Mexico Electronic Documents: Setting Up SAP Integration Suite (SAP S/4HANA, SAP ERP) - Cloud Foundry environment

TABLE OF CONTENTS

1 Disclaimer 3
2 Introduction 3
3 Prerequisites 3
3.1 Registration at SAT 3
3.2 eDocument Full Solution 4
4 Secure Connection 4
4.1 Setup of Secure Connection 4
4.1.1 Setup of Your Tenants 4
4.1.2 Retrieve and Save Public Certificates 4
4.1.3 Upload the Certificates 5
4.1.4 Authenticate Integration Flow 5
5 Configuration Steps in SAP Integration Suite 6
5.1 Deploy the Customer Certificate and Credentials to SAP Integration Suite 6
5.2 Copy Integration Package 7
5.3 Deploy Integration Flows 8
6 Configuration Steps in SAP ERP or SAP S/4HANA 13
6.1 Create Logical Ports in SAP ERP or SAP S/4HANA 13
7 Appendix 17
7.1 Generate and Import Certificates 17
7.1.1 Prerequisites 17
7.1.2 Generate PKCS#12 File from the Certificate and Key File 18
7.1.3 Import the Handshake Certificate 18

1 Disclaimer

This documentation refers to links to websites that are not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

- The correctness of the external URLs is the responsibility of the host of the Web site. Please check the validity of the URLs on the corresponding Web sites.
- The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
- SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

2 Introduction

The communication part of processing electronic documents in Mexico is taken care of by SAP Integration Suite. In order to get SAP Integration Suite working, there are some required steps on both your SAP S/4HANA or SAP ERP system and SAP Integration Suite tenant.

These steps are typically taken care of by an SAP Integration Suite consulting team, who is responsible for configuring the SAP S/4HANA or SAP ERP - SAP Integration Suite connection and maintaining the integration content and certificates/credentials on the SAP Integration Suite tenant.

Note: Although the service name **SAP Integration Suite** is used in the guide title and throughout the guide, this guide **also applies to SAP Cloud Integration running in the Cloud Foundry environment**. If you were onboarded before July 2020, the service you use is SAP Cloud Integration. The initial setup steps for the two services are different, while the integration flow settings and configuration steps in your back-end system are the same. See the **Setup of Your Tenants** section for their respective initial setup steps.

Note: This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Integration Suite tenant. It may happen, however, that in the SAP S/4HANA or SAP ERP system the access to such functionality is only partially implemented. Additionally, it may also happen that the tax authority servers do not provide all services that are described in this document. Please refer to SAP S/4HANA or SAP ERP documentation and to the relevant tax authority information, respectively.

3 Prerequisites

Before you start with the activities described in this document, ensure that the following prerequisites are met:

3.1 Registration at SAT

Registration at SAT is completed. And the following data is available:

- Certificate used for digital signatures (private key + password).
- Public certificate to verify the SOAP response deployed in the keystore of your SAP Integration Suite tenant. Obtain the certificate from SAT.

  For more information, see http://www.sat.gob.mx/informacion_fiscal/factura_electronica/Paginas/certificado_sello_digital.aspx.

Create a keystore using the private key and public key information available. Refer to chapter 7 on how to create a certificate using private and public key information available.

3.2 Full Solution Variant

The Full solution variant is installed in your test and production systems.

For the general part, refer to the Installation Guide attached to SAP Note 2134248.

For the Mexico-specific part, refer to SAP Note 2526771 for SAP ERP systems, and SAP Note 2565791 for SAPS/4HANA systems.

4 Secure Connection

4.1 Setup of Secure Connection

You establish a trustworthy SSL connection to set up a connection between the SAP back-end systems and the SAP Integration Suite.

Inbound HTTP connections are not required for Mexico. Outbound HTTP connections are required, and are supported with specific, public certificates.

You use SAP ERP Trust Manager (transaction STRUST) to manage the certificates required for a trustworthy SSL connection. The certificates include public certificates to support outbound connections, as well as trusted certificate authority (CA) certificates to support integration flow authentication.

Refer to the system documentation for more information regarding the certificate deployment to SAP back-end systems. In case of issues, refer to the following SAP notes:

- 2368112 Outgoing HTTPS connection does not work in AS ABAP
- 510007 Setting up SSL on Application Server ABAP

Note: If you encounter any issues in the information provided in the SAP Integration Suite product page, open a customer incident against the LOD-HCI-PI-OPS component.

Client Certificate

If you are using a client certificate, this must be signed by one of the root certificates supported by the load balancer. A self-signed certificate is not suitable. For more information see Load Balancer Root Certificates Supported by SAP.

4.1.1 Setup of Your Tenants

Set up your tenants, as follows:

- If you have subscribed to **Process Integration**, perform all the initial setup steps described in Initial Setup of SAP Cloud Integration in Cloud Foundry Environment.
- If you have subscribed to **Integration Suite**, perform all the initial setup steps described in Initial Setup. Note that the SAP Document and Reporting Compliance solution requires the **Cloud Integration** capability. You need to activate this capability in the step **Provisioning the Capabilities**.

4.1.2 Retrieve and Save Public Certificates

Context

Find and save the public certificates from your SAP Integration Suite worker node.

Procedure

1. Access the SAP BTP cockpit, and navigate to your subaccount (tenant) page.
2. Click the subscriptions link to display the subscriptions for your subaccount.
3. Use the tenant URL you created as defined in the prerequisites of this document. The URL has the following format: https://<tenant>.cfapps.<data center>.hana.ondemand.com, where XXXXXXX corresponds to the dynamic part and is unique for each subaccount.
4. Choose *Manage Integration Content* and select All to display the integration flows available.
5. Select an integration flow to display its details.
6. Copy the URL listed within the *Endpoints* tab and paste the URL into your web browser.
7. When prompted by the *Website Identification* window, choose *View certificate*.
8. Select the root certificate, and then choose *Export to file* to save the certificate locally.
9. Repeat these steps for each unique root, intermediate and leaf certificate, and repeat for both your test and production tenants.

4.1.3 Upload the Certificates

Store the public certificates used for your productive and test tenants.

Context

You use the SAP ERP Trust Manager (transaction STRUST) to store and manage the certificates required to support connectivity between SAP back-end systems and SAP Integration Suite.

Procedure

1. Access transaction STRUST.
2. Navigate to the PSE for **SSL Client (Anonymous)** and open it by double-clicking the PSE.
3. Switch to edit mode.
4. Choose the *Import certificate* button.
5. In the *Import Certificate* dialog box, enter or select the path to the required certificates and choose Enter.

The certificates are displayed in the *Certificate* area.

6. Choose *Add to Certificate List* to add the certificates to the *Certificate List*.
7. Save your entries.

4.1.4 Authenticate Integration Flow

Create an own certificate and get it signed by a trusted certificate authority (CA) to support integration flow authentication.

Context

You use the SAP ERP Trust Manager (transaction STRUST) for this purpose.

This process is required only if you use certificate-based authentication (that is, you choose the **X.509 SSL Client Certification** option in your settings for SOAMANAGER).

