SAP e-Way Bill for India - Integration with GSP (GST Suvidha Provider)

Via SAP Integration Suite Service in Cloud Foundry environment

GSP Integration Set Up Guide

Document History

Version	Date	Change
1.0	2020-06-12	First release of the GSP Integration Guide
1.1	2021-03-26	Updated the complete document to reflect the latest SAP Branding changes for SAP Business Technology Platform(BTP), SAP Integration Suite and Integration Flow. Updated section 4.2 ‘Deploy NIC user Credentials per GSTIN’

Contents

1 Glossary

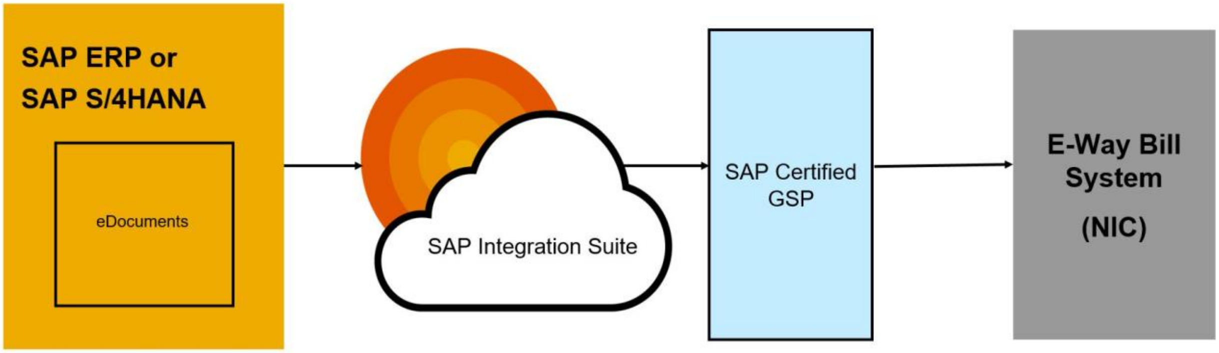
The table below lists the terms and abbreviations used throughout this document:

Term	Description
GST	Goods and Services Tax
GSP	GST Suvidha Provider
GSTIN	Goods and Services Taxpayer Identification Number
NIC	National Informatics Centre
CF	Cloud Foundry
SAP BTP	SAP Business Technology Platform

2 Introduction

Using the SAP Solution for eWay Bill India, you can generate eWay Bill Number as per the legal requirement in India.

The eWay Bill solution requires the integration between SAP Business Application (SAP ERP or SAP S/4HANA) and GSP. This document describes the steps to configure and deploy the SAP Integration Suite Flow to establish communication between SAP Business Application and GSP(s).



Note:

SAP offers two Cloud environments, namely **Neo** and **Cloud Foundry** and this document is intended for the setting-up of e-Way Bill India integration for Cloud Foundry environment.

3 Pre-requisites

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

1. You have installed in the test and productive systems all necessary SAP Notes for the eWay Bill Solution. Refer note: 2631687
2. You have performed all initial setup steps described in Initial Setup of SAP Integration Suite in Cloud Foundry Environment . After completing the Provisioning the Tenant step, you have created your own tenant URL. This is the URL (referred as WEB UI URL) needed to complete the steps described in the Configuration Steps section of this guide.
3. You have received the following information from your *GST Suvidha Provider (GSP)*:
   - GST Suvidha Provider (GSP) Integration/Set up Manual.
   - Trusted certificates from GSP for SSL handshake.
   - NIC Public Key Certificate (SAP Integration Suite expects the certificate in Base-64 encoded X.509 (*.CER*) format). For more details, see here.
   - For Sandbox access via GSP, request the NIC test user credentials from GSP directly
   - For Production access via GSP, refer here.
   - Other technical details such as API end point URLs for sandbox/production, GSP specific credentials, etc.
   - Two Integration Flows (.zip files) from GSP and save to any local location in your desktop.
     - GSP Integration Flow (Integration Flow specific to GSP)
     - Router Integration Flow (Routes eWay Bill request from SAP Business Application to specific GSP Integration Flow)

4 Configuration Steps in SAP Integration Suite

Perform the following steps:

1. Import SSL Certificates from GSP to SAP Integration Suite Tenant
2. Deploy NIC User Credentials per GSTIN
3. Deploy NIC Public Key Certificate
4. Deploying Integration Flow
5. Client Certificate-based Authentication Settings

Note:

The SSL certificate upload, Setting-up of user credentials, NIC Public Key Certificate Upload and authentication setup are all required to be done only during the initial set up of the eWay Bill Integration scenario. Subsequently, if there is an updated version of integration flow delivered, it is required to repeat only Step 4. However, in case there is a change in certificate from GSP or NIC, then step 1 or step 3 needs to be done accordingly.

4.1 Import SSL Certificates from GSP to SAP Integration Suite Tenant

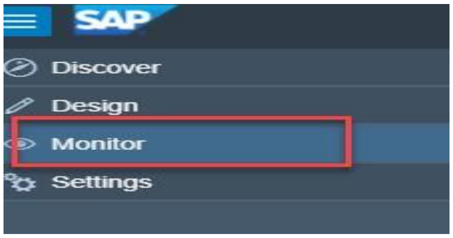
To set up an SSL connection between the SAP Integration Suite Tenant and GST Suvidha Provider (GSP), you must import the required security certificates into SAP Integration Suite Tenant Keystore.

Note:

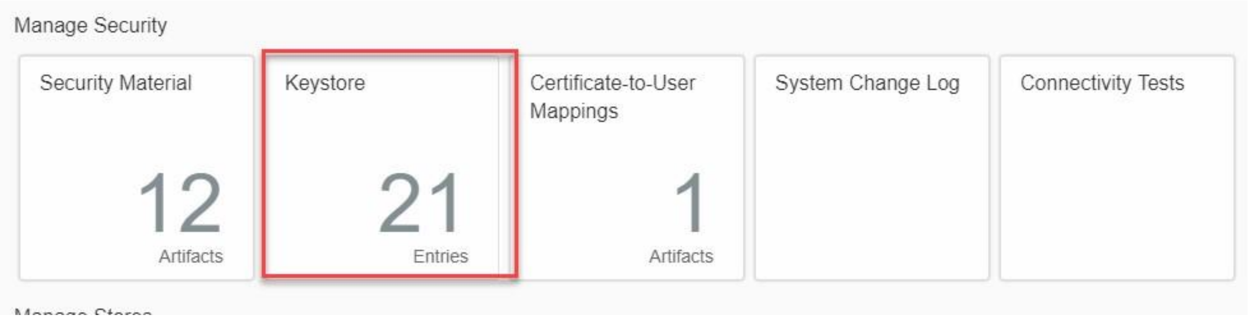
You receive these certificates from your GSP.

Procedure

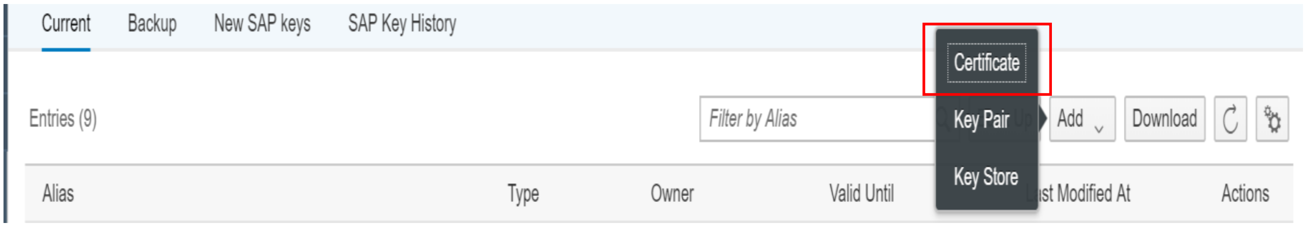
1. Access the SAP Integration Suite Tenant.
   After Provisioning the tenant as described in section Provisioning the Tenant, the URL will be created.
   Use this URL to go to the Web UI of the tenant.
2. To logon, enter your S user.
   If you get *HTTP Status 403* error, then send a mail to service@sap.com.
3. After successful login, from the menu in the upper left corner, choose *Monitor.*



