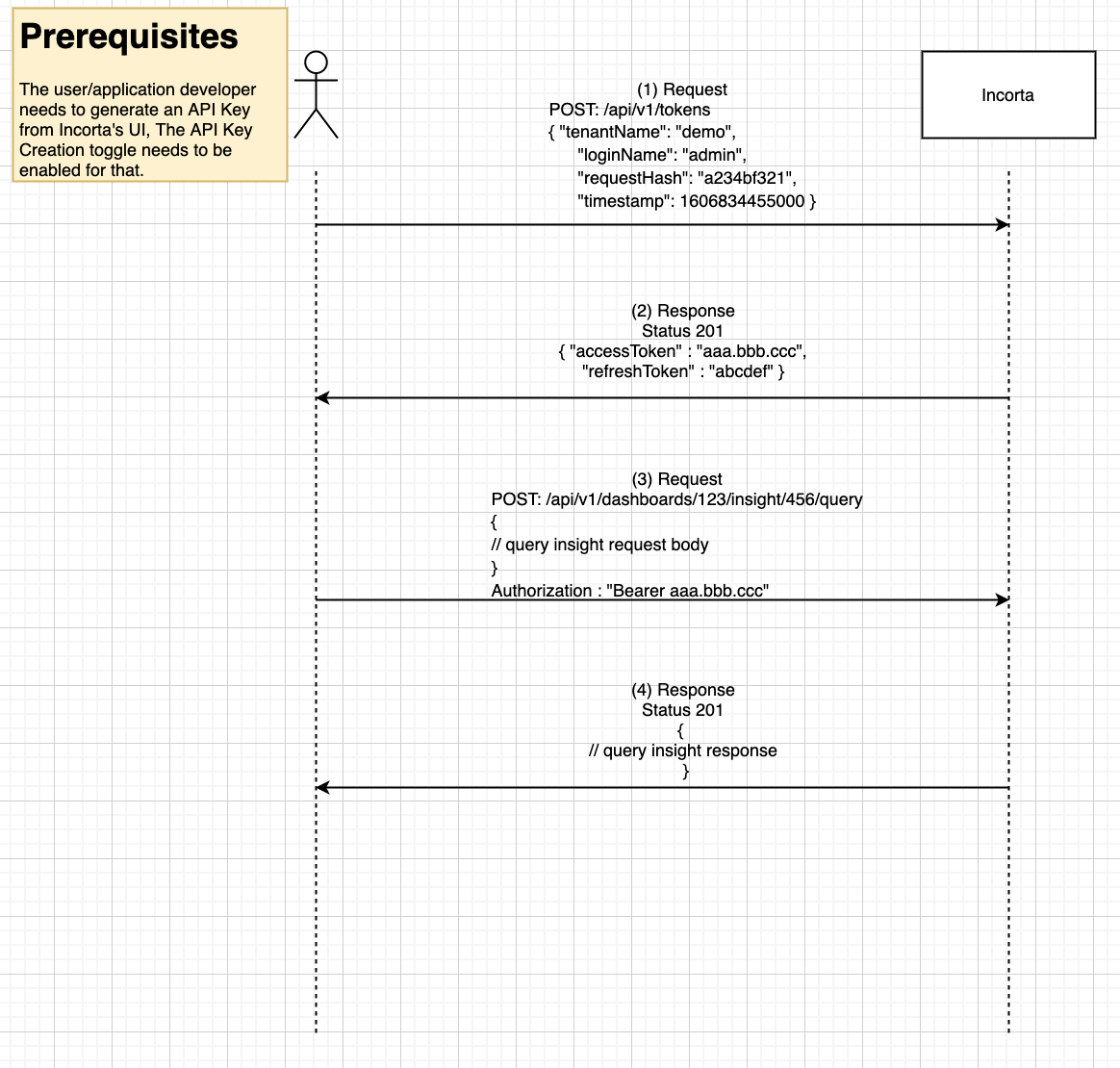
# Authentication/Authorization & acquiring Access/Refresh Tokens

The first step you need to follow to start consuming Incorta’s public REST APIs is to request an access token.

This access token will be passed as a request header when trying to access any public REST endpoint exposed by Incorta except for the following endpoints:

* /api/v1/tokens => which is used for access/refresh token generation.
* /api/v1/tokens/refresh => which is used to refresh and existing pair of access/refresh tokens.

The following diagram shows the process for requesting access/refresh token pairs:



From the above diagram, the steps to generate access/refresh token pair is as follows:

* The application developer issues an HTTP POST request to /api/v1/tokens with a request body containing
  + “tenantName” is the name of the tenant that the user belongs to
  + “loginName” is the username used by the user to login to Incorta
  + “requestHash” is the hex string representation of the output bytes from the sha256 hashing algorithm of the API Key + the current timestamp in milliseconds (sha256(api\_key + timestamp))
  + “timestamp” is the timestamp used in creating the “requestHash” in milliseconds

## Request body:

{

"tenantName": "string",

"loginName": "string",

"requestHash": "string",

"timestamp": long

}

for steps on how to generate an API key [click here](https://incorta.atlassian.net/wiki/spaces/INC/pages/1925218324/Enable+API+Key+Generation+and+Create+API+Key)

* If the API key is valid, and the timestamp is within the allowed window, Incorta will respond with access/refresh tokens pair & and an HTTP response status code 201 (Created).
  + The time window between the timestamp and calling the endpoint is configurable through the internal configuration public.apis.tokens.request.duration. The default value is 30 minutes.
  + The tokens have expiry dates, access token expires after 10 mins & refresh token expires after 20 mins. For convenience, the expiry time for each token is returned to give a hint to the consumer when the tokens need to be refreshed.

## Response body:

{

"accessToken": "string",

"refreshToken": "string",

"type": "string",

"accessTokenExpiresAt": "2020-11-23T18:02:36.901Z",

"refreshTokenExpiresAt": "2020-11-23T18:02:36.901Z"

}

* The consumer can start consuming any of the public REST APIs endpoints, for example, retrieving the data of a given insight by calling the endpoint & providing the access token as a bearer token in the **“Authorization“** request header parameter.
  + If the access token is expired or is invalid, Incorta will reject the request with HTTP status code 401.
  + For an example of consuming the query insight endpoint [click here.](https://incorta.atlassian.net/wiki/spaces/INC/pages/1476559398/Retrieving+data+for+a+given+Incorta+insight)

The user can refresh the expired access token and get new access and refresh tokens by calling /api/v1/tokens/refresh  
The user has to send the old access and refresh tokens in order to get new valid pairs, the access token could be expired but the refresh token has to be valid otherwise user will have to create new pairs using API key from /api/v1/tokens

## Request body:

{

"accessToken": "string",

"refreshToken": "string"

}

* “accessToken” is the expired JWT token that the user wants to refresh
* “refreshToken” is the refresh token that was created with the access token, the refresh token has to be still valid (not expired).

If the refresh token is still valid and the access token is authentic (generated and signed by incorta) the tokens will be refreshed successfully and the user will receive new access and refresh token pairs.

## Response body:

{

"accessToken": "string",

"refreshToken": "string",

"type": "string",

"accessTokenExpiresAt": "2020-11-23T18:02:36.901Z",

"refreshTokenExpiresAt": "2020-11-23T18:02:36.901Z"

}