Procedure

1. Access transaction STRUST.

2. Create your own PSE (for example, Client SSL Standard) and then generate a certificate sign request.
3. Export the certificate sign request as a *.csr file.
4. Arrange for the certificate to be signed by a trusted certificate authority (CA).
   If you are using a client certificate, this must be signed by one of the root certificates supported by the load balancer. A self-signed certificate is not suitable. For more information see Load Balancer Root Certificates Supported by SAP.
   The CA may have specific requirements and request company-specific data, they may also require time to analyze your company before issuing a signed certificate. When signed, the CA provides the certificate for import.
5. Navigate to the PSE for SSL Client Standard and open it by double-clicking the PSE.
6. Switch to edit mode.
7. Choose the *Import certificate* button.
8. In the *Import Certificate* dialog box, enter or select the path to the CA-signed certificate and choose *Enter*.
   The certificate is displayed in the *Certificate* area.
9. Choose *Add to Certificate List* to add the signed certificate to the *Certificate List*.
   Ensure that you import the CA root and intermediate certificates to complete the import.
10. Save your entries.
    The certificates can now be used in the SOA Manager (transaction SOAMANAGER).

5 Configuration Steps in SAP Integration Suite

5.1 Deploy the Customer Certificate and Credentials to SAP Integration Suite

If your PAC is Edicom, you can use an Edicom-specific integration flow to communicate with Edicom. If your PAC is Pegaso, you can use a Pegaso-specific integration flow to communicate with Pegaso. Before sending an XML file using either of the two integration flows, SAP Integration Suite signs it using a private/public key pair and client certificate. In these cases where the signing is done by SAP, you need to provide an SSL certificate recognized by the tax authority and a pair of private/public key. This information must be available in the keystore on your SAP Integration Suite tenant.

This integration package also provides a generic integration flow, which is meant to work with any PAC. If you use this generic integration flow to communicate with your PAC, the PAC does the signing.

Do the following to deploy your credentials and certificate on SAP Integration Suite:

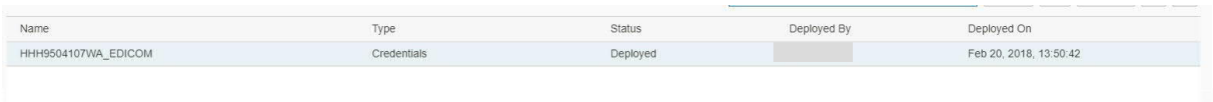
1. Deploy the certificate (as private key with an alias <RfcEmisor>) in the JAVA_KEYSTORE.
   See chapter 7 on how to create a single certificate chain containing both the private key and public certificate.

Here's an example:

Alias	Type	Owner	Valid Until	Last Modified At	Actions
hhh9504107wa	Key Pair	Tenant Administrator	May 18, 2021, 09:24:56	Feb 13, 2018, 18:06:50	

For Edicom, credentials for the endpoint must be obtained and stored in the tenant under the name **<RfcEmisor>_EDICOM**. If you have multiple company codes, you do not need to copy the package for every company code. You just need to maintain the credentials for every <RfcEmisor>.

Here's an example:

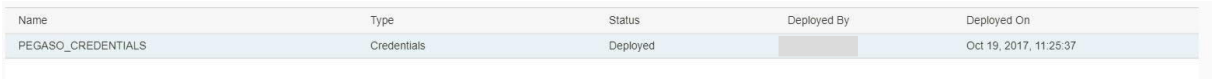


Name	Type	Status	Deployed By	Deployed On
HHH9504107WA_EDICOM	Credentials	Deployed		Feb 20, 2018, 13:50:42

Note: Your <RfcEmisor> may contain special characters that are not supported in credentials names. In this case, you need to replace the special characters with underscores (_). For example, your <RfcEmisor> is HH&9504107WA_EDICOM. The character & is invalid. You need to enter HH_9504107WA_EDICOM as your credentials name.

For Pegaso, credentials (username and password) for the endpoint must be obtained and stored in the tenant under the name **PEGASO_CREDENTIALS**. If you have multiple company codes, you must copy the package for every company code.

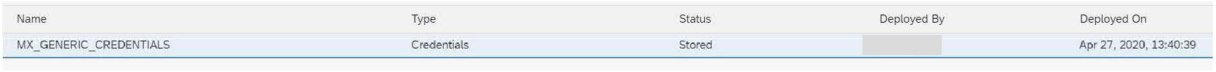
Here's an example:



Name	Type	Status	Deployed By	Deployed On
PEGASO_CREDENTIALS	Credentials	Deployed		Oct 19, 2017, 11:25:37

For other PACs, credentials (username and password) for the endpoint must be obtained and stored in the tenant under the name **MX_GENERIC_CREDENTIALS**. If you have multiple company codes, you must copy the package for every company code.

Here's an example:



Name	Type	Status	Deployed By	Deployed On
MX_GENERIC_CREDENTIALS	Credentials	Stored		Apr 27, 2020, 13:40:39

2. Deploy the public certificate for testing in the JAVA_KEYSTORE of the test tenant. Deploy the public certificate for production use in the JAVA_KEYSTORE of the production tenant.

5.2 Copy Integration Package

This package contains the following integration flows:

Integration Flow Name in WebUI	Project Names/Artifacts Name
Mexico Document Compliance	MexicoeDocument
Mexico Document Compliance Edicom	MexicoeDocument_edicom
Mexico Document Compliance Pegaso	MexicoeDocument_pegaso
Mexico Document Compliance Pegaso for Withholding Tax Certificate	MexicoWTC_Pegaso
Mexico Document Compliance Edicom for Withholding Tax Certificate	MexicoWTC_Edicom
Mexico Document Compliance Generic	MexicoeDocument_generic

There are two integration flow deployment options. The option that you should choose depends on your PAC.

Option 1

If your PAC is Edicom or Pegaso, you can use this deployment option. Deploy the following integration flows on your tenant:

Integration Flow Name in WebUI	Explanation
Mexico Document Compliance	Whether you PAC is Edicom or Pegaso, you must deploy this integration flow.
Mexico Document Compliance Edicom	If your PAC is Edicom, in addition to the integration flow **Mexico Document Compliance**, deploy this integration flow as well.
Mexico Document Compliance Pegaso	If your PAC is Pegaso, in addition to the integration flow **Mexico Document Compliance**, deploy this integration flow as well.
Mexico Document Compliance Pegaso for Withholding Tax Certificate	If your PAC is Pegaso and you want to issue electronic withholding tax certificates, in addition to the integration

	flow **Mexico Document Compliance**, deploy this integration flow as well.
Mexico Document Compliance Edicom for Withholding Tax Certificate	If your PAC is Edicom and you want to issue electronic withholding tax certificates, in addition to the integration flow **Mexico Document Compliance**, deploy this integration flow as well.

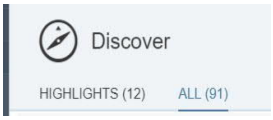
Option 2

If you choose a PAC other than Edicom or Pegaso, use this deployment option. Deploy the following integration flow on your tenant:

Integration Flow Name in WebUI	Explanation
Mexico Document Compliance Generic	You can find PACs who are SAP partners and can handle requests from this integration flow from SAP App Center. Search with the keyword "SAP Document and Reporting Compliance".

Do the following to copy the integration package:

1. Log in to your SAP Integration Suite tenant.
2. From the menu in the upper left corner, choose **Discover**.
3. Go to the tab page **ALL**.



4. In the search field, enter **SAP Document and Reporting Compliance: Electronic Documents for Mexico** and press ENTER.

5. Select the package **SAP Document and Reporting Compliance: Electronic Documents for Mexico**. In the upper right corner, choose **Copy**.

