**GSP Integration Guide** **CUSTOMER**

Document Version: 1.1 – 2021-03-25

# SAP Solution for eWay Bill India - Integration of SAP ERP or SAP S/4HANA with GST Suvidha Provider: Cloud Foundry

# Typographic Conventions

| Type Style | Description |
| --- | --- |
| *Example* | Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.<br>Textual cross-references to other documents. |
| **Example** | Emphasized words or expressions. |
| `EXAMPLE` | Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE. |
| `Example` | Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools. |
| **`Example`** | Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation. |
| **`<Example>`** | Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system. |
| `EXAMPLE` | Keys on the keyboard, for example, `F2` or `ENTER`. |

# Document History

| Version | Date | Change |
| --- | --- | --- |
| 1.0 | 2020-06-12 | First release of the GSP Integration Guide |
| 1.1 | 2021-03-25 | Updated the complete document to reflect the latest SAP Branding changes for SAP Business Technology Platform(BTP), SAP Integration Suite and Integration Flow. |

# 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 |

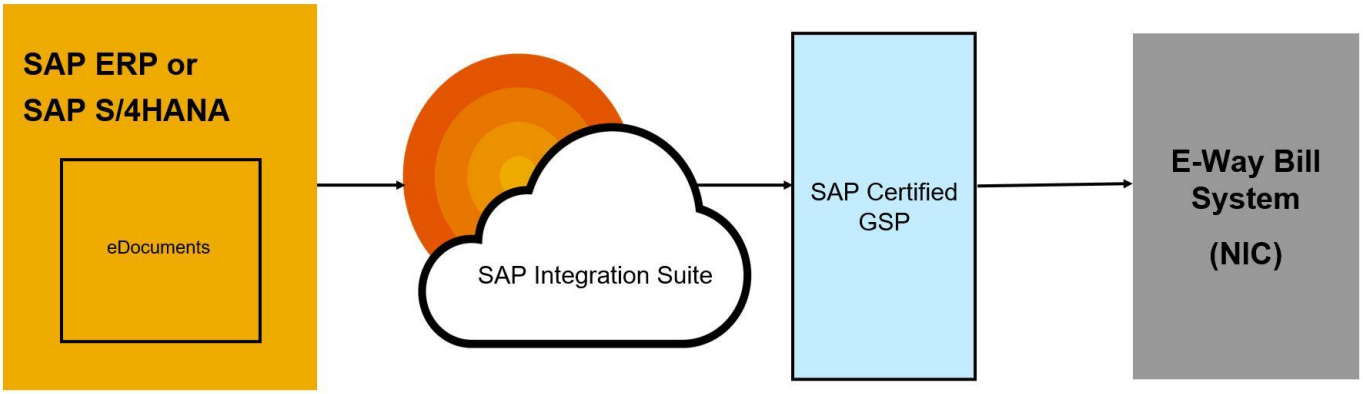
# 2 Introduction

Using the SAP solution for eWay Bill India, you can generate eWay bill number as per the legal compliance in India. The eWay bill solution requires the integration between SAP ERP or SAP S/4HANA and GSP(s). This following documentation describes the steps to adapt and deploy SAP Integration Flow to establish communication between SAP ERP or SAP S/4HANA and GSP(s).

### Note

* If you are using SAP certified GSP, you get the GSP specific pre-built integration flow and the documentation to implement the integration flow from your respective GSP(s). We recommend that you use the document provided by your GSP to implement the integration flows. To view the list of SAP certified GSPs use the SAP Note 2889709.

* If you are using non-SAP certified GSP, use this document to adapt the *GSP Integration Template* as per your company needs.




### 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 Prerequisites

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 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)*:
   - GSP Integration Manual
   - Certificates for SSL handshake

# 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. Adapt and Deploy SAP 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

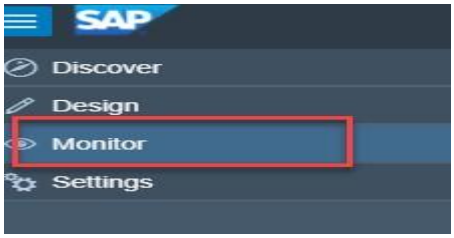
To set up an SSL connection between the SAP Integration Suite Tenant and GST Suvidha Provider (GSP), you must import the required security certificates into SAP Integration Suite Tenant Keystore.

### Note

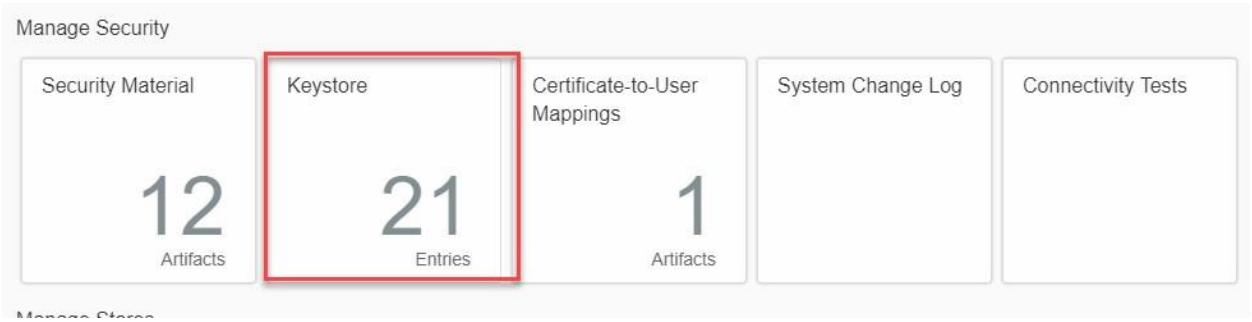
You receive these certificates from your GSP. The GSP should provide the certificate in the .CER format.

