How-To Guide
SAP Cloud for Customer
Document Version: 2.0 - 2015-04-15

How to Configure SAP HCI certificate based authentication for SAP Cloud for Customer

Document History

Document Version	Description
1.0	First official release of this guide
2.0	Reviewed Version from 2015/04/07

Table of Contents

1 Business Scenario

Certificate based authentication is a more secure way of exchanging messages from your on-premise to cloud systems. SAP supports the use of Secure Sockets Layer (SSL) and Secure Network Communication (SNC).

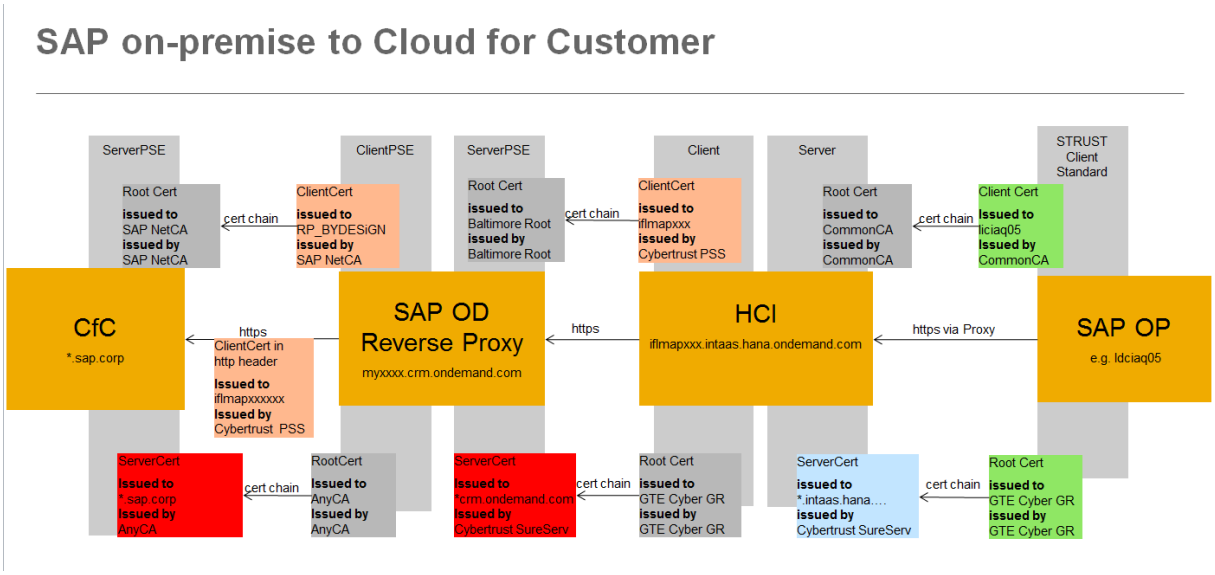
2 Prerequisites

1. Installation of SAP Web Dispatcher or any approved third-party dispatcher
2. Use Certificate based Authentication option in the sender/receiver configuration of the iFlow
3. Verify list of approved CA's for SAP on-premise client certificate signing

3 Concept

To establish basic authentication it is necessary to consider two aspects,

a. SSL trust between Servers
b. Certificate based Authentication setting for client authentication



Steps performed by Customer

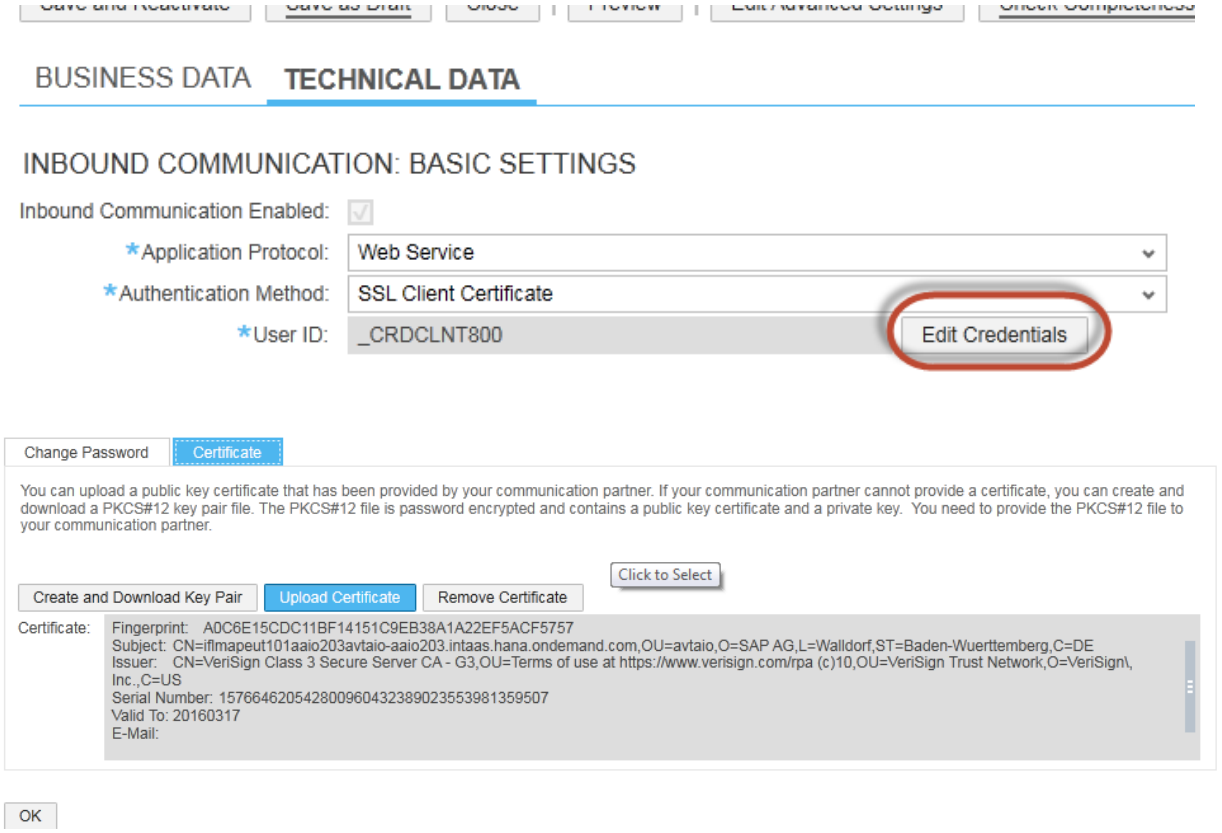
1. Get on-premise client certificate signed by an approved certification authority (CA)
2. Import HCI Server Root certificate into on-premise STRUST