5.3 Deploy Integration Flows

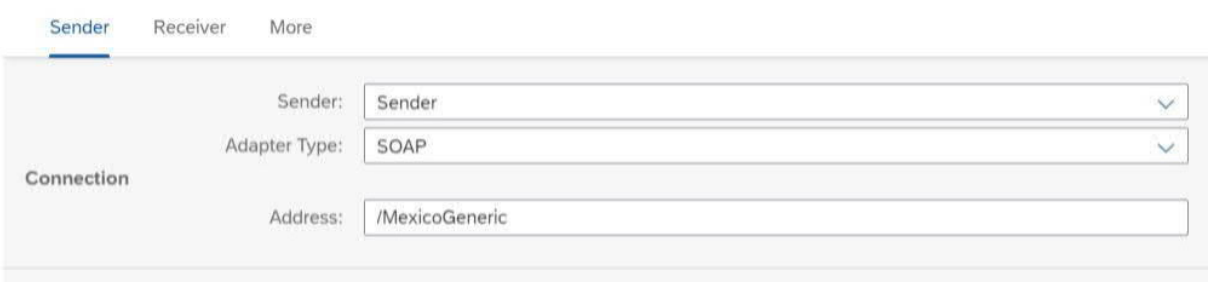
Do the following to deploy an integration flow:

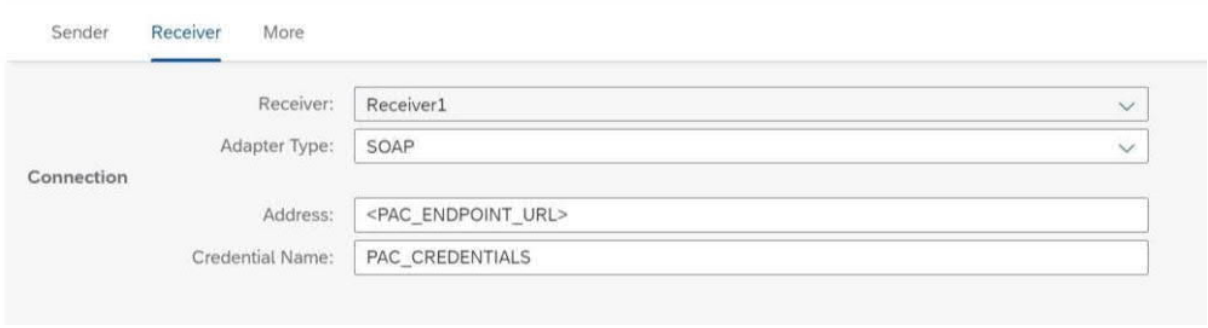
Configuring Integration Flows

1. Click on the package **SAP Document and Reporting Compliance: Electronic Documents for Mexico**.
2. Go to the **Artifacts** tab page.
3. For the integration flow that you want to deploy, choose **Actions** -> **Configure**.
4. Choose **Save**.

To deploy the generic integration flow Mexico **Document Compliance Generic**, follow the instructions below:

1. Configure the following externalized parameters:
   - **Sender**: endpoint URL of the integration flow
   - **Receiver**: endpoint URL from PAC
   - Credential Name: credential name maintained in the keystore
2. Choose **Deploy**.



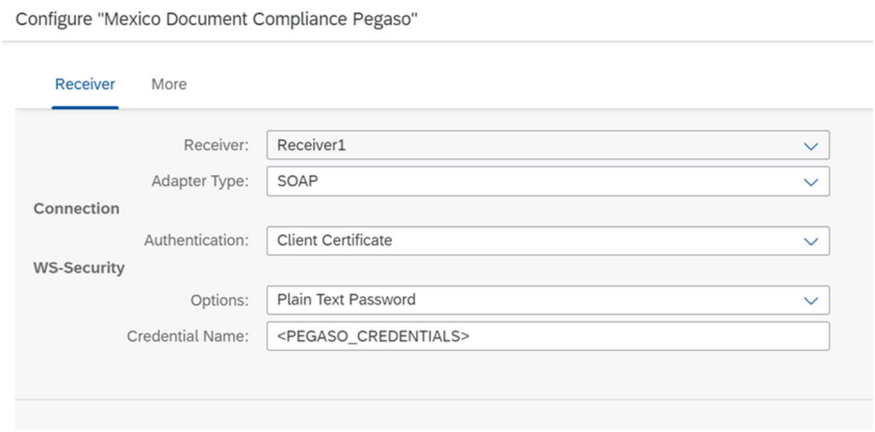


If you use the integration flow "Mexico Document Compliance Pegaso", proceed as follows:

1. Make the following settings:

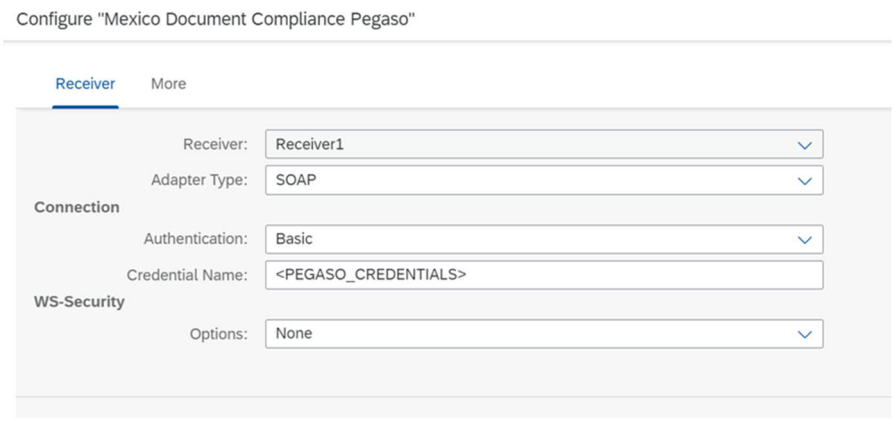
   - **Authentication**: This setting depends on the Pegaso web service that you use.

     If you use the **Gateway service** from Pegaso, select the **Client Certificate** authentication type and then make the following settings:
     - **Options**: Select **Plain Text Password**.
     - **Credential Name**: Enter the credential name that you've configured in the keystore.

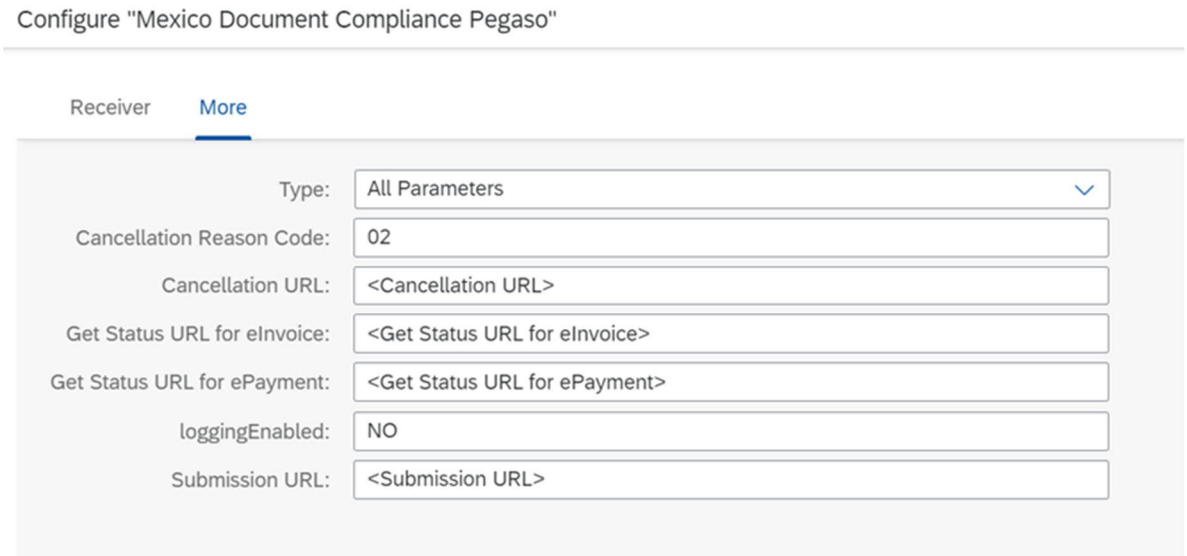


If you use the Azure service from Pegaso, select the Basic authentication type and then make the following settings:

- **Credential Name**: Enter the credential name that you've configured in the keystore.
- **Options**: Select **None**.



