).

1.3 Glossary

Term	Definition
Web service	Web services are self-contained application functions that can be processed through open standards.
Endpoint	An Endpoint, identified by its address, is a location, from where, a service that is associated with the binding of a specific interface, can be accessed.
Certificate	An electronic "identity card" that establishes a user's credentials when doing business or other transactions on the Web. It is issued by a Certification Authority (CA) and contains name, serial number, expiration date, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.
CA	An external instance that issues public-key certificates. The Certification Authority (CA) guarantees the identity of the person who is granted the certificate.
PSE	Secure location where a user or component's public-key information is stored. The *Personal Security Environment* (PSE) for a user or component is typically located in a protected directory in the file system or on a smart card. It contains both the public information (public-key certificate and private address book) as well as the private information (private key) for its owner. Therefore, only the owner of the information should be able to access his or her PSE.
ICF	Software layer in Application Server that provides an ABAP interface for HTTP, HTTPS & SMTP requests. The AS ABAP environment uses the Internet Communication Framework to communicate with Web applications in the server role and in the client role. ICF receives Web-based ABAP calls through Internet Communication Manager (ICM).
X.509	In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on (SSO) and *Privilege Management Infrastructure* (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
SOAP	SOAP, originally defined as *Simple Object Access Protoco*l, is a protocol specification for exchanging structured information in the implementation of Web Services. It relies on *Extensible Markup Language* (XML) for its message format, and usually relies on other application layer protocols such as HTTP or RPC.

2 User Administration and Authorization

2.1 Authorization Object for the *Payment Cockpit*

The payment cockpit that is inbuilt into the *solution* is secured with an authorization strategy that contains standard authorization objects. This will also be used as a screening mechanism to ensure a secure authenticated payment run and monitoring in the system.

The following authorization objects are created for Monitor: */CBCOM/PRT*

- Activity 16 – for execution the report
- Activity A9 – for resending the messages

A user must have the above mentioned authorizations to execute the payment cockpit.

3 Certificate Implementation

3.1 Overview

This section describes the configurations and the step by step approach to enable the customer's SAP ERP system, and Westpac Bank's BANKPI System along with the intermediate load balancer at the bank's end to provide a secure message communication between the customer's and the bank's landscape by using the *Client Certificate Authentication* mechanism.

3.2 Security Mechanisms

A security-level defines the way a message that is embedded in a communication channel is handled between the interacting systems. The general HTTP security levels are as follows.

- HTTP without SSL
- HTTP with SSL (=HTTPS) without client authentication.
- HTTP with SSL (=HTTPS) with client authentication.

The security level used in this integration between the customer and the bank is *HTTP with SSL client authentication*. This security level is meant to ensure that only those messages/communication that are initiated over an HTTPS connection and are authenticated by client certificates, are accepted at the integration server / load balancer security framework as applicable.

Messages are rejected and dropped if the security level of the HTTP connection is lower or not as expected at the verification point for the incoming channel.

For more Information, see SAP Note ***891877***.

3.3 Step-by-Step Instructions

3.3.1 Transaction *STRUST*

Managing certificates within the SAP environment (ABAP stack) is done through the standard transaction *STRUST*. The transaction contains a list of available PSE containers (on the left-side of the screen) and the trusted certificates that are available for them (on the right-side)

Transaction *STRUST* also provides the option of creating custom PSEs for maintaining certificates relevant to a particular scenario.

For more Information on creating and managing PSEs, see the SAP Help Portal at: http://help.sap.com/saphelp_nw04/helpdata/en/59/6b653a0c52425fe10000000a114084/content.htm

The following figure shows a sample *STRUST* screen:

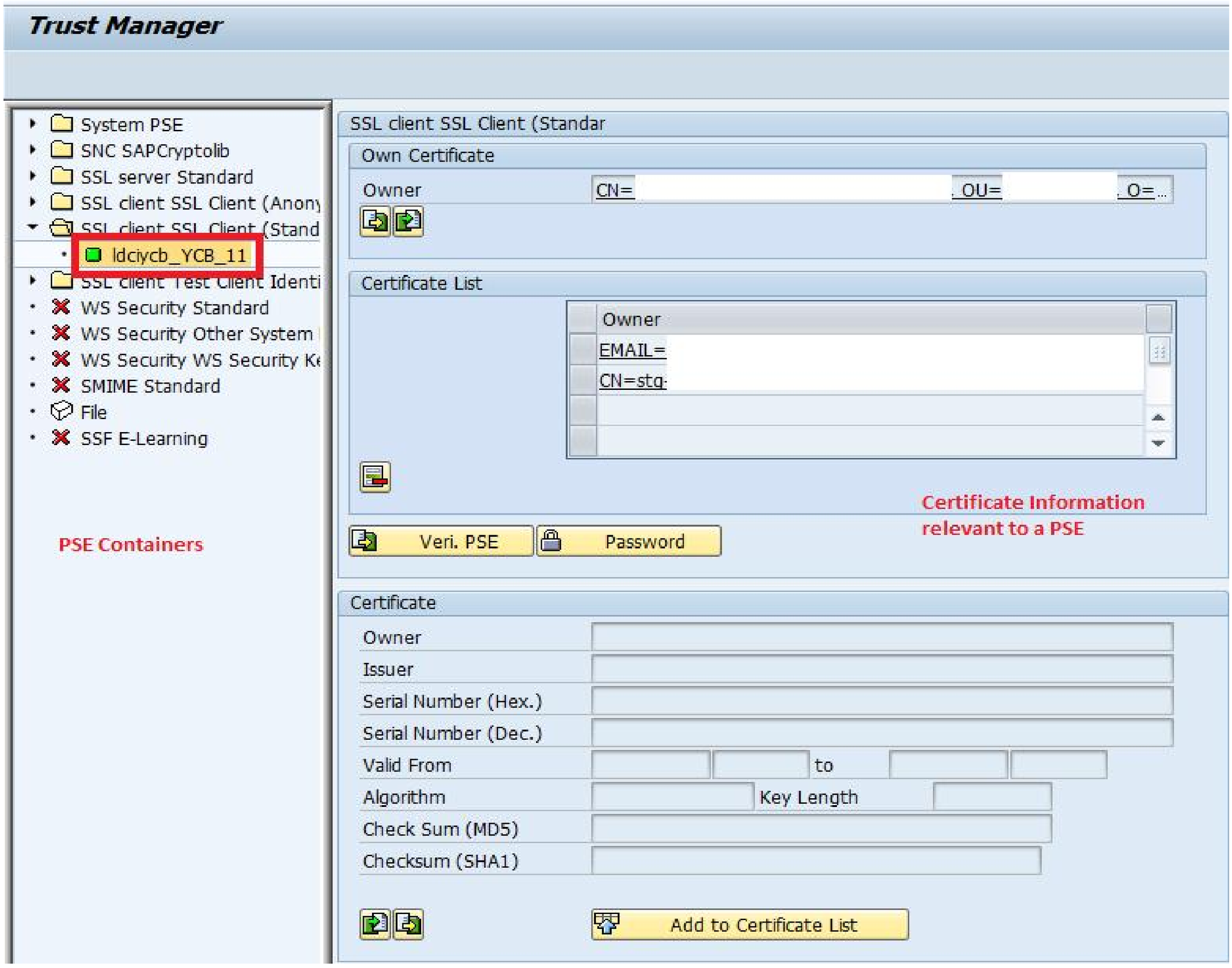

Figure 1

3.3.2 Certificates Used – Scenario Information

Figure 2 shows the technical implementation of the security configurations across the customer's and bank's landscapes

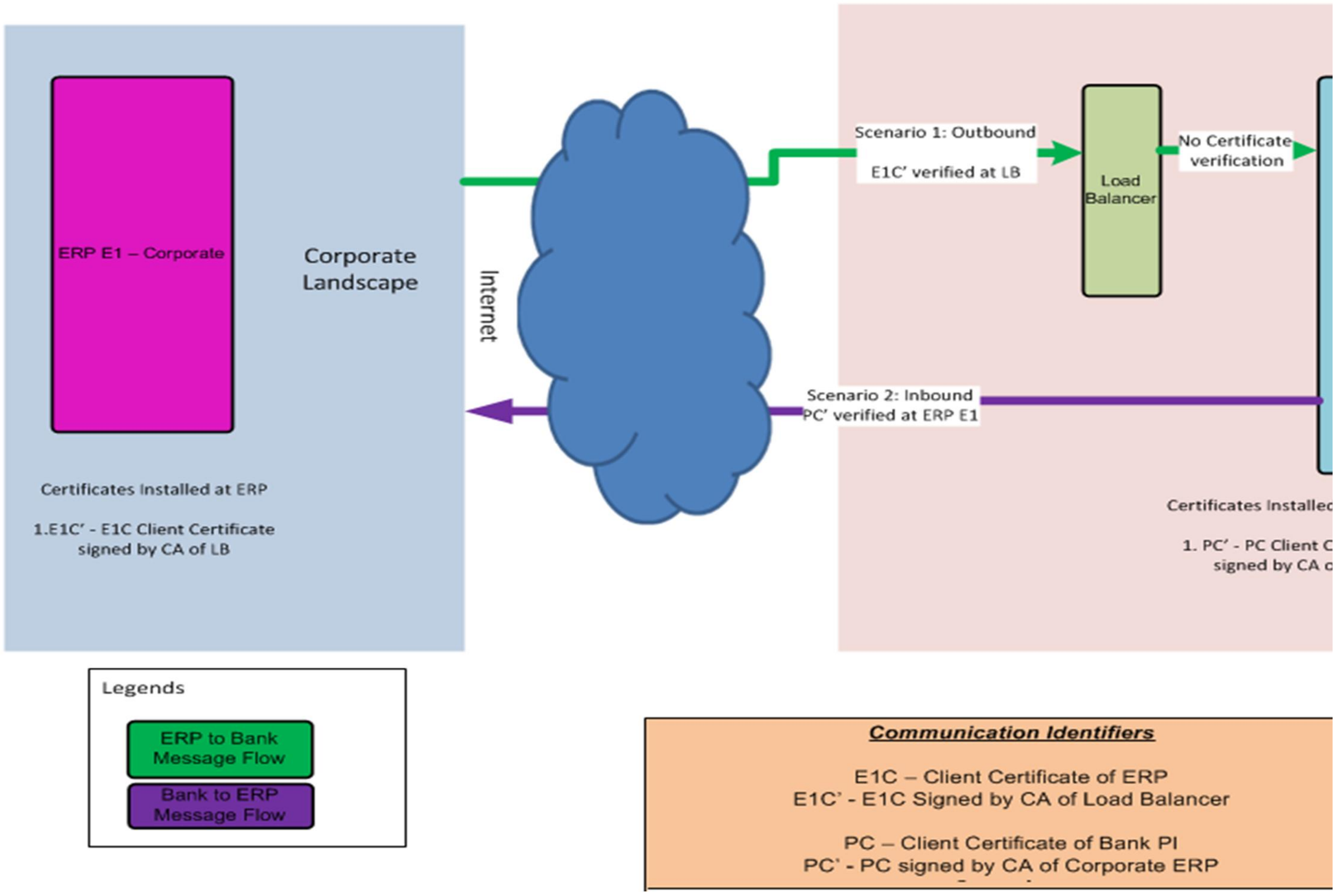

Figure 2

Details of installed Certificates:

The following table provides details of various certificates that are used as a part of security configurations for the integration scenarios between customer's SAP ERP and BANKPI.