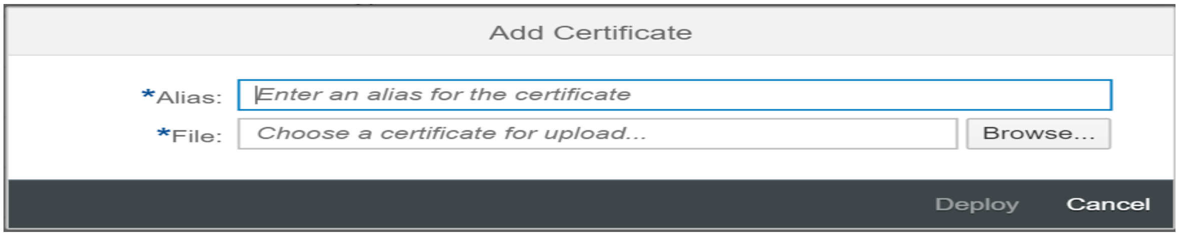
4. *Choose Manage Security and then Keystore.*



5. Click Add > **Certificate** > **Add Certificate**



6. Enter an alias to identify the certificate. Browse the certificate from local desktop and then Deploy.


Add Certificate
*Alias:
Enter an alias for the certificate
*File:
Choose a certificate for upload...
Browse...
Deploy
Cancel

Note:

To perform the above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**

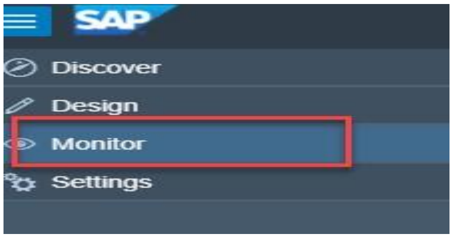
The certificate should be in Base-64 encoded X.509(.CER) format. Refer here.

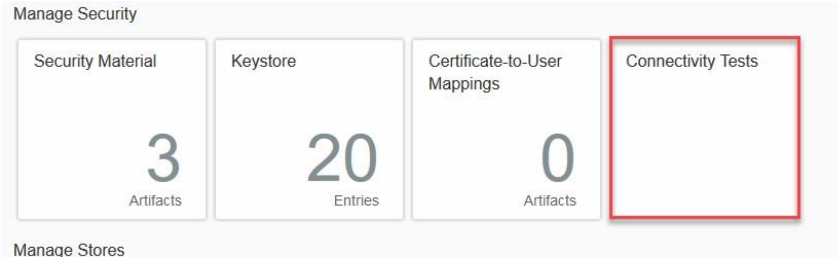
7. Check the connectivity with GSP.

   You can perform the Connectivity test with the GSP by using the feature TLS Connectivity Test as mentioned here.

   1. Run connectivity test using the *Monitor-> Manage Security- >Connectivity Tests.*
   2. *Enter the GSP Base URL without http(s). Enter port.*
   3. *Click* **Send**

      On successful connection, system displays successful response message.




Manage Security

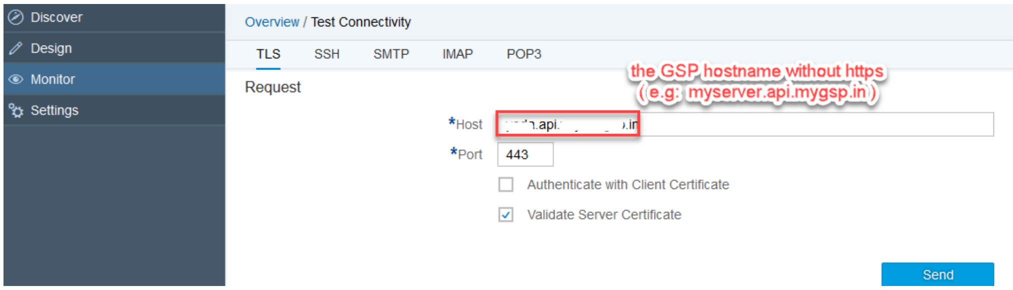
Security Material 3 Artifacts

Keystore 20 Entries

Certificate-to-User Mappings 0 Artifacts

Connectivity Tests

Manage Stores



the GSP hostname without https
(e.g: myserver.api.mygsp.in)

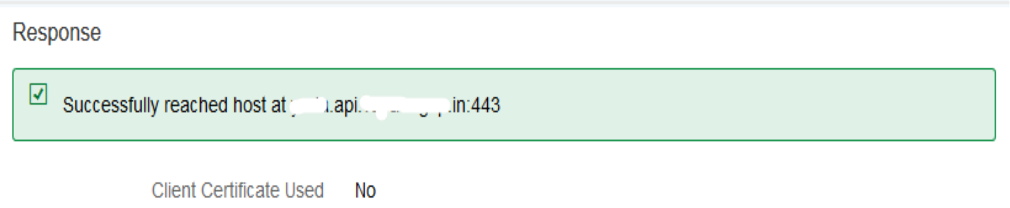
Request

*Host [redacted].api.[redacted].in

*Port 443

□ Authenticate with Client Certificate

☑ Validate Server Certificate


Response

☑ Successfully reached host at [redacted].api.[redacted].in:443

Client Certificate Used No

4.2 Deploy NIC User Credentials per GSTIN

Add NIC User Credentials entries per GSTIN to the User Credentials Service of SAP Integration Suite tenant by following the process mentioned here

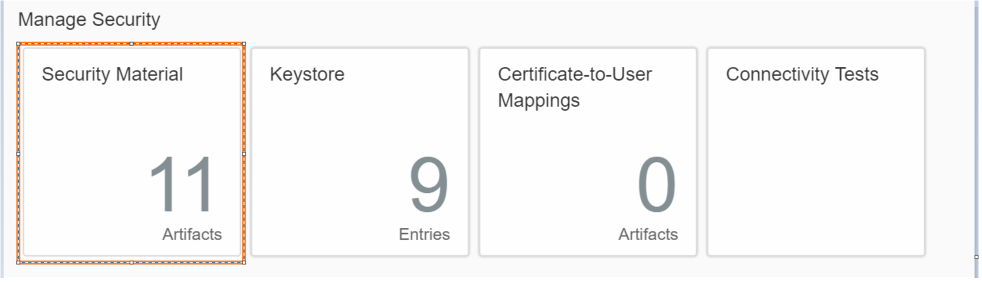
Note:

To perform above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**

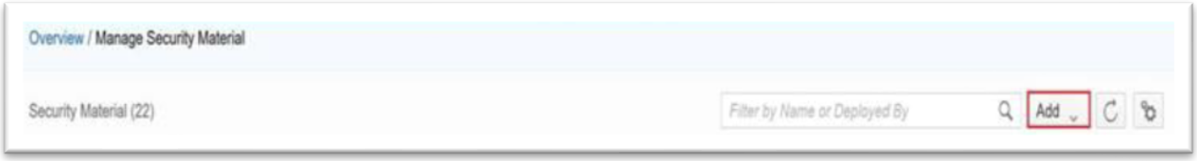
Refer GSP Registration on NIC Portal for details.

To add NIC User Credentials per GSTIN to SAP Integration Suite:

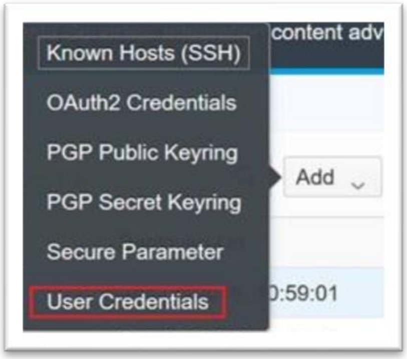
1. Navigate to Monitor > Manage Security > Security Material.