- **Submission URL**: Enter the endpoint URL of the web service that submits electronic invoices and payment documents.
- **Cancellation URL**: Enter the endpoint URL of the web service that cancels electronic invoices and payment documents.
- **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests. **Note**: If you have already implemented SAP Note 3152004, you can fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents (BADI_EDOCUMENT_MX_CANCEL)**. In that case, leave this parameter blank. Otherwise, you must specify a fixed cancellation reason code using this parameter.
- **Get Status URL for eInvoice**: Enter the endpoint URL of the web service that gets statuses of invoice cancellation requests.
- **Get Status URL for ePayment**: Enter the endpoint URL of the web service that gets statuses of payment cancellation requests.
- **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.



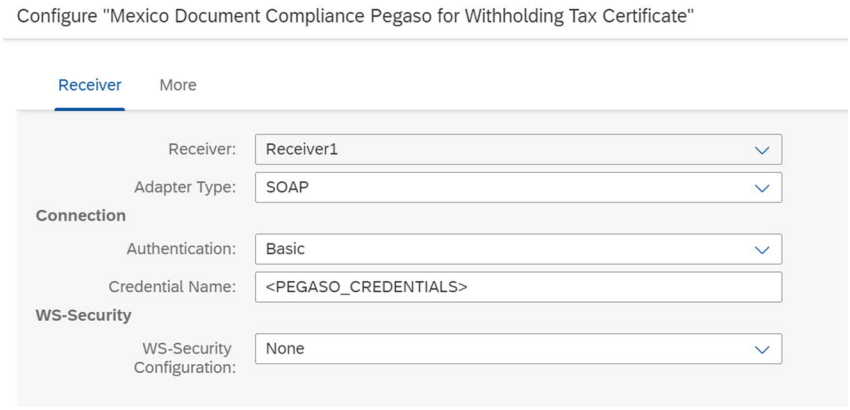
2. Choose **Deploy**.
3. Test the connection.

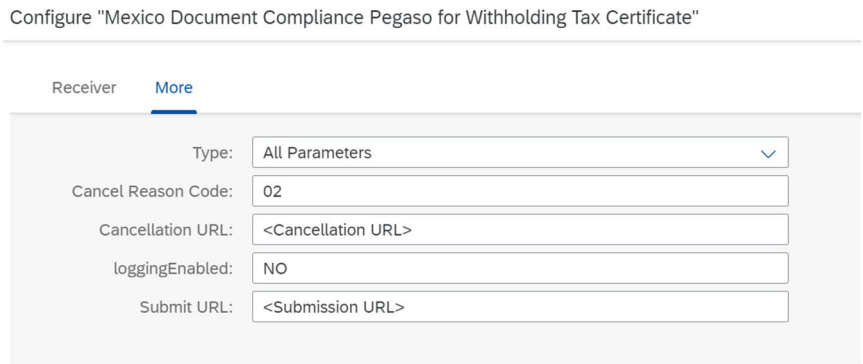
Before testing, ensure the handshake certificate from Pegaso is already deployed in the keystore of the tenant. There is no constraint on the alias here. When downloading the handshake certificate, you can store it under any name.

If you use the integration flow “Mexico Document Compliance Pegaso for Withholding Tax Certificate”, proceed as follows:

1. Make the following settings:

- **Authentication**: Select the Basic authentication type and then make the following settings:
  - **Credential Name**: Enter the credential name that you’ve configured in the keystore.
  - **WS-Security Configuration**: Select **None**.
- **Submission URL**: Enter the endpoint URL of the web service that submits withholding tax certificates.
- **Cancellation URL**: Enter the endpoint URL of the web service that cancels withholding tax certificates.
- **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests.
  Note: If you have already implemented SAP Note 3155584, you can fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents (BADI_EDOCUMENT_MX_CANCEL)**. In that case, leave this parameter blank. Otherwise, you must specify a fixed cancellation reason code using this parameter.
- **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.





2. Choose **Deploy**.
3. Test the connection.

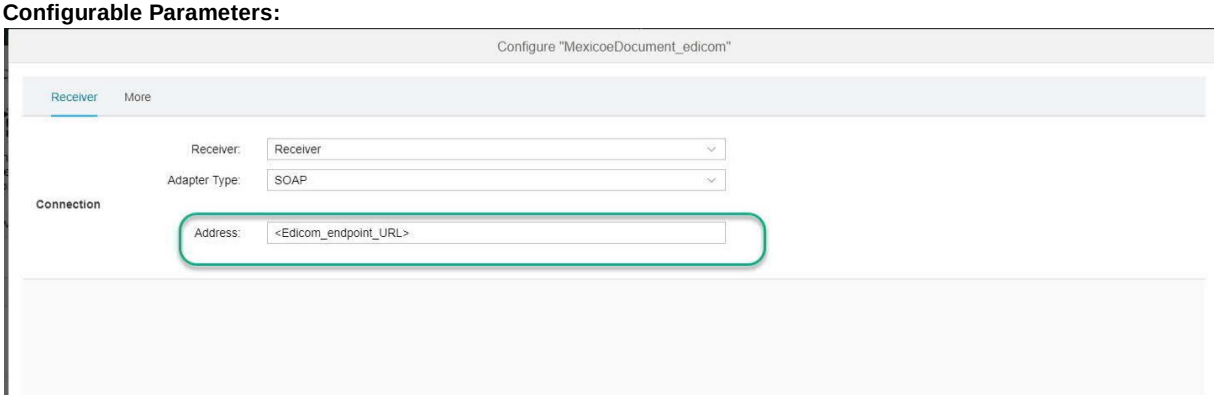
Before testing, ensure the handshake certificate from Pegaso is already deployed in the keystore of the tenant. There is no constraint on the alias here. When downloading the handshake certificate, you can store it under any name.

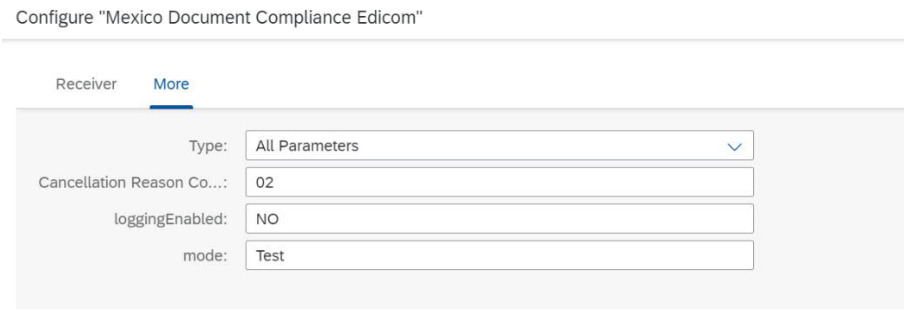
If you use the integration flow “Mexico Document Compliance Edicom”, proceed as follows:

1. Configure the following externalized parameters of the integration flow **Mexico Document Compliance Edicom**:
   - **Address**: Enter the endpoint URL from Edicom.
   - **mode**: The default mode is Test. Possible values are Test and Prod. Choose a mode based on the runtime environment. Edicom uses a common url for test and production modes.
   - **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests. **Note**: If you have already implemented SAP Note 3152004, you can fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents (BADI_EDOCUMENT_MX_CANCEL)**. In that case, leave this parameter blank. Otherwise, you must specify a fixed cancellation reason code using this parameter.
   - **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.
2. Choose **Deploy**.