## Procedure

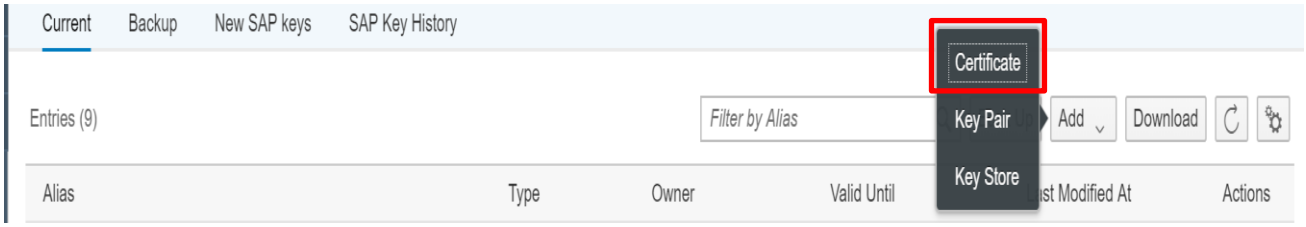
1. Access the SAP Integration Suite Tenant.
   After Provisioning the tenant as described in section Provisioning the Tenant, the URL will be created.
   Use this URL to go to the Web UI of the tenant.
2. To logon, enter your S user.
   If you get *HTTP Status 403* error, then send a mail to service@sap.com.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



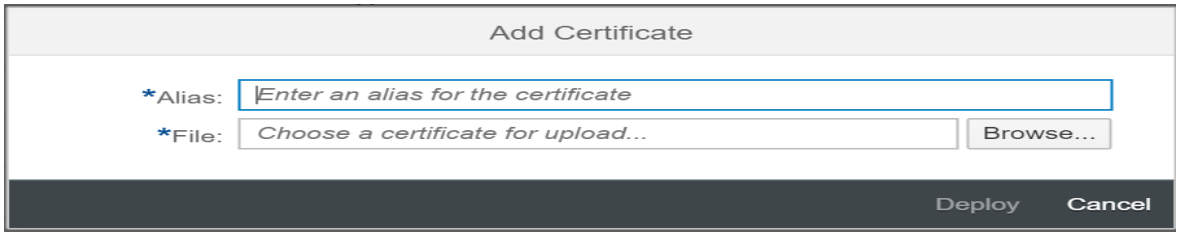

4. *Choose Manage Security and then Keystore.*




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



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




## Note

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

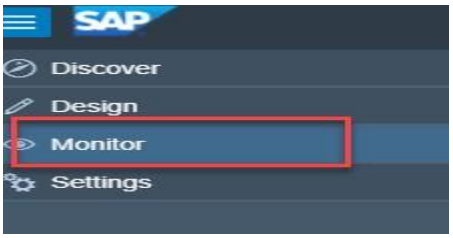
The certificate should be in Base-64 encoded X.509(.CER) format. Refer here.

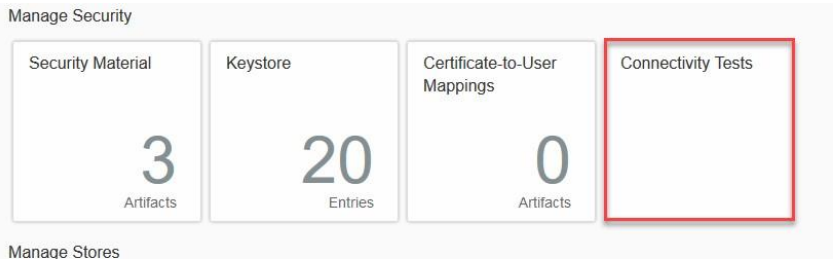
7. Check the connectivity with GSP.

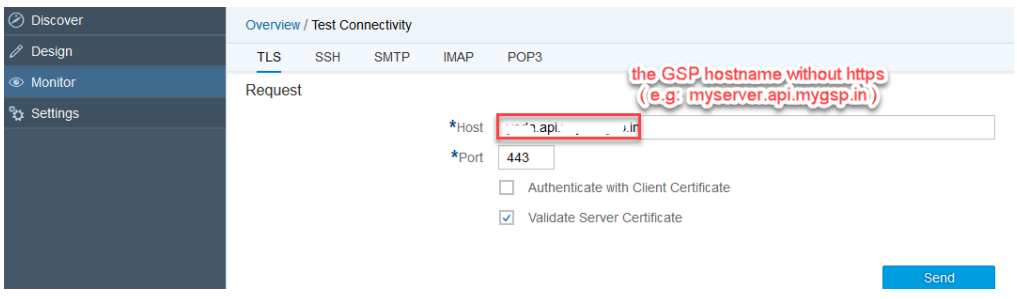
   You can perform the Connectivity test with the GSP by using the feature TLS Connectivity Test as mentioned here.