4 Step-by-Step Procedure

Example: SAP on-premise to SAP Cloud for Customer

4.1 SAP cloud application Configuration: Enable Certificate Authentication in Inbound Communication Arrangement

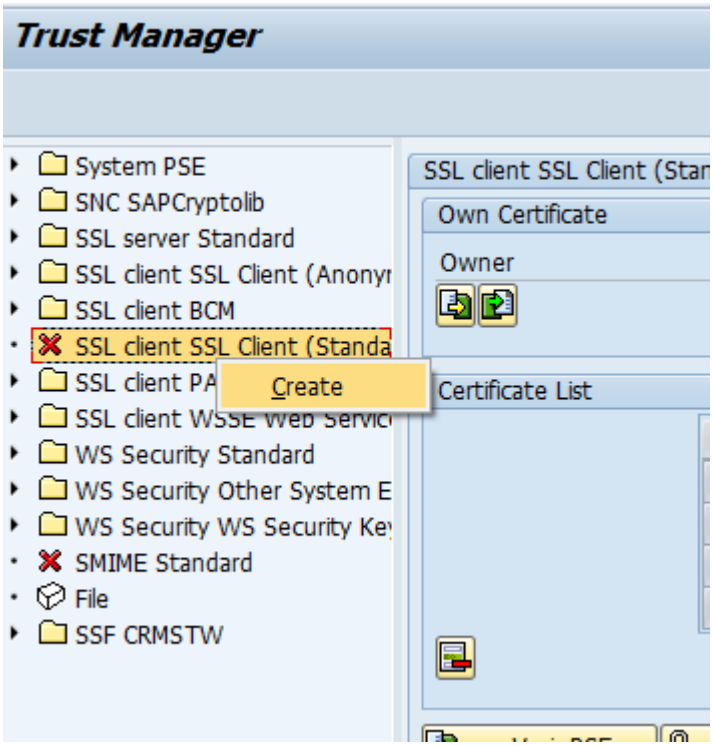
Go to the Communication Arrangements under the Administrator Work center and for the Inbound Request, upload the HCI client certificate for the generated system user



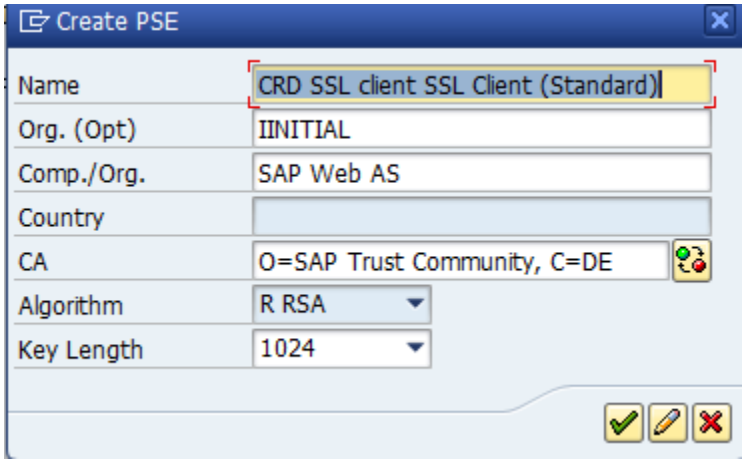
4.2 SAP on-premise Configuration: Get SSL Client certificate signed by valid Certificate Authority (CA) and Import HCI Server Root certificate into STRUST Client Standard

Create SSL client PSE in STRUST

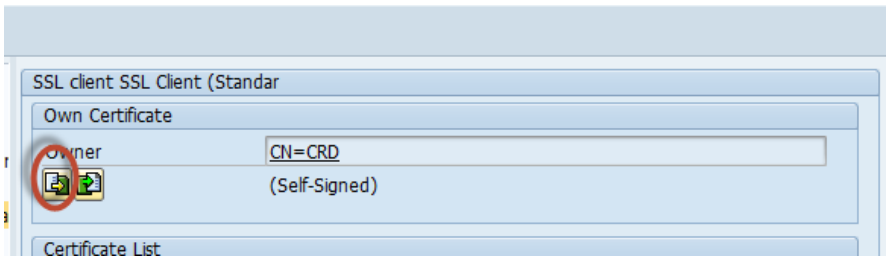
1. Select the SSL Client Standard entry, right click and select Create