   Before testing, download the handshake certificate from the endpoint that Edicom has provided and store it in the keystore of the tenant. There is no constraint on the alias name that you use to store this certificate. You can store it under any name.

Configurable Parameters:





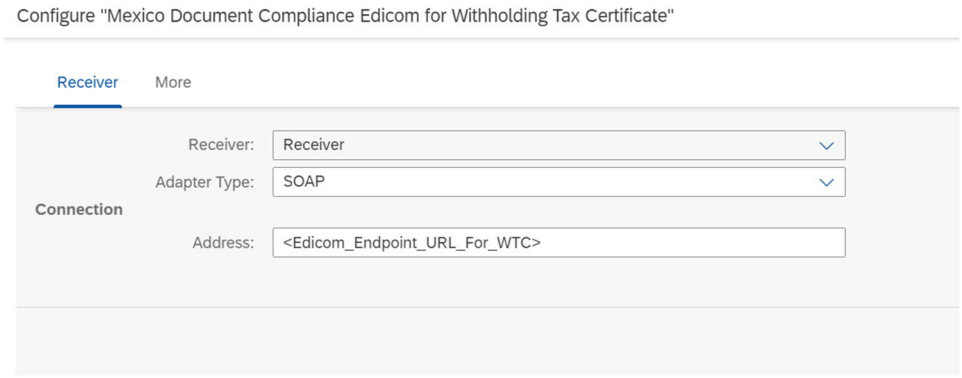
After deploying all the required integration flows, note down the URLs of the endpoints for each service. The endpoints are used in the communication arrangement configurations.

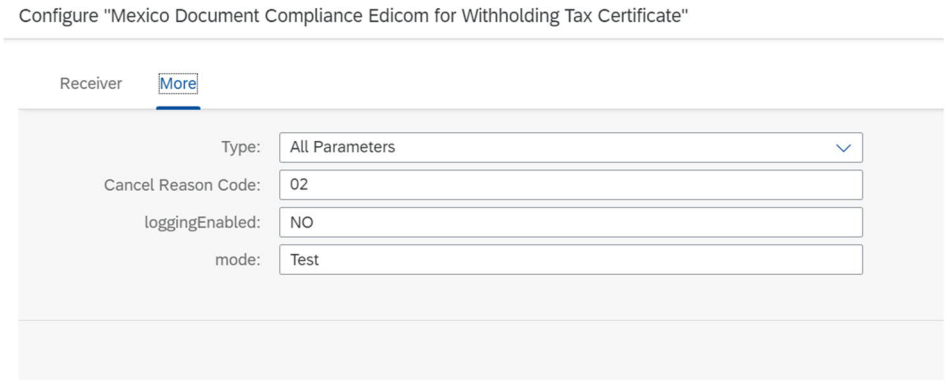
If you use the integration flow "Mexico Document Compliance Edicom for Withholding Tax Certificate", proceed as follows:

1. Make the following settings:

   - **Address**: Enter the endpoint URL from Edicom that submits withholding tax certificates.
   - **mode**: The default mode is Test. Possible values are Test and Prod. Choose a mode based on the runtime environment. Edicom uses a common url for test and production modes.

- **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests.
  Note: If you have implemented SAP Note 3155584, you can fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents (BADI_EDOCUMENT_MX_CANCEL)**. In that case, leave this parameter blank. Otherwise, you can must specify a fixed cancellation reason code using this parameter.
- **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.





2. Choose **Deploy**.
3. Test the connection.

Before testing, ensure the handshake certificate from Pegaso is already deployed in the keystore of the tenant. There is no constraint on the alias here. When downloading the handshake certificate, you can store it under any name.

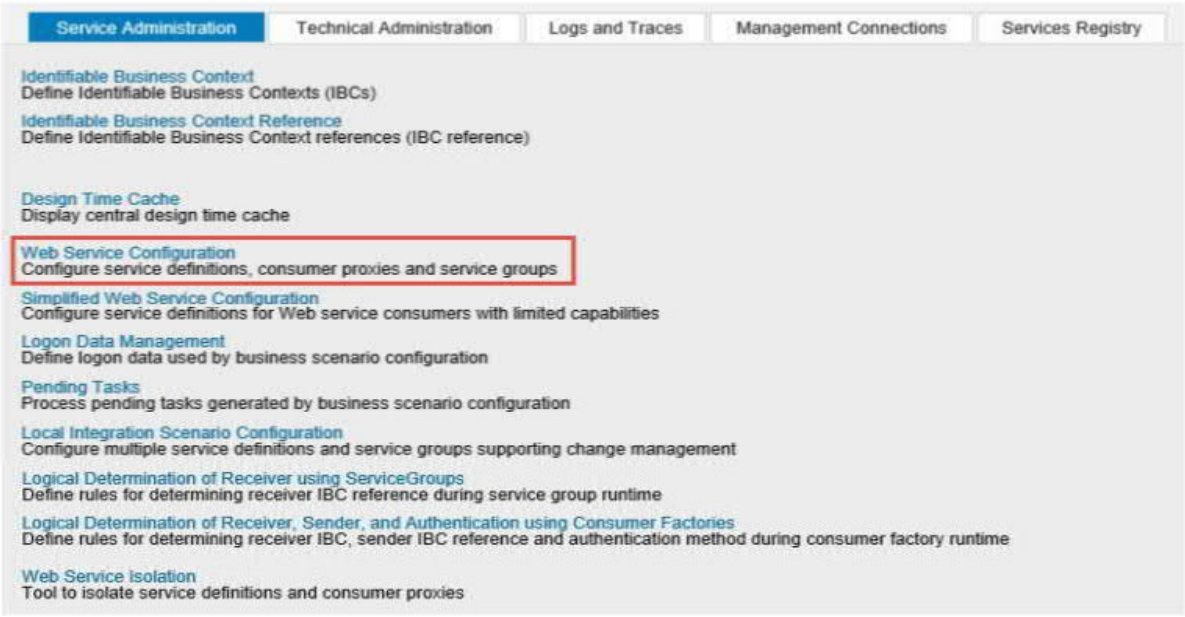
6 Configuration Steps in SAP ERP or SAP S/4HANA

6.1 Create Logical Ports in SAP ERP or SAP S/4HANA

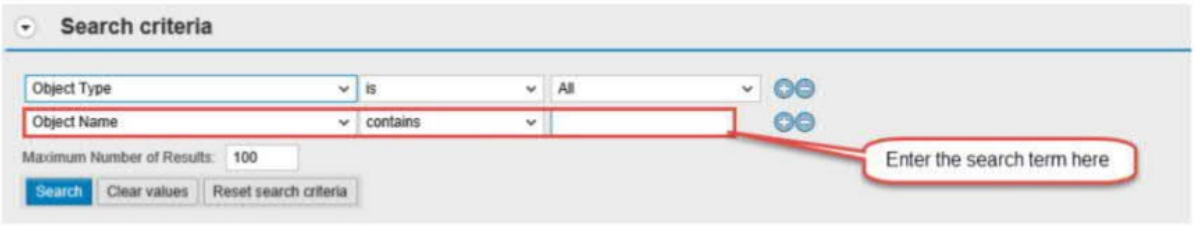
Proxies must be connected to the SAP Integration Suite tenant via logical ports. In the SAP ERP or SAP S/4HANA test system, the logical ports are configured to connect to the test SAP Integration Suite tenant. In the productive SAP ERP or SAP S/4HANA system, the logical ports are configured to connect to the productive SAP Integration Suite tenant.

