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

TABLE OF CONTENTS

1 DISCLAIMER ... 3

2 INTRODUCTION ... 3

3 PREREQUISITES ... 3
3.1 Registration at SAT ... 3
3.2 Configuration of Document Compliance for Mexico ... 3
3.3 Setup of SAP Cloud Platform Integration ... 3

4 CONFIGURATION STEPS IN SAP CLOUD PLATFORM INTEGRATION ... 3
4.1 Deploy the Customer Certificate and Credentials to SAP Cloud Platform Integration ... 4
4.2 Copy the Integration Package ... 4
4.3 Deploy Integration Flows ... 5

5 CONFIGURATION STEPS IN SAP S/4HANA CLOUD ... 8
5.1 Configure a Communication System ... 8
5.2 Configure a Communication Arrangement ... 10

6 APPENDIX ... 11
6.1 Generate and Import Certificates ... 11
6.1.1 Prerequisites ... 11
6.1.2 Generate PKCS#12 File from the Certificate and Key File ... 11
6.1.3 Import the Handshake Certificate ... 11

1 Disclaimer

This documentation refers to links to Web sites 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 Cloud Platform Integration. In order to get SAP Cloud Platform Integration working, there are some required steps on both your SAP S/4HANA Cloud system and SAP Cloud Platform Integration tenant.

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

Note: This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Cloud Platform Integration tenant. It may happen, however, that in the SAP S/4HANA Cloud tenant 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 Cloud 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 Cloud Platform Integration tenant. Obtain the certificate from the 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 6 on how to create a certificate using private and public key information available.

3.2 Configuration of Document Compliance for Mexico

For more information, see the documentation for Document Compliance for Mexico on SAP Help Portal at https://help.sap.com/viewer/product/SAP_S4HANA_CLOUD. Select your product version. In the *Product Assistance* section, select a language and then select *Country/Region-Specific Functions -> Mexico -> General Functions -> Document Compliance for Mexico*.

3.3 Setup of SAP Cloud Platform Integration

You have performed all initial setup steps described in Initial Setup of SAP Cloud Platform Integration in Cloud Foundry Environment. After completing the tenant provisioning step, you get your own tenant URL.

4 Configuration Steps in SAP Cloud Platform Integration

Perform the below steps to set up the iFlows.

4.1 Deploy the Customer Certificate and Credentials to SAP Cloud Platform Integration

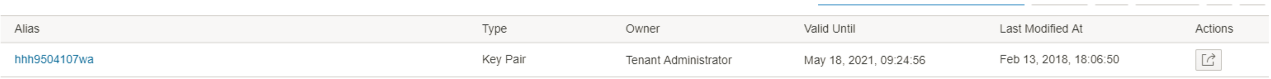
If your PAC is Edicom, you can use an Edicom-specific iFlow to communicate with Edicom. If your PAC is Pegaso, you can use a Pegaso-specific iFlow to communicate with Pegaso. Before sending an XML file using either of the two iFlows, SAP Cloud Platform Integration signs it using a private/public key 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 Cloud Platform Integration tenant.

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

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

1. Deploy the certificate (as private key with the alias <RfcEmisor>) in the JAVA_KEYSTORE.
   See chapter 6 on how to create a single certificate chain containing both private key and public certificate.

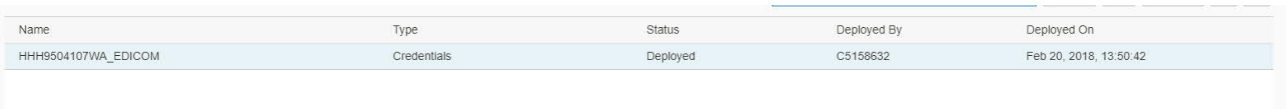
   Here's an example:



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>.

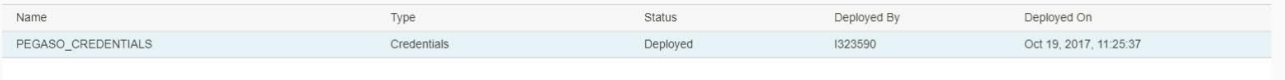
Here's an example:



Name	Type	Status	Deployed By	Deployed On
HHH9504107WA_EDICOM	Credentials	Deployed	C5158632	Feb 20, 2018, 13:50:42

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.

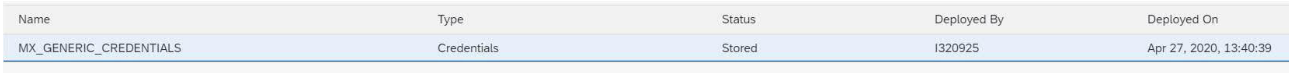
Here's an example:



Name	Type	Status	Deployed By	Deployed On
PEGASO_CREDENTIALS	Credentials	Deployed	I323590	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	I320925	Apr 27, 2020, 13:40:39

2. Deploy the public certificate for STAGING in the TEST tenant's JAVA_KEYSTORE and the public certificate for PRODUCTION in the PRODUCTION tenant's JAVA_KEYSTORE.

   The details on how to create a jks file are available in chapter 6.