Scenario Information	Certificate Type	Signing Authority	Installation Location
Corporate ERP to BANKPI via load balancer See section 3.3.3 for implementation details	Client certificate	Trusted signing authority of load balancer in the Westpac landscape	Corporate ERP
BANKPI to Customer's SAP ERP See Section 3.3.4 for Implementation Details	Client certificate	Trusted signing authority of corporate ERP system	BANKPI

3.3.3 Security Configurations in the Customer's ERP

This section deals with the security configurations to be implemented in the customer's SAP ERP system for communication between ERP and BANKPI via load balancer.

Note: We have used the SSL client standard PSE for all communications and scenarios that leverages the solution and establishes connectivity with the mentioned security configurations. The steps given in sections 3.3.3 and 3.3.4 describe the same.

Step 1: Expand the folder of PSE – *SSL Client SSL Client Standard* in the ERP system as shown in figure 3. Double-click on the corresponding entry. The PSE will have the root certificate of the concerned ERP system as shown in the following figure:

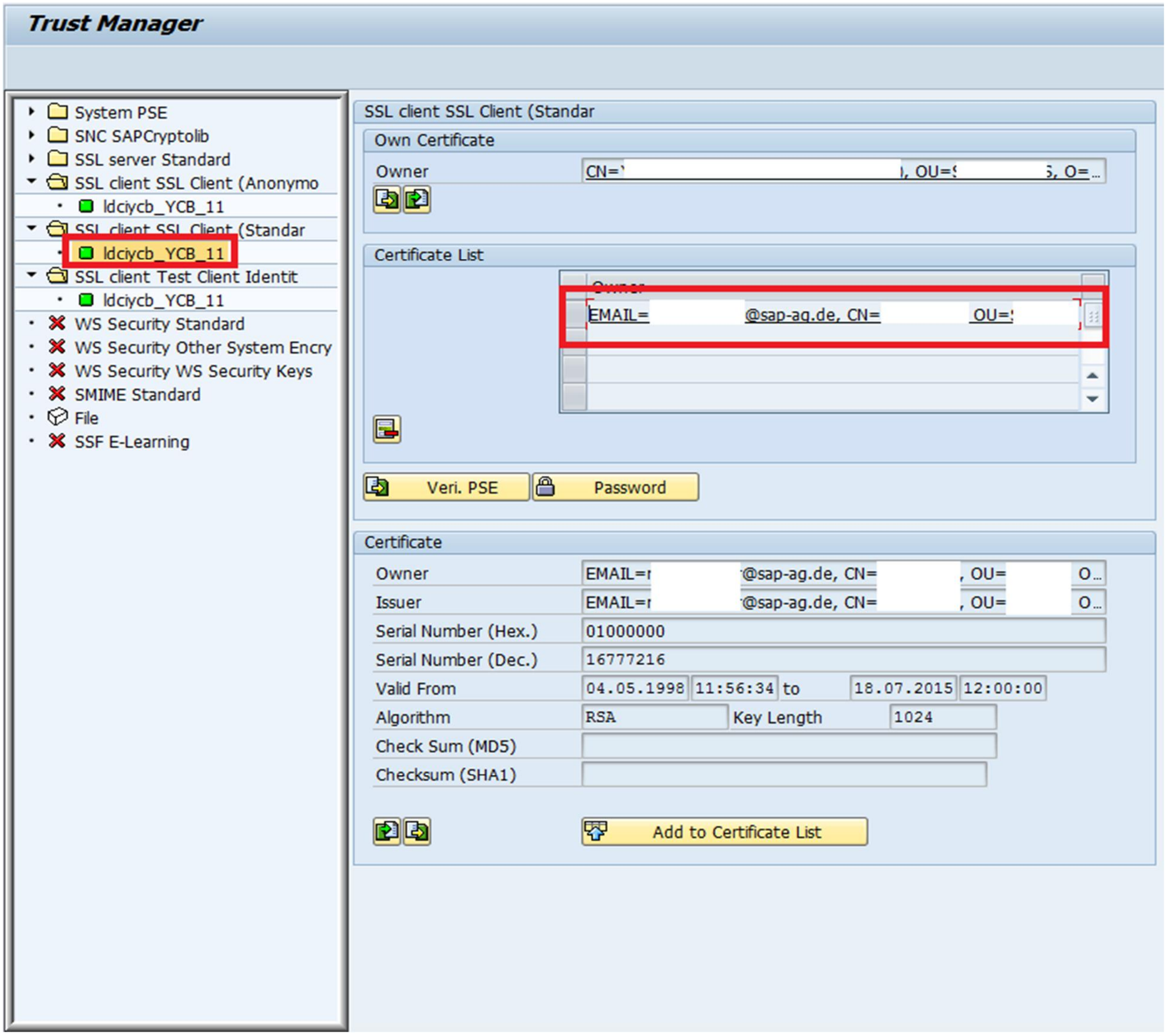

Figure 3

Step 2: Choose *Create Certificate Request* to copy the certificate request as shown.

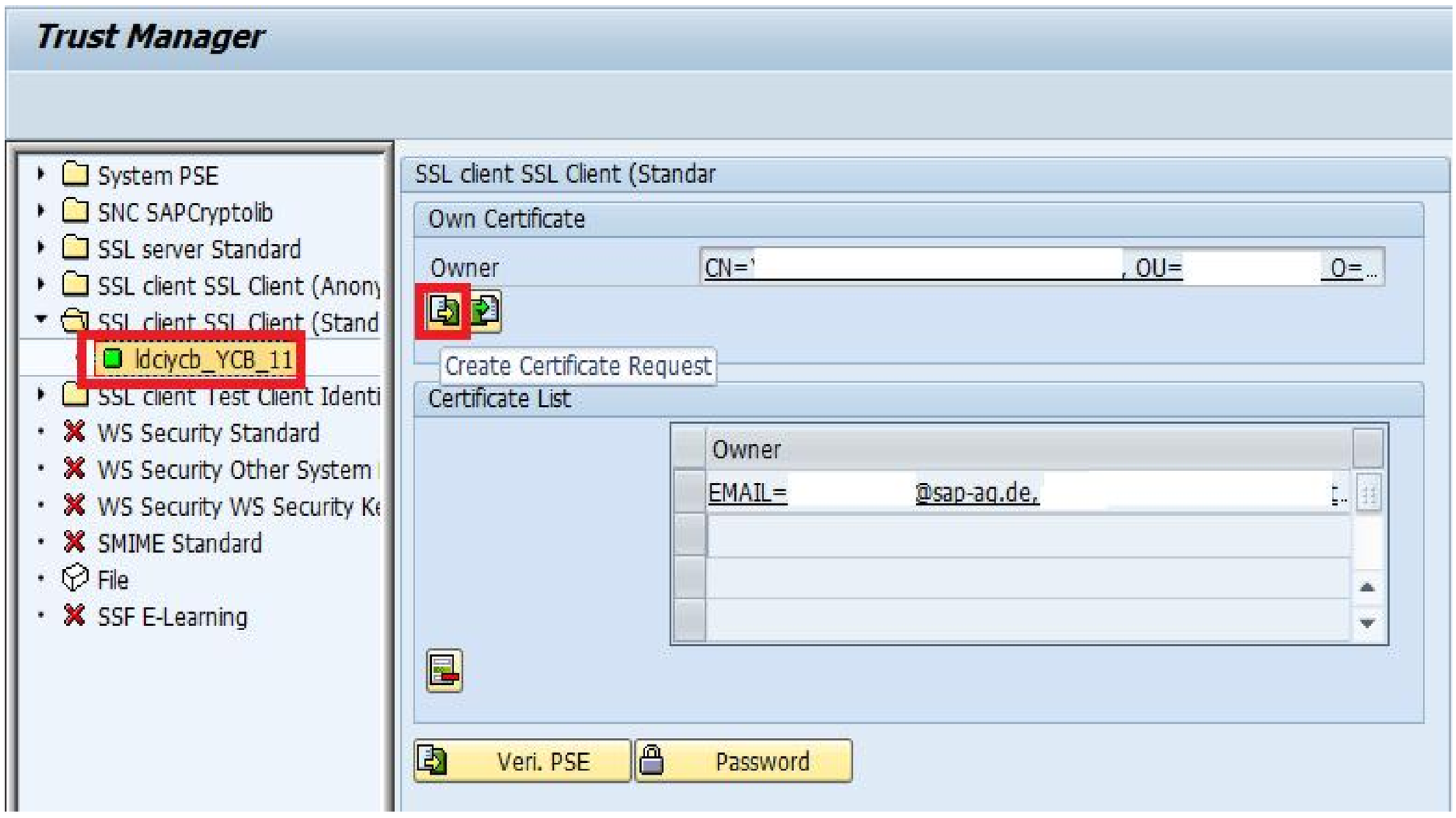

Figure 4

Step 3: Copy the certificate request and store it in the buffer. This certificate request now needs to be signed in PKCS #7 format (ideally) by the bank's LB trusted Authority.