Proceed as follows:

1. In your SAP ERP or SAP S/4HANA system, go to transaction *SOAMANAGER* and select **Web Service Configuration**.



2. Search for the proxies for Mexico with the search term **CO_EDO_MX_***



For the Pegaso-specific or Edicom-specific integration flow, the following proxies are available:

Proxy Name	Logical Port Name	Description	Path
CO_EDO_MX_CFDI_EDOCUMENTS * See SAP Note 2593892 for the functionality that this proxy provides.	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoeDocuments
CO_EDO_MX_CFDIE_EDOCUMENTS * Available since integration package version 1.0.10 See SAP Note 2825133 for the functionality that this proxy provides.	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoeDocuments
CO_EDO_MX_CFDIE_DOCUMENTS_V3 * Available since integration package version 1.0.21 See SAP Note 3131470 for the functionality that this proxy provides.	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoeDocuments
CO_EDO_MX_WTCE_DOCUMENTS * Available since integration package version 1.0.21 (Pegaso) and version 1.0.30 (Edicom). See SAP Note 3149915 for the functionality that this proxy provides.	MX_WTC	WTC eDocuments	/cxf/MexicoeDocuments

CO_EDO_MX_CFDIE_DOCUMENTS_V4 * Available since integration package version 1.0.29. See SAP Note 3167390 for the functionality that this proxy provides.	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoeDocuments
CO_EDO_MX_WTCE_DOCUMENTS_V2 * Available since integration package version 1.0.29 (Pegaso) and version 1.0.30 (Edicom). See SAP Note 3167428 for the functionality that this proxy provides.	MX_WTC	WTC eDocuments	/cxf/MexicoeDocuments

If you use the generic integration flow, use the following proxy:

Proxy Name	Logical Port Name	Description	Path
CO_EDO_MX_CFDIE_EDOCUMENTS	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoGeneric

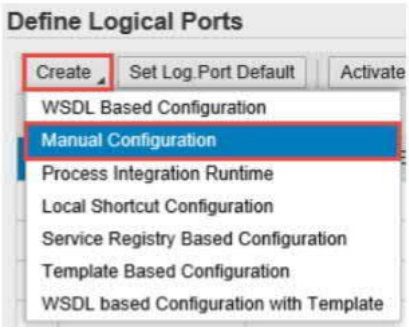
Both the logical port name and path can be customized.

Note: You must maintain the maintenance view EDOSOASERV for each company code in your SAP ERP or SAP S/4HANA system.

For example:

SOA SERVICE NAME	Company code	Logical Port	SOA Service Description
MX_EDOCUMENT	XXXX	MX_EDOCUMENT	Mexico eDocument SOA service
MX_WTC	XXXX	MX_WTC	Mexico Electronic Withholding Tax Certificate SOA Service

3. In the result list, select a proxy and create a logical port for it. Choose *Create* > *Manual Configuration*.

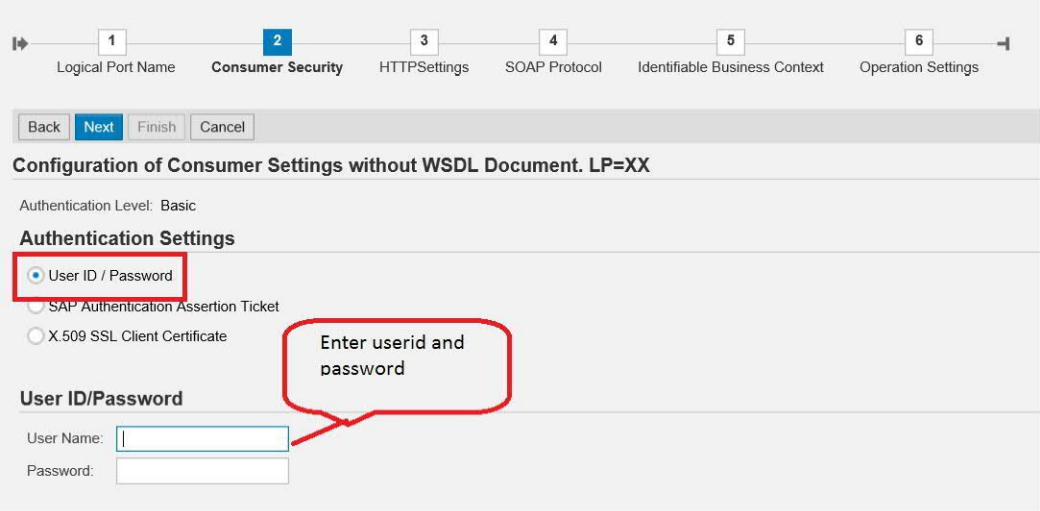


4. Enter the logical port name and a description.

5. The **Consumer Security** configuration depends on the security being used for the SAP ERP or SAP S/4HANA - SAP Integration Suite communication.

a. If you use the basic authentication, enter the value of the **clientid** for *User Name*, and the value of **clientsecret** for *Password*. You create these values for your service instance in SAP Integration Suite. See Creating Service Instances.

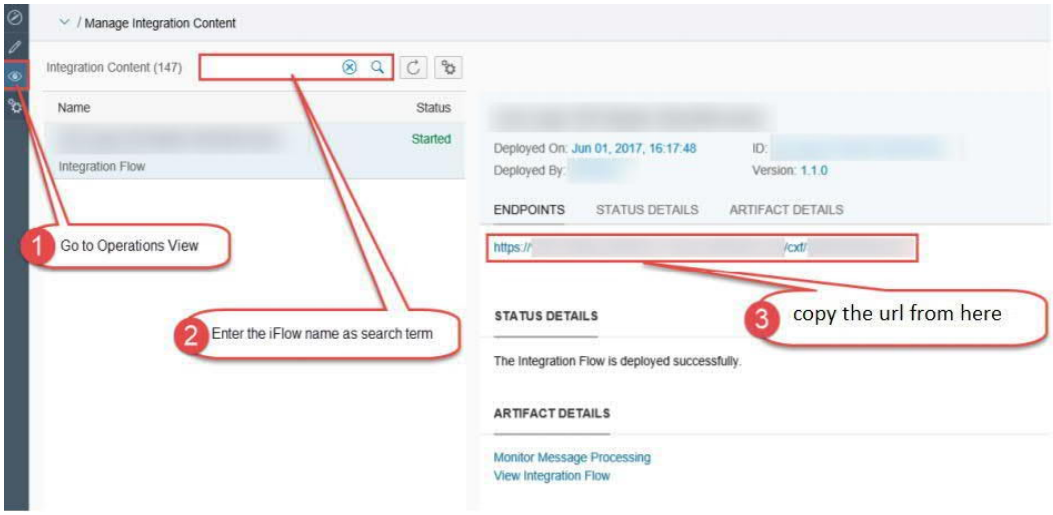
b. If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have uploaded to STRUST. You must configure this certificate in SAP Integration Suite too. For that you create a service instance using the required grant type. You create the service key using the certificate uploaded to the STRUST. For more information, see Defining a Service Key for the Instance in the Cloud Foundry Environment.