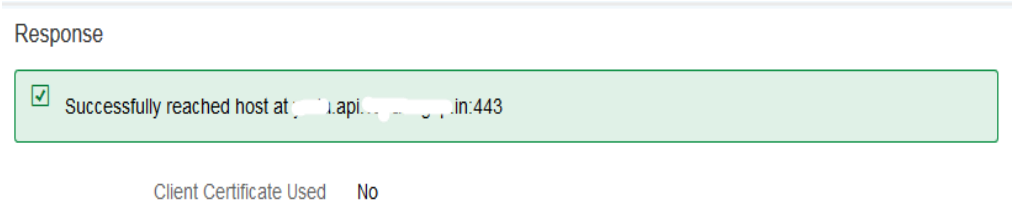
   1. Run connectivity test using the *Monitor-> Manage Security- >Connectivity Tests.*
   2. *Enter the GSP Base URL without http(s). Enter port.*
   3. *Click* **Send**

      On successful connection, system displays successful response message.



## 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

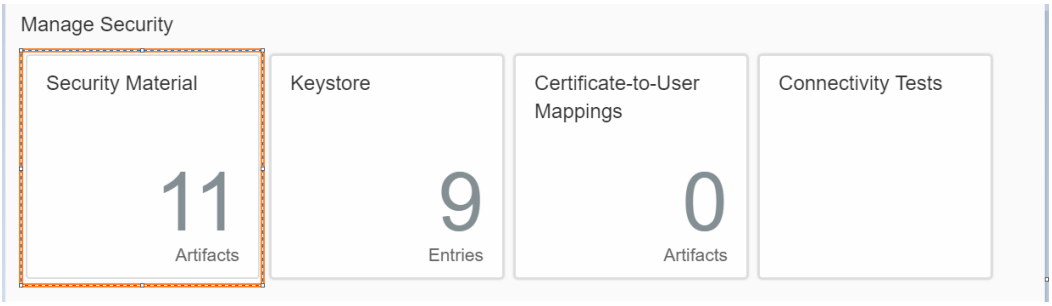
To perform the above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**

Refer GSP Registration on NIC Portal for details.

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

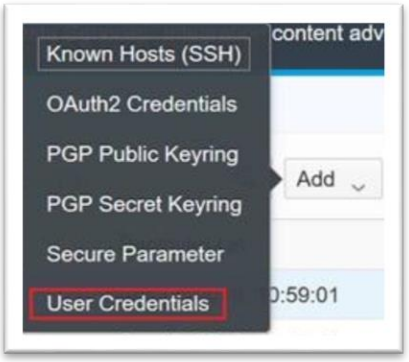
1. Navigate to Monitor > Manage Security > Security Material.

.

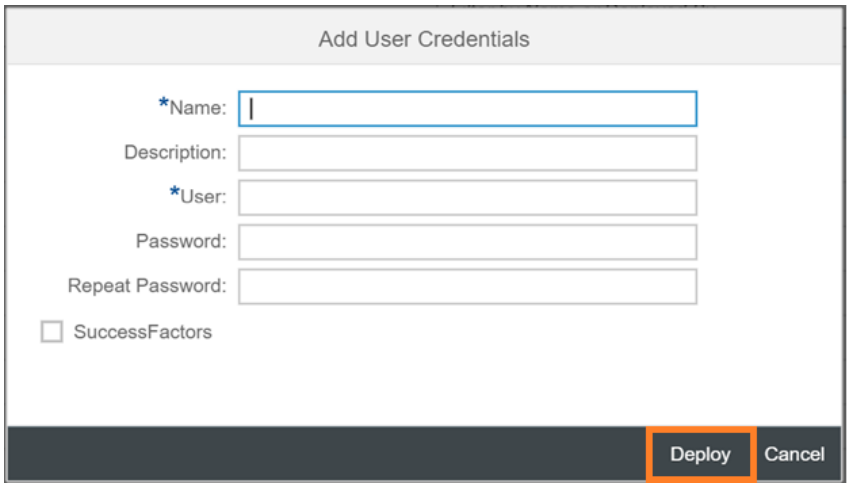



2. Add a new user credential.


3. Click User Credentials




4. Add and Deploy the user credentials



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.

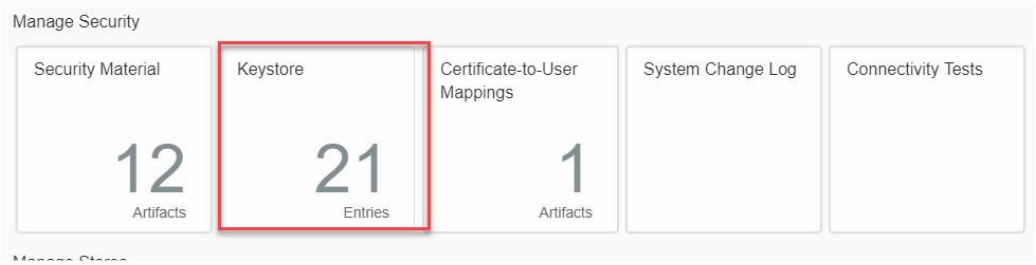
| | |
|---|---|
| Name | GSTIN of the business place to which the user belongs / GSTIN of the business place with suffix '_ewb' |
| Description | Any relevant text (optional) |
| User | API User ID created in NIC portal (production) or received from GSP (pre-production) |
| Password/ Repeat password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