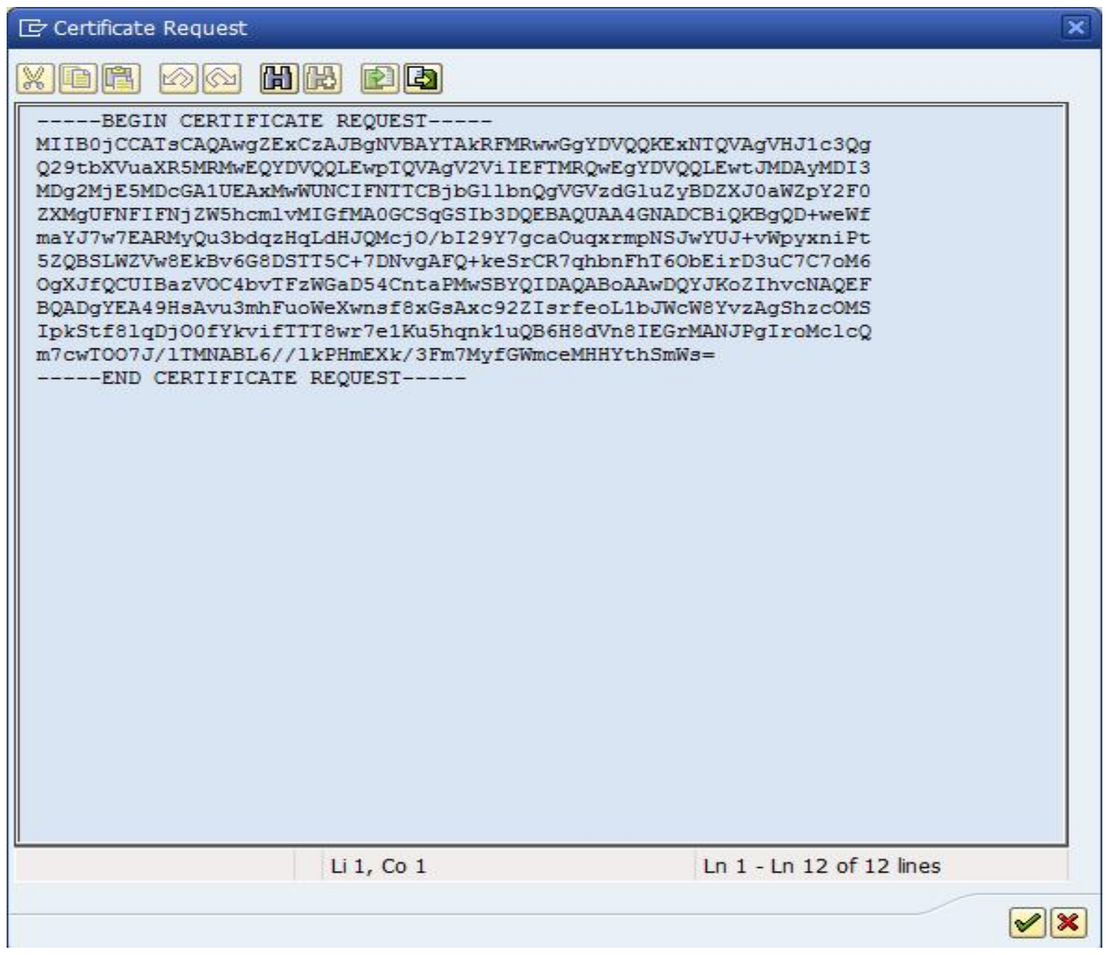

Figure 5

Step 4: Once the signed certificate response has been received from the bank, it should be imported in the same SSL client SSL standard PSE. Choose *Import Certificate Response* as shown in Figure 6.

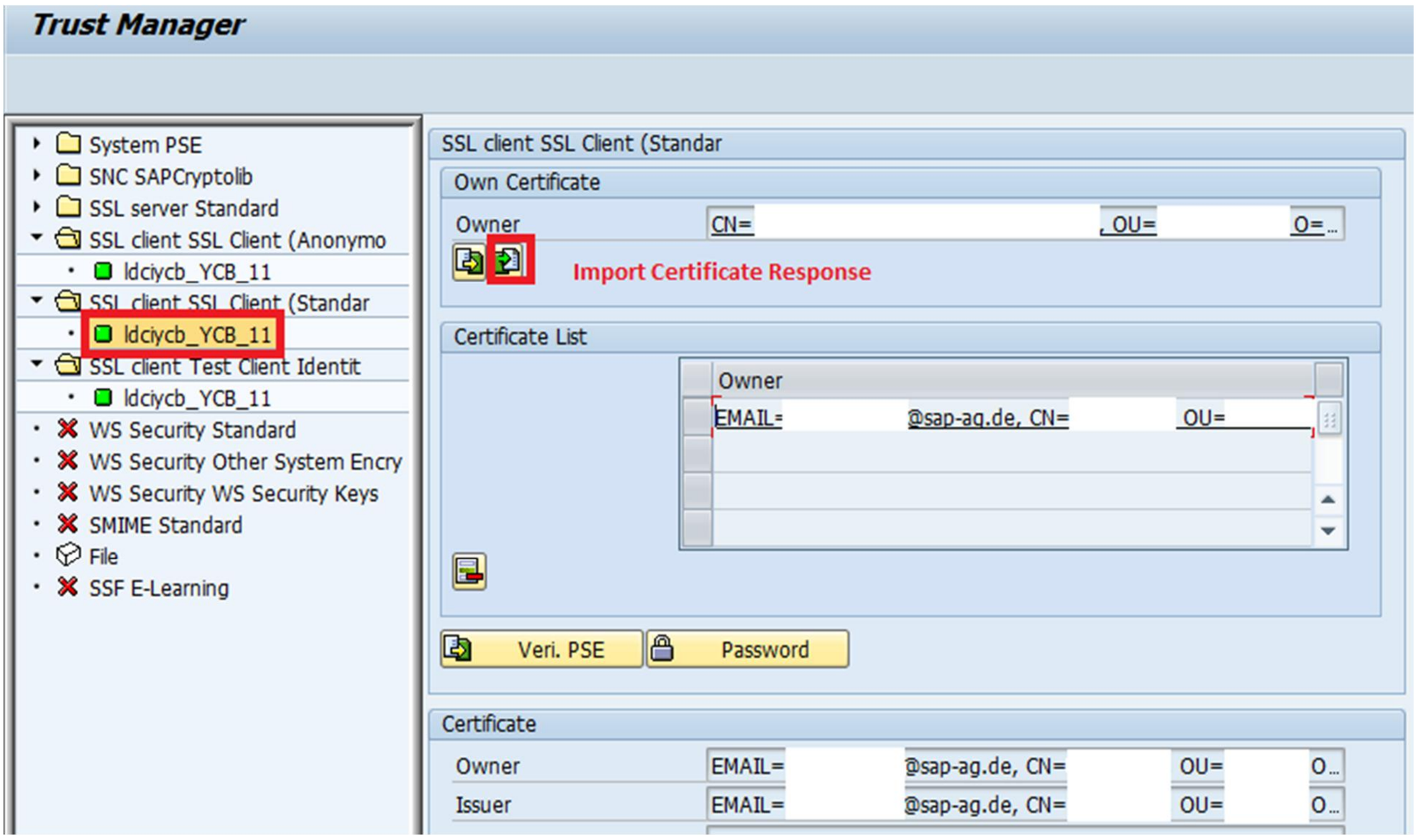

Figure 6

Step 5: Copy the response and choose *Import Certificate Response* as shown in Figure 6. The certificate response should be input and saved for it to be registered in the PSE as shown below.

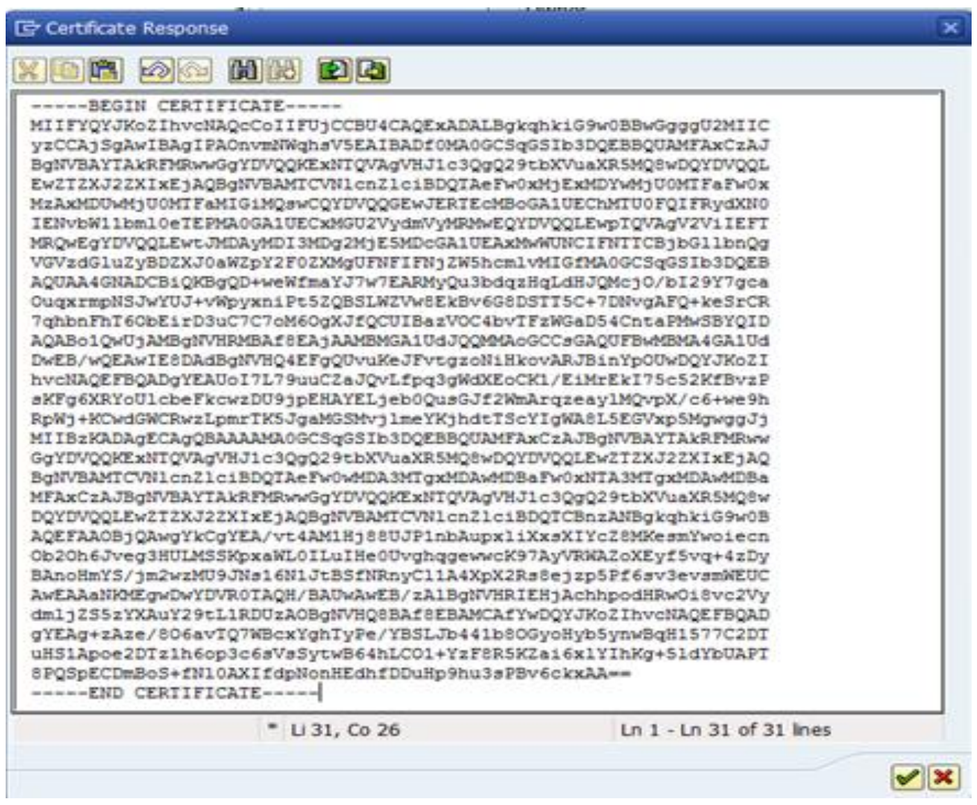

Figure 7

Step 6: Save the response. You can see that the Issuer name has changed to the credentials from the signing authority presented by the bank as shown in Figure 8.

