TOKEN OAUTH

Obtinerea tokenului de acces de tip JWT

În momentul în care este înregistrată aplicația, aceasta se va conecta, utilizând valorile obținute. În interfața dezvoltată se vor utiliza informațiile rezultate în urma procesului de înrolare a aplicației, după cum urmează:

1. Client ID
2. Client Secret
3. Callback URL (Redirect URI) disponibil

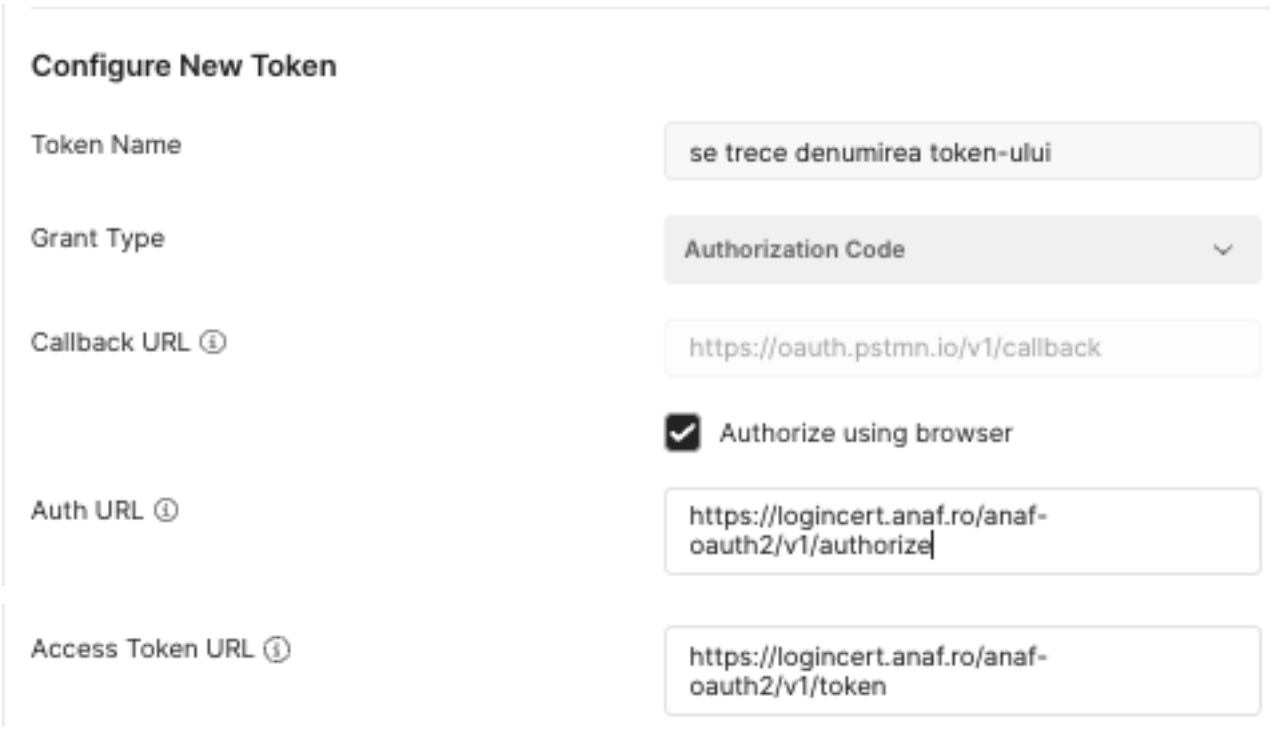
Se vor avea în vedere următoarele configurări/setari pentru obtinerea tokenului de acces:

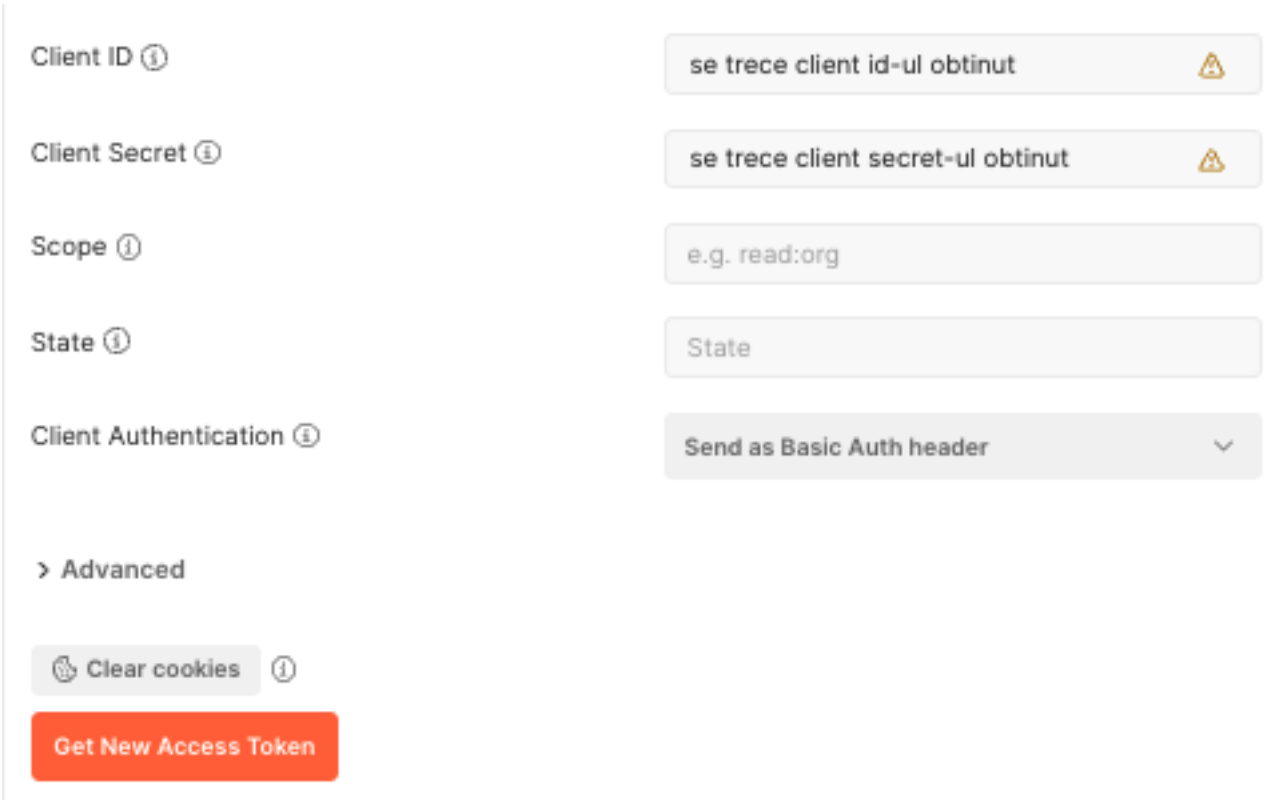
- Type: OAuth 2.0
- Add Authorization Data to: Request Headers
- Grant Type: Authorization Code
- Callback URL: configurat de client la înrolarea aplicației
- URL-ul pentru autorizare: https://logincert.anaf.ro/anaf-oauth2/v1/authorize
- URL-ul pentru revocarea tokenului: https://logincert.anaf.ro/anaf-oauth2/v1/revoke
- Client ID: obtinut de client la inrolarea aplicatiei

- Client Secret: obtinut de client la inrolarea aplicatiei
- Client Authentication de tipul: Send as Basic Auth header

Atașăm o captură de ecran pentru obținerea tokenului de acces OAUTH, folosind utilitarul POSTMAN varianta Desktop(o versiune cat mai recenta). Scope se lasa necompletat. State se lasa necompletat.