## 4.3 Deploy NIC Public Key Certificate

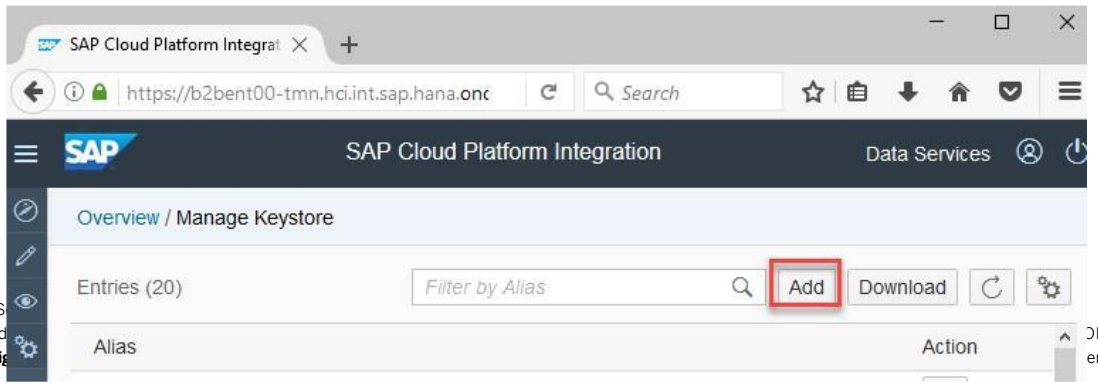
You need to add the NIC Public Key Certificate. You get this certificate from your GSP.

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

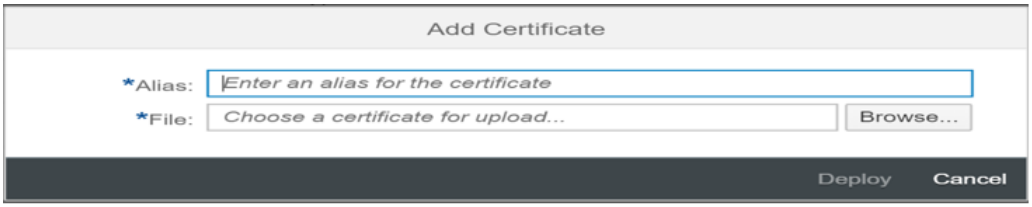
1. Navigate to **Monitor** > **Manage Security** > **Keystore**


2. Click Add > **Certificate** > **Add Certificate**




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




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 Adapt and Deploy SAP Integration Flow

Use the following steps to adapt the integration flows as per your company needs.

1. Logon to SAP Integration Suite through your S user.
   If you get *HTTP Status 403* error, then send a mail to service@sap.com.
2. After successful login, from the menu in the upper left corner, choose *Discover. Click All.*
3. In the subsequent screen, search for *ERP Integration with GST Suvidha Provider for India e-Way Bill* catalog package.
   The system displays the *ERP Integration with GST Suvidha Provider for India e-Way Bill* catalog package.
4. Click *Copy*.
   The system copies the package content to the tenant account.
5. From the menu in the upper left corner, choose *Click to work with content packages.*
   The system displays the Design screen.
6. Click on the package *ERP Integration with GST Suvidha Provider for India e-Way Bill* and in the subsequent screen choose ARTIFACTS.
   The system displays different Integration Flows. *The ERP Integration with GST Suvidha Provider for India e-Way Bill* content catalog package contains the following integration flows.

| Integration Flow Name in Web UI | Description |
|---|---|
| GSP Integration Template | Template Integration Flow to be adapted to specific GSP |
| Router Integration Template | Routes e-Way Bill request from SAP ERP or SAP S/4HANA to specific GSP Integration Flow |

7. Select the GSP Integration Template Integration Flow and adapt it. You adapt the template to use it for your GSP. For more information, see Adapt and Deploy GSP Integration Template Integration Flow
8. Deploy the updated 'GSP Integration Template' Integration Flow
9. Deploy 'Router Integration Template' Integration Flow

Result

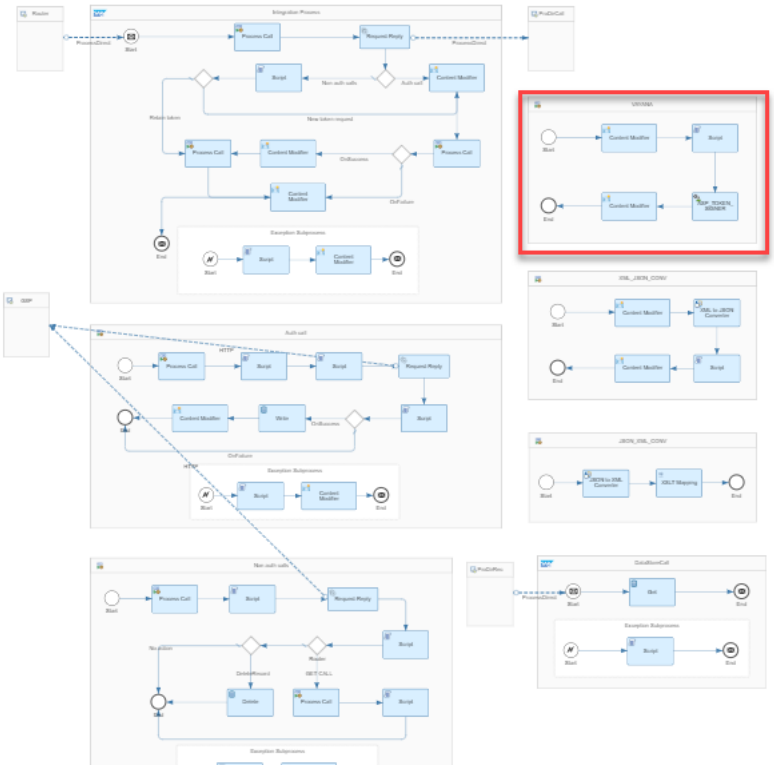
You have established the connection between *SAP ERP or SAP S/4HANA and your GST Suvidha Provider (GSP)*.