6. On the **HTTP Settings** tab page, select the **URL components** radio button and make the following settings:

Setting	Value
Protocol	Select HTTPS.
Host	Enter the host name of the integration flow that you want to communicate with.
Port	Enter 443, which is the standard port for the HTTPS protocol.
Path	Find the path of the related integration flow from your SAP Cloud Integration tenant or SAP Integration Suite tenant.
Proxy	Enter the information about your company's network proxy.

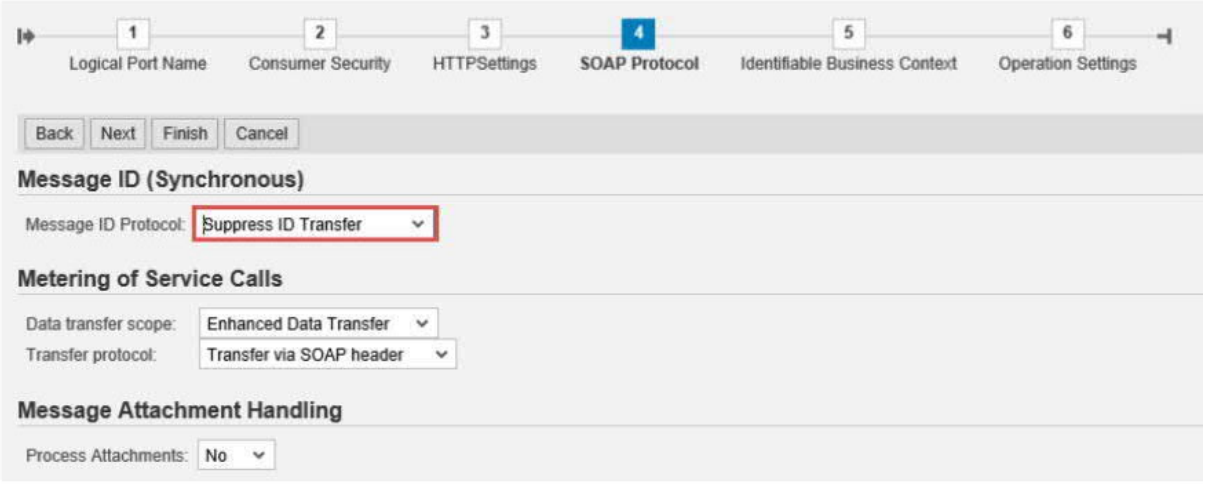
To find the Host, go to SAP Integration Suite Web UI. Under **Managed Integration Content**, go to **Monitor** -> **All**. Use the search to find your integration flow as shown in the screenshot below:



:

The entries for the Proxy fields depend on your company's network settings. The proxy server is needed to enable the connection to the Internet through the firewall.

7. On the **Messaging** tab page, set the value of the **Message ID Protocol** field to **Suppress ID Transfer**.



8. No settings are required in the tabs **Identifiable Business Context** and **Operation Settings**. Just select **Next** and then **Finish**.

7 Appendix

7.1 Generate and Import Certificates

7.1.1 Prerequisites

- Install OPENSSL in your system (http://slproweb.com/products/Win32OpenSSL.html).
- You can also download Keystore Explorer for creating the keystore. (http://keystore-explorer.sourceforge.net/downloads.php)

7.1.2 Generate PKCS#12 File from the Certificate and Key File

After the successful installation of openssl for Windows, follow the steps below to generate the keystore file that you can import into SAP Integration Suite:

1. Open Command Prompt in the folder where openssl is installed.
2. Convert the key file to pkcs8 format.
   openssl pkcs8 -inform DER -in aaa010101aaa_CSD_01.key -passin pass:a0123456789 -outform PEM -out CSD_01.key.pem -passout pass:a0123456789
3. Convert the certificate to pkcs8 format.
   openssl x509 -inform DER -in aaa010101aaa_CSD_01.cer -outform PEM -out CSD_01.cer.pem.
4. Append the certificate and key file to one file.
   copy CSD_01.key.pem+CSD_01.cer.pem CSD_01_chain.pem.
5. Convert the pem file to pkcs12.
   openssl pkcs12 -in CSD_01_chain.pem -passin pass:a0123456789 -export -out CSD_01.p12 -name SAT -passout pass:a0123456789

In the Keystore Explorer, make the following settings:

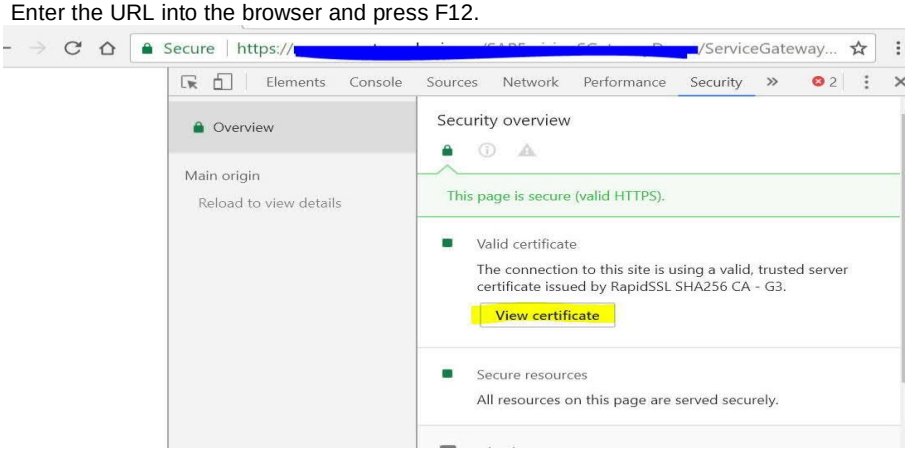
1. Click on **Create a New Keystore**. Select JKS as the type of the new Keystore.
2. Choose **Tools** -> **Import Key Pair** and select the pkcs12 file.
3. Enter a password and click on **Save**.

As the next step, you import the JKS file into the Keystore of SAP Integration Suite under the alias described in step 1 of the section **Deploy the Customer Certificate and Credentials to SAP Integration Suite**.