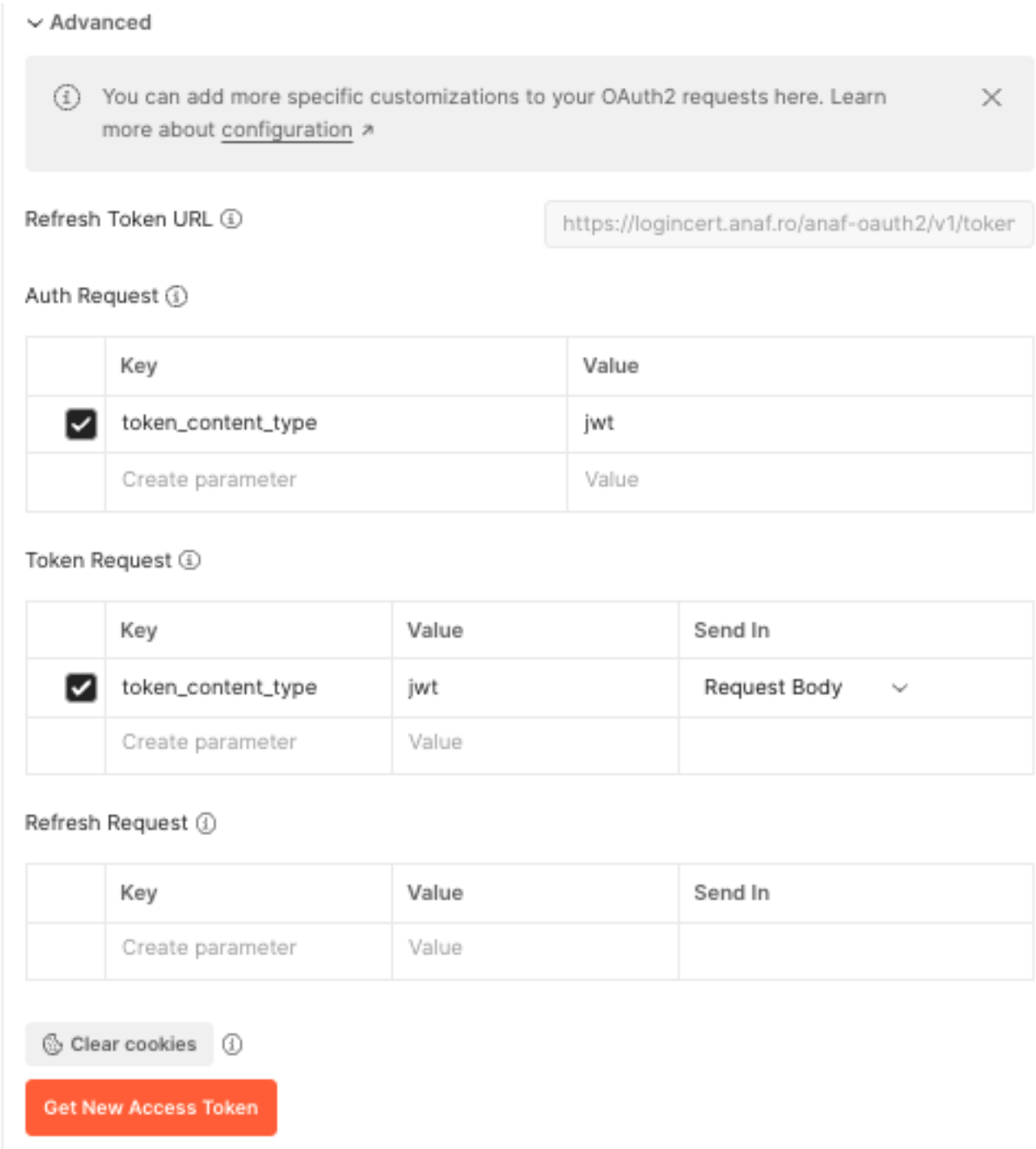
Vă rugăm să completați câmpurile întocmai ca în captura de mai jos. Nu completați câmpurile care sunt goale în captura de ecran.