## 4.4.1 Adapt and Deploy GSP Integration Template

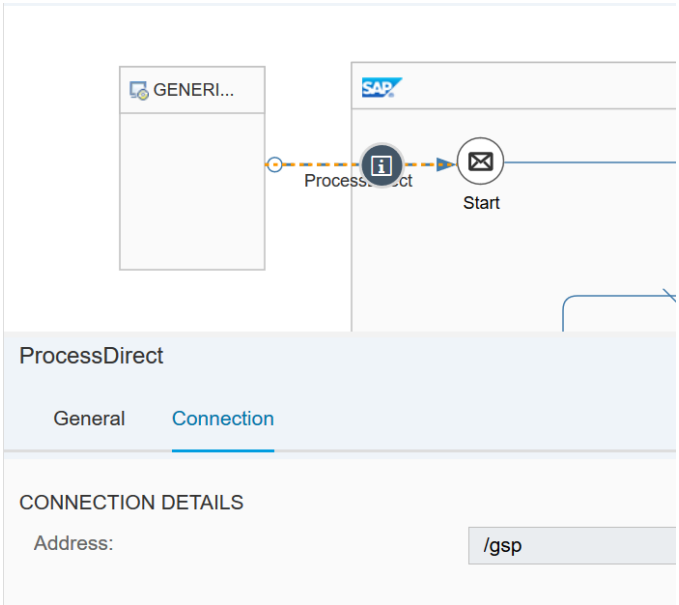
This template enables you to adapt the integration flow to specific GSP.

Following are the steps to adapt the GSP Integration Template Integration Flow

1. From the menu in the upper left corner, choose **Click to work with content packages**.
   The system displays the Design screen.
2. Select the GSP Integration Template Integration Flow.
   The system displays the Integration Flow screen.
3. Click **Edit** and adapt the GSP specific authentication for the highlighted sections as shown in the below diagram.

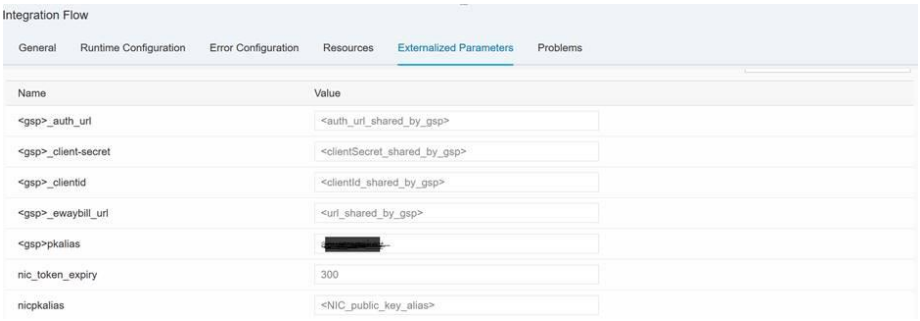


4. Click on the Process Direct as shown below.



5. Choose the connection tab. In the Address field replace the system populated GSP name with your company specific GSP name. Note that you should use the same GSP name as in the above screen in EDOINEWBGSPV view in SAP ERP or SAP S/4 HANA.
6. Click **Configure**.

   The system displays the Integration Flow screen. Choose the Externalized Parameters tab and modify the parameters as shown below:




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.

7. Save your changes.

8. Click **Deploy** to deploy the modified integration flow.

### 4.4.2 Deploy Router Integration Template

This integration flow routes e-Way Bill request from SAP ERP or SAP S/4HANA to specific GSP Integration Flow.

1. Select the Router Integration Template Integration Flow.
2. Click **Deploy** to deploy the integration flow.

Note

After the deployment, check if the integration flow is in **Started** state. You can check this in the Web UI by choosing *Monitor->Manage Integration Content*.

After successful deployment, the endpoint URL is *https://<Tenant Runtime URL>/cxf/indiaewaybilledoc*

*This URL needs to be maintained in the SOAManager configuration.*


## 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.

https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/4509f605e83c4c939a91b81eb3a6cdea.html

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.