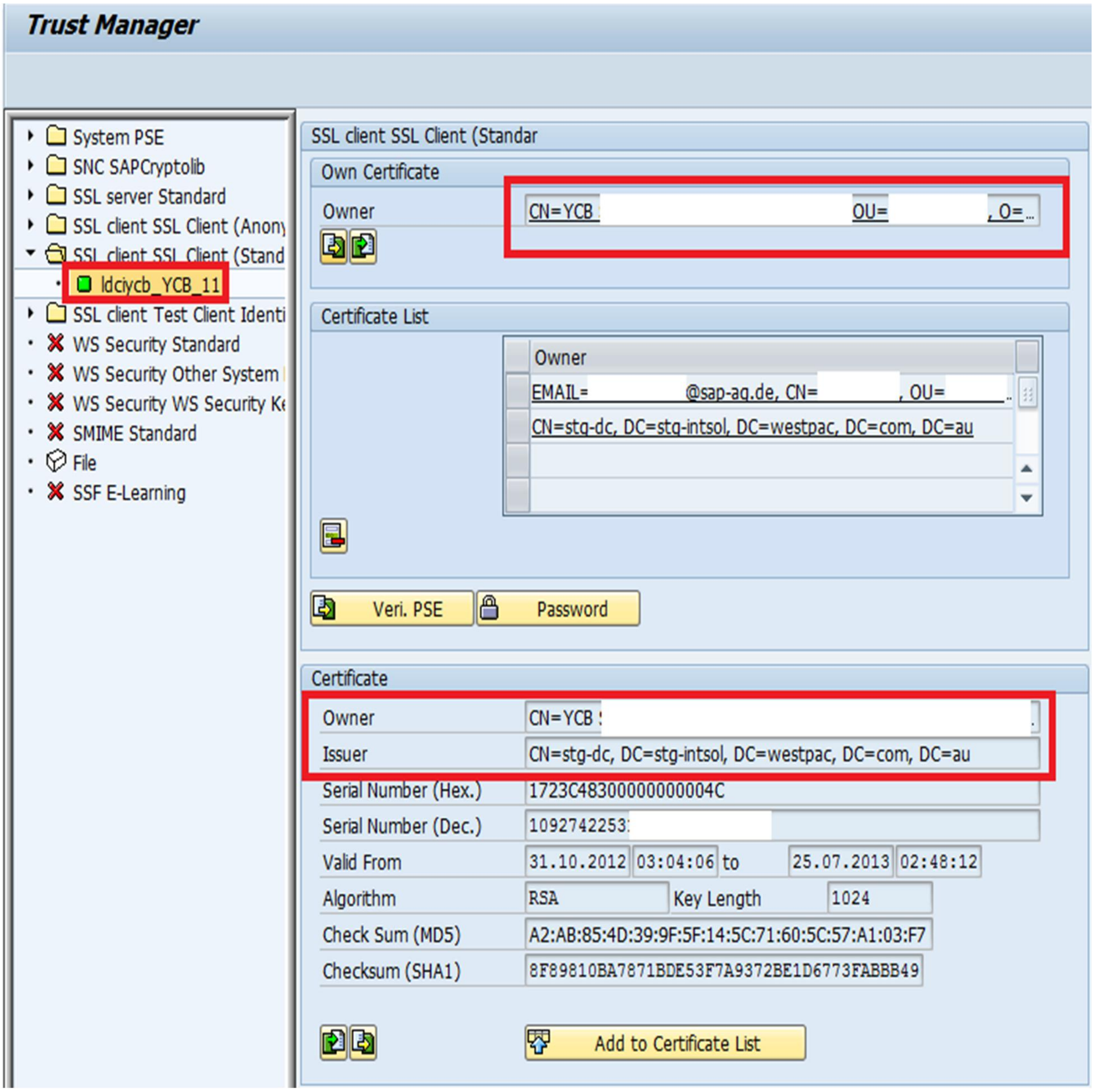

Figure 8

Step 7: Choose *Add to Certificate List* to add this certificate to the current PSE list as shown in Figure 9.

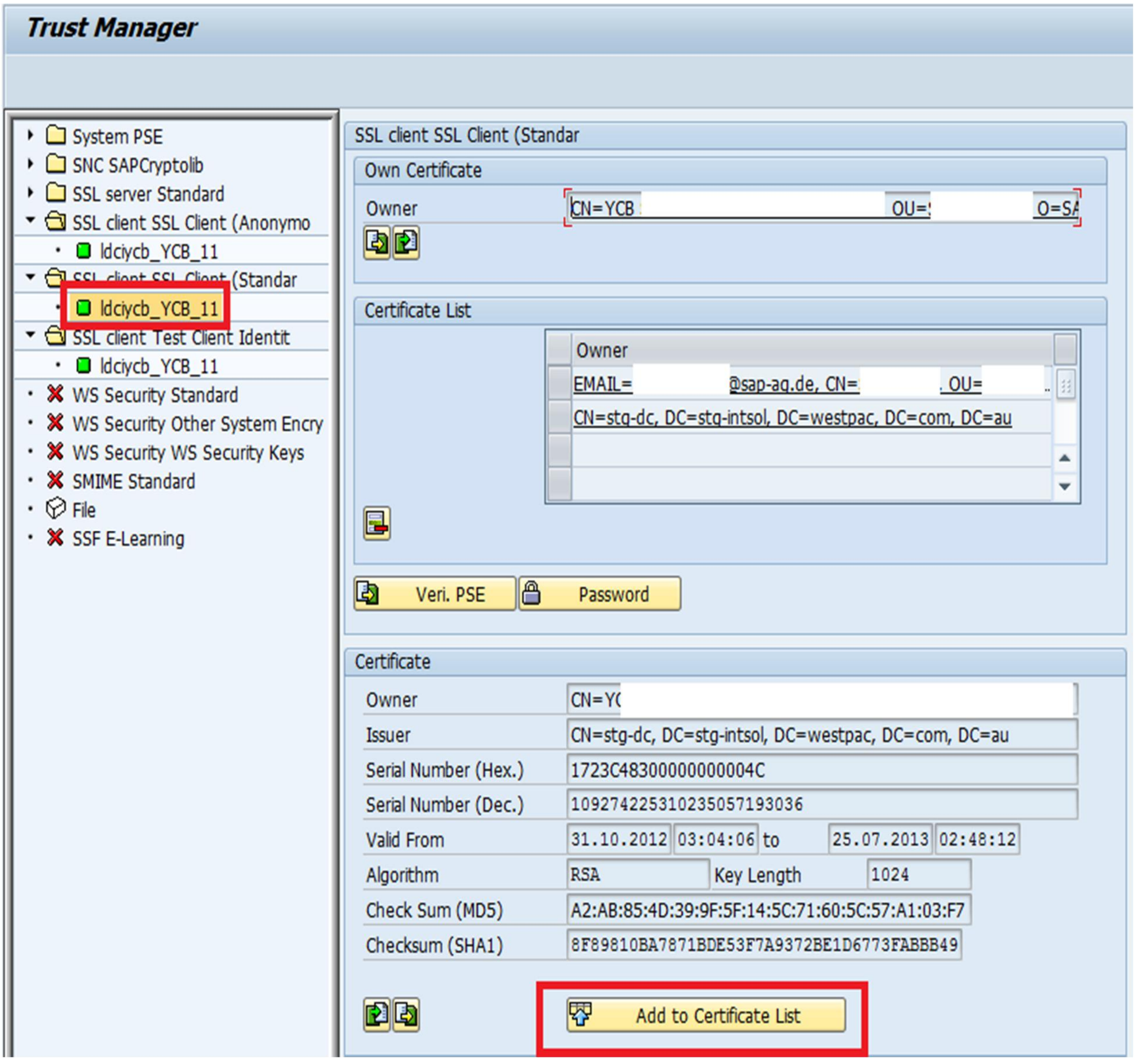

Figure 9

Step 8: After completing the steps described above, execute a *DISTRIBUTE ALL* and restart ICM for the changes to come into effect.

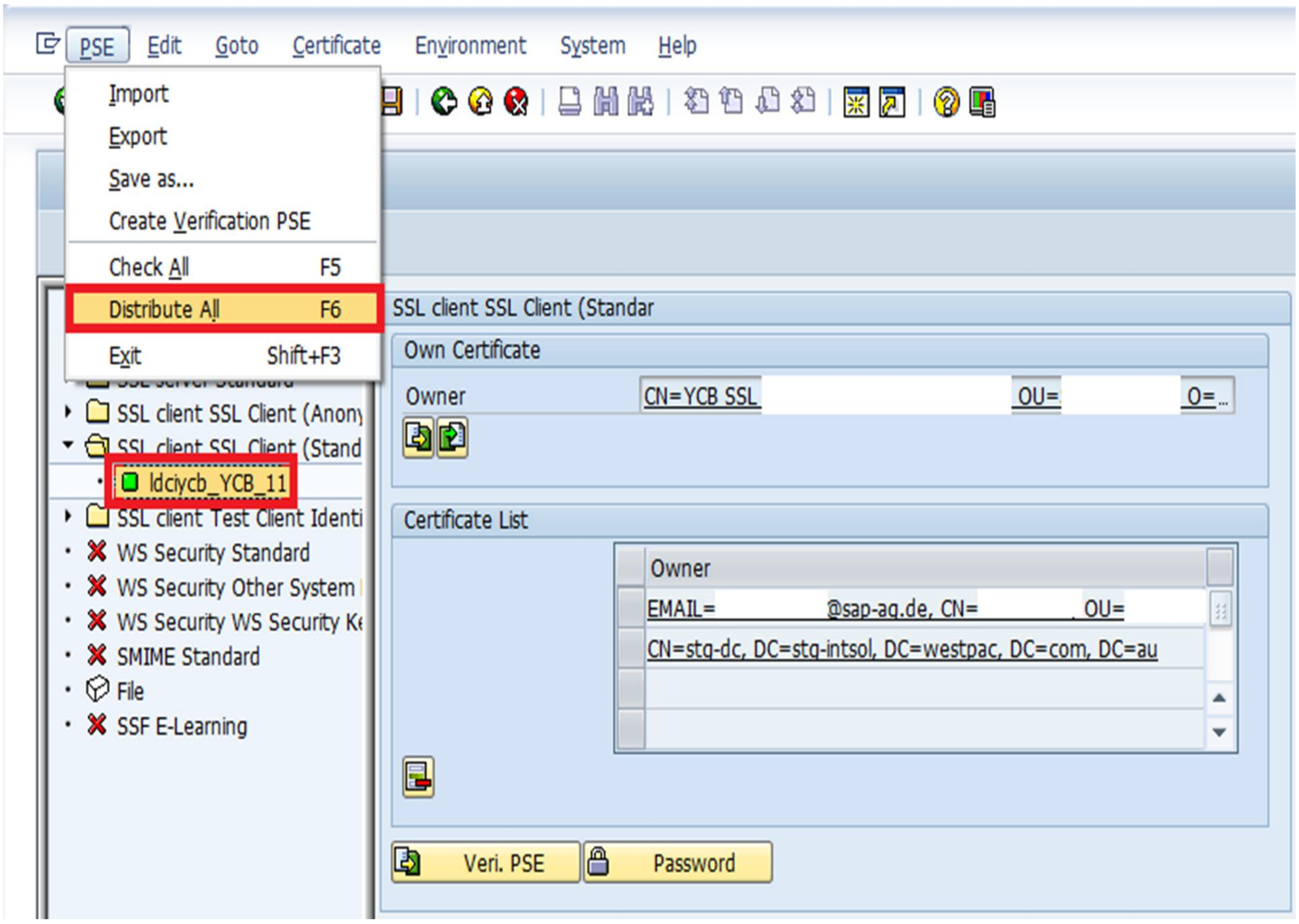

Figure 10

3.3.4 Steps after Certificate-Installation in SAP ERP

The steps given in section 3.3.3 describe how the trusted authority of the load balancer at the bank's side signs the client certificate for the ERP. The key store view of this PSE – SSL client standard ***DFAULT*** can now be used to implement the security configuration for communication via SOAMANAGER from ERP to BANKPI as shown in the Figure 12.

