

**TURKCELL MOBILE CONNECT**

**API DOCUMENT**

**Ver.1.0**

**12.01.2018**



[1 About Mobile Connect API 3](#_Toc504481442)

[1.1 Mobile Connect info and extra documents on GSMA 4](#_Toc504481443)

[2 End Point Details 5](#_Toc504481444)

[2.1 Authentication End Point 5](#_Toc504481445)

[2.1.1 Request 5](#_Toc504481446)

[2.1.1.1 Mandatory Parameters 5](#_Toc504481447)

[2.1.1.1.1 About Scope parameter 6](#_Toc504481448)

[2.1.1.1.2 About ACR Values 6](#_Toc504481449)

[2.1.1.2 Optional Parameters 7](#_Toc504481450)

[2.1.2 Redirect URI 7](#_Toc504481451)

[2.1.3 Response 8](#_Toc504481452)

[3 Token End Point 10](#_Toc504481453)

[3.1 Request 10](#_Toc504481454)

[3.1.1 Header Mandatory Parameters 10](#_Toc504481455)

[3.1.2 Query Mandatory Parameters 10](#_Toc504481456)

[3.1.3 Response 10](#_Toc504481457)

[3.1.4 Sample Token Request via using Postman 11](#_Toc504481458)

[3.1.4.1 Authorization 11](#_Toc504481459)

[3.1.4.2 Header of Request 11](#_Toc504481460)

[3.1.4.3 Body of Request 12](#_Toc504481461)

[3.1.4.4 Response 12](#_Toc504481462)

[4 UserInfo End Point 13](#_Toc504481463)

[4.1 Request 13](#_Toc504481464)

[4.1.1 Header Mandatory Parameters 13](#_Toc504481465)

[4.2 Response 13](#_Toc504481466)

[4.2.1 Mandatory Parameters 13](#_Toc504481467)

[4.2.2 Optional Parameters 13](#_Toc504481468)

[4.3 Sample UserInfo Request via using Postman 14](#_Toc504481469)

# About Mobile Connect API

Mobile Connect is basically an extended type of Outh 2.0

* + **https://tools.ietf.org/html/rfc6749** (RFC 6749)
  + but there are some differents from RFC 6749 which you can find in:

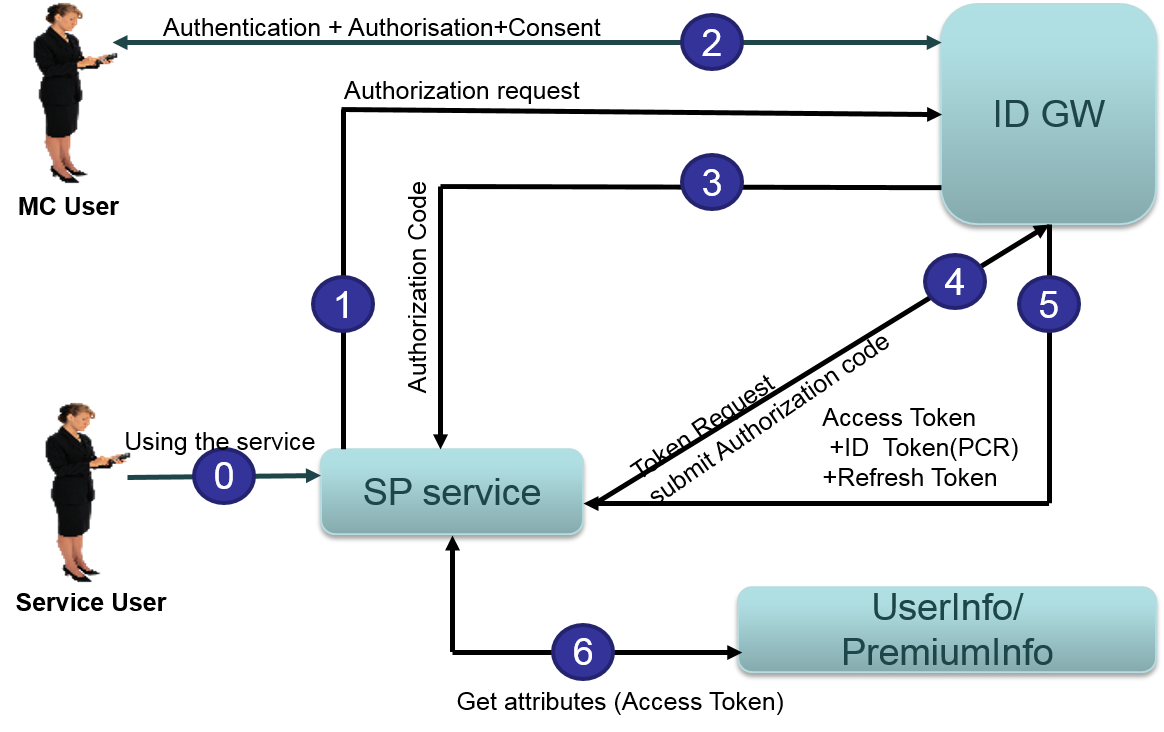
**https://github.com/GSMA-OneAPI/Mobile-Connect/tree/master/specifications**