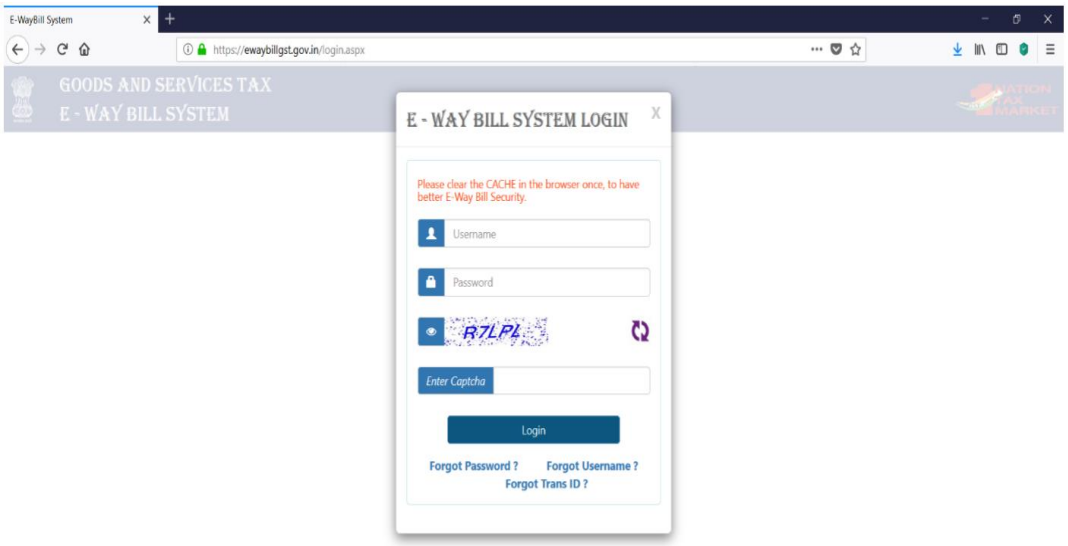
# 5 Appendix

## 5.1 GSP Registration on NIC Portal

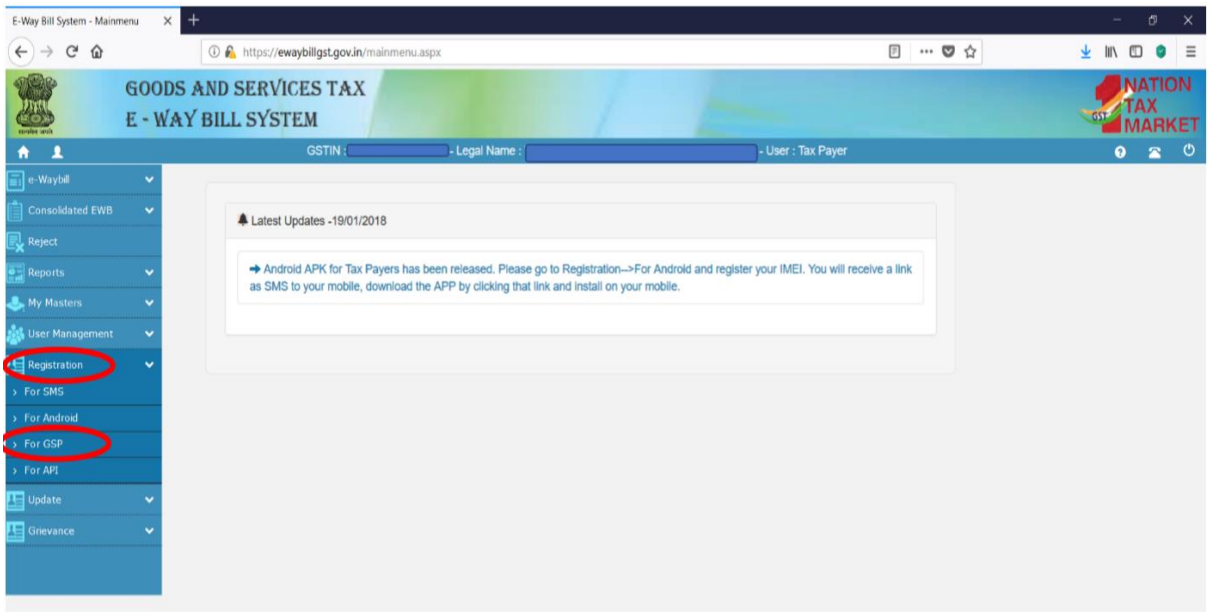
To register your login credentials for e-Way Bill API access through GSP in NIC portal.

Procedure:

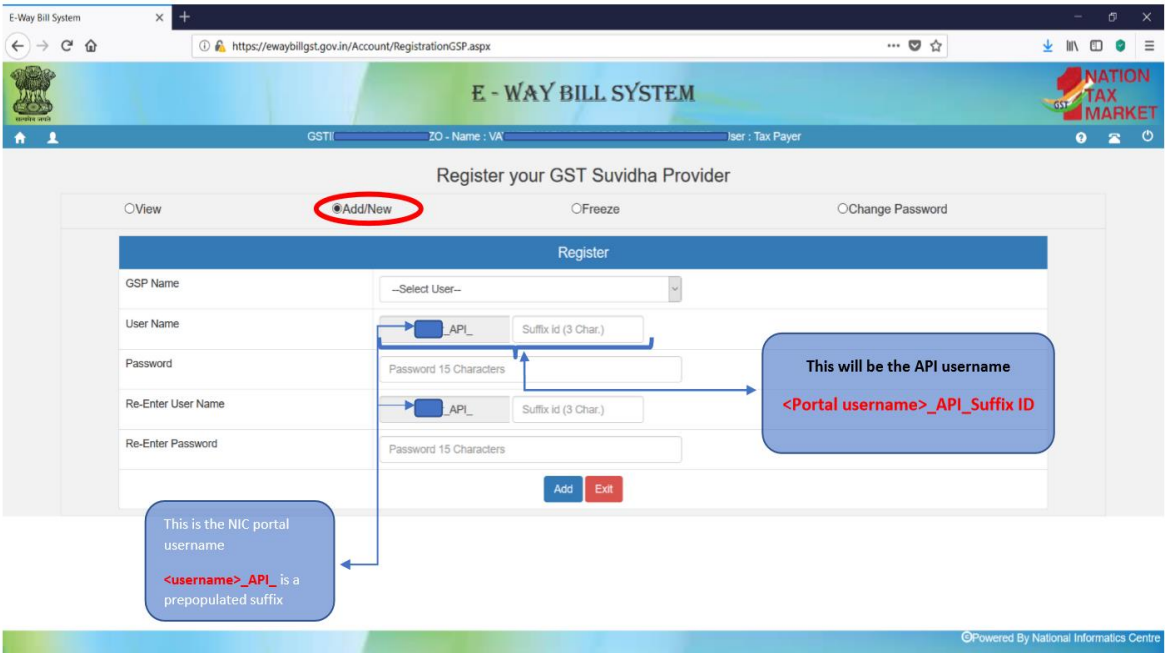
1. Login to NIC web portal (https://ewaybill.nic.in)