4.2 Copy the Integration Package

This package contains the following iFlows:

iFlow 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 Generic	MexicoeDocument_generic

There are two iFlow 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 iFlows on your tenant:

iFlow Name in WebUI	Explanation
Mexico Document Compliance	Whether you PAC is Edicom or Pegaso, you must deploy this iFlow.
Mexico Document Compliance Edicom	If your PAC is Edicom, in addition to the iFlow Mexico Document Compliance, deploy this iFlow as well.
Mexico Document Compliance Pegaso	If your PAC is Pegaso, in addition to the iFlow Mexico Document Compliance, deploy this iFlow as well.

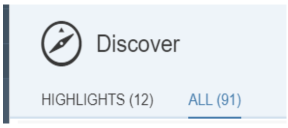
Option 2

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

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

Do the following to copy the integration package:

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



4. In the search field, enter **SAP Document Compliance: Electronic Invoices and Payment Receipt Complements for Mexico** and press ENTER.
5. Select the package **SAP Document Compliance: Electronic Invoices and Payment Receipt Complements for Mexico**. In the upper right corner, choose **Copy**.

4.3 Deploy Integration Flows

Do the following to deploy an iFlow:

Configuring iFlows

1. Click on the package **SAP Document Compliance: Electronic Invoices and Payment Receipt Complements for Mexico**.
2. Go to the **Artifacts** tab page.

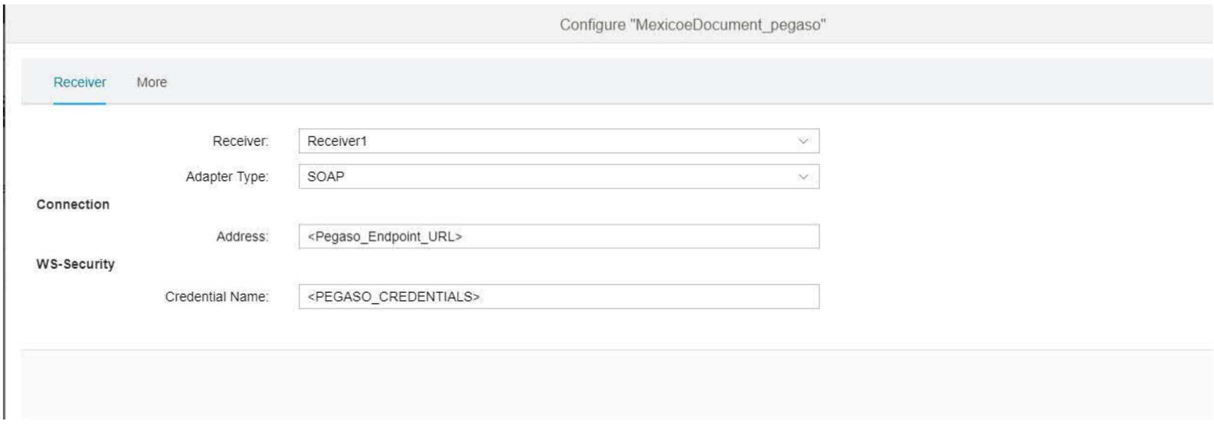
3. For the iFlow that you want to deploy, choose **Actions** -> **Configure**.
4. Choose **Save**.

For Pegaso, follow the instructions below:

1. Configure the following externalized parameters of the iFlow **Mexico Document Compliance Pegaso**:
   - URL: endpoint URL of the webservice from Pegaso
   - eInvoice_URL: endpoint URL for getting statuses of eInvoice cancellation requests
   - ePayment_URL: endpoint URL for getting statuses of ePayment cancellation requests

2. Enter the credential name that is maintained in the keystore.
3. Execute checks and deploy the iFlow in the tenant.
4. Before testing, ensure the handshake certificate from Pegaso is downloaded and deployed in the tenant's keystore. There is no constraint in the alias here. So, download and store it under any name.

Configurable Parameters:



Configure "MexicoeDocument_pegaso"

Receiver: Receiver1

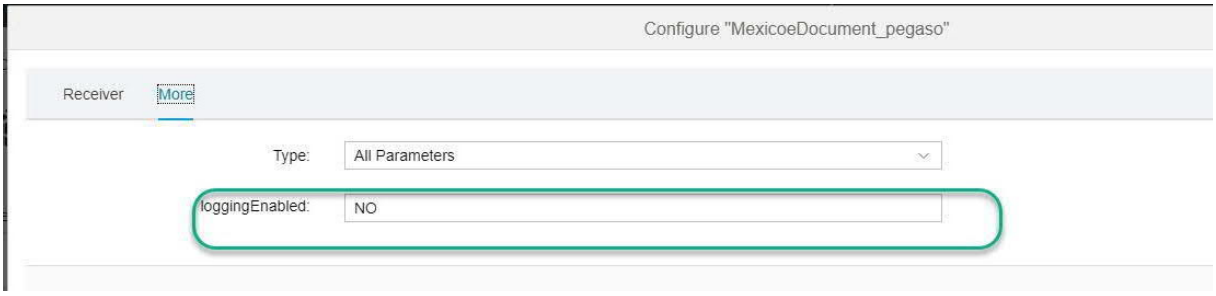
Adapter Type: SOAP

Connection

Address: <Pegaso_Endpoint_URL>

WS-Security

Credential Name: <PEGASO_CREDENTIALS>



Configure "MexicoeDocument_pegaso"