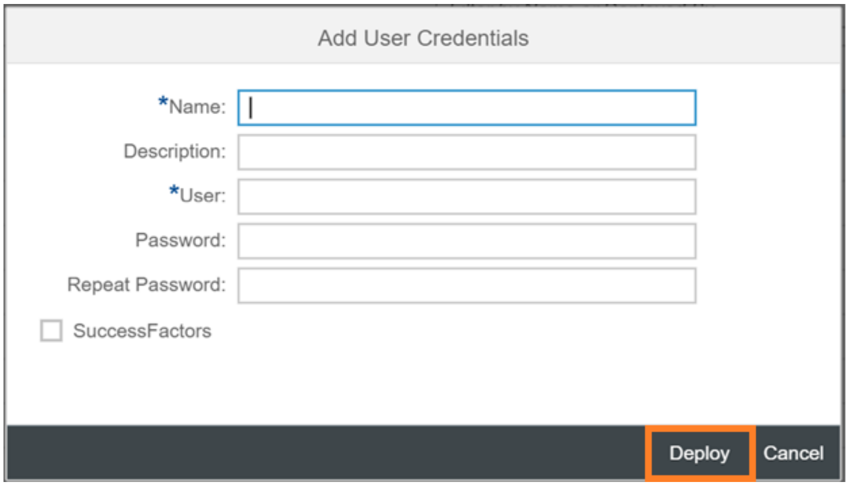
2. Add a new user credential.


Overview / Manage Security Material
Security Material (22)
Filter by Name or Deployed By
Add

3. Click User Credentials



4. Add and Deploy the user credentials


Add User Credentials

*Name:

Description:

*User:

Password:

Repeat Password:

□ SuccessFactors

Note:

In the Name field, enter the GSTIN of the business place to which the user belongs.

If the user credentials are created explicitly for eWay bill, then, maintain the name field with the suffix '_ewb' (Ex : 27AAAPI3182M002_ewb).

The suffix (_ewb) is case sensitive

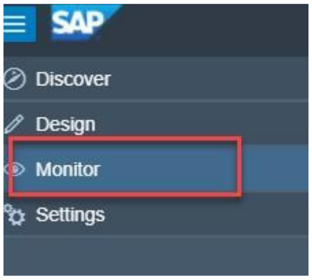
Name	GSTIN of the business place to which the user belongs / GSTIN of the business place with suffix '_ewb'
Description	Any relevant text (optional)
User	API User ID created in NIC portal (production) or received from GSP (pre-production)
Password/ Repeat password	Password

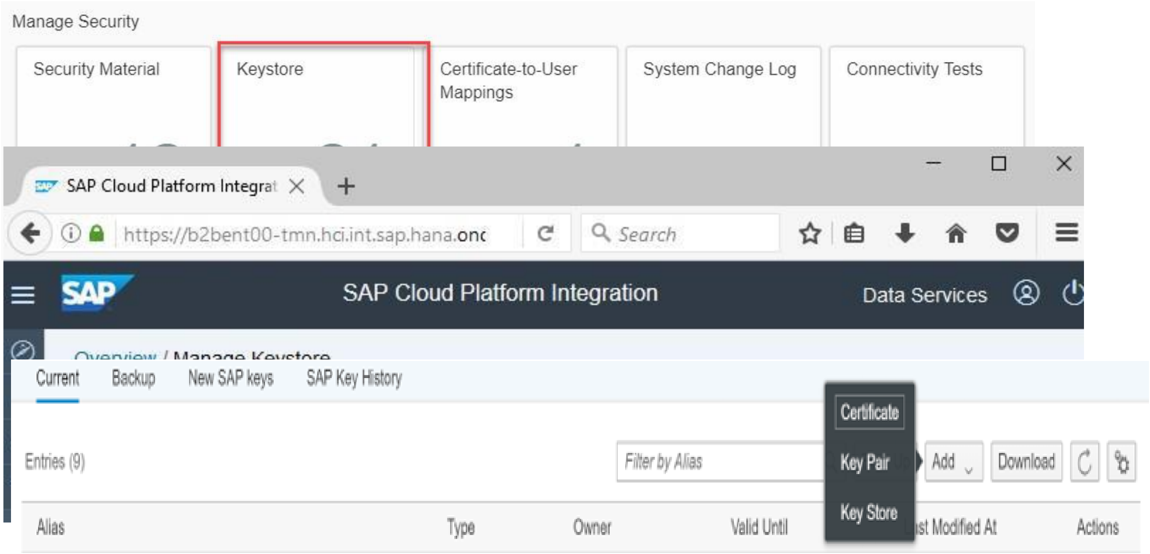
4.3 Deploy NIC Public Key Certificate

You need to add the NIC Public Key Certificate. You get this certificate from your GSP.

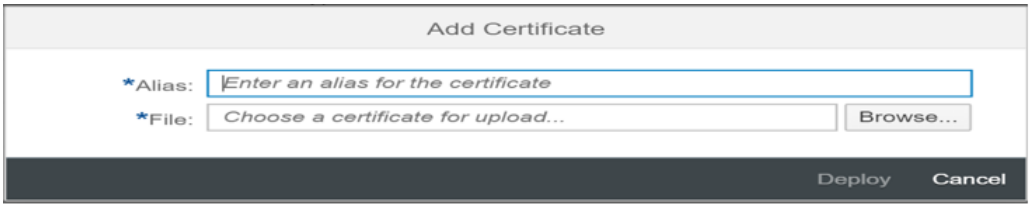
Follow the below steps to add the NIC Public Key Certificate to the SAP Integration Suite KeyStore.

1. Navigate to **Monitor** > **Manage Security** > **Keystore**



2. 

3. Enter an alias(**niccert**) to identify the certificate. Browse the NIC Public Key Certificate from local desktop.


Add Certificate
*Alias:
Enter an alias for the certificate
*File:
Choose a certificate for upload...
Browse...
Deploy
Cancel

4. Click **Deploy**

Note:

To perform the above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**

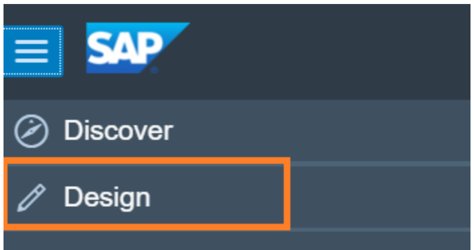
The certificate should be in Base-64 encoded X.509(.CER) format. For more information, see here.

4.4 Deploying Integration Flow

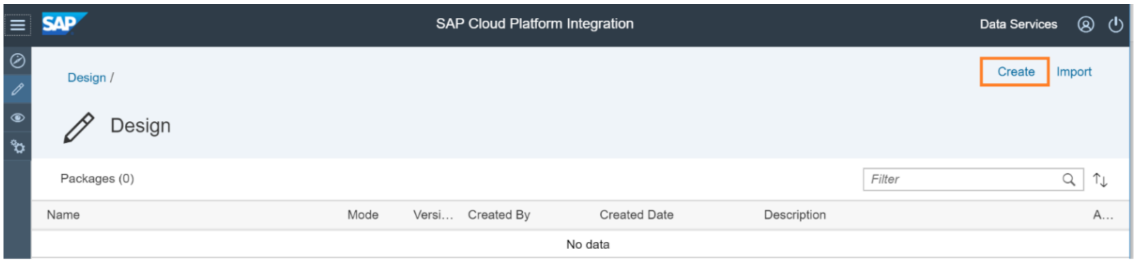
1. Creating content package: (one-time activity)

   To create a content package, follow the steps:

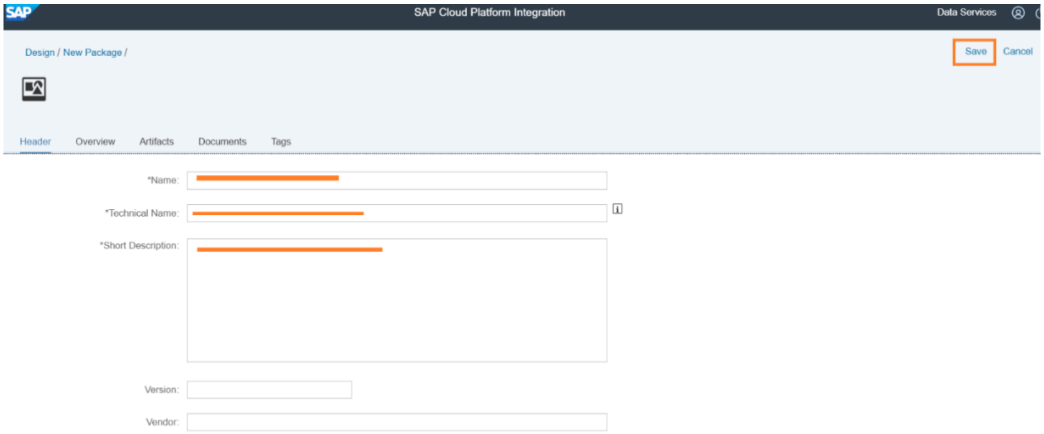
   1. Go to Design.