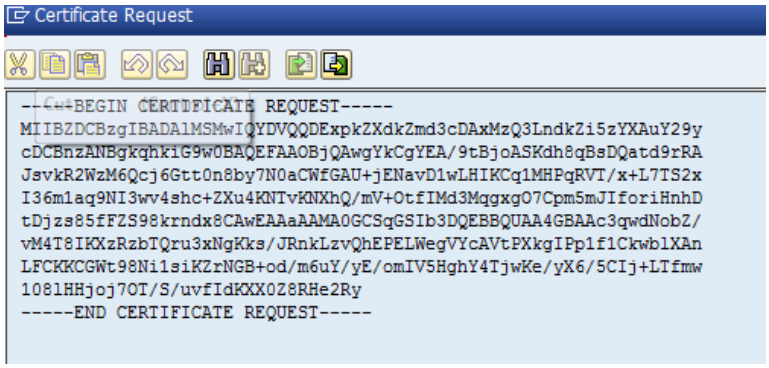
2. Enter a name for the new client PSE:



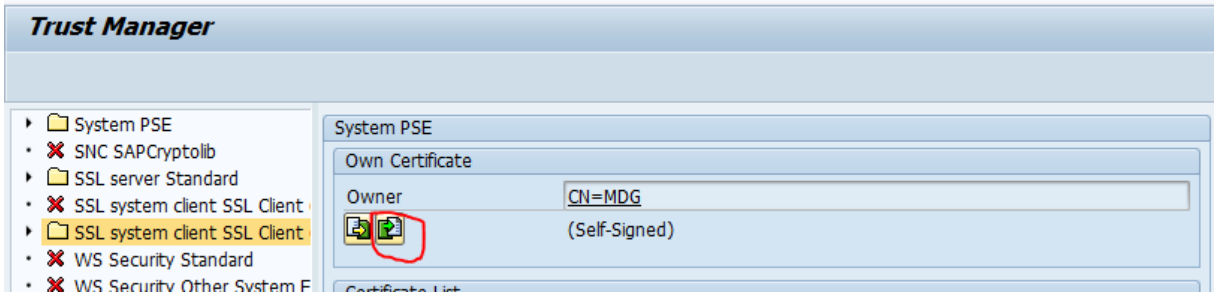
3. Open the PSE you have just created and do the following:
In the maintenance section select the icon to create certificate request.



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

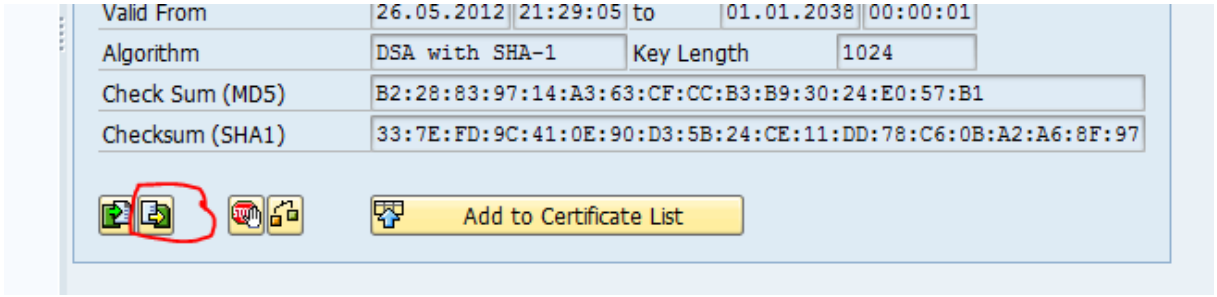


8. Get the certificate signed by a CA that is trusted by HCI Load Balancer. For full list of CA's see Appendix. This may take a couple of days. When you receive the Certificate Response, import it into STRUST within the same PSE from where you have created the Certificate Request.

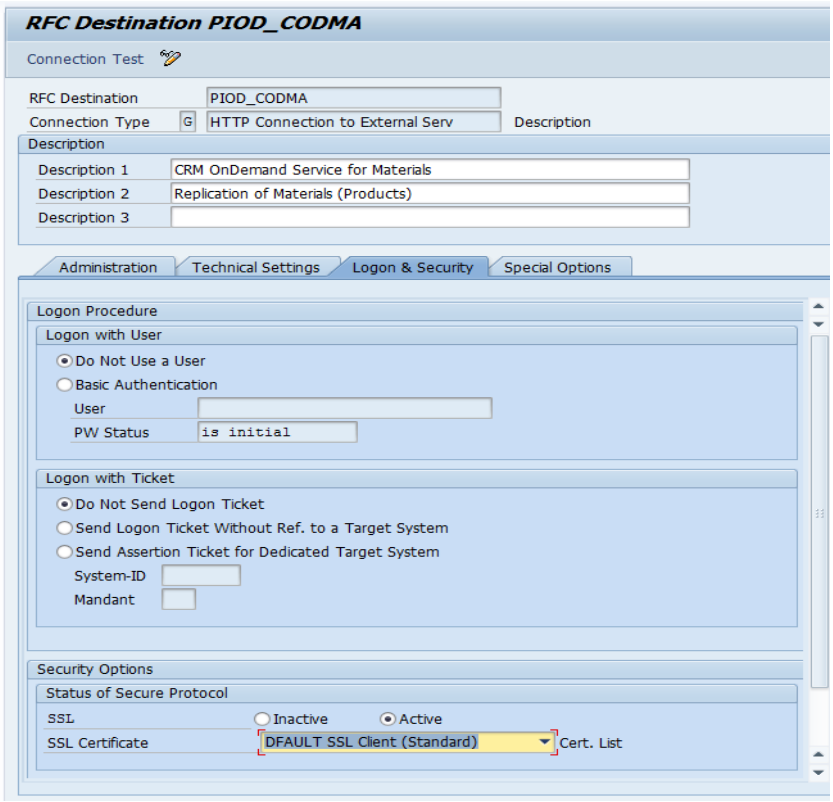


As a result your PSE should now have a CA signed client certificate.