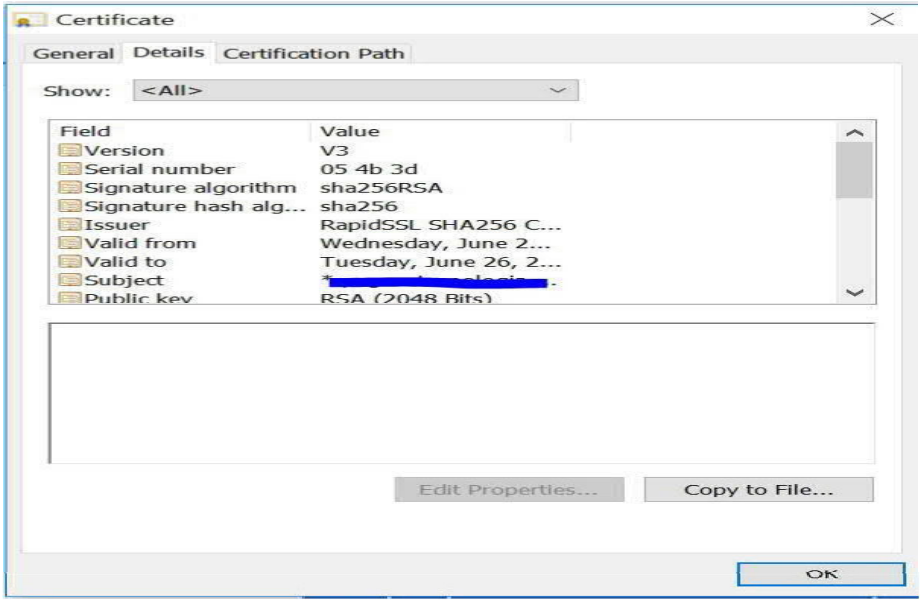
7.1.3 Import the Handshake Certificate

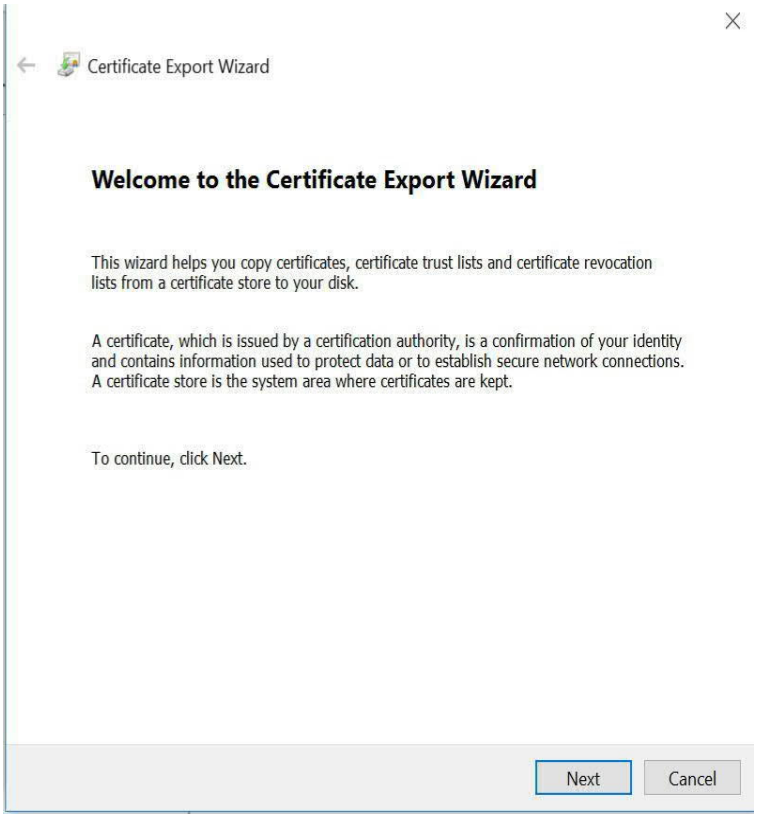
Irrespective of whether the signing happens in SAP Integration Suite or not, you must download the handshake certificate from the endpoint that is used to connect to the PAC.

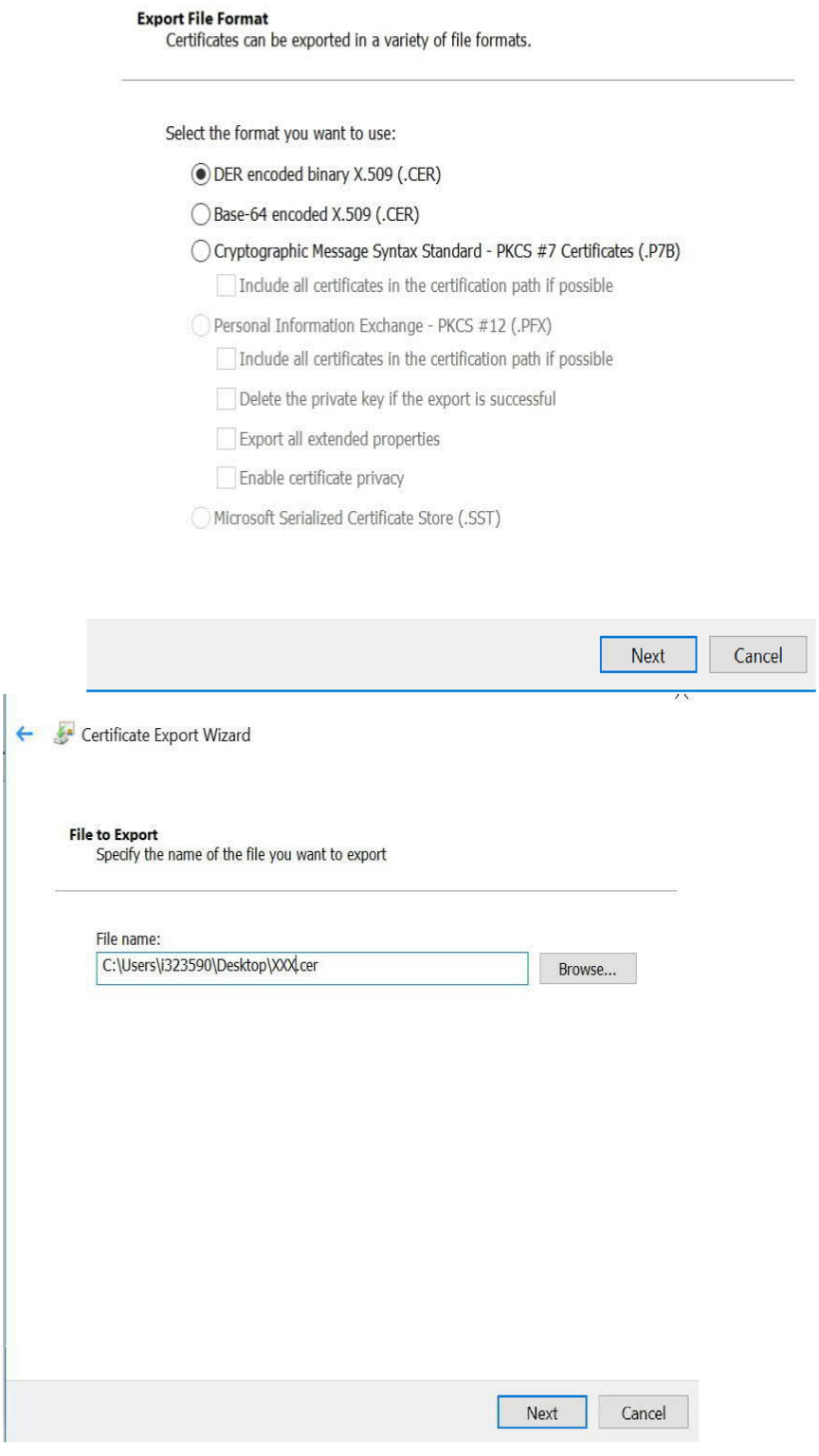
1. Enter the URL into the browser and press F12.



2. Click on *View certificate* -> *Copy to file*, choose *Next* and select options as below until you reach *Finish*. You can import this certificate into a keystore and load it to the SAP Integration Suite tenant keystore.


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
05 4b 3d
Signature algorithm
sha256RSA
Signature hash alg...
sha256
Issuer
RapidSSL SHA256 C...
Valid from
Wednesday, June 2...
Valid to
Tuesday, June 26, 2...
Subject
Public key
RSA (2048 Bits)
Edit Properties...
Copy to File...
OK


Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel


Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Enable certificate privacy
Microsoft Serialized Certificate Store (.SST)
Next
Cancel
Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\i323590\Desktop\XXX.cer
Browse...
Next
Cancel

www.sap.com