Type: All Parameters

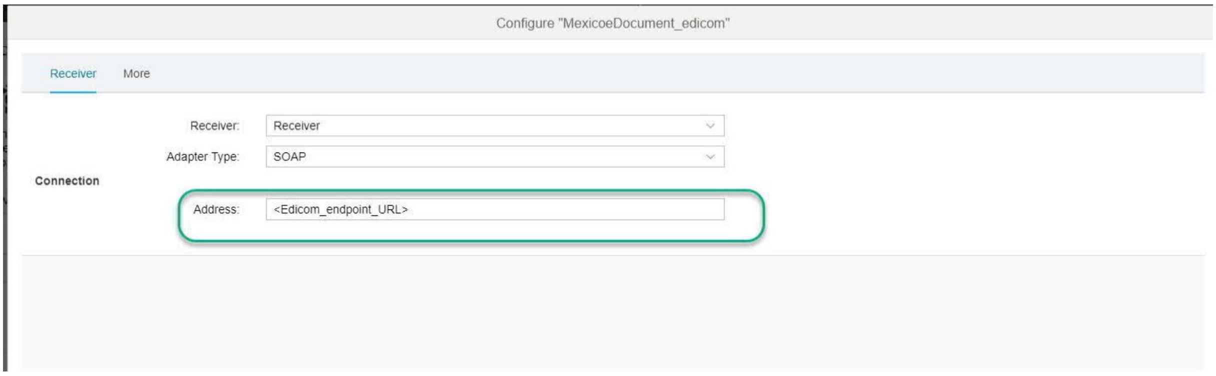
loggingEnabled: NO

For Edicom, follow the instructions below:

1. Configure the following externalized parameters of the iFlow **Mexico Document Compliance Edicom**:
   - url: 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.

2. Execute checks and deploy the iFlow.
3. Before testing, download the handshake certificate from the endpoint which Edicom has provided and store itin the tenant's keystore. There is no dependency on the alias name which you use to store this certificate. You can store it under any name.

Configurable Parameters:



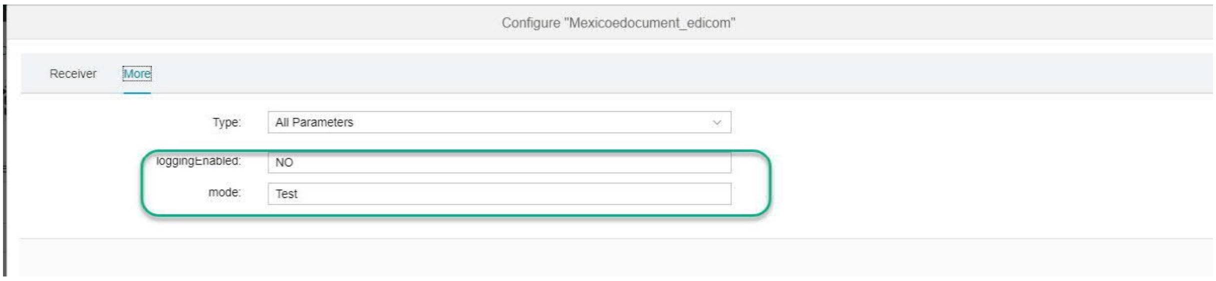
Configure "MexicoeDocument_edicom"

Connection

Receiver: Receiver

Adapter Type: SOAP

Address: <Edicom_endpoint_URL>



Configure "Mexicoedocument_edicom"

Type: All Parameters

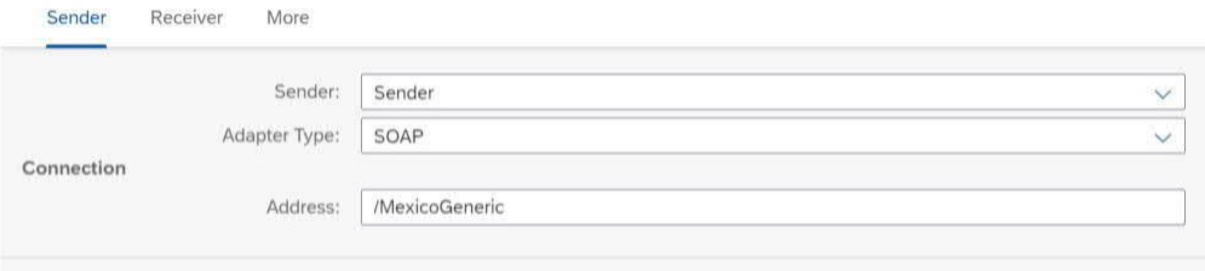
loggingEnabled: NO

mode: Test

For the generic iFlow ***Mexico Document Compliance Generic***, follow the instructions below:

1. Configure the following externalized parameters:
   - Sender Address: endpoint URL of the iFlow
   - Receiver Address: endpoint URL from PAC