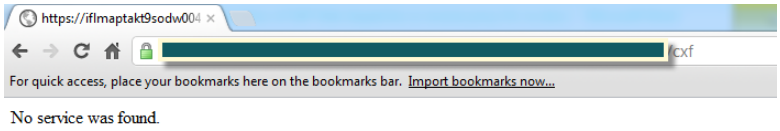
9. You should export this client certificate and use it later on for the iFlow configuration (see chapter 4.3.)



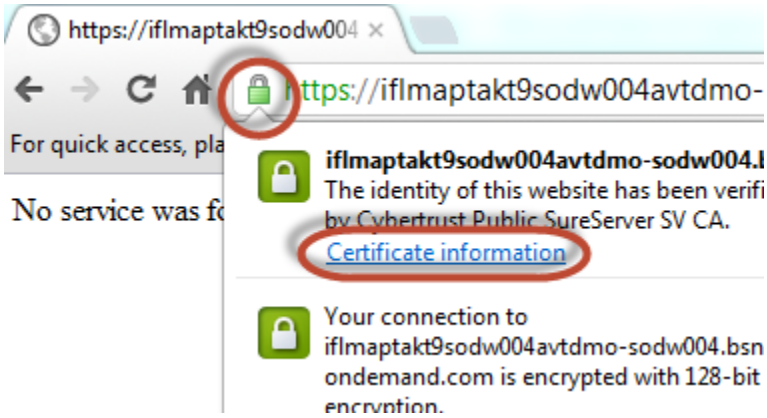
10. In SM59, go to the Logon and Security tab for each of the HTTP destinations.



11. Open a web explorer and enter the URL of the worker node that was provided in the onboarding email adding the path /cxl at the end, by example https://<host>:<port>/cxf

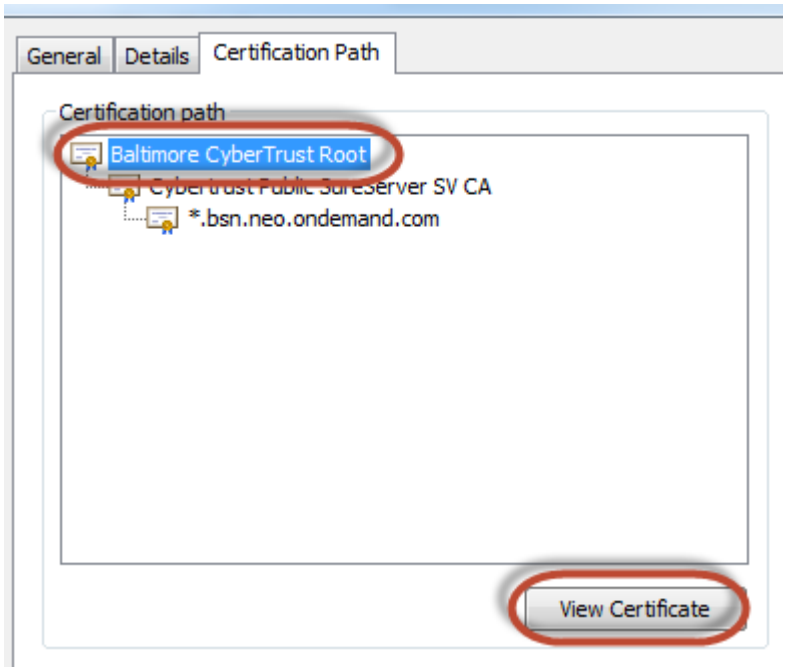


12. When connected use the web explorer to get the certificate, by example in Chrome you clicks in the lock icon at the left of the URL and then click in certificate information.