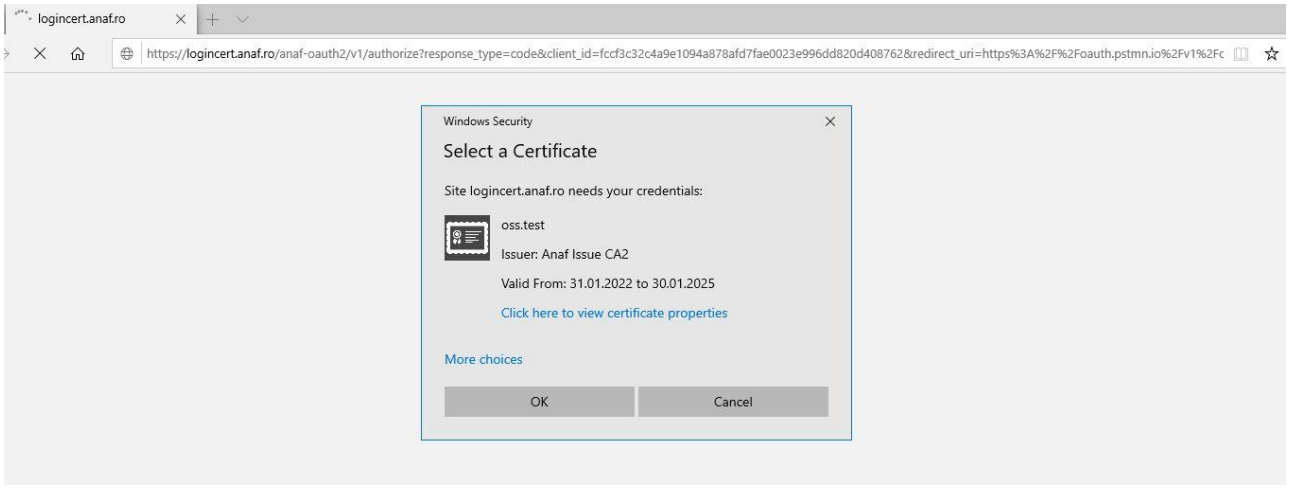
Se face expand la Advanced si se completeaza urmatoarele campuri:

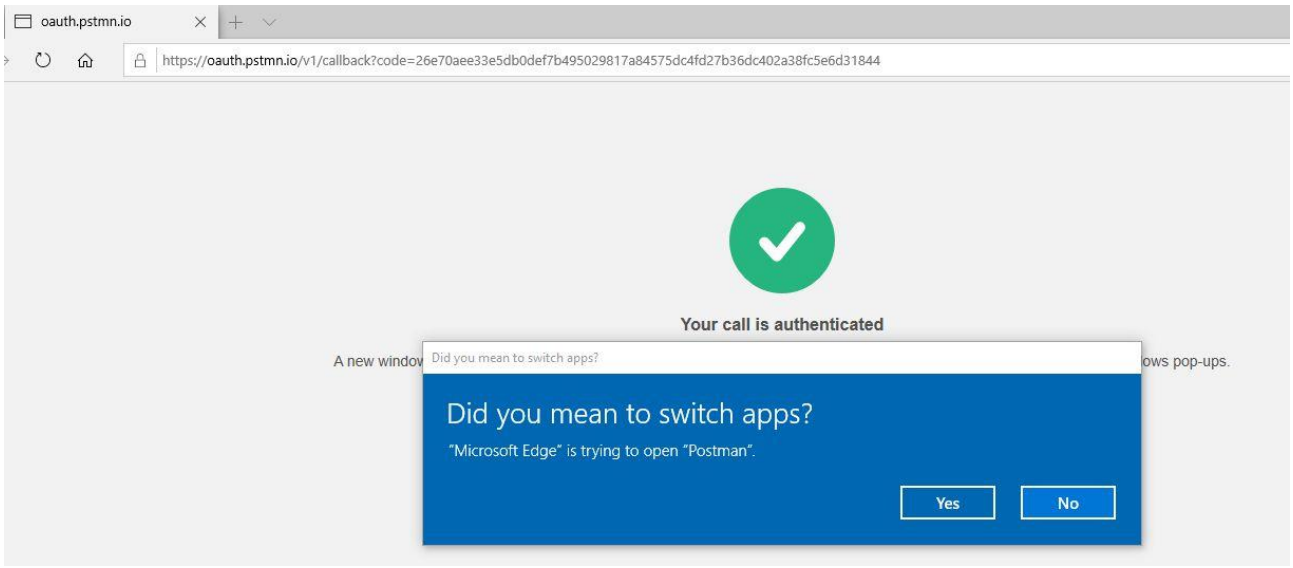
- Auth Request, Key=token_content_type, Value=jwt
- Token Request, Key=token_content_type, Value=jwt, Send In=Request Body

