S4HANA to MASTEREDI - Document Compliance Mexico

Table of Contents

1 Purpose

Quick start the development of Document Compliance: Electronic Documents for Mexico using Service provider MasterEDI.

2 Overview

This document details the configuration steps for sending the eInvoice or ePayment from SAP S/4HANA to SAT through PAC MASTEREDI.

Message Flow

- S/4 HANA sends the eDocument for Mexico from the EDOC_COCKPIT.
- SAP Cloud Integration signs eDocument and sends to MASTEREDI.
- MasterEDI will validate the eDocument and sends the invoice to SAT.
- The eInvoice approval / rejection status is returned to S/4 HANA.

2.1 Prerequisites/Assumptions

- The eDocument Full solution is installed in your test and production systems.
- Registration at SAT is completed.
- Certificate used for digital signature (private key + password) is provided by the customer.
- Please refer to SAP Note 2526771 for SAP ERP systems, and SAP Note 2565791 for SAP S/4HANA systems.
- For sender ERP/S/4HANA system Basic authentication is used.

2.2 Integration Specification

Type of Integration (outbound or inbound)	Outbound
Data Source Entities	S4HANA
Average Number of Records	1
Maximum number of Records	1
Processing Type	Request-Reply
Job Schedule	Flexible – As per business Requirement
Data Description (xml, comma delimited etc…)	XML
Target Location	MasterEDI

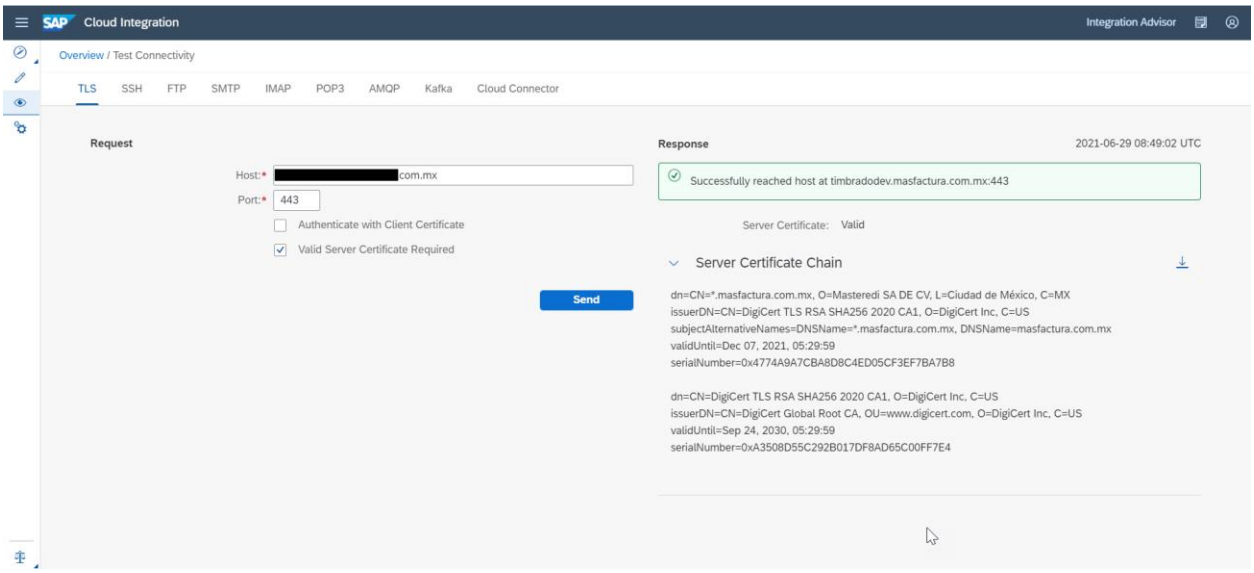
3 SAP Cloud Integration Configuration

3.1 Download the Retrieve and Save Public Certificates

- Open the worker node URL / Cloud Integration endpoint URL in your web browser.
- When prompted by the Website Identification window, choose View certificate.
- Select the root certificate, and then choose Export to file to save the certificate locally.
- Repeat these steps for each unique root, intermediate and leaf certificate, and repeat for both your test and production tenants.

3.2 SSL Certificates

The certificates for SSL connectivity with MASTEREDI should be deployed on Cloud Integration.



