**GST API Authentication and Authorization FAQ**

1. How is authentication & authorization designed in GST System APIs?

Ans: GST System APIs and rest based services and every APIs call is authenticated using below two-step process:

* First step to check whether caller has permission to access GST API URL or not. This is done by checking “**clientid**” and “**client-secret**” attribute of request header. Clientid and client-secret will be provided only to authorized GSPs (GSPs can further provide it to their registered GSP) by GST System. If request carries valid values of these attributes, then only this request will be passed on to the next layer.
* Second step is to check whether this request possess valid “Authorization Token” or not. For getting Authorization token, authentication APIs need to be called first. (See second question’s answer for detail.)

First step ensure that request is coming through authorized GSP. Second step ensure that calling application has authorization of “Tax Payer” to do function like upload invoices, filing returns etc. This gives tax payer complete control on API Usage (GSP/ASP application cannot perform any action on GST System without Taxpayer consent.)

1. How to authenticate for accessing GST APIs?

Ans: GST System uses below mention three authentication APIs for authentication and authorization. For details visit <https://developer.gstsystem.co.in/apiportal/taxpayer/authentication> (developer portal) page. Please do read “more info” link on this page for getting more detail on authentication.

* [Request for OTP](https://developer.gstsystem.co.in/apiportal/)
* [Request for Authorization token](https://developer.gstsystem.co.in/apiportal/)
* [Request for extension of authorization token](https://developer.gstsystem.co.in/apiportal/)

First API is to get OTP for authentication. This API expect an app\_key from calling application. app\_key is a AES 256 bit random secure key. Please refer sample code available at developer portal ( “How to Start”->download-> samplecode\_auth\_encrypt\_decrypt.zip) to know , how to generate it in java.

Second API is to get Authorization token and session key (sek). This API expect “otp” and “app\_key”. Details of this API are available at above link. This token and sek is valid for 360 minutes as per current design. In this API response, GST System also provide an attribute called “expiry”. This attribute indicates the longer session duration selected by tax payer for example: if Tax payer has selected 12 hours then it will come 720 minutes. It means that user has only allowed refresh till 720 minutes from start of the session after that refresh API will not work and Tax payer session has to be again started with “OTP” authentication.

Third API is for extension of current session. This extension is only possible if “Tax Payer” has explicitly given a consent to GST System through https://gst.gov.in (Tax payer will have an option for this in my profile section) .Current session can only be extended till the time duration selected by Tax payer, again through portal. As per current design it can be for maximum 30 days.

1. What are “Longer Session” and why are they required?

Ans: Companies having large number of invoices and high level of automation will require a way to automatically push invoices in to GST System on a regular interval. It will not be possible for them to regularly authenticate using “OTP”. To cater this need GST System provides “Long Session” feature for such tax payers. Question number 2 answer explain the process to opt this feature.

If Tax payer choose “Longer Session”, then also “Authorization Token” will expire in x mins ( Currently it is configured at 360 mins) but calling system will be able to get new “Authorization Token” without “otp”. Such “Tax Payer” will authenticate first time with “OTP” but for next y days (Currently it could be maximum 30 days), system will be able to get new token without any “OTP” authentication. Calling system has to still get “New Authorization Token” before x mins, otherwise again Tax payer has to provide “OTP”.

1. Can a tax payer can simultaneously access GST Portal and GST System APIs?

Ans. “Yes”, it is possible but Tax payer should avoid concurrent updation of same information as it may lead to inconsistent results. This option has been provided as some of the features like payment is exclusively available on GST Portal and GST System want to allow Tax Payer to keep on using other functions like uploading invoices, filing returns simultaneously through APIs.

1. Can a tax payer access GST System through more than one GSP/ASP application?

Ans. “Yes”, it is currently allowed as there are various business scenario where it will be needed. As every authentication request require explicit consent of Tax payer through ‘otp’, chances of misuse of this feature are minimal. This option will provide “Tax Payer” an ability to choose any ASP/GSP application at any time. But if a Tax payer has chosen a “Long session”, he will only be able to access from one GSP/ASP application at a time. Still this is not a “lock in”, Tax payer can go to GST Portal anytime and break long session.

It is highly recommended that GSP/ASP application should implement “Role Based Access Control” and develop a centralized module to collect/get information from GST System to avoid concurrent access of GST System API. As most common requirement for this feature is for the companies having multi location & multiple user roles.

1. Will two authentication request share same “Authorization Token” if made in quick interval?

Ans. “No”, they will be different with their own lifecycle and sek.

1. What are the logic steps to generate “refresh token”?

Ans. If user has opted for long session then this API can be called. Steps for generating refresh token will be as below:

1. Generate a new “app\_key”.
2. Encrypt this with the old “sek” (key used to encrypt/decrypt the payload)
3. Provide old auth token in request.
4. After successful validation system will receive new “sek” and auth\_token for new session.
5. What would happen if auth\_token expires and a transaction is on (ie. posted to GST System already)?

Ans: There could be two scenarios in it.

1. Auth Token expires before hitting the GST System API gateway. GST System will give error “session expire” or any other error specified in error codes for it in API specification.
2. Auth Token expires after hitting the GST System API gateway. GST System will process it and response will be encrypted with old “sek” (“sek” for expired auth token).

So in summary either calling system will get an error or get a response encrypted with old “sek”.