2. Enter the credential name that is maintained in the keystore.
3. Execute checks and deploy the iFlow in the tenant.

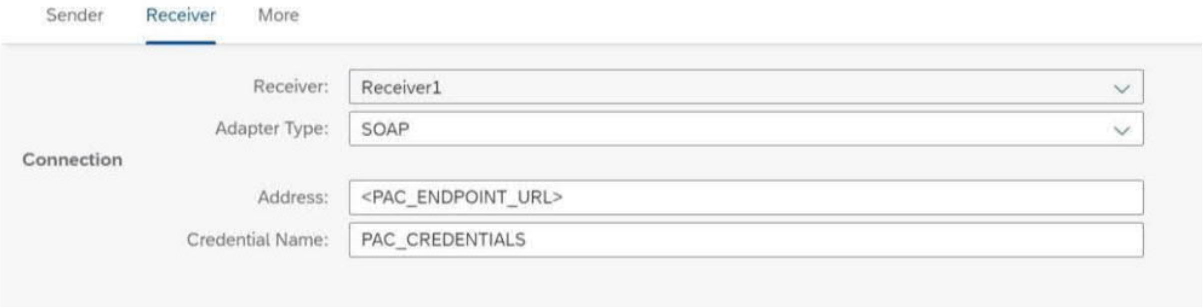


Connection

Sender: Sender

Adapter Type: SOAP

Address: /MexicoGeneric



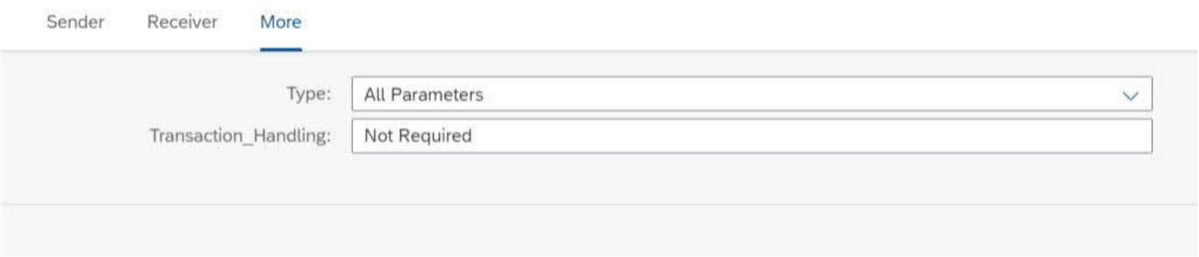
Connection

Receiver: Receiver1

Adapter Type: SOAP

Address: <PAC_ENDPOINT_URL>

Credential Name: PAC_CREDENTIALS



Type: All Parameters

Transaction_Handling: Not Required

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

5 Configuration Steps in SAP S/4HANA Cloud

5.1 Configure a Communication System

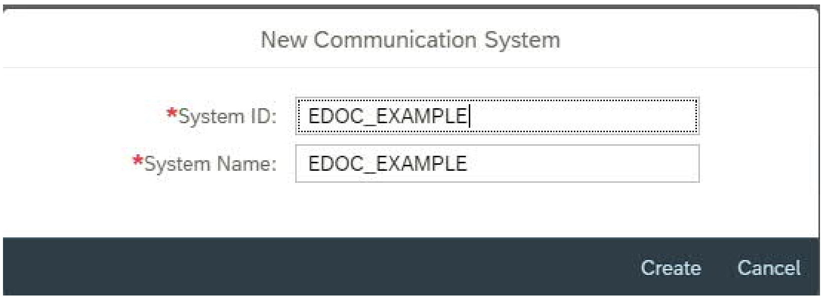
Note the following:

- Communication management settings are not transportable and should be explicitly maintained in quality and production systems.
- The S/4HANA Cloud user, who is following the guide, must be assigned to a business role that contains the business catalog SAP_BCR_CORE_COM for accessing communication management apps.

Make settings as follows:

1. Login to your SAP S/4HANA Cloud tenant.
2. Find and launch the app **Communication Systems.**

3. Click **New**. In the pop-up window, enter the ID and description of your communication system. It is recommended to name it like *EDOC_<name of SAP Cloud Platform Integration tenant>*. For example, *EDOC_EXAMPLE* for a tenant host name beginning with *example-tmn*.