* Service Provider calls 3 end-points to achieve Mobile Connect Login
  + authentication
    - authenticate user via GSM number
    - produce authentication-code
    - client2server
    - directly opened Mobile Connect authentication url via web browser
  + token
    - authenticate Service Provider with client/secret and authentication code
    - consumes authentication-code and produce token
    - server2server
    - IP restricted on Mobile Connect
      * You should provide your server dns info to access it
  + userInfo
    - gives user attributes
      * **PCR (Pseudonymous Customer Reference)**:
        + The PCR is a unique id that always represents a specific user.
        + public profile: always share with Service Provider
        + Service Provider has to use PCR to relate Mobile Connect and its own Subcription System.
      * phone\_number
      * e-mail (verified or unverified)
      * name and family name
* Service Provider must provide a service to get authentication codes after called authentication end-point called “***redirect uri***”
  + “redirect uri” called by client browser by http redirect (http 302)
  + after authentication done Mobile Connect redirects the client browser to Service Provider redirect uri
* Mobile Connect endpoints start with:
  + Prod: <https://mobcon.turkcell.com.tr/>
  + Test: <https://mobcon-test.turkcell.com.tr/>

## Mobile Connect info and extra documents on GSMA

Service Providers can get the required integration (for Discovery API platform & Turkcell Mobile Connect platform) documents from the below link (CPAS05 doc.);

<https://github.com/GSMA-OneAPI/Mobile-Connect/tree/master/specifications>



# End Point Details

## Authentication End Point

### Request

**Test URL:** https://mobcon-test.turkcell.com.tr/mobileconnect /oauth/authorize

**Prod URL:** https://mobcon.turkcell.com.tr/mobileconnect /oauth/authorize

**http method:** GET

|  |
| --- |
| Sample URL |
| https://mobcon-test.turkcell.com.tr/mobileconnect /oauth/authorize?client\_id=client&scope=openid%20phone&redirect\_uri=http://10.201.213.62:19041/MC\_Demo/mcResult.html&response\_type=code&state=State0.p26wdplbsx5k1972v5cdi&nonce=Nonce0.vdl4rjul2btzy24wnimabrzfr&prompt=login&acr\_values=2&display=page&ui\_locales=tr&claims\_locales=tr |

#### Mandatory Parameters

|  |  |
| --- | --- |
| URI Parameter | **Description** |
| client\_id | This is your application id from your settings on Mobile Connect Platform  **Type:** string |
| scope | A space-delimited list of the permissions you are requesting  **Type:** string   * openid * phone * profile * email |
| redirect\_uri | Where Mobile Connect sends the user after the user grants or denies consent. If user approves then SP should get authentication\_code with this URI. See [Redirect URIs](https://dev.fitbit.com/build/reference/web-api/oauth2/#redirect-uris) below. **Type**:URI |
| response\_type | The value MUST be “code”, to indicate that the grant type flow to be used is Authorisation Code.  **Type:** string |
| acr\_values | The recommended values are the LOAs as specified in ISO/IEC 29115 Clause 6 – 1, 2, 3, 4 – representing the LOAs of **LOW, MEDIUM, HIGH and VERY HIGH**  **Type:** string |
| state | This parameter will also be added to the redirect URI and it is for against cross-site request forgery (CSRF)  It should be produced as random for each request  **Type:** string |
| nonce | The value SHOULD be unique per session to mitigate replay attacks  **Type:** string |

##### About Scope parameter

Mobile Connect “scope” values determine the specific set of claim values to return in the response.