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



3. The system displays existing GSP (if any login credentials were already created for API access through GSP). Click on the radio button “Add/New”

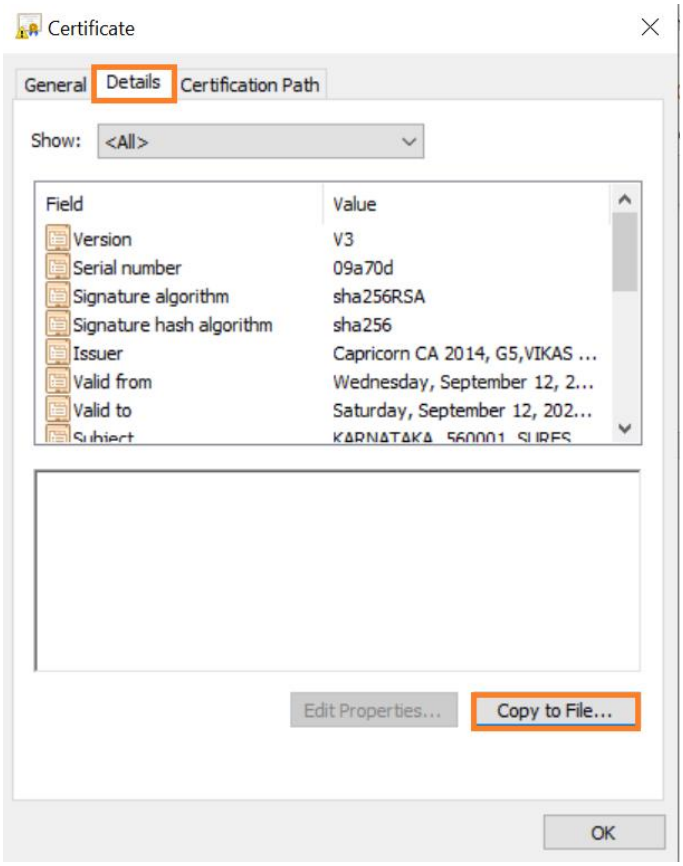



4. Click on GSP Name dropdown box and select the appropriate GSP from the dropdown list of GSPs. Next, enter your username, password. Choose “Add” to register your login credentials for E-way Bill API access through appropriate GSP.

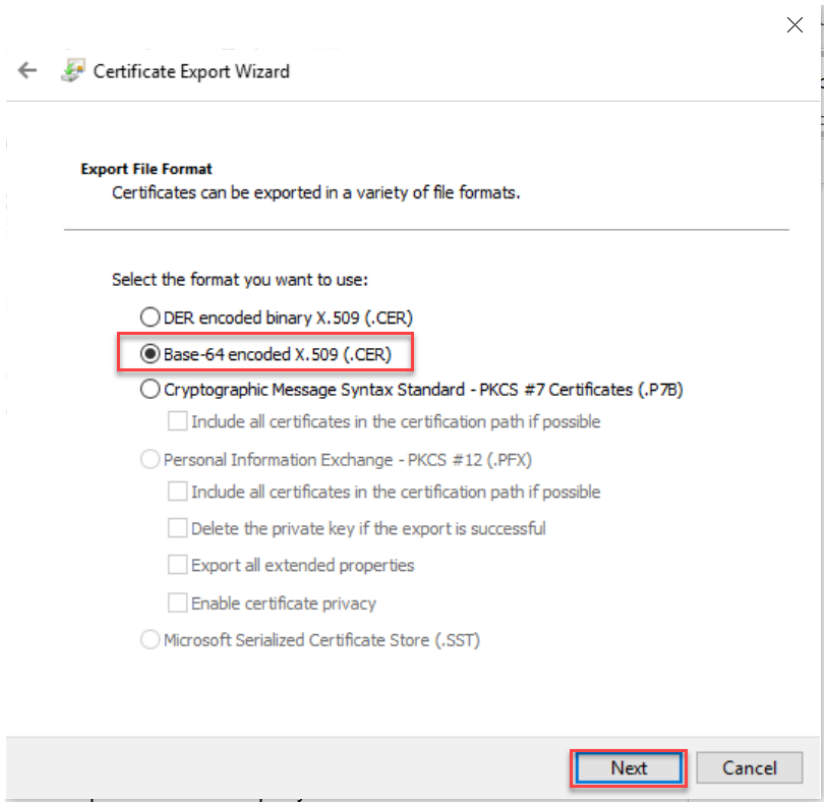
## 5.2 Exporting Certificate as Base-64 encoded X.509(.CER) format.