New Communication System

*System ID: EDOC_EXAMPLE

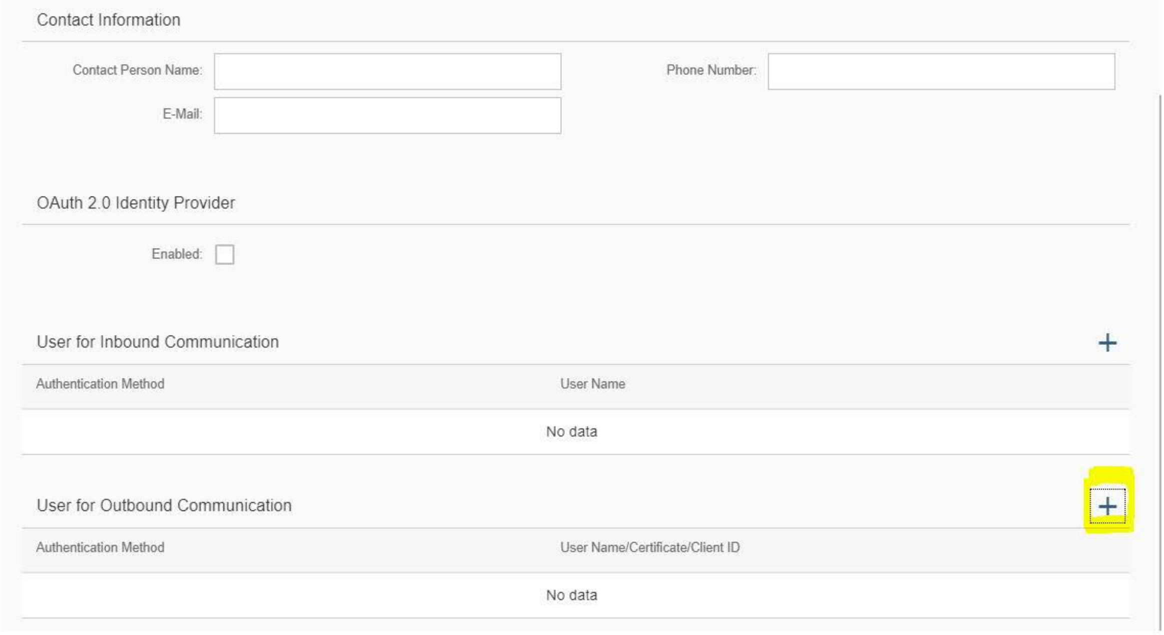
*System Name: EDOC_EXAMPLE

4. Click **Create**.
5. On the next page, enter the host name and port of your tenant.

You can find the host name for your SAP Cloud Platform Integration tenant, as follows:

a. From the menu on the left, choose **Monitor**.
b. Select **Manage Integration Content (All)**.
c. Search for the integration flow for the scenario you are configuring.
d. Find the host name from the **Endpoints** tab.
e. The composition of an endpoint URL is **https://<host name>/<path>**.

6. Scroll down and press the '+' button next to **User for Outbound Communication**.



Contact Information

Contact Person Name:

Phone Number:

E-Mail:

OAuth 2.0 Identity Provider

Enabled: □

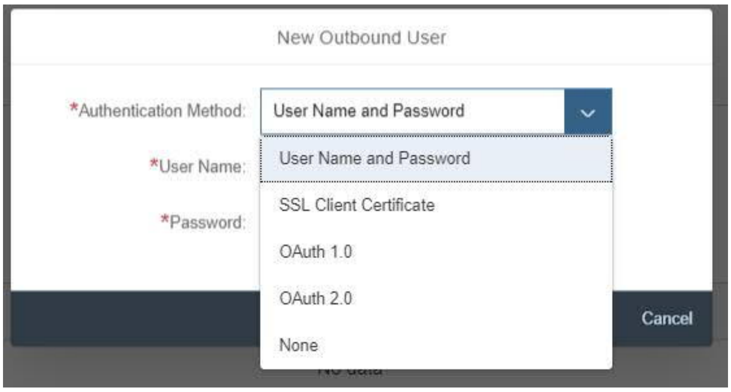
User for Inbound Communication

Authentication Method	User Name
No data	

User for Outbound Communication

Authentication Method	User Name/Certificate/Client ID
No data	

7. In the new popup window, select the appropriate authentication method to connect to your SAP Cloud Platform Integration tenant.



New Outbound User

*Authentication Method: User Name and Password

*User Name:

*Password:

- For the authentication method *User Name and Password*, 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 Cloud Platform Integration. See Creating Service Instances.

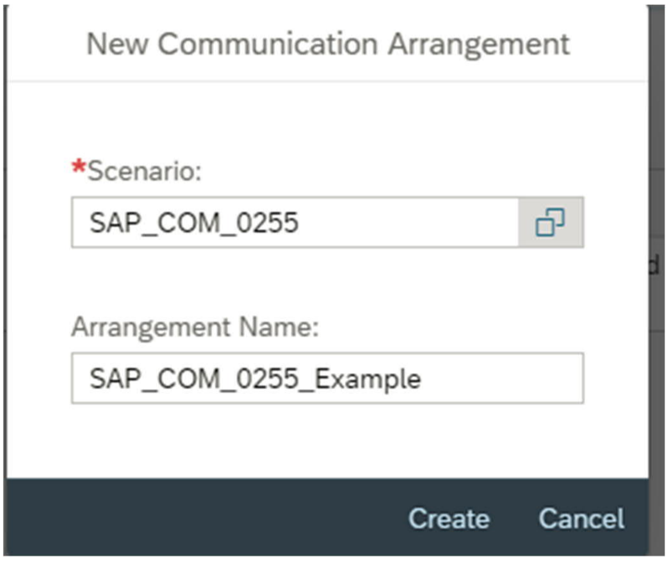
- For the authentication method *SSL Client Certificate*, select *X.509 SSL Client Certification* and choose Create. You must configure this certificate in SAP Cloud Platform Integration too. For that you create a service instance using the required grant type. You create the service key using the certificate uploaded to SAP S/4HANA Cloud. For more information, see Defining a Service Key for the Instance in the Cloud Foundry Environment.

