E-INVOICE SANDBOX SYSTEM

(Testing tool for development of e-Invoice APIs)

E-Invoice Sandbox System https://einv-apisandbox.nic.in provides the essential information for developers to integrate the e-Invoicing operations exposed by NIC-IRP through APIs with their respective ERPs and financial accounting systems. The home page is accessible from anywhere without any login and provides complete information on the APIs exposed.

The purpose of this portal includes registration by eligible Taxpayers/GSPs, testing of the APIs in the sandbox environment, the technical documentation on each of the API that is exposed for consumption and a web based test environment where one can understand the details of the steps involved in consuming the APIs.

This portal is designed as testing tool for e-invoice APIs. The developer can easily understand the process involved in preparation, encryption and decryption of the request payload and calling the API and getting the response payload. He/She can also upload his/her request payloads and see the results/responses of the same, which could be success or failure.

Apart from this, "Resources" section on the homepage allows the user to adopt themselves with the knowledge of IRN, Understanding the attributes used in JSON and mapping with their technical name, Masters for country, currency, port and state, General master inclusive of details such as type of transactions, document type, unit, mode of transport etc., List of common errors, Sample codes in JAVA and C#, .NET. The portal also provides answers to "Frequently Asked Questions" and "Best practices" are suggested while using the APIs processes for getting access to production environment. Regular updates regarding the portal are displayed in the "Announcement" section and details of latest versions of APIs etc. are provided in the "Release Notes" section.

Taxpayers/GSPs receive multiple benefits by seamless integration of the e Invoicing process with the existing ERP or financial accounting system. Same data is not required to be entered in two systems, eliminating chances of data redundancy, integrates the E-Way bill generation process as well. There are many more benefits attained as per appropriate implementation strategies.

GSPs/Taxpayers should meet certain pre-requisites to get the access to production environment. Access to e-invoice system will be provided after the evaluation of the Summary test report on sandbox that is to be provided by the user once all the testing in pre-production environment is done. There must be a nominated Project manager or Technical SPOC for the project issues/matter. 4 Indian public static IPs for whitelisting at the NIC end.

API Overview

E-Invoice APIs are used to interact and exchange the data between Taxpayer/GSP systems and the e-Invoice system. The data that is exchanged is always encrypted and the RESTful APIs are exposed over the SSL. The APIs can be accessed only after a successful token based authentication.

APIs that receive the data for addition or updation use the http POST method and those which provide data based on certain inputs use GET method. Eligible API user has to complete a self-registration process to get the required credentials such as client id, client secret, user id and

password. Using these credentials, one has to call the authentication API to get authenticated with the NIC's e-Invoicing API system.

On successful authentication, an authentication token and SEK (Session Encryption Key) is generated by the system and provided to the user. These two are valid for 1 hour on the sandbox environment and for 6 hours in the production environment.

E-Invoice API has two set of credentials – Client ID, Client Secret (For GSPs) and User ID, Password (For Taxpayers with GSTIN). If the taxpayer is enabled to access the API directly, then they will get Client ID, Client Secret that can be used PAN India for all sister concerned GSTINs with same PAN. API Credentials for Sandbox is available on registration in the API sandbox portal. And API Credentials for Production is available after completion of the boarding process. Pl visit website for more details.

API Specifications

Authentication

Access of API requires authentication using credentials. The credentials have to be generated by the taxpayers and get the "**auth token**" (*valid for 360 minutes*). Same auth token is used to access subsequent APIs. Any hits to this API within the validity will return the same token. Nonetheless there is a provision to forcefully generate a new token within the last 10 minutes of expiry by calling this API with setting "True" the "**ForceRefreshAccessToken**".

Further on the same page the user can view the image depicting the exchange of request and response between the systems of Taxpayer and IRP. Request and response payloads details as well as the sample JSONs (Request and Response) are given. FAQs regarding the authentication API are also provided for additional help to the user.

Generate IRN

This API is for registering the invoice or generation of the invoice reference number - IRN. Here the request payload has to be as per the e-invoice JSON schema given in the portal. User can view the image that shows how the request header, request payload and the response payload are exchanged between the tax payer system and the IRP system.

Request and response payloads as well as the sample JSONs (Request and Response) are given. JSON schema is also provided. Next is the validations that the API consumer has to consider while developing the consuming application needs to implement. The details are concluded with the FAQs related to the generate IRN.

Cancel IRN

This API is used for cancelling an e-Invoice within the stipulated time by passing the IRN. This API uses the POST method. User can click on the above link for Request and response payloads, sample JSONs (Request and Response), JSON schema, Validations and FAQs to see detailed information.

Get E-Invoice Details

This API provides the e-Invoice details for an IRN. It uses the HTTP GET method. The IRN for which the details are required should be passed as a value to IRN attribute. The request header contains the attributes as in case of POST APIs. The response JSON is encrypted using the SEK. On decrypting the encrypted payload, the JSON in plain text will be as shown. The decrypted JSON contains the IRN details, signed invoice and signed QR code.