3.3 Secure Parameters deployed in Cloud Integration

- The secure parameters must be created in Manage Security Material with Type Secure Parameter.
- The secure parameters corresponding to MASTEREDI user and password need to be created in the below format prefixed with the RFcEmissor value:
  <RFcEmissor>_ME_USER
  <RFcEmissor>_ME_PASSWD

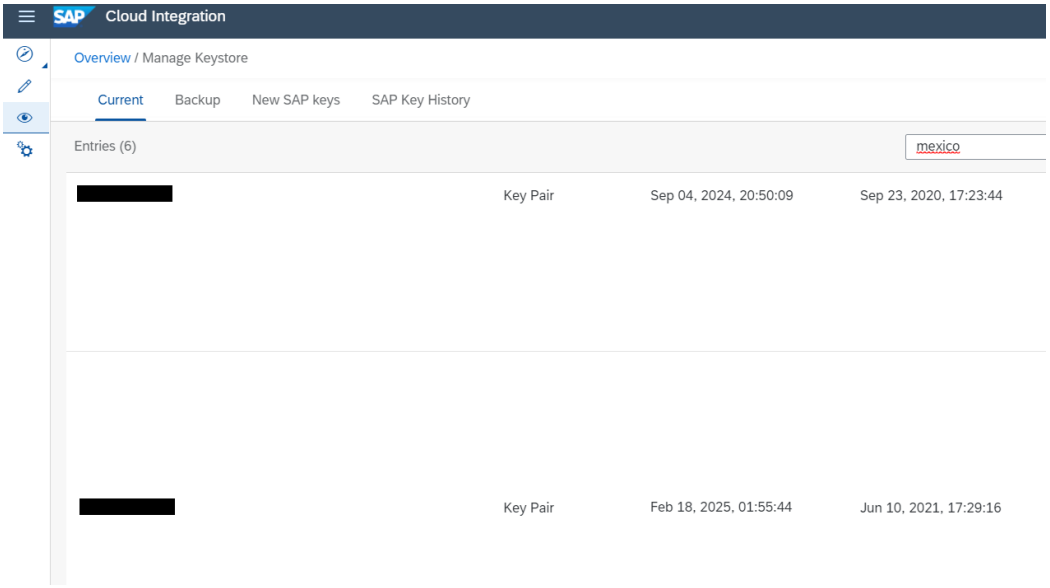
3.4 Deploy the Customer Certificate to SAP Cloud Integration

1.Follow the steps in Appendix to generate the PKCS#12 File from the certificate and key file provided by the customer.

2.Deploy the Customer Certificate to SAP Cloud Integration.

For deploying the customer certificate in the Key Store Explorer, follow the below steps:

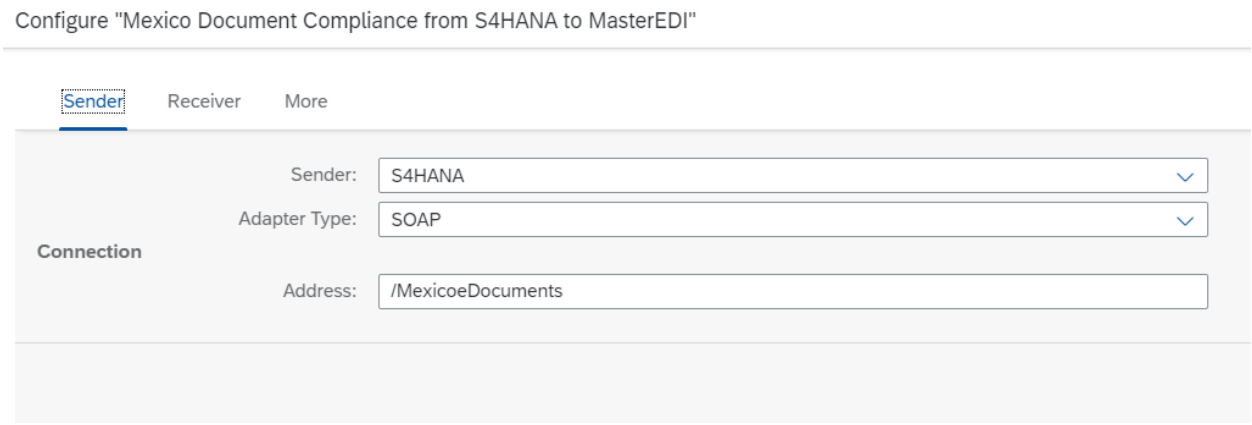
- Click on Add Key Pair.
- Enter the Alias. (This should be same as the RfcEmissor)
- Select the Key pair file to be uploaded.
- Enter a password and click on Save.