8. Save the changes.

5.2 Configure a Communication Arrangement

1. Log in to your SAP S/4HANA Cloud tenant.
2. Find and launch the app **Communication Arrangements**.

3. Click **New**. In the pop-up window, enter the ID and description of your communication system.
4. In the new popup window, enter the scenario SAP_COM_0255 and an arrangement name. It is recommended to choose a name like SAP_COM_0255_<name of SAP Cloud Platform Integration tenant>. For example, SAP_COM_0225_EXAMPLE for a tenant host name beginning with example-tmn.

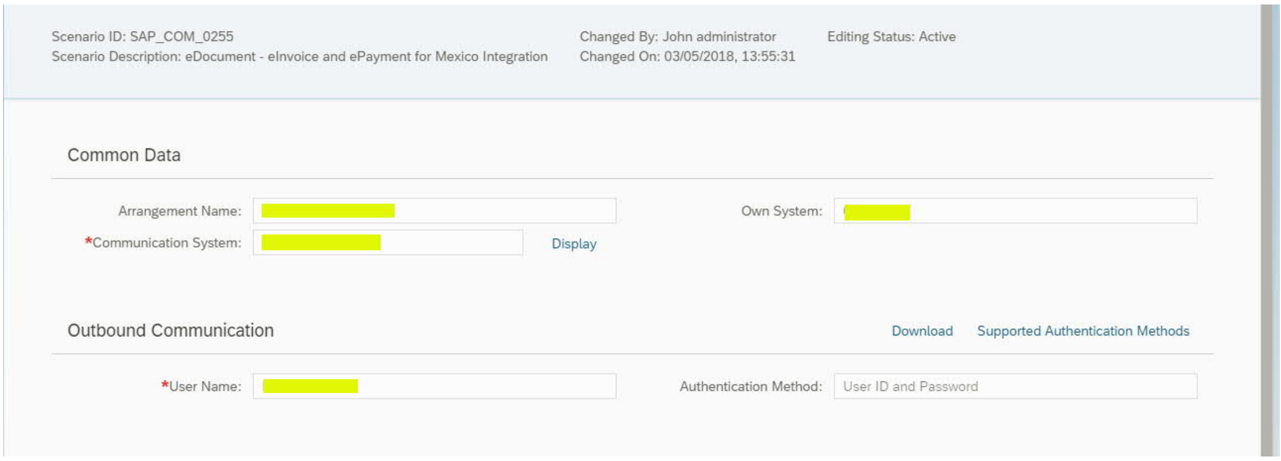


New Communication Arrangement

*Scenario: SAP_COM_0255

Arrangement Name: SAP_COM_0255_Example

5. Click **Create**.
6. In the new window, choose the communication system created in the previous step.



Scenario ID: SAP_COM_0255
Scenario Description: eDocument - eInvoice and ePayment for Mexico Integration

Changed By: John administrator
Changed On: 03/05/2018, 13:55:31

Editing Status: Active

Common Data

Arrangement Name:

Own System:

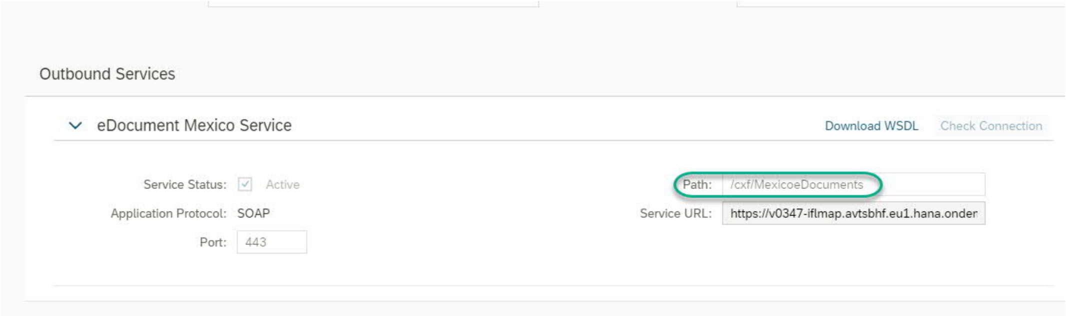
*Communication System:

Outbound Communication

*User Name:

Authentication Method: User ID and Password

7. Scroll down and enter the path part for your integration flow URL for all outbound services.



Outbound Services

eDocument Mexico Service

Service Status: ☑ Active

Application Protocol: SOAP

Port: 443

Path: /cxf/MexicoeDocuments

Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onder

8. Save the changes.

6 Appendix

6.1 Generate and Import Certificates

6.1.1 *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)

6.1.2 *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 Cloud Platform Integration:

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 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:

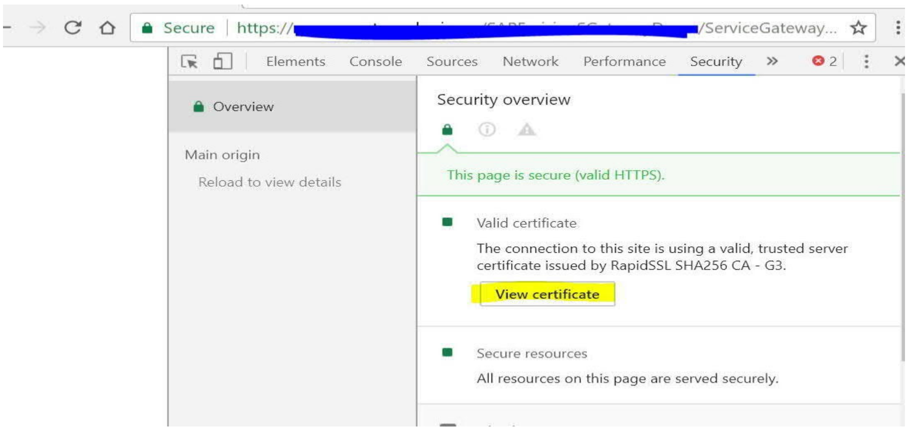
1. Click on *Create a New Keystore*, select the type of new Keystore as JKS.
2. Choose *Tools->Import Key Pair* and select the pkcs12 file created.
3. Enter a password and click on *Save*.
4. The created JKS file can be imported into SAP Cloud Platform Integration Keystore under a specific alias.

The same *alias* should be used as *external parameter* while deploying the iFlow.

6.1.3 *Import the Handshake Certificate*

Irrespective of whether the signing happens in SAP Cloud Platform Integration 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.



This page is secure (valid HTTPS).

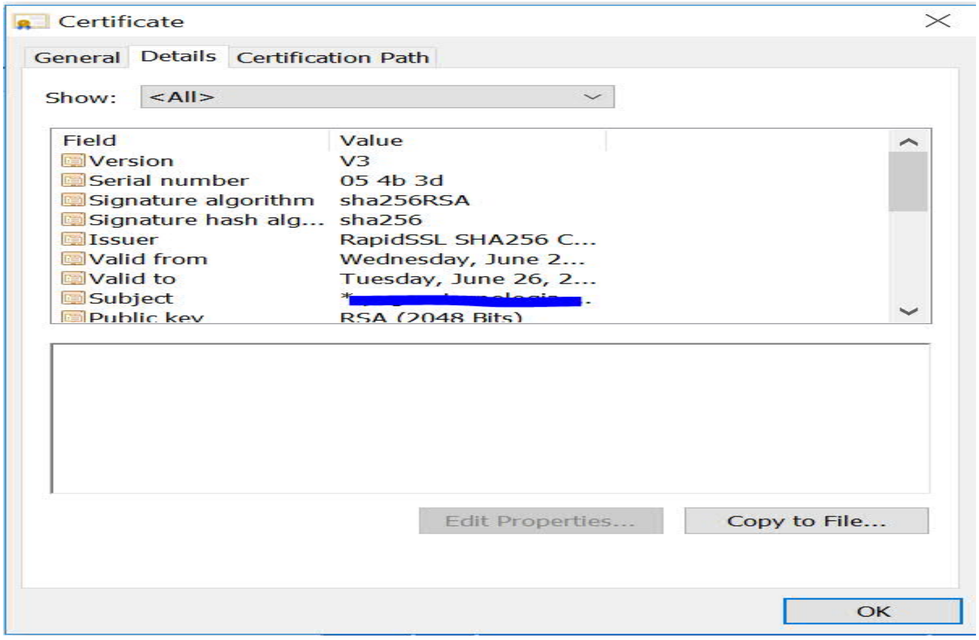
Valid certificate

The connection to this site is using a valid, trusted server certificate issued by RapidSSL SHA256 CA - G3.

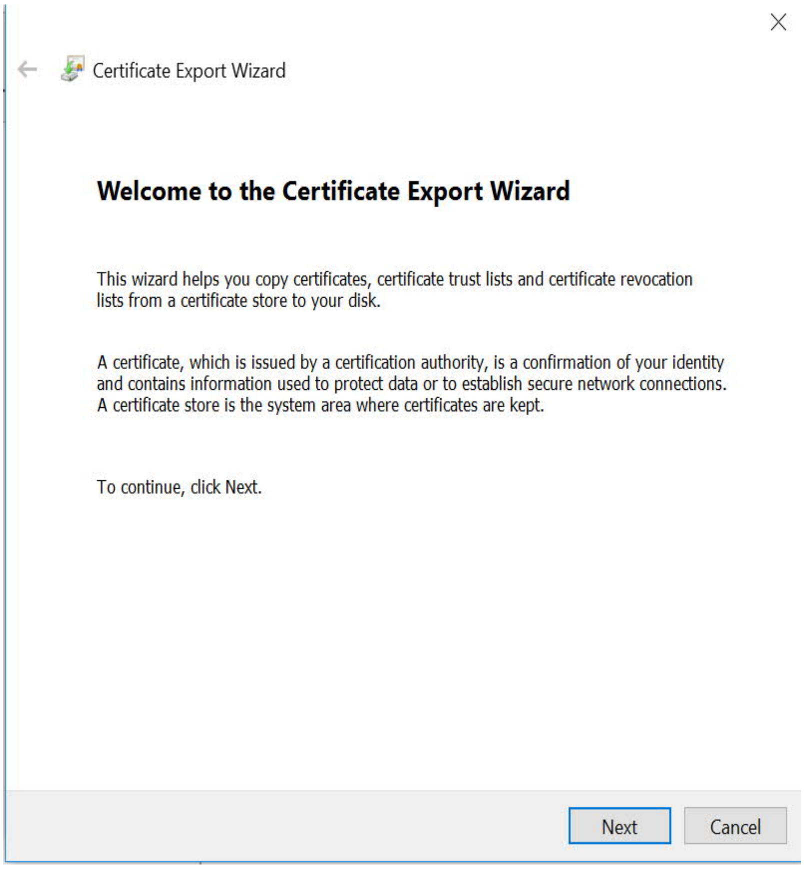
Secure resources

All resources on this page are served securely.