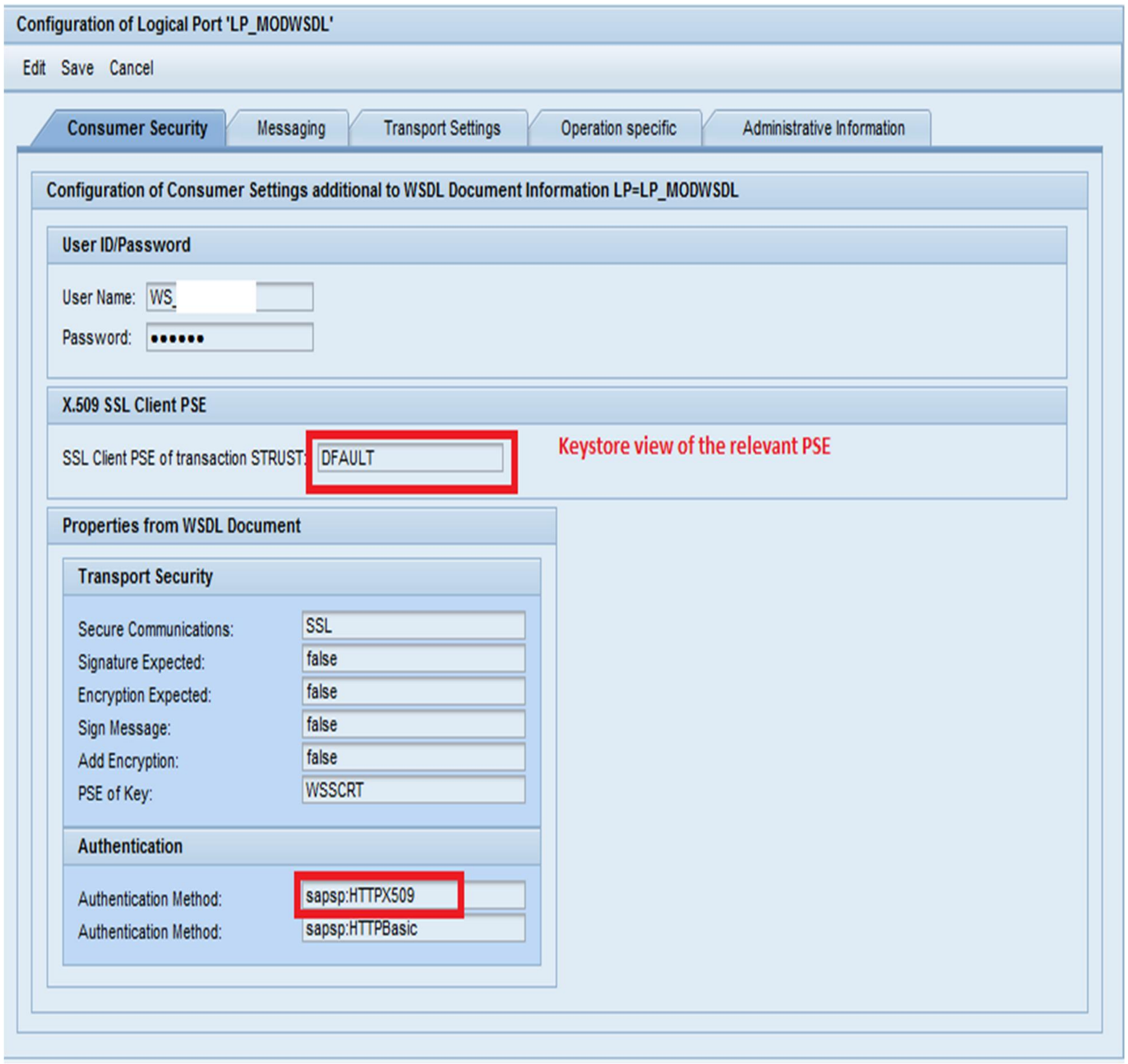

Figure 11

For more details on this configuration and its usability, see the solution configuration guide.

3.4 Generic Steps – Creating a PSE (If required)

- The steps documented in this section should **ONLY** be implemented if the security configuration, as has been explained above, is to be carried out by creating Individual PSE's for every scenario relevant to a customer.
- The steps mentioned in sections 3.3.3 - 3.3.4 and in section 3.5 should be implemented in the given order after completing the steps in Section 3.4.

Step 1: Create a PSE by accessing the STRUST transaction.

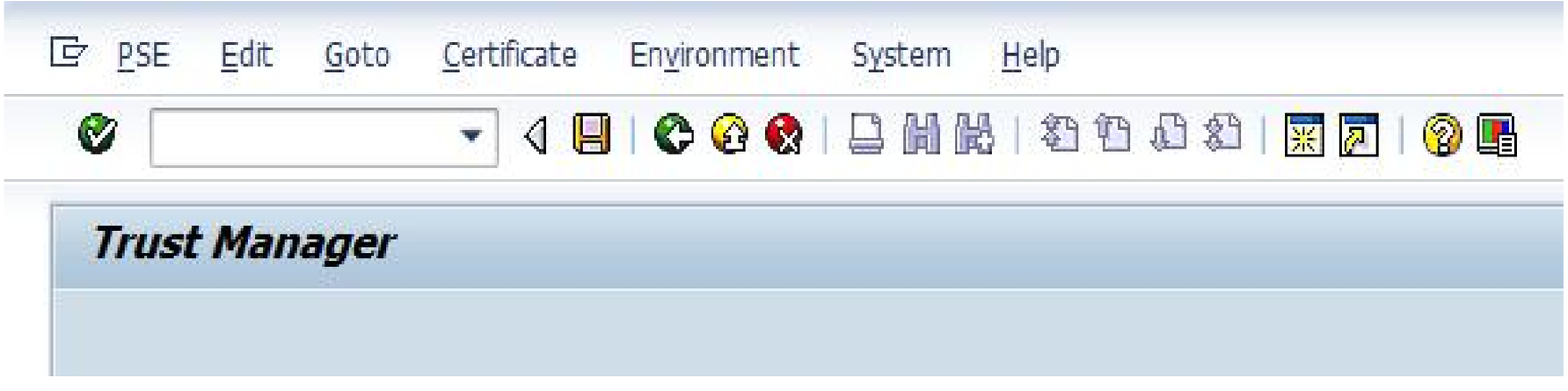

Figure 12

Step 2: From *Environment* menu, select *SSL Client Identities*.

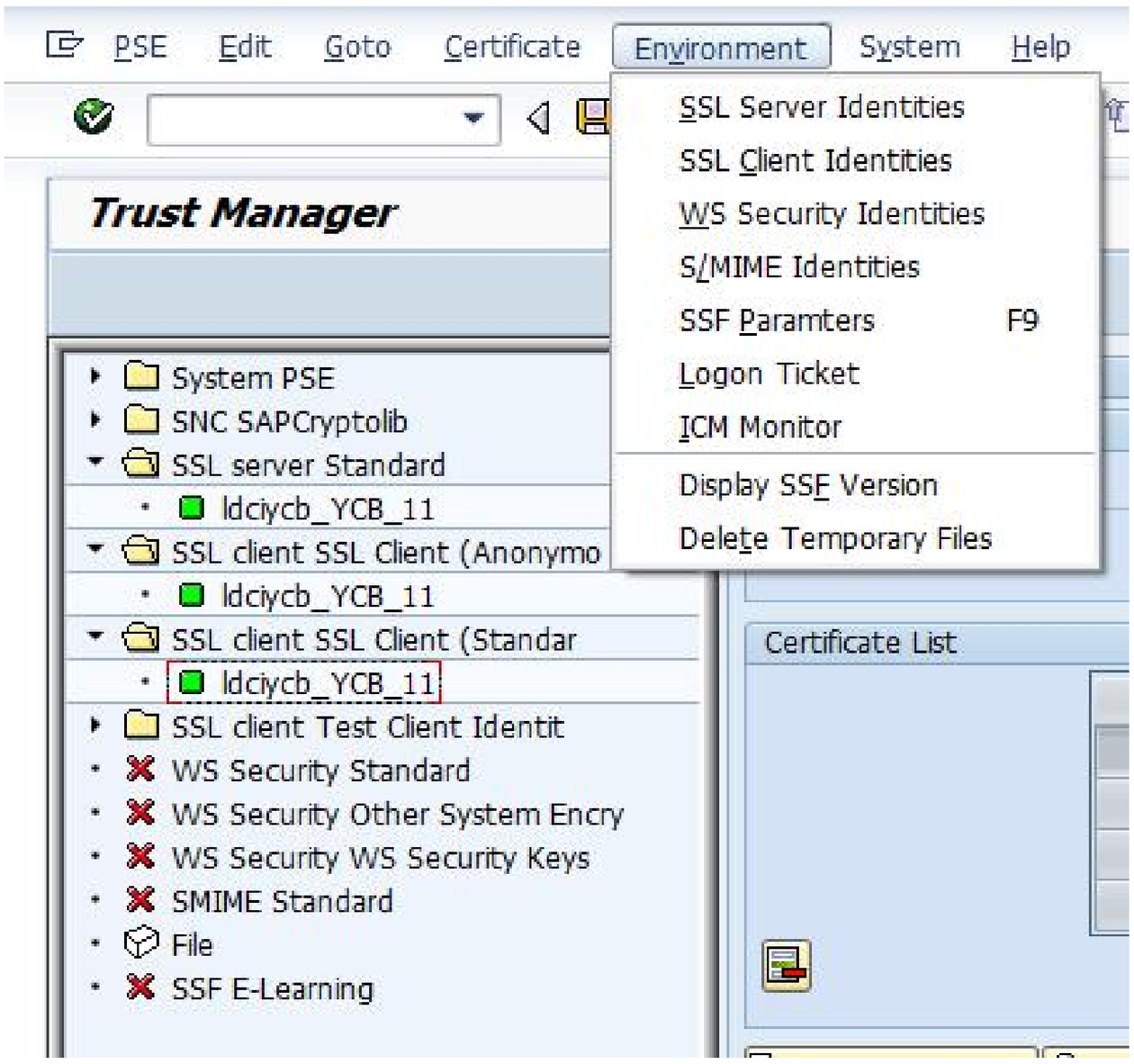

Figure 13

Step 3: Choose *New Entries* to create a new PSE.