3.5 Endpoint Configuration

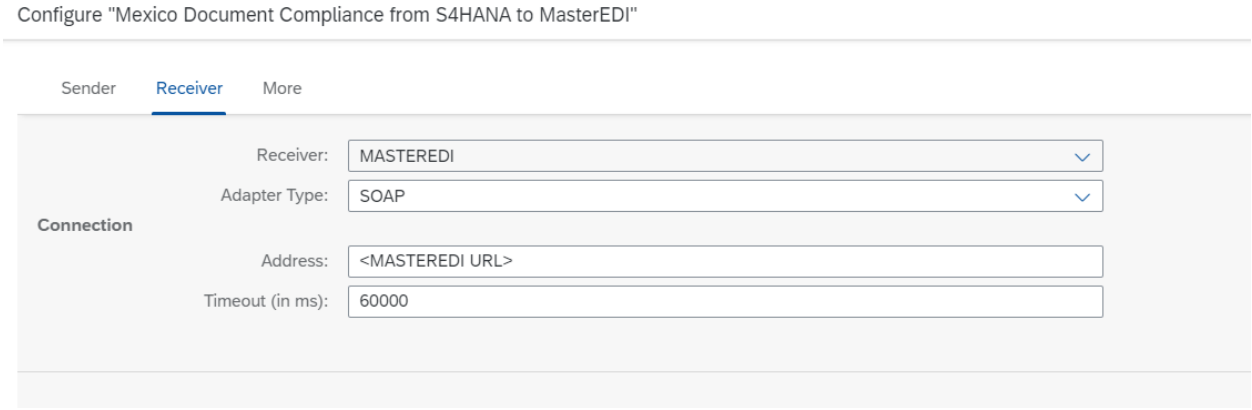
Soap Sender

Configure the Address for the connection from S/4HANA system.



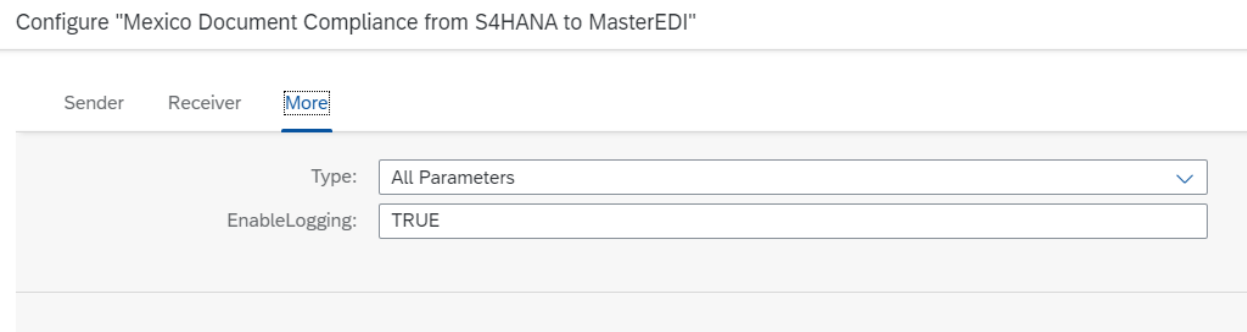
HTTP Receiver

Note: Import the server certificate in Cloud Integration tenant before configuring the channel.



Parameters Usage Guide

To enable payload logging, configure the Logging Parameter (possible values: TRUE/FALSE).