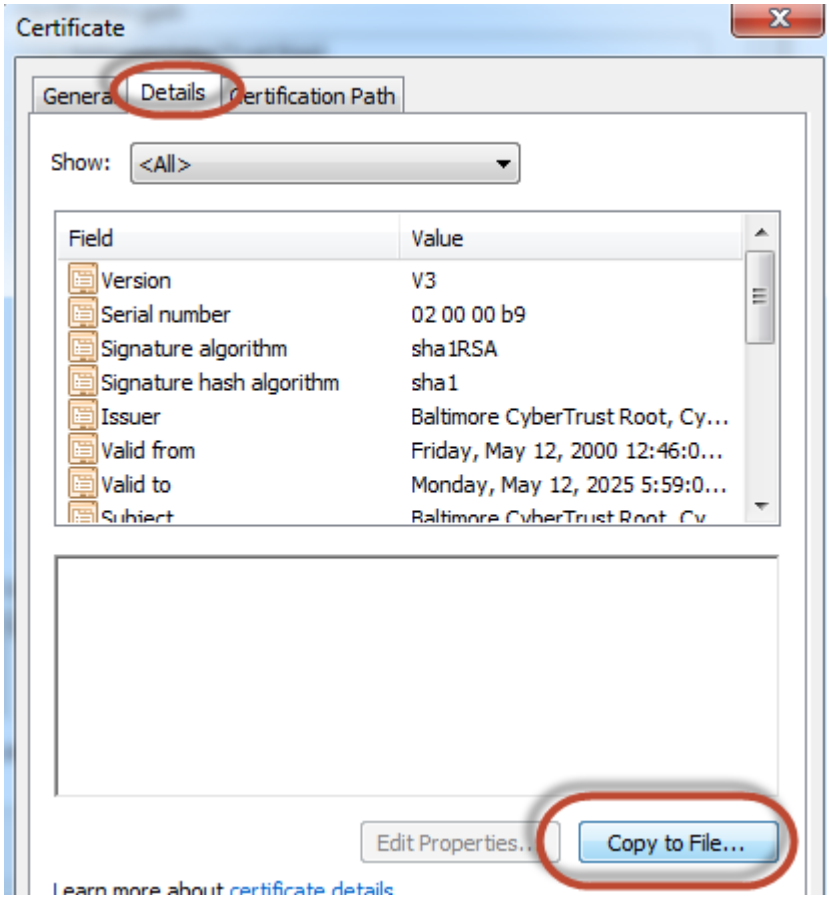


13. From the Certification Path select first root certificate and click View Certificate.

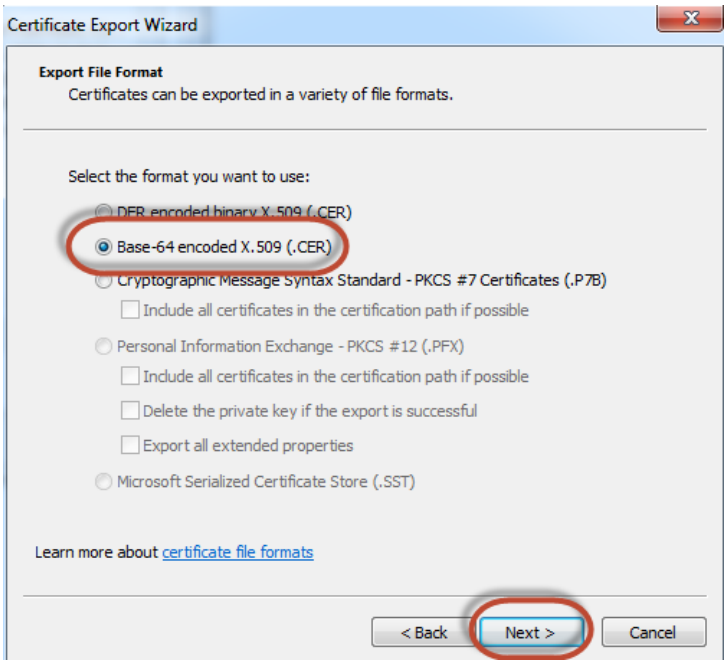
Important Note: The screenshots below are only example certificates – the certificates actually used on the HCI server might be different. Following the below procedure will provide the valid certificates.



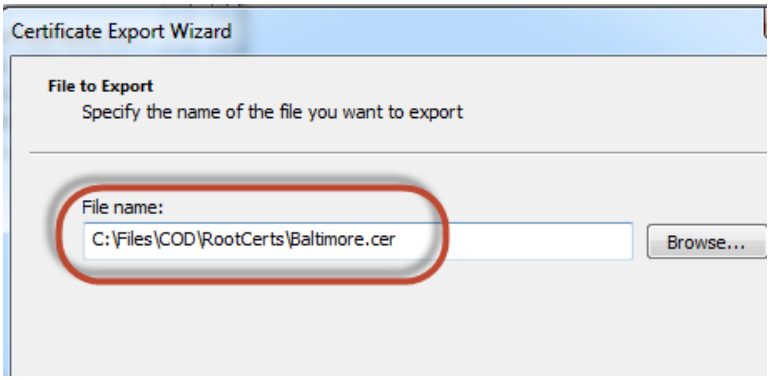
14. Click in the menu Details and the click the button Copy to file



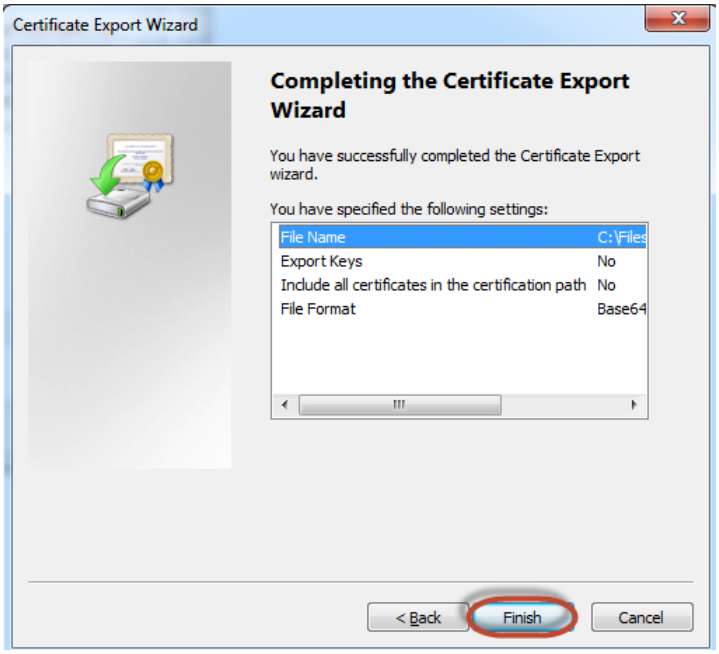
15. Click Next
16. Select Base-64 encoded x.509 (.CER) and click Next.