Scope values definition:

The scope value “openid” is mandatory to indicate that the request is an OpenID Connect request. The other scope values are related to the UserInfo.

|  |  |  |  |
| --- | --- | --- | --- |
| Value | Mandatory in Spec | Mandatory in Profile | Description |
| openid | Mandatory | Mandatory | This value indicates the Request is an OpenID Connect request. |
| profile | Optional | Optional | Requests access to the default basic profile claims: name, family\_name, given\_name, middle\_name, nickname, preferred\_username, profile, picture, website, gender, birthdate, zoneinfo, locale, and updated\_at. |
| email | Optional | Optional | Request access to the claims : email and email\_verified |
| address | Optional | Optional | Requests access to the claim : address  Currently not provided by Mobile Connect |
| phone | Optional | Optional | Requests access to the claims : phone\_number and phone\_number\_verified |

##### About ACR Values

How are the levels defined in Mobile Connect?

Within Mobile Connect there are 4 levels of assurance identified as per the ISO/IEC 29115 Clause 6:

|  |  |  |  |
| --- | --- | --- | --- |
| Level | Description | Exists in Mobile Connect? | ACR Value |
| 1 – Low | Little or no confidence in the asserted identity. | No / out of scope | 1 |
| 2 – Medium | Some confidence in the asserted identity. | Yes | 2 |
| 3 – High | High confidence in the asserted identity. | Soon | 3 |
| 4 – Very High | Very high confidence in the asserted identity. | No | 4 |

#### Optional Parameters

|  |  |
| --- | --- |
| URI Parameter | **Description** |
| display | specifies the user interface display for the Authentication and Consent flow. Now, only “page” is supported **Type:** string |
| prompt | specify to the Authorisation Server whether to prompt or not for reauthentication and consent.  Now, only “login” is supported **Type:** string |
| login\_hint | An indication to the IDP/Authorisation Server on what ID to use for login.  The login\_hint can contain the MSISDN or the Encrypted MSISDN and SHOULD be tagged as MSISDN:<Value> and ENCR\_MSISDN:<Value> respectively – in case MSISDN or Encrypted MSISDN is passed in login\_hint. Encrypted MSISDN value is returned by Discovery API in the form of "subscriber\_id"  MSISDN must be encrypted with Mobile Connect public key that is provided by Turkcell  This parameter is only used for if SP implements its own Login page  **Type**:string |
| ui-locales  claims-locales | Specifies the language used in Mobile Connect pages, supported values:   * en (English), tr (Turkish) * Default value is Turkish   **Type:** string |

### Redirect URI

* The client MUST provide one or more “redirect uri” to be used for responding back for Authorisation Requests through redirect.
* Redirect URI is a simple http listener that takes authentication code from Mobile Connect Platform.
* Service Providers have to provide their “redirect uri” while registration.
* You can see furthermore details on the next “Response” section.

### Response

* Mobile Connect Authentication Response is met by the Redirect URI of Service Provider.
* So, in redirect uri SP has to check code first from query parameter
  + If code exists then go for token by exchange code
  + If not then SP should watch the error parameter
* State if for to avoid reply attacks

|  |
| --- |
| Sample URL |
| HTTP/1.1 302 Found    Location: https://client.mid.org?code=SplxlOBeZQQYbYS6WxSbIA  &state=af0ifjsldkj |

|  |  |
| --- | --- |
| URI Parameter | **Description** |
| code | Authorisation Code as per OAuth 2.0. To be used as parameter in Token request to exchange for Tokens **Type:** string |
| state | The same value as the "state" parameter sent during the authentication request. Use as a security mechanism to confirm that the response comes from the same authentication requests  **Type:** string |
| error | if code parameter is missing in the response then SP should check the error parameter.  USER\_DID\_NOT\_APPROVE:User denies from Click Ok, it comes only for ClickOK authentication type  FRAUD\_DETECTED: when user tries to break the authentication urls  BROKEN\_SESSION: when user session is expired or does not exist  TIMED\_OUT: when authentican messages expired  **Type**:string |