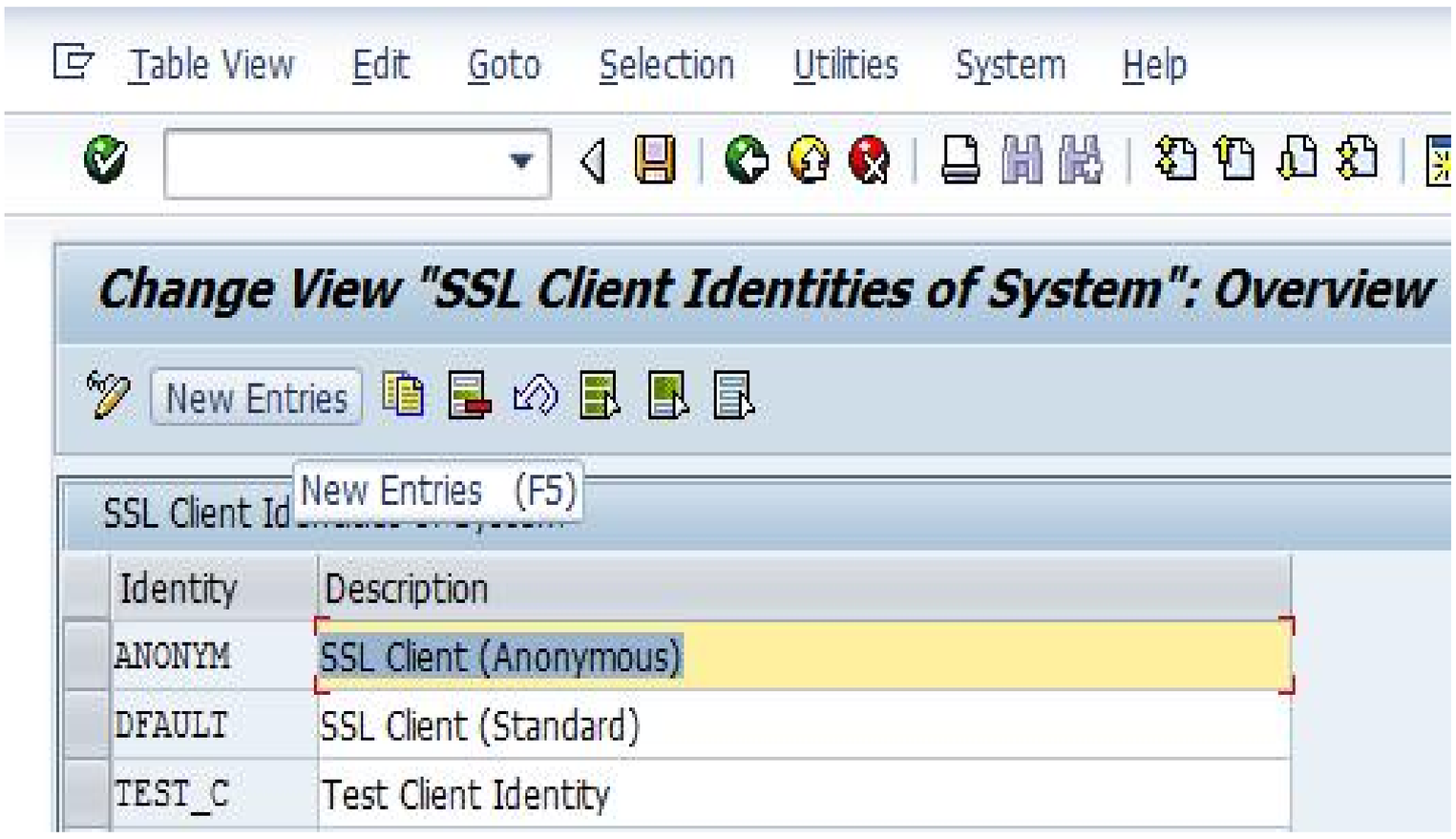

Figure 14

Step 4: Maintain a new PSE entry, for example *TESTV* as shown. Save and return to the initial screen.

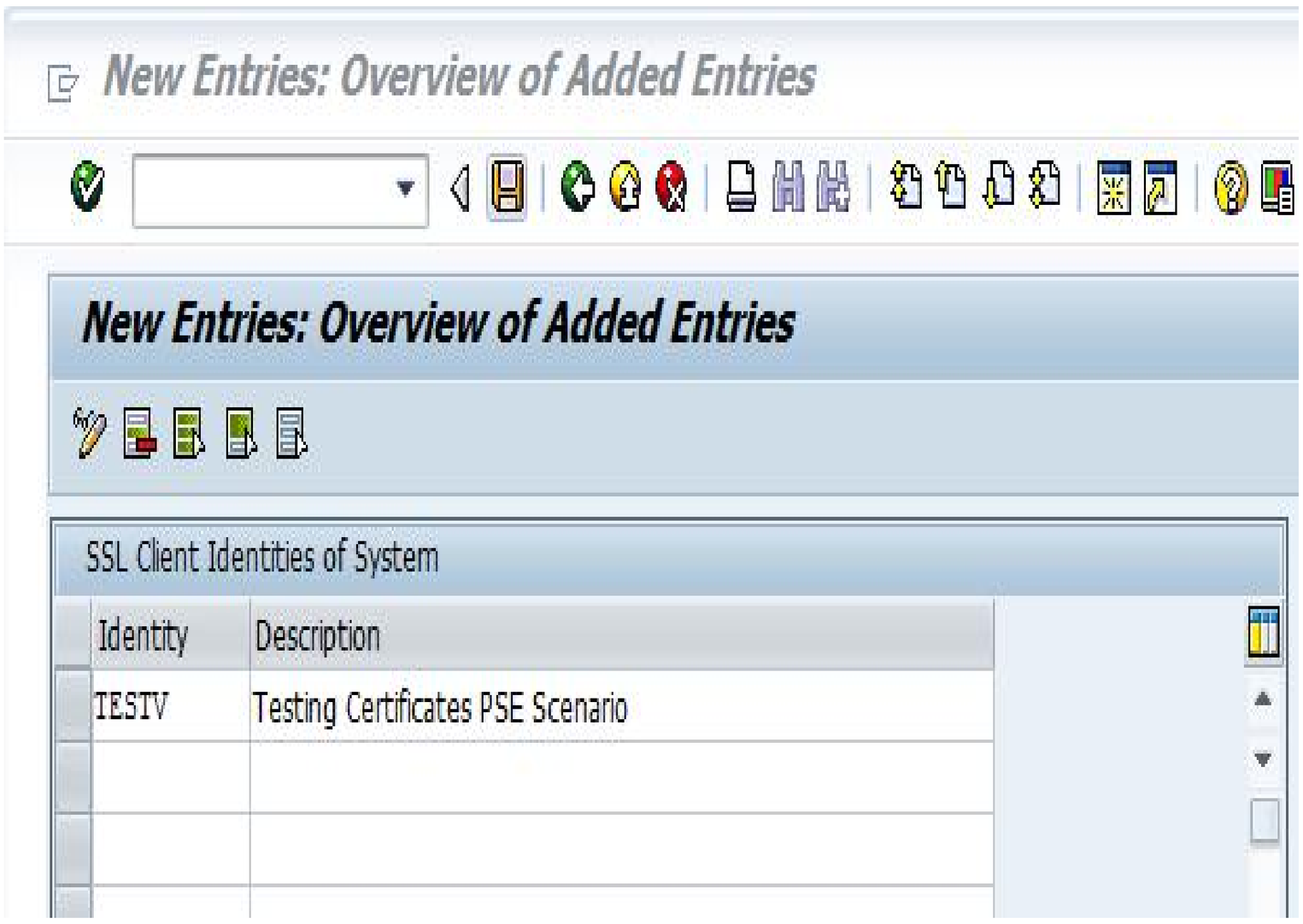

Figure 15

Step 5: You can see that the newly-created PSE has a red cross in the left column bar. Right-click this and choose *Select* to maintain the parameters of this PSE.

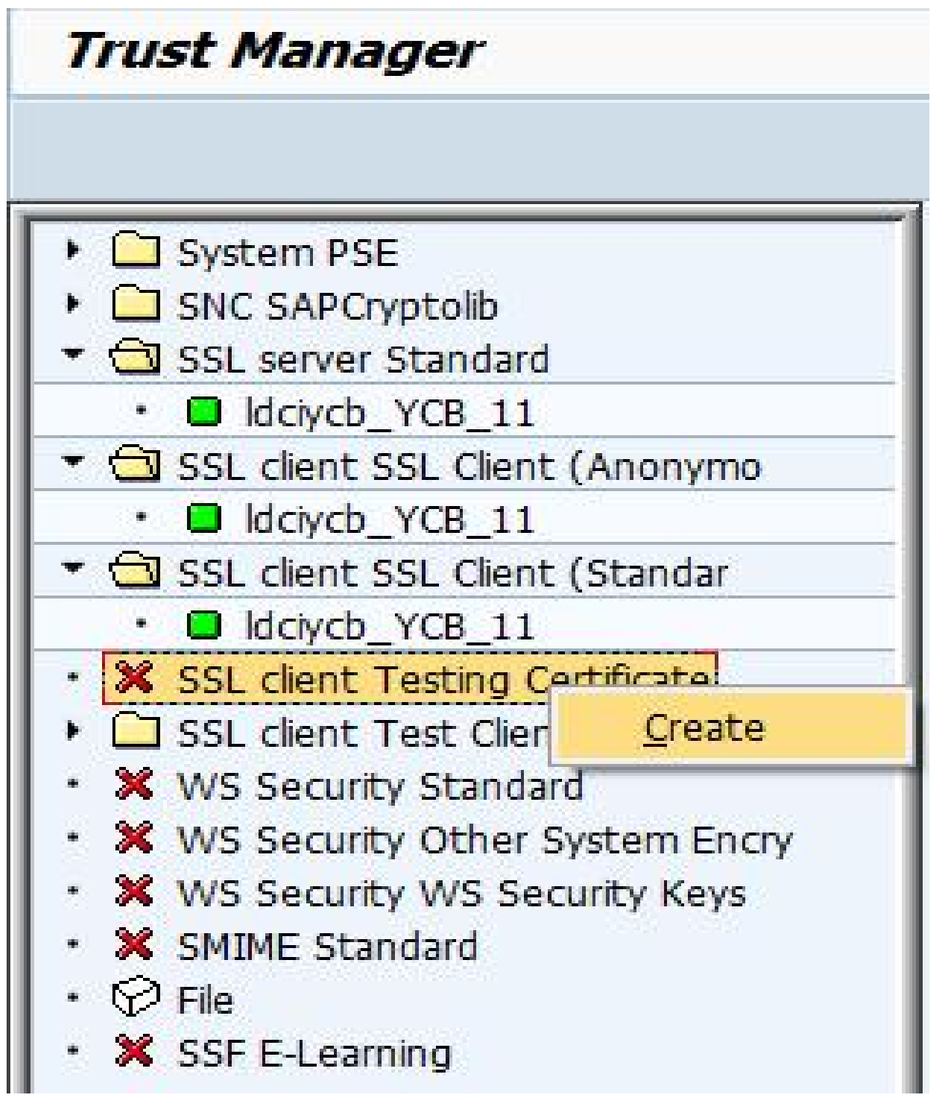

Figure 16

Step 6: Choose *OK* to maintain the entry. The folder for the PSE will be created.