2. Choose Create.



3. Enter appropriate **Name** and **Description** and click **Save**.



The content package is created.

2. Updating content package

   When you already have previous version of integration flow deployed in your tenant and need to replace it with new integration flow, then follow below instructions

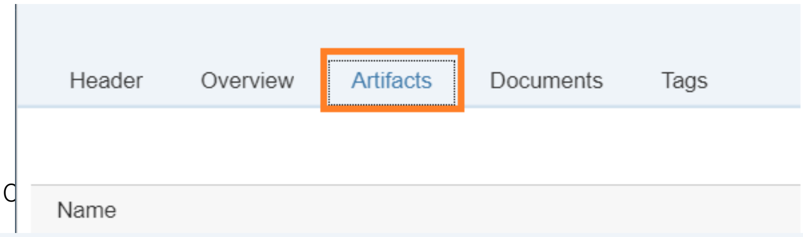
   - Choose the content package under which the previous integration flow is deployed.
   - Click on "Edit" button (seen in left side)
   - Go to artifacts tab, click on action icon configure. Copy the values of the fields maintained over there locally, as it can be used later if GSP confirms these parameters are valid or get the exact latest externalized parameters values. Close the configure pop-up screen.
   - Select the integration flow, click on action icon delete.

Note:

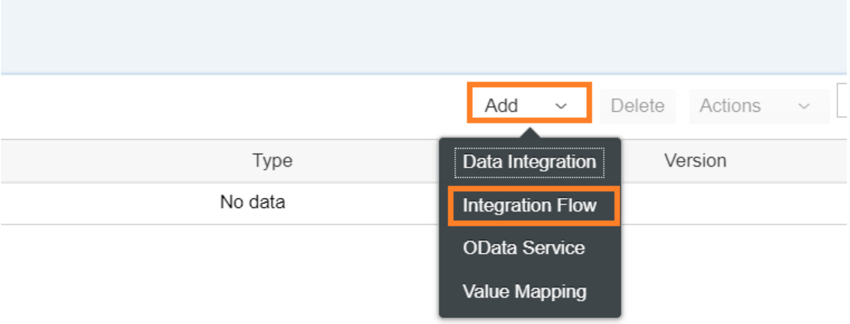
Repeat this 'Updating content package' step for each of the Router and GSP integration flows.

4.4.1 Deploying Router Integration Flow

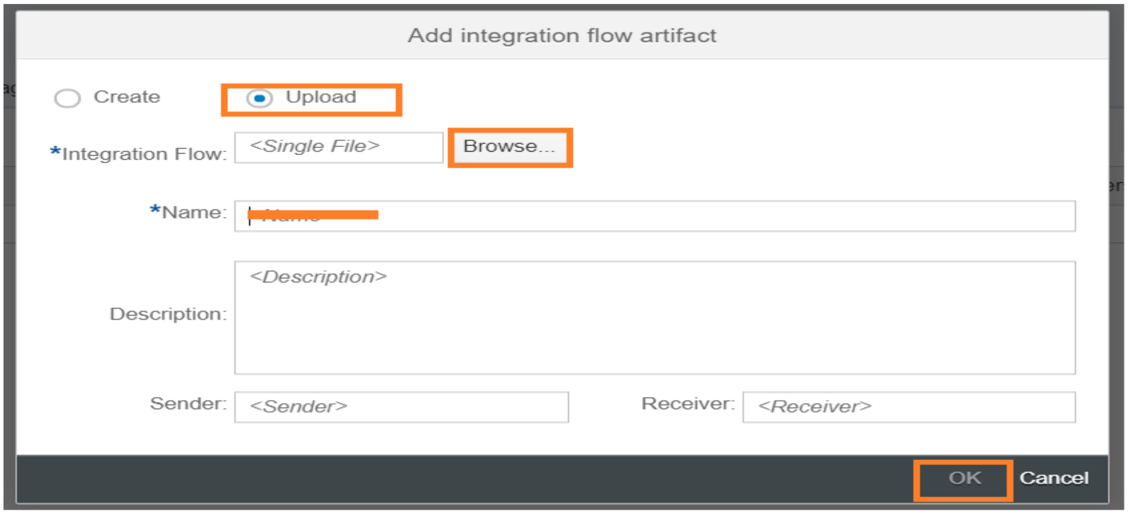
1. Within the same content package, Choose Artifacts.



2. C



3. Select Upload.
4. Browse for the appropriate integration flow (.zip file)
5. Enter the Name and Description and click Ok.

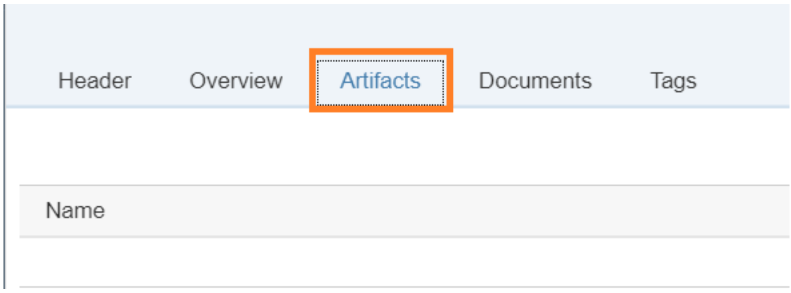


Integration flow is successfully added.

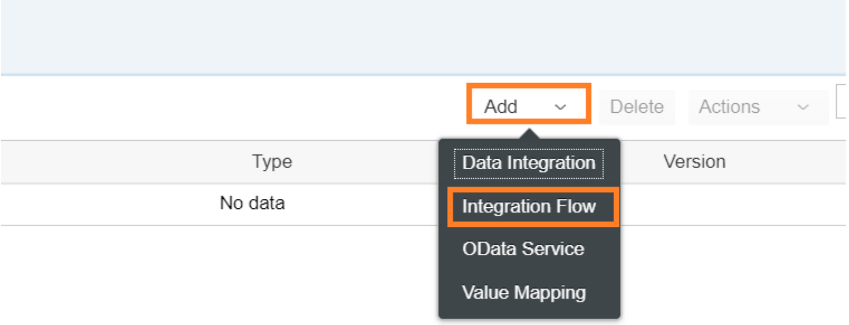
6. Select the Router integration flow.
7. Click **Deploy**.

4.4.2 Deploying GSP Integration Flow

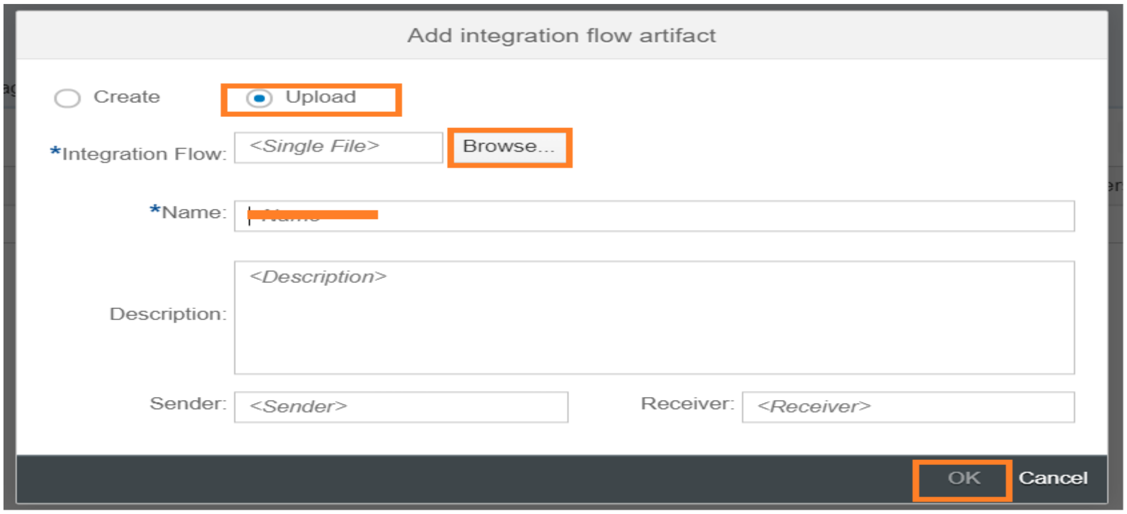
1. In the same content package, Choose Artifacts.