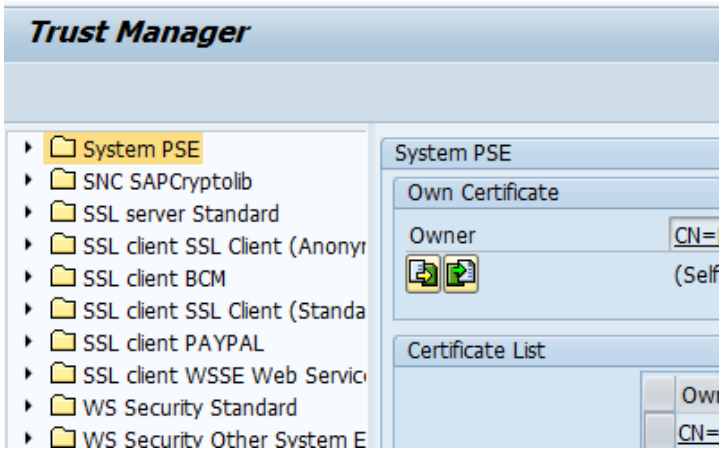
17. Select the location of the file and click Next.



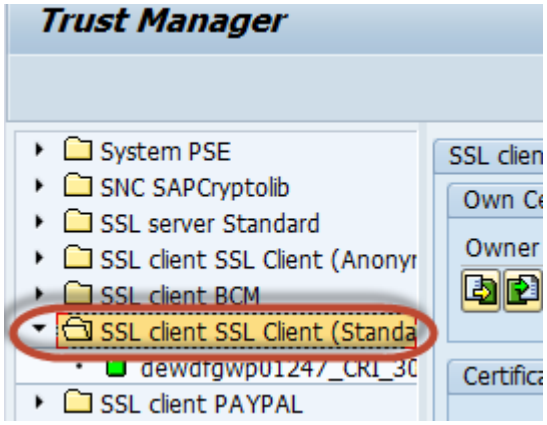
18. Click Finish.



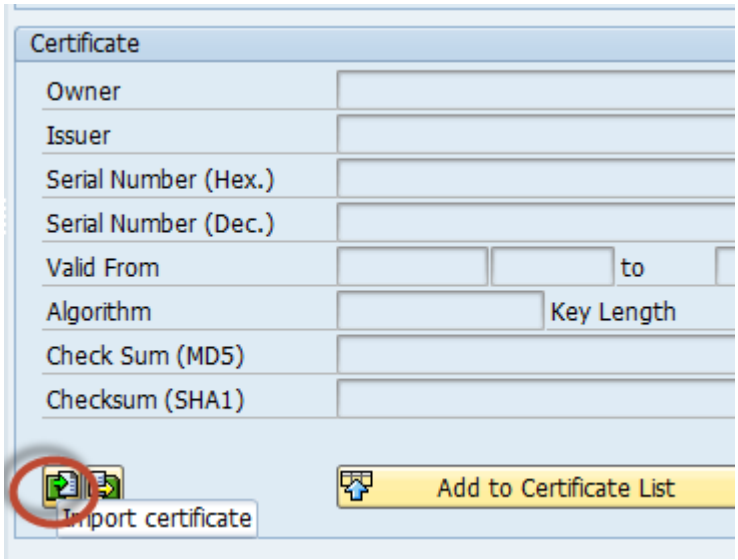
19. Call transaction STRUST



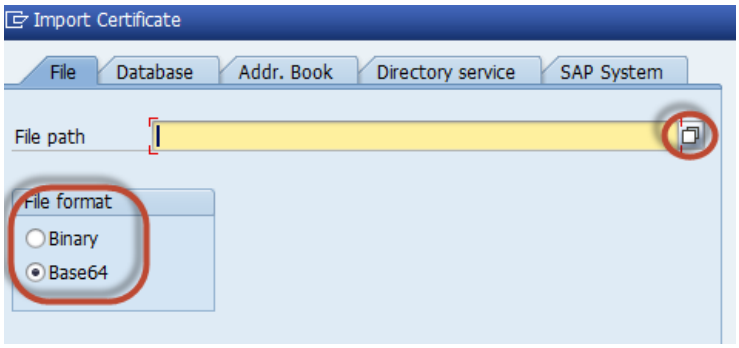
20. Open the SSL Client SSL client Standard PSE



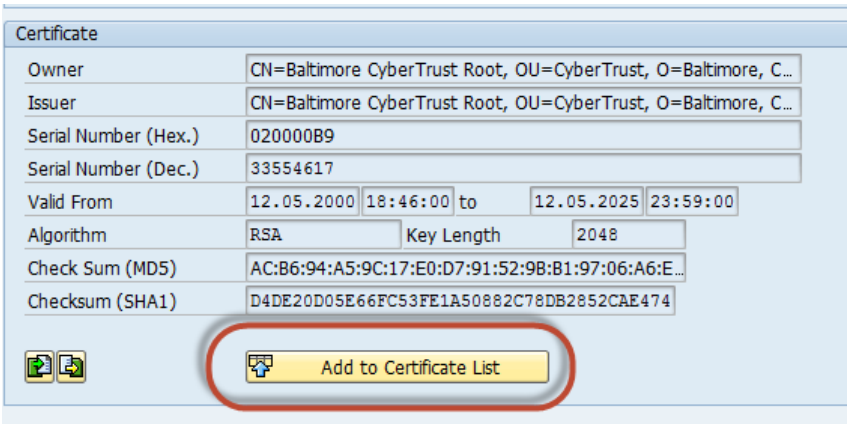
21. In the Certificate area, click in the Import Certificate button.