|  |
| --- |
| ***When Authentication URL is called from mobile applications;***   * ***IOS:***    + *should be used* [***SFSafariViewController*** *class*](https://developer.apple.com/library/ios/documentation/SafariServices/Reference/SFSafariViewController_Ref/) *instead of switching to Safari*   + *Using* [*WKWebView*](https://developer.apple.com/library/ios/documentation/WebKit/Reference/WKWebView_Ref/)*or* [*UIWebView*](https://developer.apple.com/library/ios/documentation/UIKit/Reference/UIWebView_Class/) *class is not allowed* * ***Android:***   + *should be used* [***Chrome Custom Tabs***](https://developer.chrome.com/multidevice/android/customtabs)*instead of switching to the default browser*   + *Using* [*WebView*](http://developer.android.com/reference/android/webkit/WebView.html) *is not allowed*   ***When Authentication URL is called from mobile web browser;***   * ***webview*** *should be used*   ***When Authentication URL is called from mobile web browser;***   * *We offer to use in iframe to achieve a great user experience*   + *You can look through the Turkcell web site (http://www.turkcell.com.tr) “Hızlı Giriş” for details* |

# Token End Point

## Request

**Test URL:** <https://mobcon-test.turkcell.com.tr/mobileconnect/oauth/token>

**Prod URL:** https://mobcon.turkcell.com.tr/mobileconnect /oauth/ token

**http method:** POST

### Header Mandatory Parameters

|  |  |
| --- | --- |
| URI Parameter | **Description** |
| Authorization | HTTP Basic authorization to access the API. Base64 encoded String of your "<client\_id>:<client\_secret>" (please note, these are client\_id, client\_secret value from the discovery response.)  **Type:** string |
| Content-Type | Describe the format of the "POST" data that is being sent across. Always set to "application/x-www-form-urlencoded"  **Type:** string |

### Query Mandatory Parameters

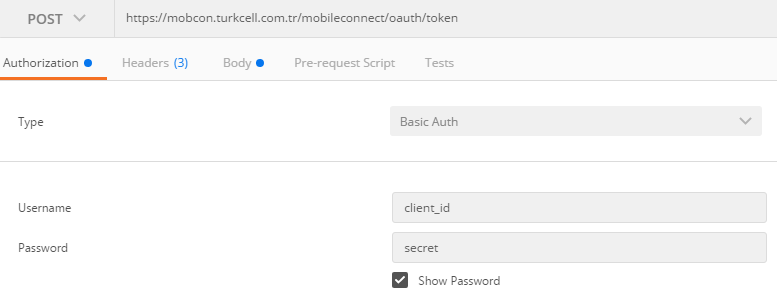
|  |  |
| --- | --- |
| URI Parameter | **Description** |
| Authorizationcode | The "code" parameter you received from the Authentication request's response  **Type:** string |
| grant\_type | The type of "code" that is being submitted. Always set to "authorization\_code"  **Type:** string |
| redirect\_uri | Used as an extra level of security. If a mis-matched redirect\_uri is passed (other than the registered), error will be thrown. Set the value to your registered redirect\_uri in URL Encoded format **Type**:URI |

### Response

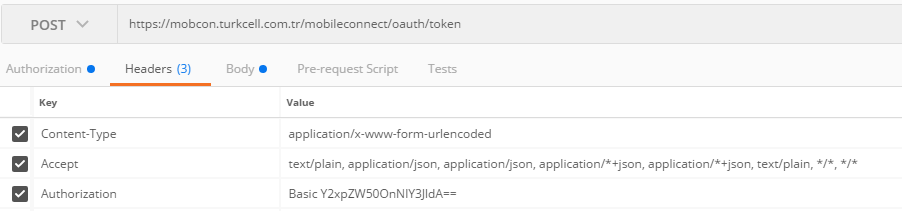
|  |  |
| --- | --- |
| URI Parameter | **Description** |
| access\_token | OAuth 2.0 access\_token, used to get the UserInfo object from the UserInfo end-point and can be reused for accessing other protected resources, if required **Type:** string |
| token\_type | The type of token received. In Mobile Connect case, it should always be "Bearer"  **Type:** string |
| expires\_in | Expiration time in seconds from the time of generation of the response  **Type:** string |
| id\_token | Additional token used in OIDC to provide the Identity token claim. A Base64URL encoded String, when decoded contains all the claims in JSON format   * **Currently it is not used in Mobile Connect**   **Type:** string |