2. Click Add and choose Integration Flow.

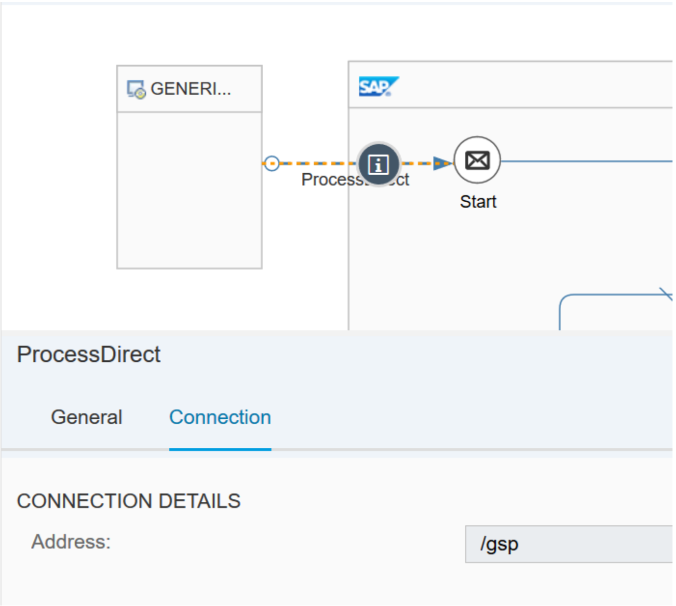


3. Select Upload.
4. Browse for the appropriate integration flow (.zip file)
5. Enter the Name and Description and click Ok.



Integration flow is successfully added. For more information, see here.

6. Select the GSP Integration Flow. The Integration Flow screen is displayed.
7. Click on the Process Direct as shown below.



ProcessDirect

General | Connection

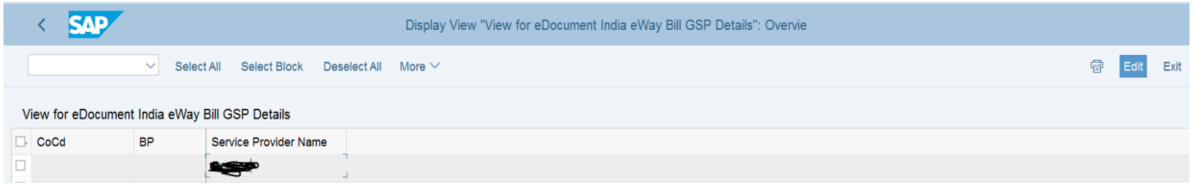
CONNECTION DETAILS

Address: /gsp

Choose the Connection tab. Copy the value in Address field without slash to the service provider name in the SAP Business Application -> sm30 -> view EDOINEWBGSPV

Note:

The value is case sensitive.



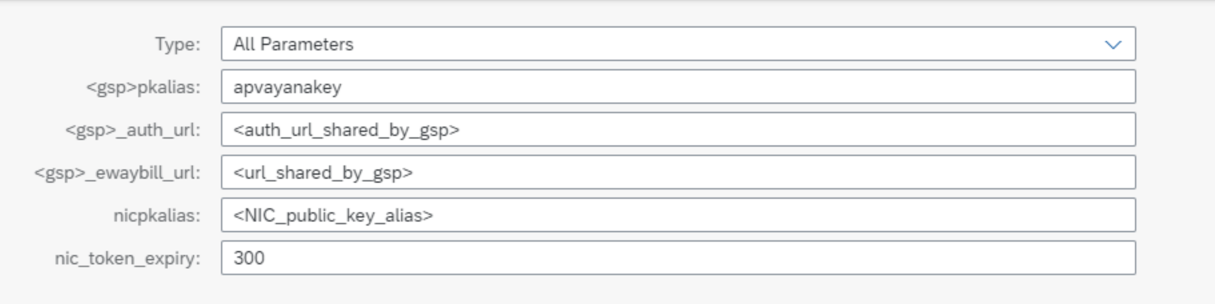
Display View "View for eDocument India eWay Bill GSP Details": Overvie

View for eDocument India eWay Bill GSP Details

CoCd	BP	Service Provider Name
		[redacted]

8. Click **Configure**.

   Choose the tab More and modify the parameters as shown below:



Type: All Parameters

<gsp>pkalias: apvayanakey

<gsp>_auth_url: <auth_url_shared_by_gsp>

<gsp>_ewaybill_url: <url_shared_by_gsp>

nicpkalias: <NIC_public_key_alias>

nic_token_expiry: 300

Note:

- In field nicpkalias, you enter the alias(**niccert**) of NIC Public Key Certificate.

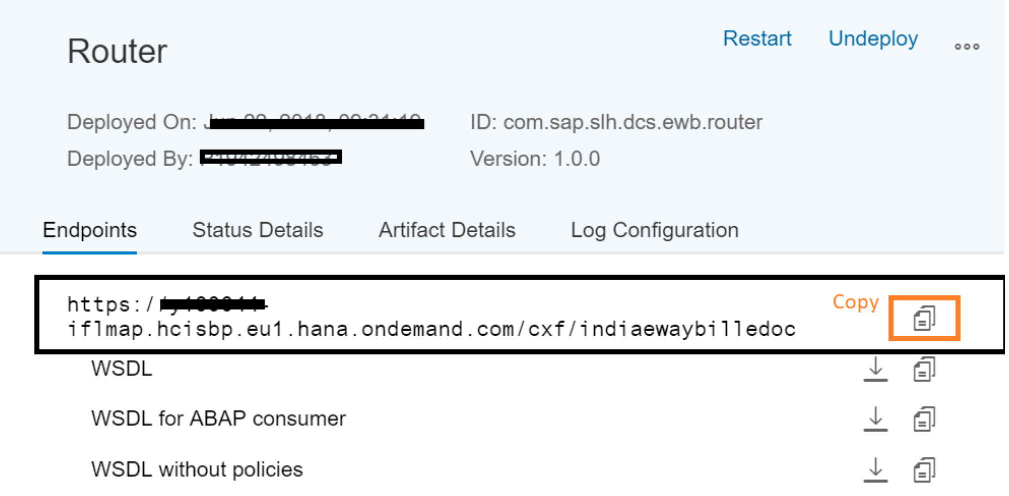
  You have already deployed NIC Public Key Certificate in KeyStore as described in section Deploy NIC Public Key Certificate

- You receive details about other fields from your GSP.

9. Save your changes.
10. Click **Deploy** to deploy the modified integration flow.

Note:

- After the successful deployment, verify that the integration flows are in the Started state by clicking Monitor -> Manage Integration Content.
- To obtain the Endpoint URL:
  I. Click Monitor > Manage integration Content
  II. Choose the Router integration flow.
  III. The Endpoint URL can be found on the right side of the page.