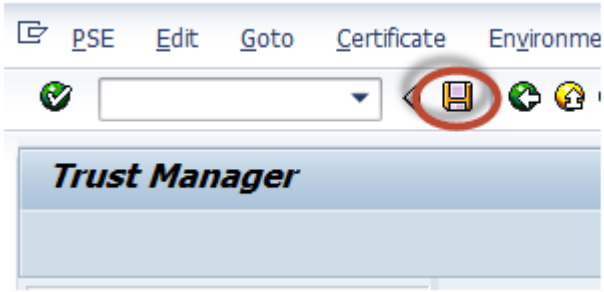


22. Import the root certificate you just have downloaded in Base64 format



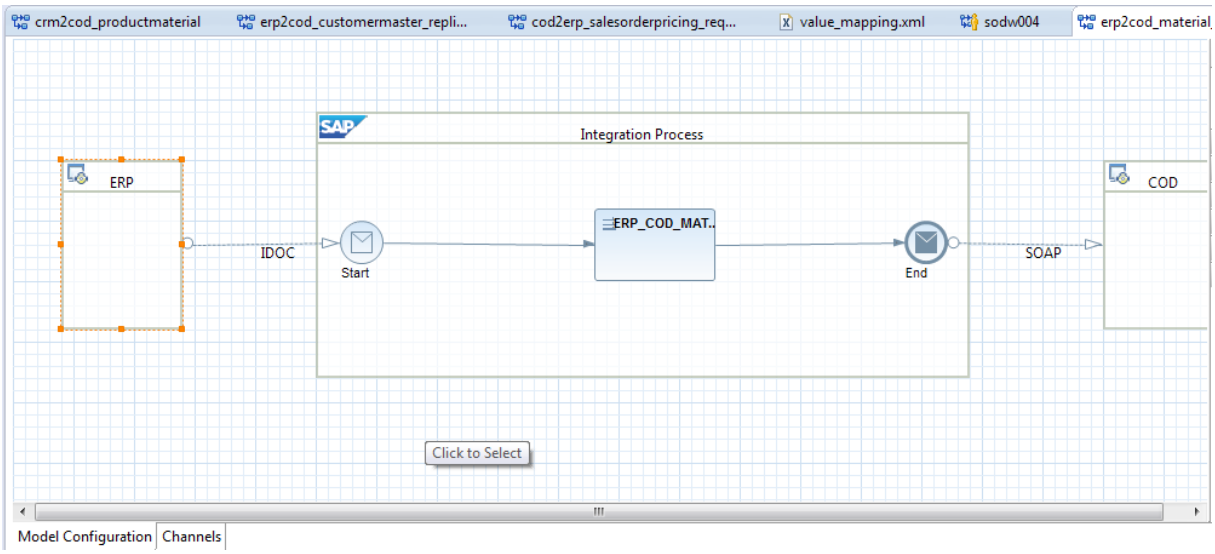
23. Add the imported certificate into the certificate list clicking in the Add to Certificate List button.
Important note: It is sufficient to import the root certificate into STRUST. Intermediate Certificates are not needed and they should not be imported.

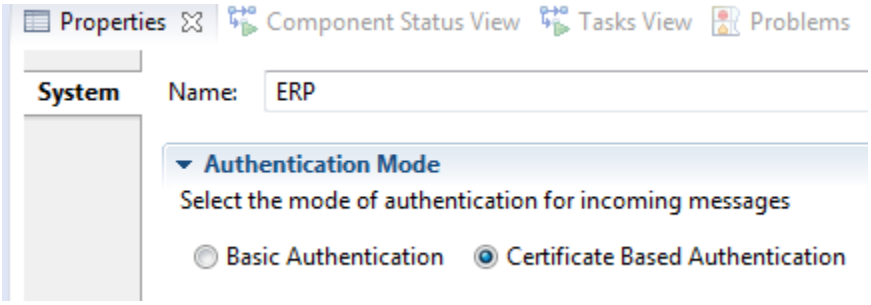




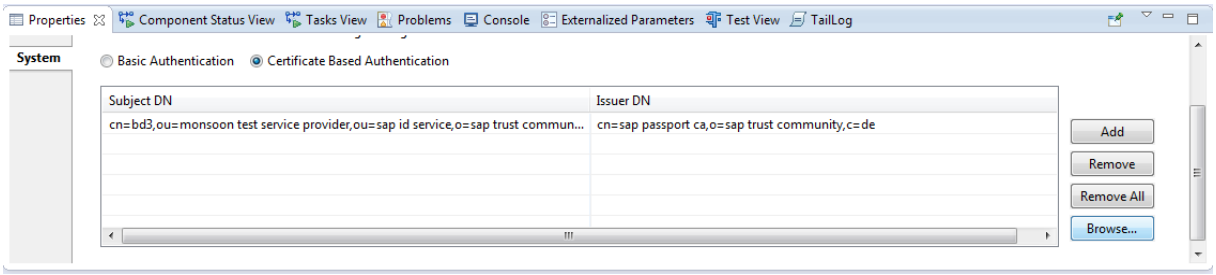
4.3 SAP HCI Configuration: Assign certificate based authentication and upload sender client certificates to iFlow

1. Choose the option of certificate authentication from ERP to HCI.





2. Upload the client certificate of the sender (in this example, we upload the SAP on-premise SSL client certificate which you exported in step 9 of chapter 4.2.) using the browse option and selecting the client certificate saved locally.