4 SAP S/4HANA Configuration

4.1 STRUST

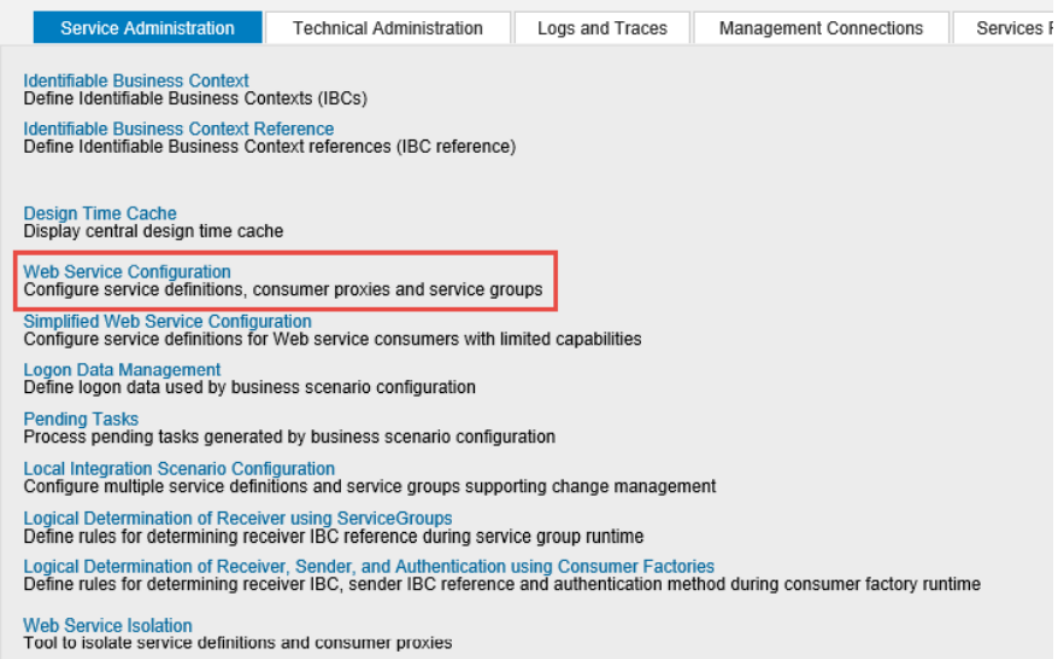
The certificates required to support connectivity between SAP back-end systems and SAP Cloud Integration is imported to STRUST.

- Access transaction STRUST in SAP S/4 HANA System.
- Select to the PSE for SSL Client (Anonymous).
- Switch to Edit mode.
- Select the Import certificate button.
- In the Import Certificate dialog box, enter or select the path to the required certificates.
- Select the certificates downloaded in section 3.1 and choose Enter.
- The certificates are displayed in the Certificate area.
- Choose Add to Certificate List to add the certificates to the Certificate List.
- Save your entries.

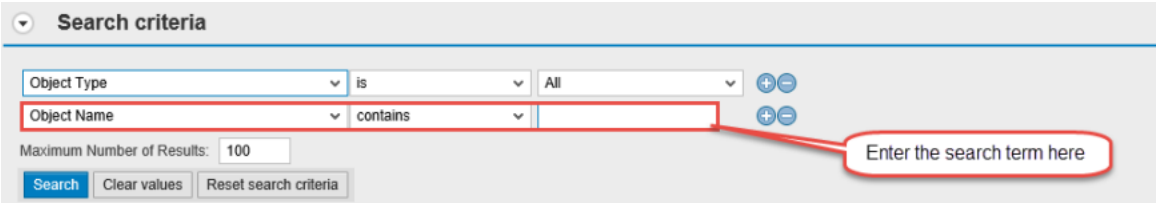
4.2 SOAMANAGER Configuration

You configure proxies which are needed to connect to the SAP Cloud Integration tenant via logical ports.

In your SAP back-end system, go to the SOAMANAGER transaction and search for Web Service Configuration.



Find the proxies for eDocument for Mexico with search term CO_EDO_MX*.



Configure the logical ports for the proxy listed in the following table:

Proxy Name	Logical Port Name	Path
CO_EDO_MX_CFDIE_DOCUMENTS	MX_EDOCUMENT	/cxf/MexicoeDocuments

5 Appendix

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)

Generate PKCS#12 File from the Certificate and Key File

Once OpenSSL for Windows is installed, follow the steps below to generate the keystore file that you can import into SAP Cloud Integration.

- Open command prompt in the folder where openssl is installed.
- 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

- Convert the certificate to pkcs8 format.

openssl x509 -inform DER -in aaa010101aaa_CSD_01.cer -outform PEM -out CSD_01.cer.pem

- Append the certificate and key file to one file.

copy CSD_01.key.pem+CSD_01.cer.pem CSD_01_chain.pem

- 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