### Sample Token Request via using Postman

#### Authorization

****

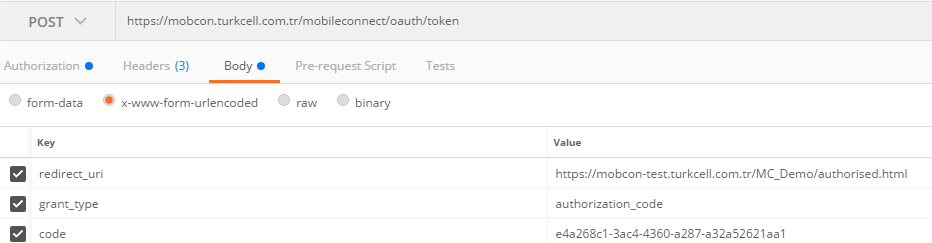
#### Header of Request

****

|  |  |
| --- | --- |
| Key | Value |
| Content-Type | application/x-www-form-urlencoded |
| Accept | text/plain, application/json, application/json, application/\*+json, application/\*+json, text/plain, \*/\*, \*/\* |
| Access-Control-Allow-Origin | mobcon.turkcell.com.tr |
| Authorization | Basic VGVzdFVzZXIxOnRlc3Q= |

* **You have to change accunt information that is given in “**Authorization**”, that is an example:**
  + **“Basic ” + Base64.encode(username + “:” + password)**

#### Body of Request

****

|  |  |
| --- | --- |
| Key | Value |
| redirect\_uri | https://mobcon-test.turkcell.com.tr/MC\_Demo/authorised.html |
| grant\_type | authorization\_code |
| code | f8daedc2-92ff-4226-a51d-64b7ba91d2b5 |

#### Response

* Here is an example of Token End Point response
  + You can see 3.1.3 for parameter details

|  |
| --- |
| token response={  "access\_token":"eyJhbGciOiJSUzI1NiJ9.eyJleHAiOjE1MTEwMjE2NTYsImF1ZCI6IngtZ1pKOG1FbmpvTGlBZ3JmdWRIQ0VadnVmT29hZnZmMVMiLCJpc3MiOiJodHRwOlwvXC9sb2NhbGhvc3Q6ODA4MFwvbW9iaWxlY29ubmVjdFwvIiwianRpIjoiMGU2Y2UxMjktNDA3OS00MzQ0LTk3ZjQtN2E1NjFkYWMwYzFkIiwiaWF0IjoxNTA4NDI5NjU2fQ.hwtVM3a62A6\_6bPqLe8PEyHV8IQ85FvMikLPO\_ewJvuc6I88zeWI0TvgUxxuNuppqPGHloGW59TXwcd3y6g8vpPv1L2e-3CzJSVfklX7nbviYOOE3XOPvCq\_5ObU59GoVLaGAg3AawMoZ1Cjwklcwtr\_TQP\_afAUTTwnaeYwGMk",  "token\_type":"Bearer",  "expires\_in":2591999,  "scope":"phone email openid profile",  "id\_token":"eyJhbGciOiJSUzI1NiIsImtpZCI6InJzYTEifQ.eyJhdXRoX3RpbWUiOjE1MDg0Mjk2NTYsImV4cCI6MTUxMTAyMTY1Niwic3ViIjoiN2U0YmE4NTUtYjQ0Yi00YTZjLWI1YWQtNjk0NmY4YWEyYTI3IiwiYXpwIjoieC1nWko4bUVuam9MaUFncmZ1ZEhDRVp2dWZPb2FmdmYxUyIsIm5vbmNlIjoiTm9uY2UwLmVzOXlubWs0dnA2cnk0NmswbzcweXN5dmkiLCJhdWQiOlsieC1nWko4bUVuam9MaUFncmZ1ZEhDRVp2dWZPb2FmdmYxUyIsbnVsbF0sImlzcyI6Imh0dHA6XC9cL2xvY2FsaG9zdDo4MDgwXC9tb2JpbGVjb25uZWN0XC8iLCJpYXQiOjE1MDg0Mjk2NTYsImFjciI6IjIiLCJhbXIiOlsiT0siLCJPVFAiXSwia2lkIjoicnNhMSJ9.vSJsYW3TeeqnvyG\_07U1umlRPm107Ofv0XlohE8M-8o8BIBXBgDgjaB4X1P67OG\_8z37o5UMUock8mEkz0B88zzhWhf5\_OVHk2RBbrB95HFmms7ZYUn2ReqWH6u1RNZSSznWFmSFz6yOD8xefqdbuDepsyXIIQv6x4LgzZqenHE"  } |

# UserInfo End Point

A basic API that provides the user's basic profile in JSON Object. To access this API, an access\_token is required.