Deployed On: [redacted]

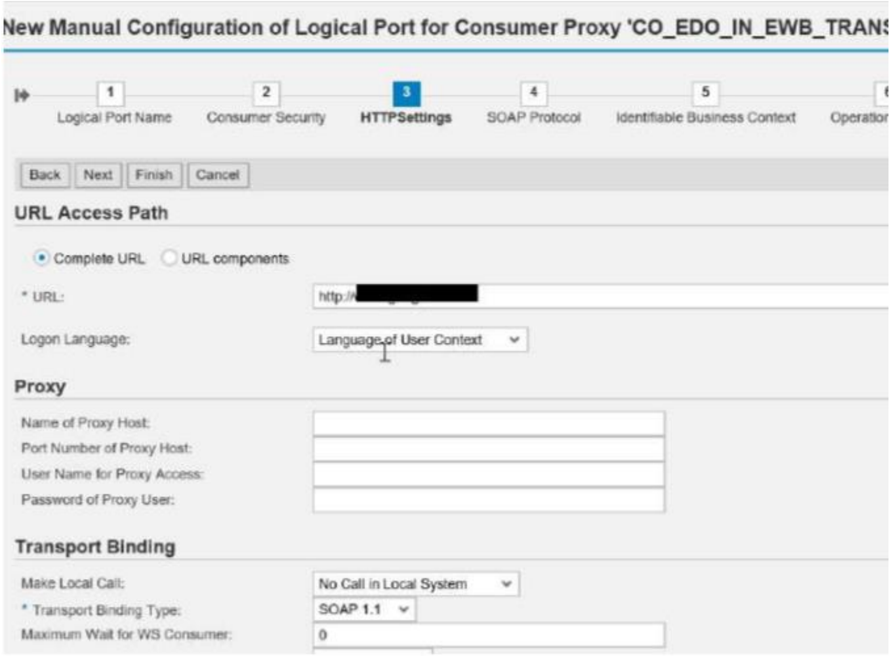
Deployed By: [redacted]

ID: com.sap.slh.dcs.ewb.router

Version: 1.0.0

```
https://[redacted]
iflmap.hcisbp.eu1.hana.ondemand.com/cxf/indiaewaybilledoc
```

IV. This URL must be configured in the SOA Manager.


New Manual Configuration of Logical Port for Consumer Proxy 'CO_EDO_IN_EWB_TRANS

URL Access Path

● Complete URL ○ URL components

* URL: http:/[redacted]

Logon Language: Language of User Context

Proxy

Name of Proxy Host:

Port Number of Proxy Host:

User Name for Proxy Access:

Password of Proxy User:

Transport Binding

Make Local Call: No Call in Local System

* Transport Binding Type: SOAP 1.1

Maximum Wait for WS Consumer: 0

- For issues with:
    - SAP Integration Suite tenant: Report under SAP component: LOD-HCI-PI-OPS
    - eWay Bill: Report under SAP component: XX-CSC-IN-EWB
    - GSP system access: Report through GSP defined support mechanism

4.5 Client Certificate-based Authentication Settings

For client certificate-based authentication and authorization in SAP Integration Suite Tenant in Cloud Foundry (CF), the private key pair provisioned with the tenant (alias `sap_cloudintegrationcertificate`) needs to be available in the Keystore (this certificate exists in the tenant by default) and the client certificate used for the inbound call to SAP Integration Suite needs to be maintained in the service key.

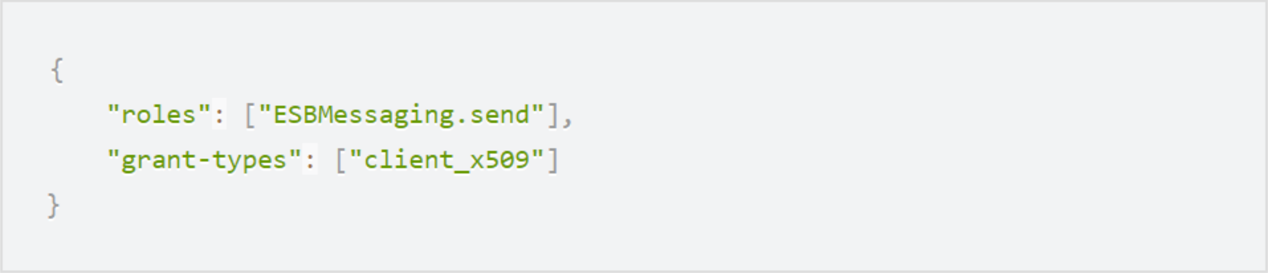
To enable certificate-based authentication between source system to SAP Integration Suite, the certificate presented by source system should be signed by one of the Certification Authorities (CA) approved by SAP BTP. Self-signed certificates cannot be used.

Refer to the below SAP help document on the list of supported CAs.

Load Balancer Root Certificates Supported by SAP

Details on setting up client certificate-based authentication in Cloud Foundry is as follows:

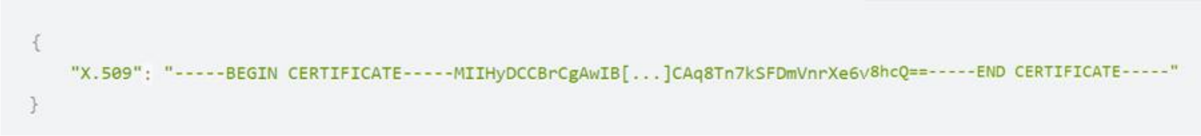
1. Download the client certificate corresponding to SSL client SSL standard PSE from strust.
2. When creating the service instance in CF, to enable client-certificate based authentication, specify “`client x509`” as the grant type.



```
{
    "roles": ["ESBMessaging.send"],
    "grant-types": ["client_x509"]
}
```

More details on creating service instances in Cloud Foundry can be found in the SAP online documentation at Creating a Service Instance in the Cloud Foundry Environment.

3. When creating the service key, provide a Name and in the Configuration Parameters, add the encoded client certificate (from step 1) in the following JSON format:



```
{
    "X.509": "-----BEGIN CERTIFICATE-----MIIHyDCCBrCgAwIB[...]CAq8Tn7kSFDmVnrXe6v8hcQ==-----END CERTIFICATE-----"
}
```

Note that the client certificate is a PEM-encoded X.509 certificate. Remove all line breaks, otherwise the user interface will not accept the entry.

More details on defining service keys in the Cloud Foundry environment can be found at Defining a Service Key for the Instance in the Cloud Foundry Environment.

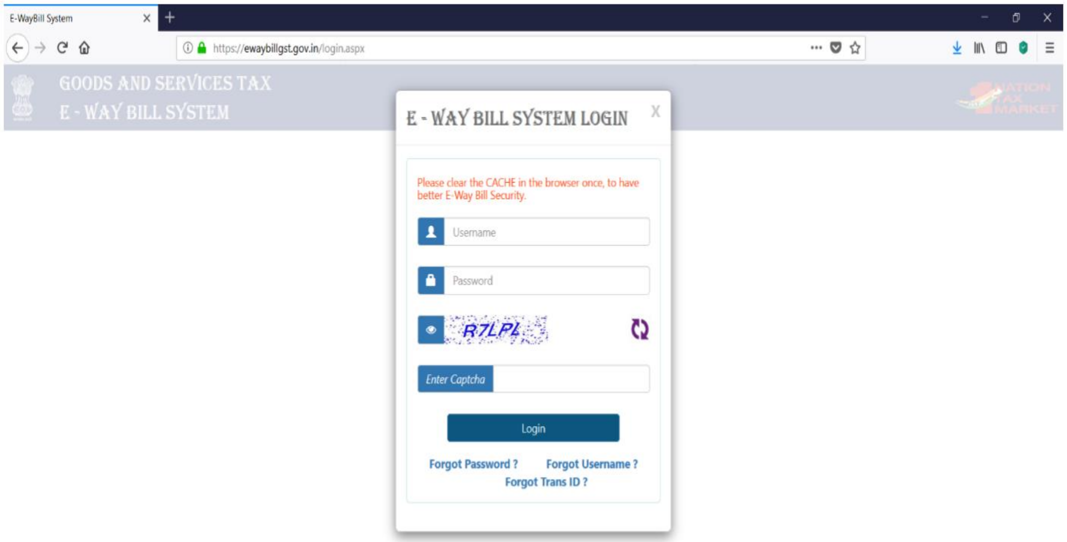
5 Appendix

5.1 GSP Registration on NIC Portal

To register your login credentials for e-Way Bill API access through GSP in NIC portal.