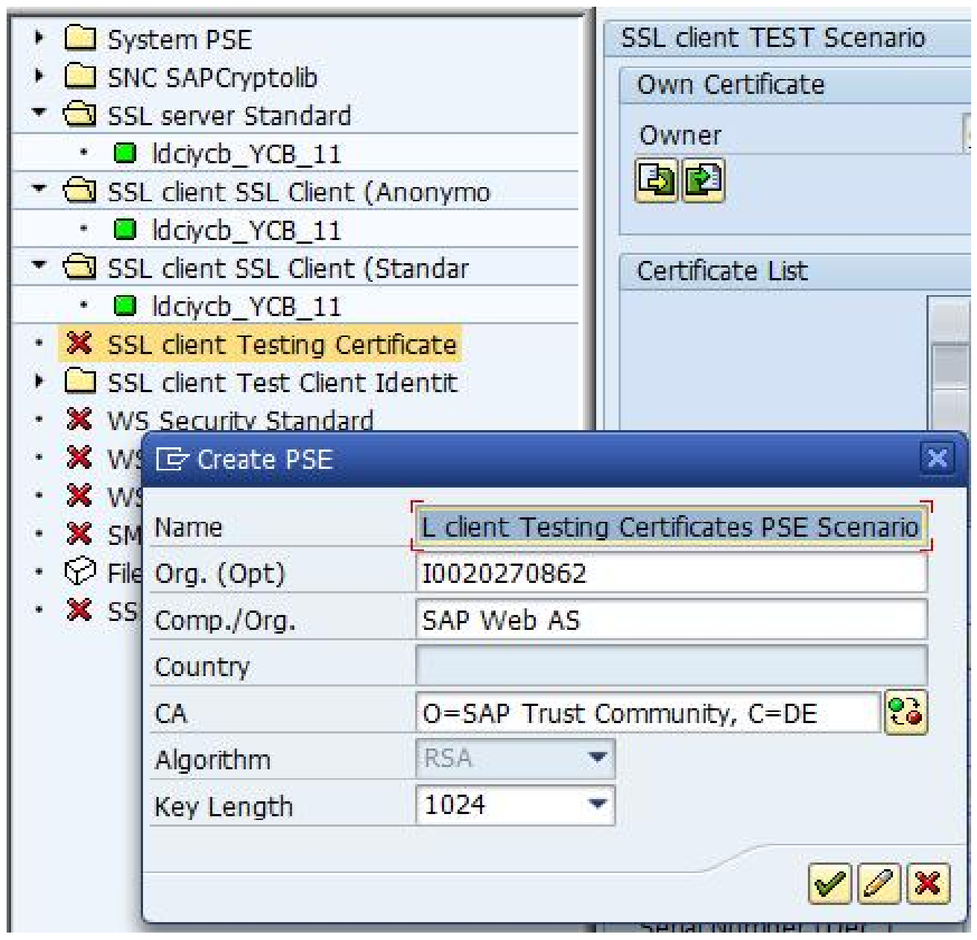

Figure 17

Step 7: Double-click on the folder of the created PSE to get the certificate information.

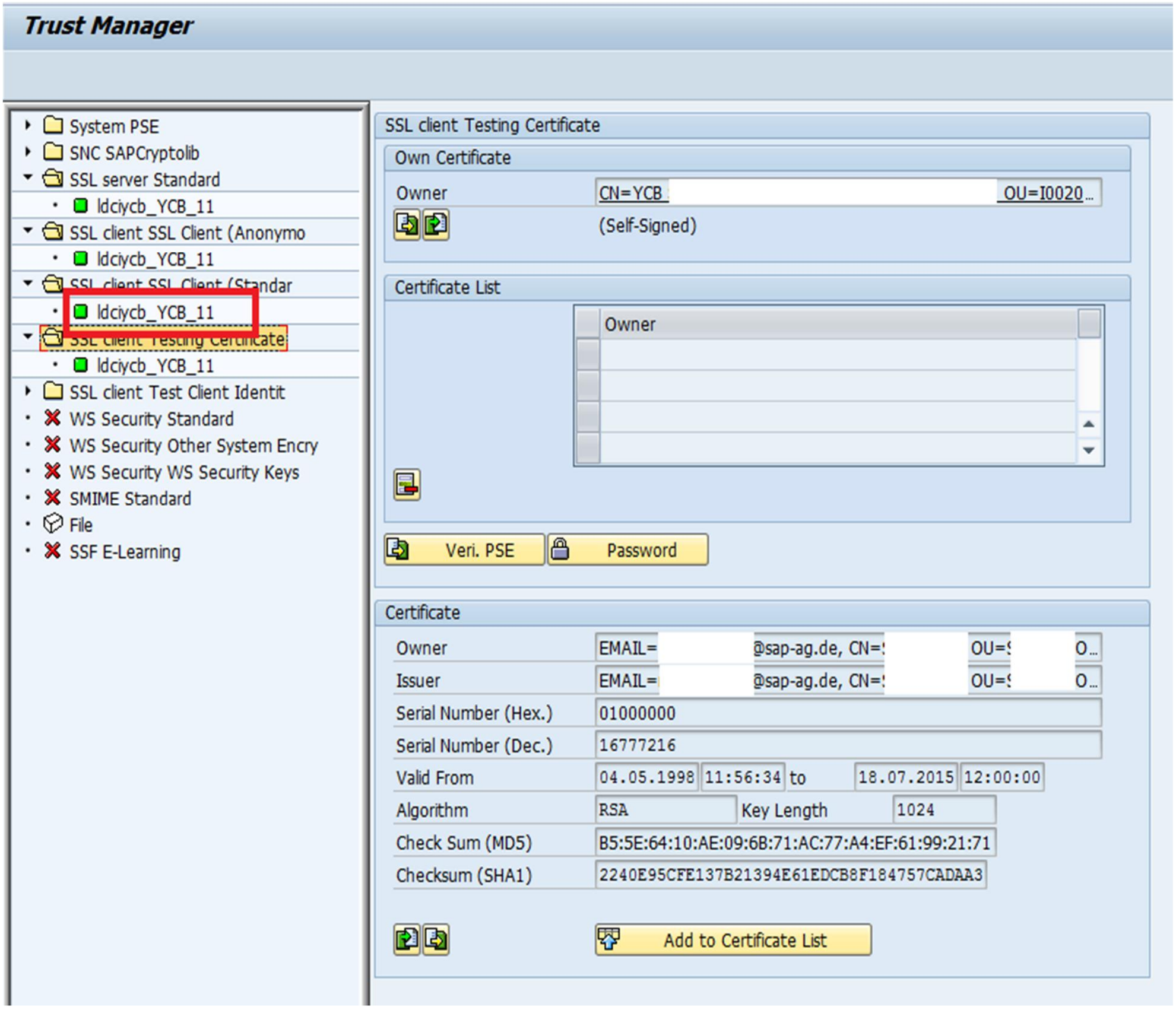

Figure 18

This PSE is now ready to be used for security scenarios.

3.5 Installing a Root Certificate – Generic Procedure

The steps documented in this section should **ONLY** be implemented if the security configuration, as explained above, is to be carried out by creating Individual PSEs for every scenario that is relevant to a customer.

The steps mentioned in sections 3.3.3 - 3.3.4 and section 3.5 should be implemented in the mentioned order after completing the steps in section 3.4.

Step 1: Open transaction *STRUST* for the PSE where the root certificate must to be installed.

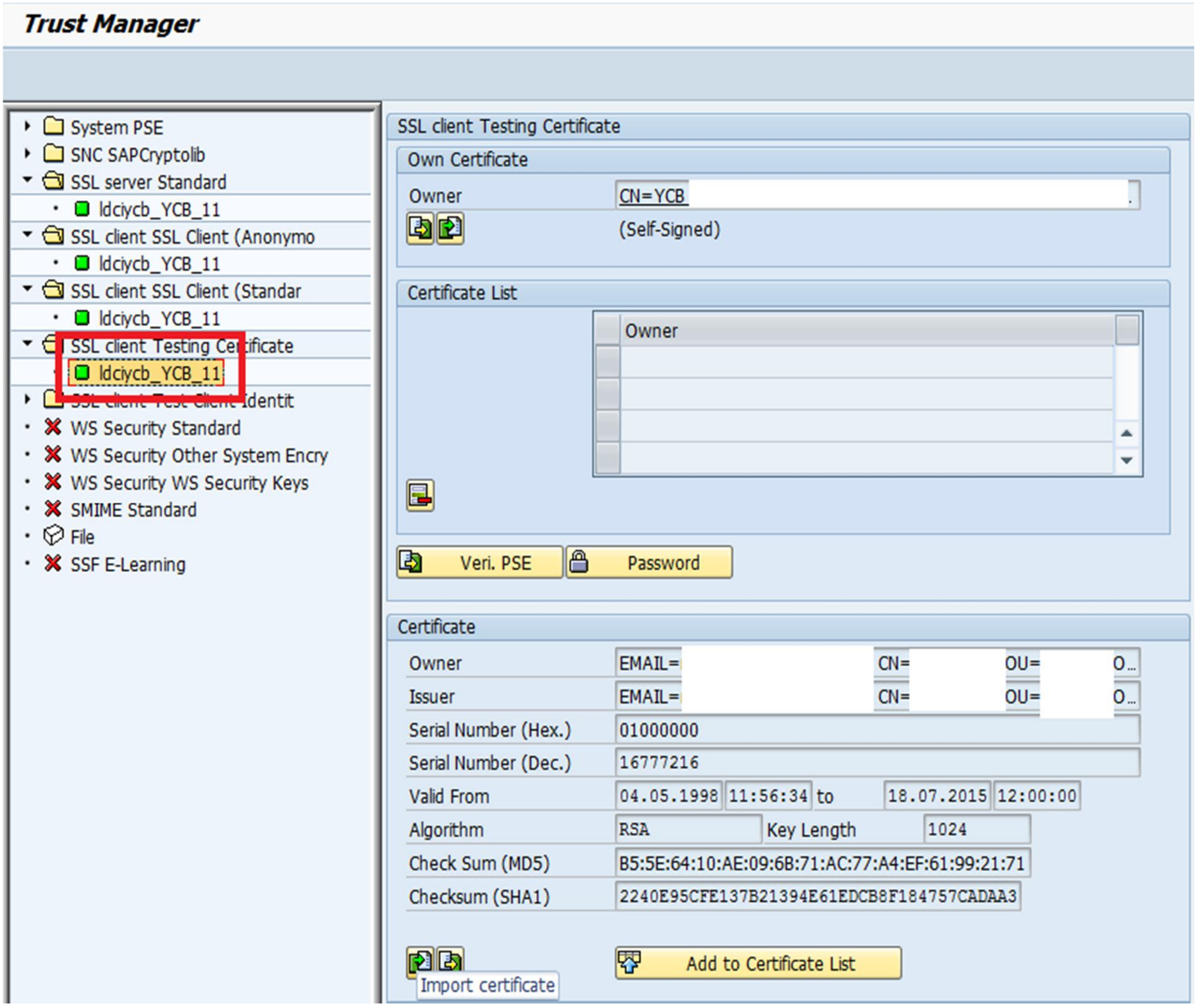

Figure 19

Step 2: Choose *Import Certificate Request* and specify the path of the downloaded root certificate.