1. Double click the certificate. Goto Details -> Copy to File

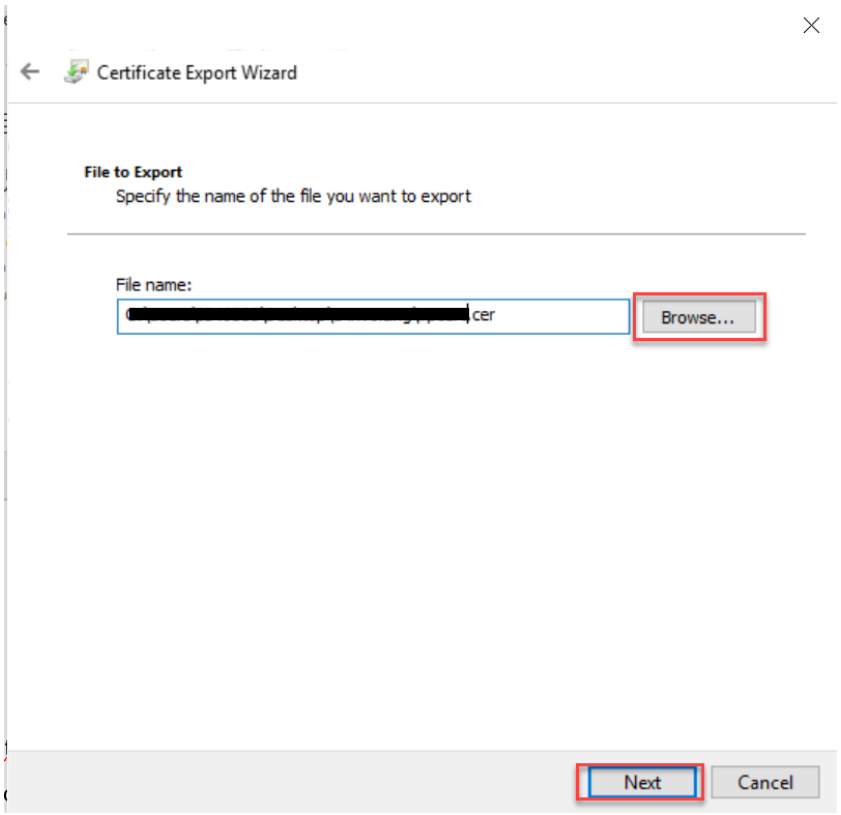
   A new window opens. Click **Next**.



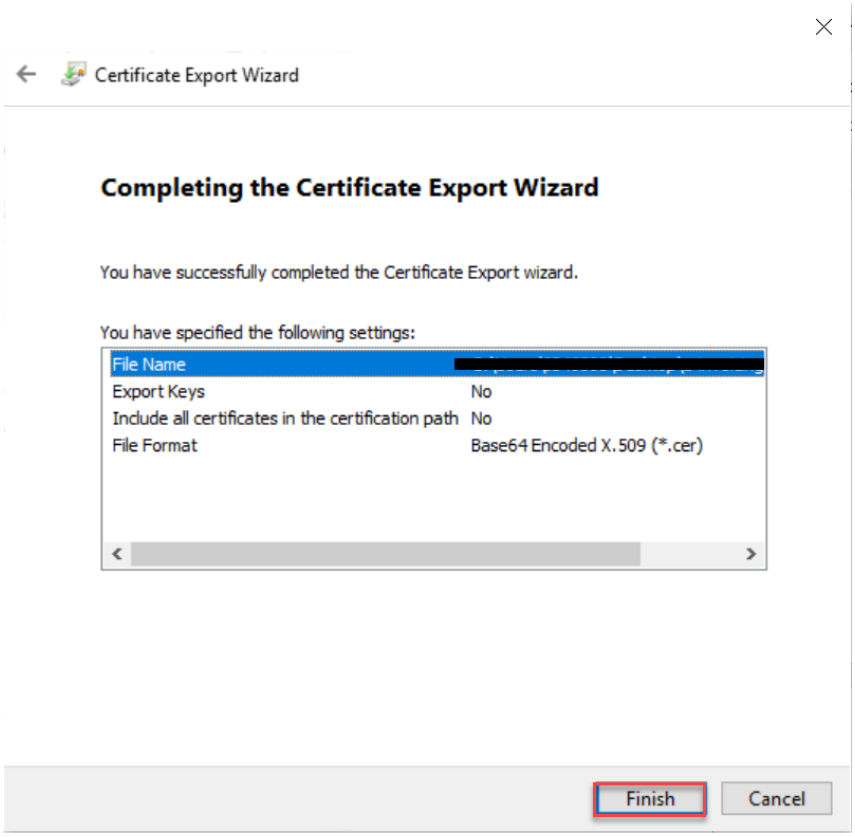

2. Select Base-64 encoded X.509(.CER) and click **Next**



3. Browse the path where the certificate has to be saved and click **Next**.




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



## 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

www.sap.com/contactsap