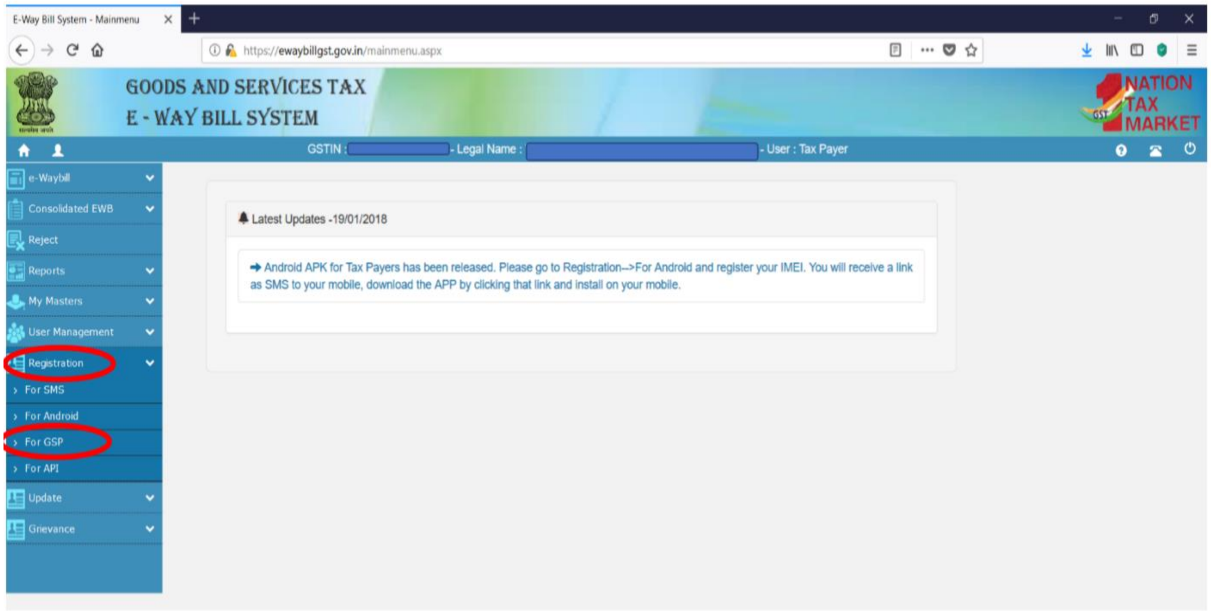
Procedure:

1. Login to NIC web portal (https://ewaybill.nic.in)



Please clear the CACHE in the browser once, to have better E-Way Bill Security.

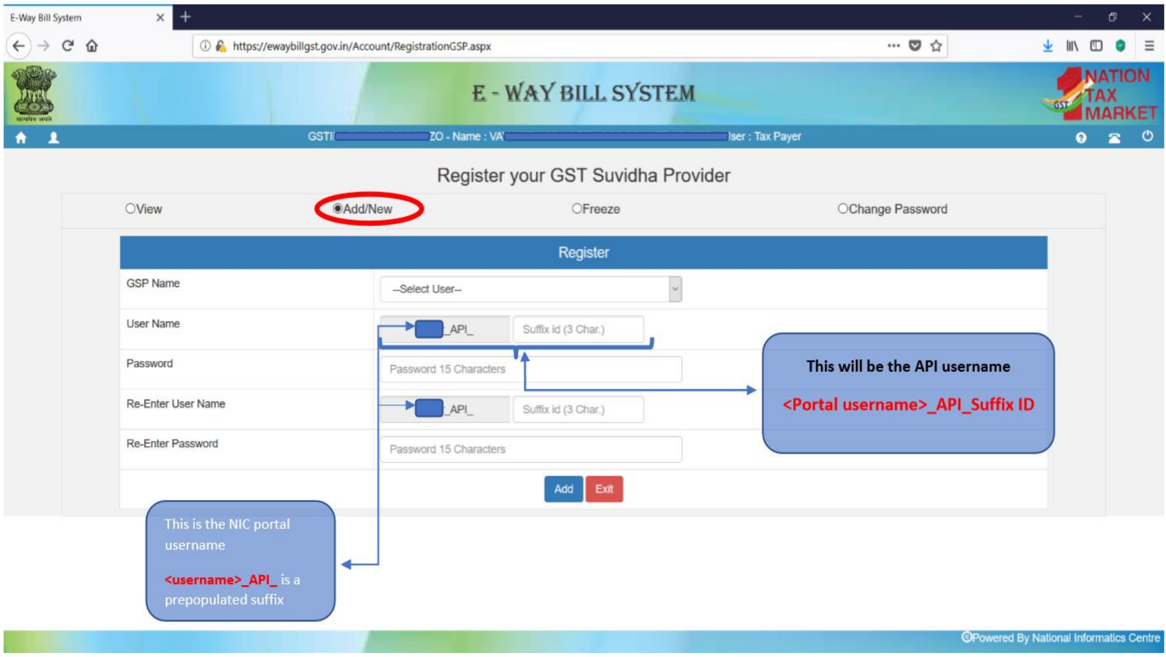
2. On the Menu bar in the left side margin of the webpage, click on Registration and then click on "For GSP"



GSTIN : [redacted] - Legal Name : [redacted] - User : Tax Payer

Latest Updates -19/01/2018

Android APK for Tax Payers has been released. Please go to Registration-->For Android and register your IMEI. You will receive a link as SMS to your mobile, download the APP by clicking that link and install on your mobile.



E-Way Bill System
https://ewaybillgst.gov.in/Account/RegistrationGSP.aspx
E - WAY BILL SYSTEM
NATION TAX MARKET
GSTI[redacted]ZO - Name : VA[redacted]ser : Tax Payer

Register your GST Suvidha Provider

○View ●Add/New ○Freeze ○Change Password

Register

GSP Name	--Select User--
User Name	[redacted]_API_ Suffix id (3 Char.)
Password	Password 15 Characters
Re-Enter User Name	[redacted]_API_ Suffix id (3 Char.)
Re-Enter Password	Password 15 Characters

Add Exit

This will be the API username

<Portal username>_API_Suffix ID

This is the NIC portal username

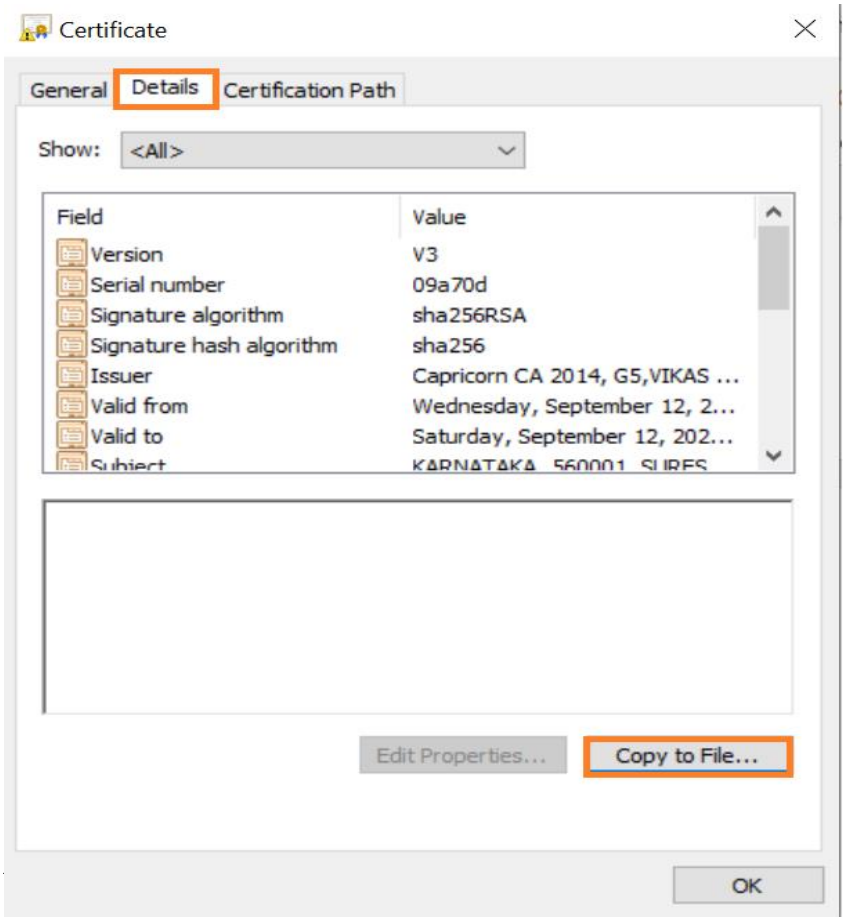
<username>_API_ is a prepopulated suffix

GSP).