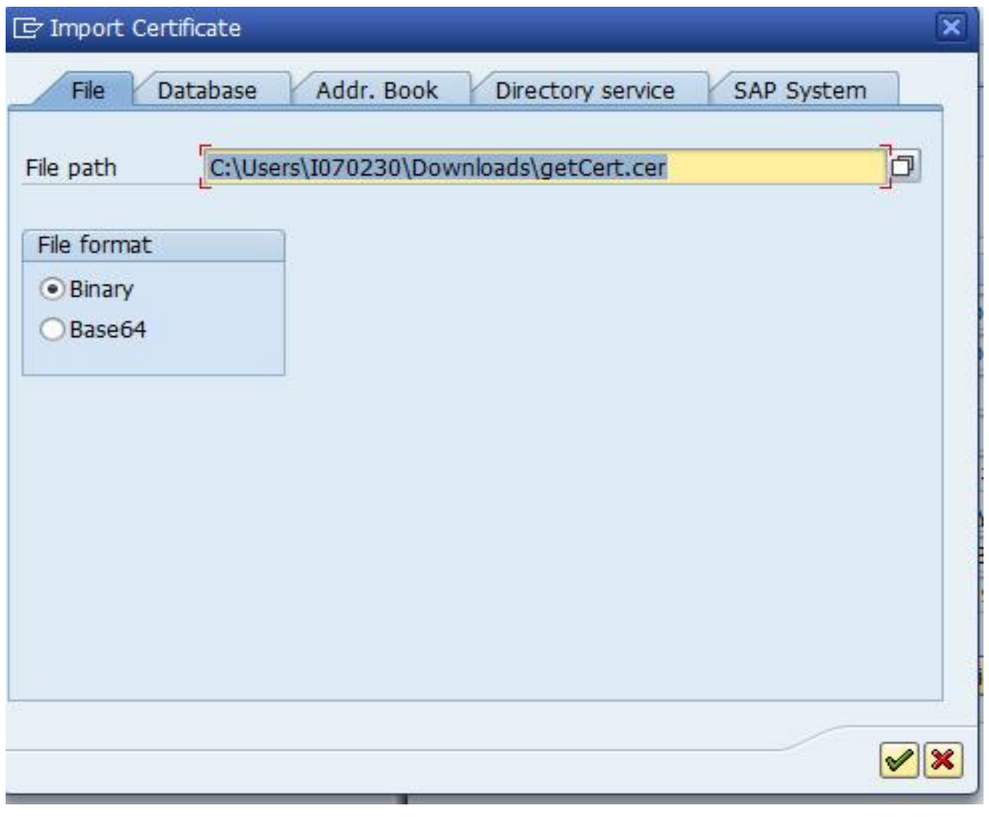

Figure 20

Step 3: Choose *OK;* you can now see the root certificate in the PSE as shown below.

STRUST before Import

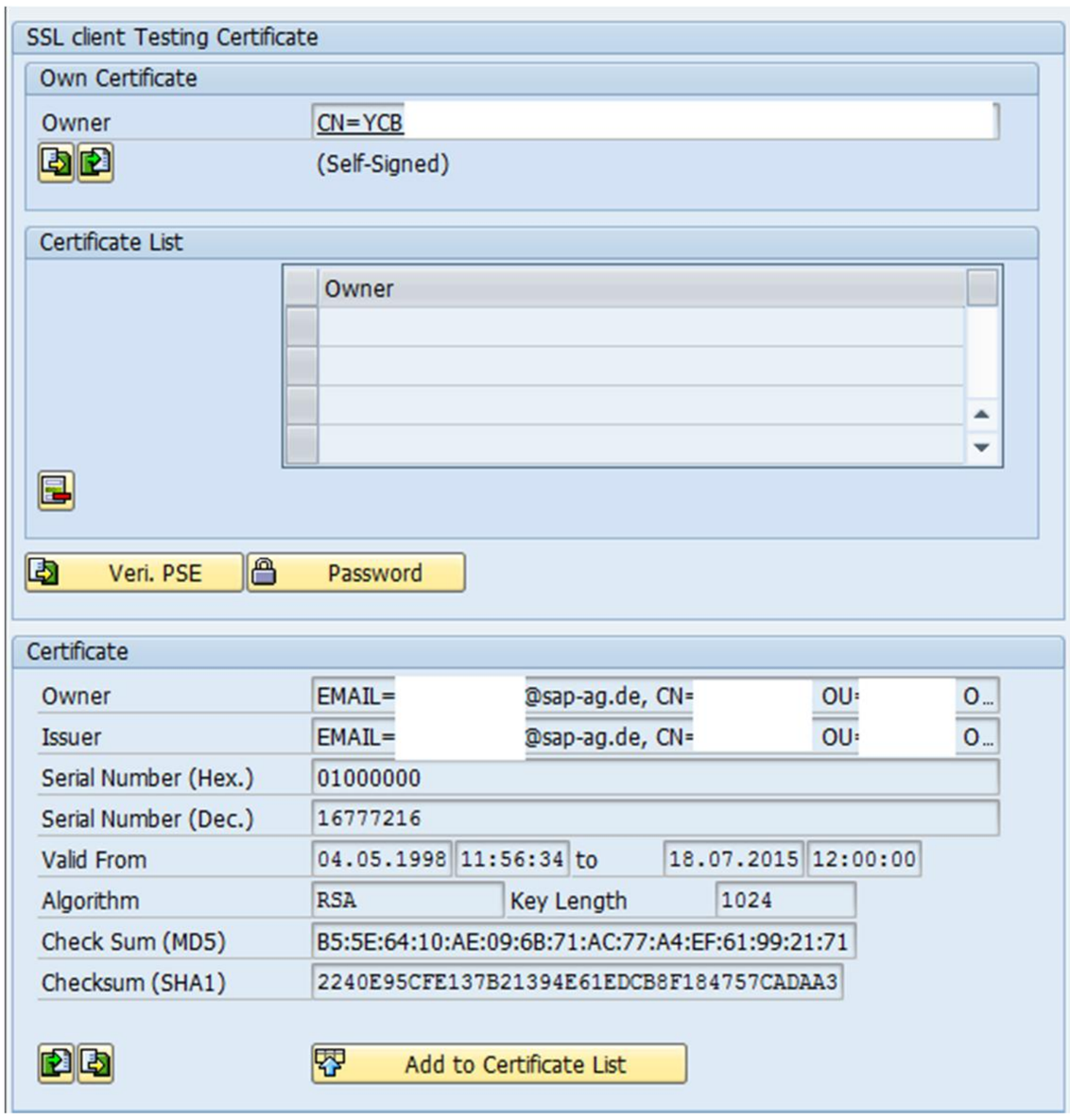

Figure 21

STRUST after Import

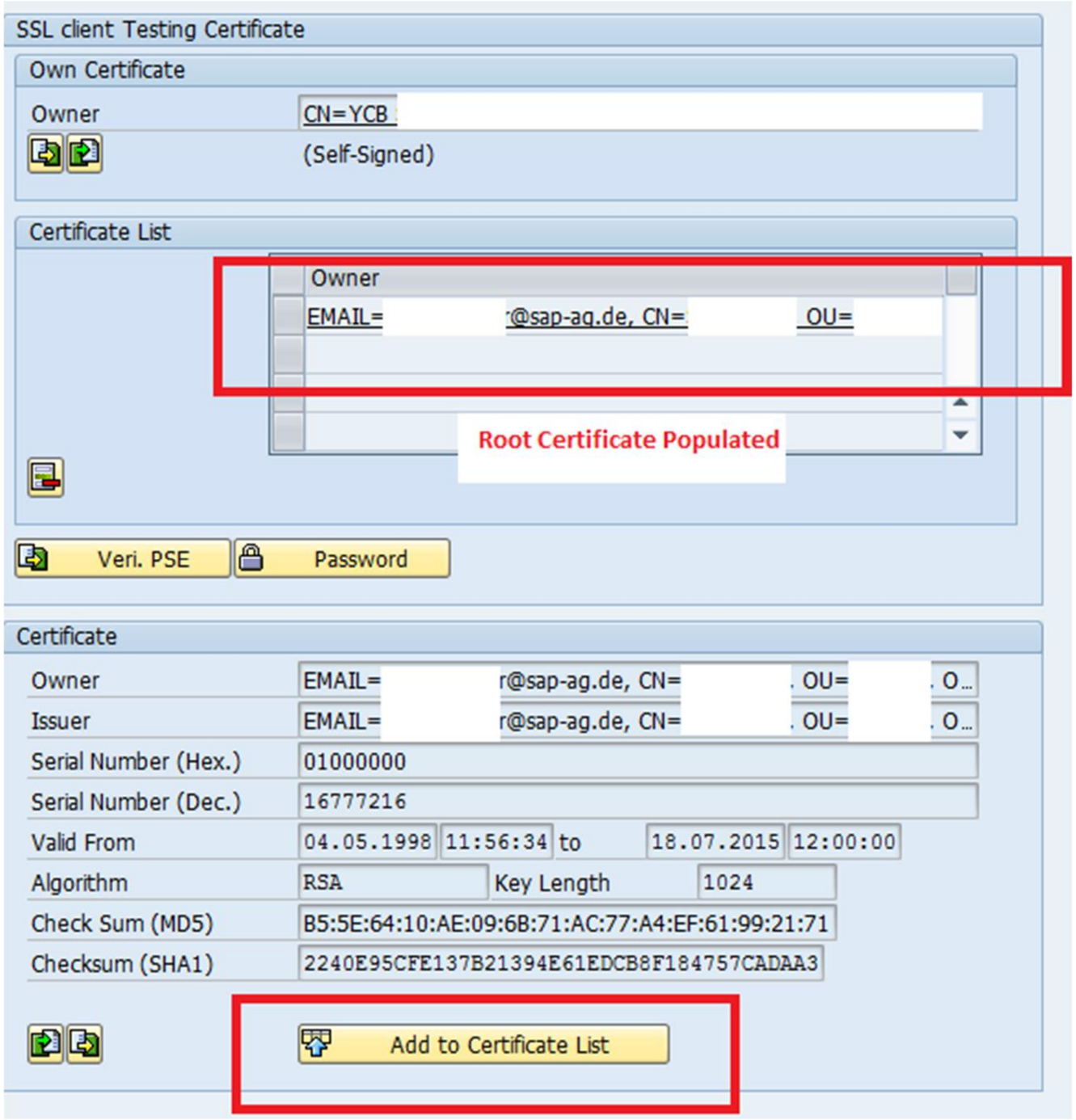

Figure 22

4 Security Issues

For any issues regarding certificates and security-related configurations, raise a ticket under component BC-SEC-WSS