3. Save and Deploy the iFlow

5 Appendix:

5.1 List of trusted CA's of HCI Load Balancer

SSL termination between ERP and HCI happens on the HCI Load Balancer. Therefore the Client certificate of ERP has to be trusted there

You can find the list of all the supported certification authorities, in the HCI documentation:

1. Go to https://cloudintegration.hana.ondemand.com/PI/help
2. Open the complete documentation, say click SAP HCI for process integration complete documentation (HTML).
3. Go to Connecting a Customer System to SAP HCI・ Concepts of Secure Communication・ HTTPS-Based Communication・ Load Balancer Root Certificates Supported by SAP.

In case you need to sign your client certificate from another CA which is not part the current trust list you can send an approval request for this CA as a ticket to the component LOD-HCI

5.2 Certificate Chains

Typically the certificate you get signed by the CA is signed by a chain of certificates containing one or several intermediate certificates and one root certificate. During SSL handshake the client (ERP) will send the complete chain without root certificate to the server. The client certificate will therefore be trusted when the root certificate is available within HCI Load Balancer trust list. Intermediate certificates are not needed within the Load balancer and should be avoided whenever possible.

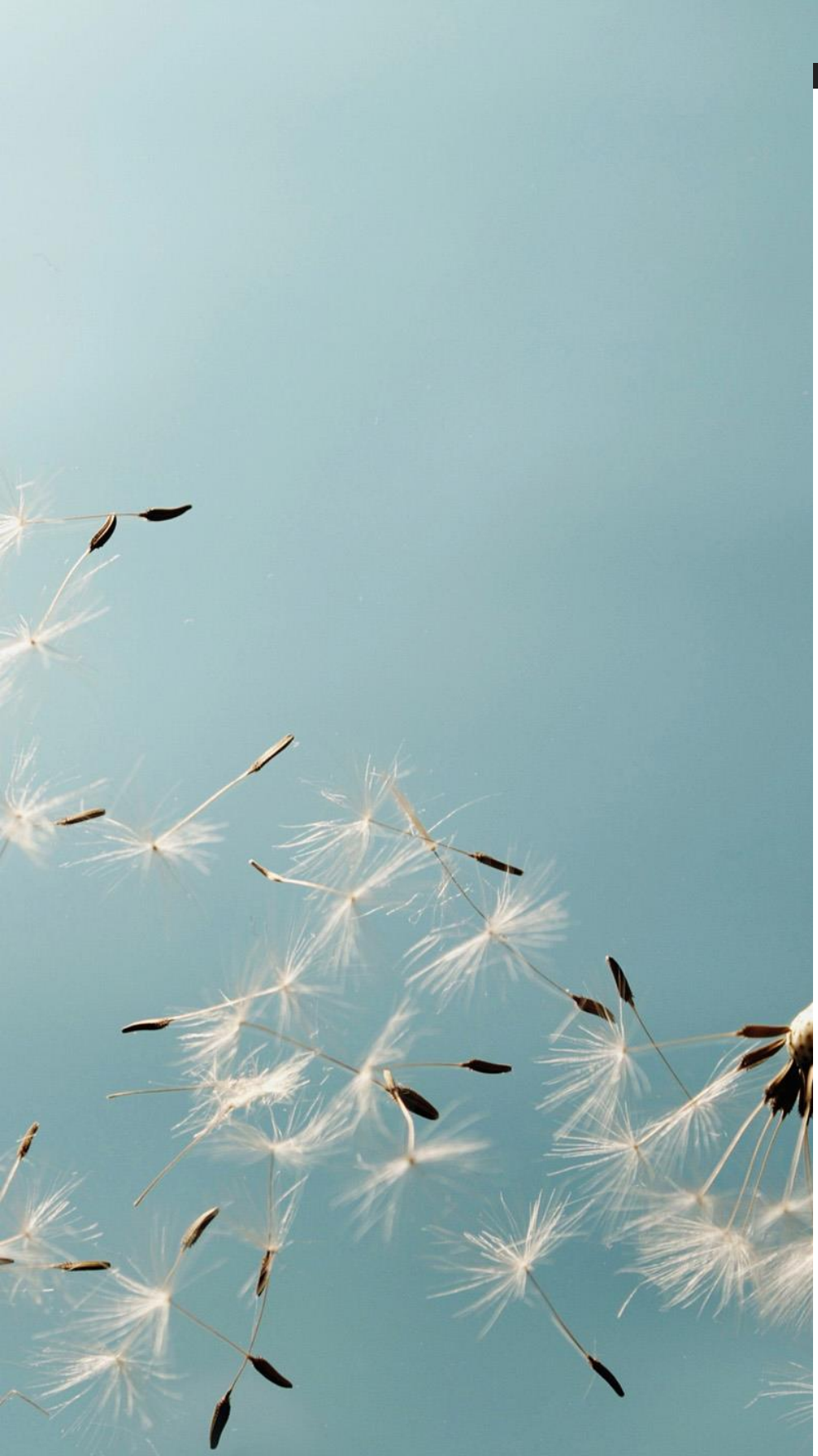
You can find out the complete chain of your client certificate by two ways:

1) The CA will typically provide you the full chain together with the certificate response
2) In ERP you can retrieve the certificate chain on OS level (or even on the ABAP server with transaction SE38 and report RSBDCOS0) with the following command:

   sapgenpse get_my_name -p SAPSSLC.pse -v 2>&1

5.3 Further Readings

There are several good blogs around this topic on SCN. As an example you can look at this:
http://scn.sap.com/docs/DOC-61145



www.sap.com/contactsap