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 Cloud Platform Integration tenant keystore.



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	*[redacted].
Public key	RSA (2048 Bits)



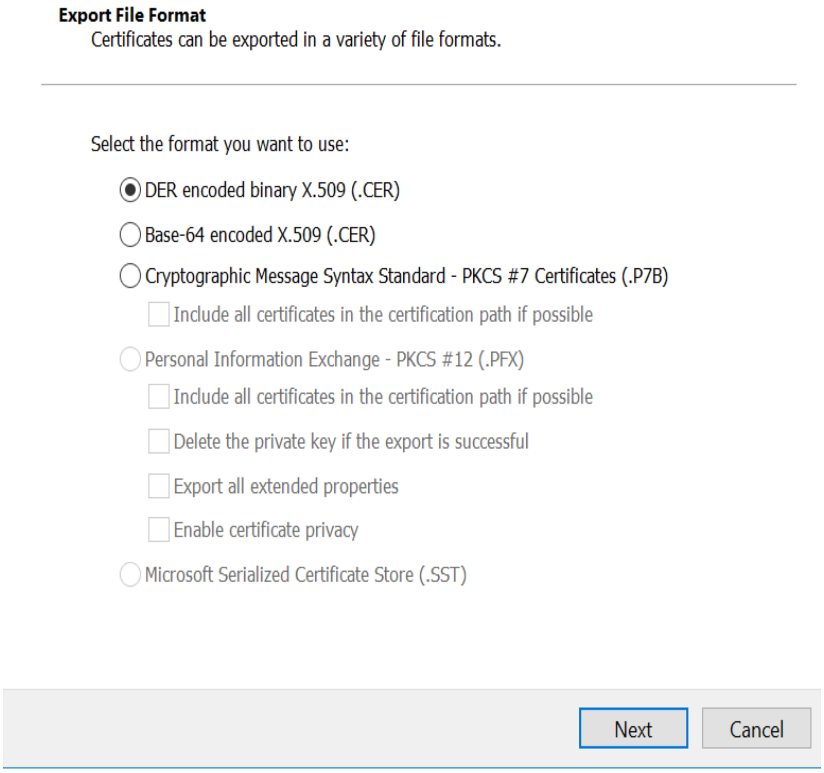
Certificate Export Wizard

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.



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)

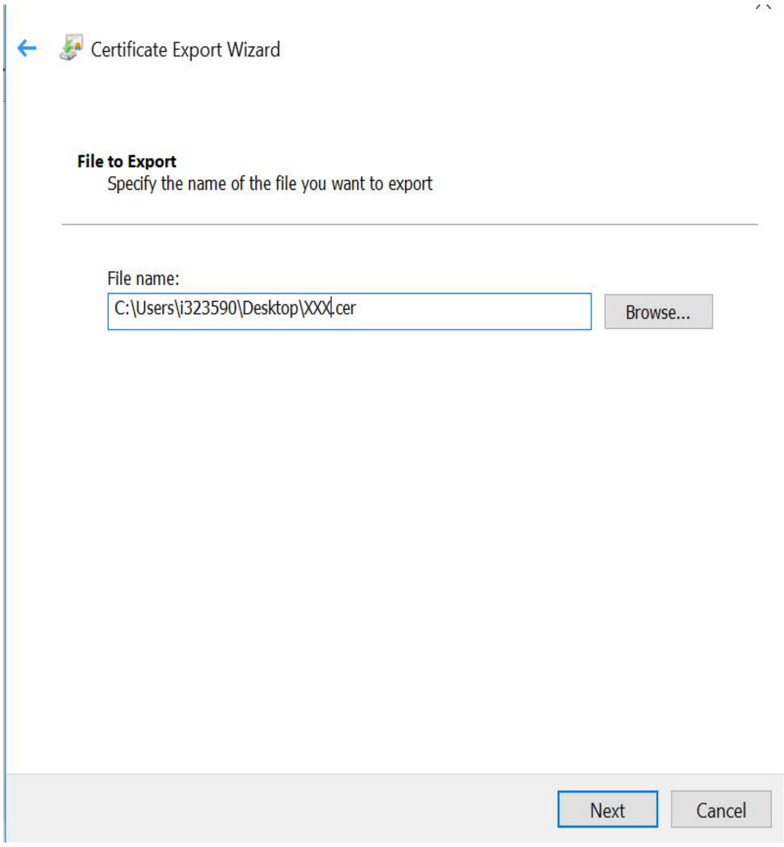
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



File to Export

Specify the name of the file you want to export

File name:

C:\Users\i323590\Desktop\XXX.cer

www.sap.com