4. Click on GSP Name dropdown box and select the appropriate GSP from the dropdown list of GSPs. Next, enter your username, password. Choose "Add" to register your login credentials for E-way Bill API access through appropriate GSP.

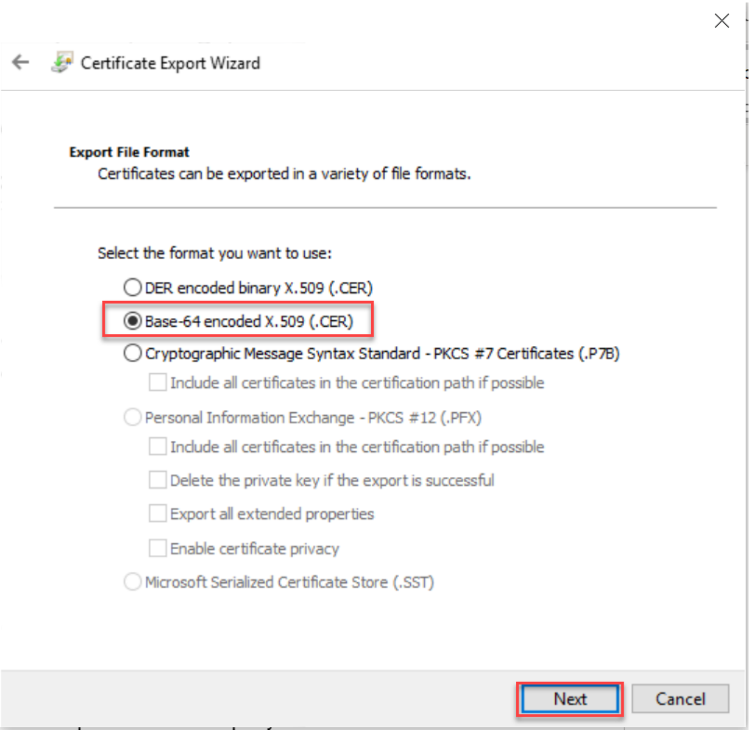
5.2 Exporting Certificate as Base-64 encoded X.509(.CER) format

1. Double click the certificate saved in the local desktop. Go to Details -> Copy to File...
   A new window opens. Click **Next**.



Field	Value
Version	V3
Serial number	09a70d
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Capricorn CA 2014, G5,VIKAS ...
Valid from	Wednesday, September 12, 2...
Valid to	Saturday, September 12, 202...
Subject	KARNATAKA 560001 SURES

2. Select Base-64 encoded X.509(.CER) and click Next.

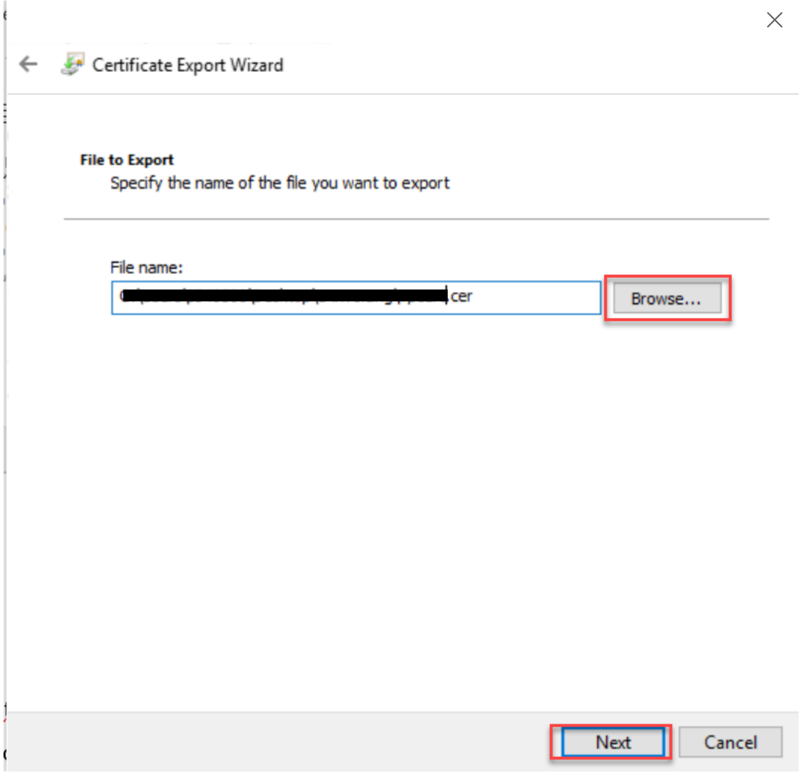


Export File Format
Certificates can be exported in a variety of file formats.

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)

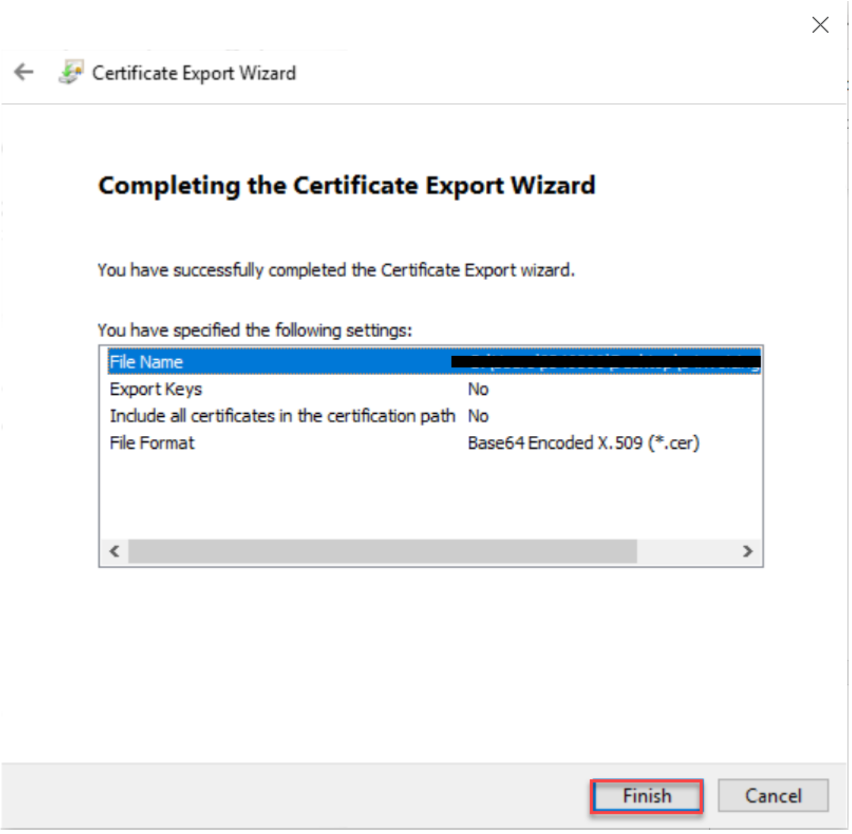
3. Browse the path where the certificate must be saved and click next.



File to Export
Specify the name of the file you want to export

File name:
[redacted]cer

4. Click Finish. Certificate will be saved in the selected location.



Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	[redacted]
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

5.3 Useful links:

- SAP Integration Suite: https://help.sap.com/viewer/product/CLOUD_INTEGRATION/Cloud/en-US
- SAP Integration Suite – Overview of Authorization Groups:
  https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/4b4ba1c553474259b5be661f4ef0702c.html
- SAP Integration Suite – User Credentials:
  https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/6912d63bbbc64aee8bbd4ff10314c60c.html
- SAP Integration Suite – Importing a Keystore:
  https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/0db193a325a94675928e717c9310734a.html
- SAP Integration Suite – Importing a Certificate:
  https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/03cf78a217574e7abd75bfbba990c085.html