## Request

**Test URL:** <https://mobcon-test.turkcell.com.tr/mobileconnect/userinfo>

**Prod URL:** https://mobcon.turkcell.com.tr/mobileconnect /userinfo

**http method:** GET

### Header Mandatory Parameters

|  |  |
| --- | --- |
| URI Parameter | **Description** |
| Authorization | Bearer access\_token  **Type:** string |
| Content-Type | Describe the format of the "GET" data that is being sent across. Always set to "application/x-www-form-urlencoded"  **Type:** string |

## Response

### Mandatory Parameters

|  |  |
| --- | --- |
| URI Parameter | **Description** |
| sub | PCR stands for "Pseudonymous Customer Reference". This is a unique identifier that Mobile Connect uses to reference an end user **Type:** string |
| updated\_at | Time at which the user’s profile data was last updated.  Its represented as the number of seconds from 1970-01-01T0:0:0Z as measured in UTC until the date/time  **Type:** Number |

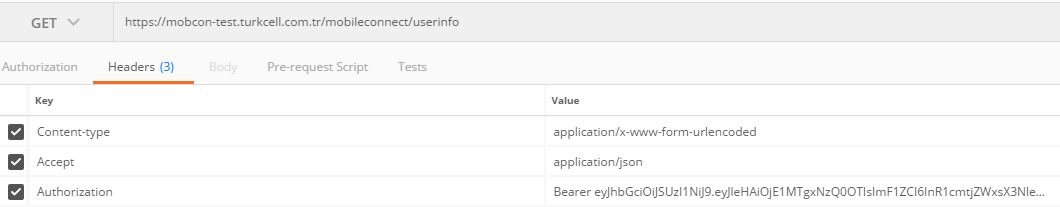
### Optional Parameters

**These parameters are available only:**

* Service Provider has right to ask to user for consent
* and user gives consent

|  |  |
| --- | --- |
| URI Parameter | **Description** |
| phone\_number | If user gives consent to share  **Type:** string |
| phone\_number\_verfied | TRUE if the phone number is verified, FALSE otherwise  It is expected always TRUE if user gives consent  **Type:** Boolean |
| name | First name and middle name if exists  **Type:** string |
| family\_name | surname  **Type:** string |
| email | **Type:** string |
| email\_verified | TRUE if the email address is verified, FALSE otherwise  **Type:** Boolean |

## Sample UserInfo Request via using Postman

****

|  |  |
| --- | --- |
| Key | Value |
| Content-Type | application/x-www-form-urlencoded |
| Accept | application/json |
| Access-Control-Allow-Origin | mobcon.turkcell.com.tr |
| Authorization | Bearer eyJhbGciOiJSUzI1NiJ9.eyJleHAiOjE1MTIxMjczODQsImF1ZCI6IlRlc3RVc2VyMSIsImlzcyI6Imh0dHA6XC9cL2xvY2FsaG9zdDo4MDgwXC9tb2JpbGVjb25uZWN0XC8iLCJqdGkiOiI2NDZmNjQ5NC04MzcwLTRhMGMtYWJiYi05YTRhMWU0MjUxMjYiLCJpYXQiOjE1MTIwNjczODR9.frcorR7y3SyDdzccxyYh6B3J0NwDeY\_Sz5G1aqUDMvKRdQeHiTE3FYrJ5VLQbdV1sOMhwZ\_aM5tujg6aeXFETzTArvdOA3nLsjct2-uQn4yYN0NaiOJF\_R2YKyJ-Ycmjtg3ZbMtSsx6pRGr3eYDWEGtjMAhbtUJvw9Bt3XUU6JA |

* **You should send Access Token that you received from Token End Point**

**Response**

|  |
| --- |
| **{**  **"sub": "60b4d739-1211-4635-b8de-1691c3f67337",**  **"updated\_at": "1507894650602",**  **"phone\_number": "5457694831",**  **"phone\_number\_verified": true**  **}** |

**Token and UserInfo end point Postman Project is in the file below:**