Generate E-Way Bill Details

This API is used to generate the e-waybill using Invoice Registration Number (IRN). E-Way bill cannot be generated for cancelled IRN. User can click on the above link for Request and response payloads, sample JSONs (Request and Response), JSON schema and Validations to get detailed information.

Get GSTIN Details

This API provides the taxpayer details for a given GSTIN. It uses HTTP GET method. Further on the same page the user can view request and response payloads details as well as the sample JSONs for GETGSTIN. FAQs regarding this API are also provided for additional help to the user.

API Testing Tool

Open https://einv-apisandbox.nic.in and click on "Login" link.

Registration and Login

The eligible API user needs to get registered in the e-Invoicing sandbox environment of NIC-IRP to get credentials created to test the API integration with their system. Click on "Register Here" and enter the required values to complete the registration process**.** The registration can be done by the eligible tax payers or the GSPs.

While registering, tax payer will provide the GSTIN and the GSP provides the PAN number. Once entered, the trade name automatically appears. The user needs to enter the mobile number and the email ids as registered with the GSTN. Validity of these details can be checked clicking on the "Validate" button. Once validated, click on "Send OTP" link, which will send the OTP and opens up additional fields with client id, client secret and provision to enter the user id and password. This will complete the registration process. Thus generated client id, client secret, user id and password will be used for accessing the APIs. Now the user can successfully login to the system.

Add GSTIN

In home page, in top right corner, click on "Add Test GSTIN". If the logged in user is the eligible tax payer, he/she can also create additional user accounts for their counterparts who have registered in other states based on the same PAN. If the logged in user is a GSP, they can create accounts for other eligible tax payers. The process is similar to registration process. List of already registered GSTIN is also displayed.

Get Token

In the home page, click on "Get Token". Here the developer can understand the steps involved in calling the authentication API successfully. This is mandatory and it also helps to identify the correctness of the client id and client secret. The URL and other credentials are auto populated except the password that must be entered. The test tool generates an App key which is a random 32 byte array.

- Click on the "Sample JSON", to view the request payload in the "Payload – plain Text" box that also shows the password and app key.
- Click on the "Encrypt payload" link to encrypt the password and the app key using the IRP public key, for the actual request payload and populate in the "Payload – encrypted" box. The developer can also copy and paste the payload generated by their code during development phase in this box to test.
- Click on "Generate Token" button. This will send the request to the server, get the response and populate the encrypted response JSON in "Response – Encrypted" box.

- Click the “Decrypt Response” link, the SEK in the response is decrypted using the app key and the whole JSON is shown in “Response - Plain Text box”.

Post Method

In the home page, click on “Post Methods” link. Here the user can see how the APIs that use the HTTP POST methods work. Select any API from the dropdown list. The end point of the respective API will appear in the box below. The parameters that go as part of the request header are shown for the reference including the authentication token. The decrypted SEK which is a byte array is represented as a string.

- Click on “Sample JSON” to populate the sample request JSON in “Payload - plain text” box. Make sure the document number is unique, the document date as of today/yesterday, seller GSTIN and seller pin code is of the logged in user. The user can change values of various other attributes to test and analyse how the validations work.
- Click on “Encrypt Payload”, the request JSON will be encrypted using the SEK and populated in the “Payload – Encrypted” box. The developer can paste own encrypted payload here to test the encryption process and proceed further.
- Click on “Generate IRN” button. This will call the generate IRN API and post the encrypted payload, the response i.e. encrypted JSON will be shown in “Response – Encrypted” box and the same after decrypting using SEK will be shown in “Response – Plain Text”. In the response, one can see the acknowledgement number, date, IRN.
- If E Way Bill generation is part of the request, response has E Way Bill details, signed Invoice and signed QR code. Other post APIs work similarly. The differences would be in the end point and the request payload in the “Request – plain text box”.

Get Method

In the home page, click on “Get Methods” link. The user can see how the APIs that use the HTTP GET methods work. Choose one from the dropdown list of APIs using the post methods. IRN that is already generated may be pasted in the box below in case of the Get e-invoice by IRN. The next box shows the complete URL along with the IRN as the parameter value. The header parameters, authentication token and SEK are also shown.

- Click on the “Get Request Response” button. This will call the Get IRN details API , the encrypted JSON (response) will be shown in “Response – Encrypted” box and the same after decrypting using SEK will be shown in “Response – Plain Text”
- Other Get APIs work similarly. The differences would be in the end point and the way the required attributes are passed in the URL.

Go to the right side menu.

- “Get public key” link provides the public key for encrypting the password and the appkey while authenticating in the sandbox environment.
- “API End points” has all the end points for the published APIs.
- “Encrypt/Decrypt” is for the user to verify and compare their encryption and decryption outputs to the outputs generated by this tool by providing the SEK used and the string to be encrypted or decrypted.
- “Validate JSON” helps to validate the JSON created by the end user application against the schema.

For further details, Pl visit this web site - https://einv-apisandbox.nic.in

---