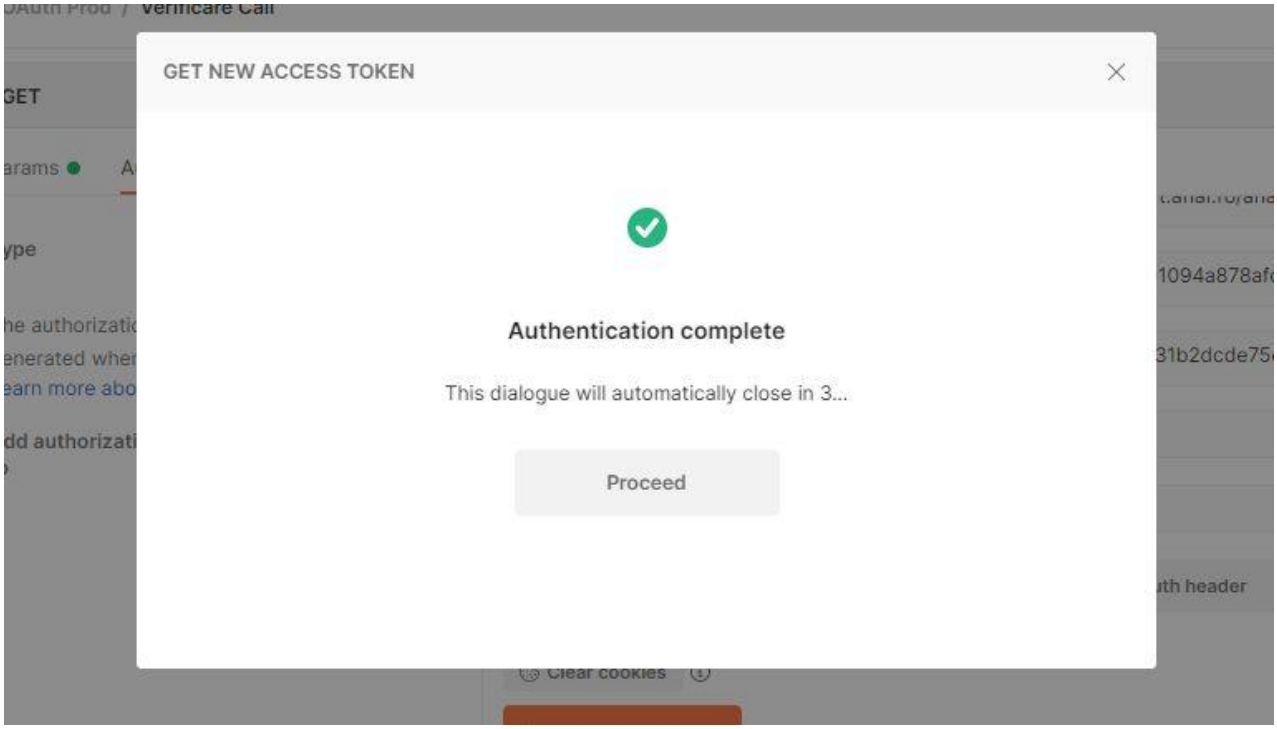


Cei doi parametrii token_content_type=jwt se trimit odata pe Query pentru requestul de Authorizare si in corpul requestului (Request Body) pentru requestul de obtinere al token-ului.

După apăsarea butonului “Get New Access Token” se va prezenta certificatul digital cu rol SPV PJ


logincert.anaf.ro
https://logincert.anaf.ro/anaf-oauth2/v1/authorize?response_type=code&client_id=fccf3c32c4a9e1094a878afd7fae0023e996dd820d408762&redirect_uri=https%3A%2F%2Foauth.pstmn.io%2Fv1%2Fc
Windows Security
Select a Certificate
Site logincert.anaf.ro needs your credentials:
oss.test
Issuer: Anaf Issue CA2
Valid From: 31.01.2022 to 30.01.2025
Click here to view certificate properties
More choices
OK
Cancel


oauth.pstmn.io
https://oauth.pstmn.io/v1/callback?code=26e70aee33e5db0def7b495029817a84575dc4fd27b36dc402a38fc5e6d31844
Your call is authenticated
A new windo
ows pop-ups.
Did you mean to switch apps?
Did you mean to switch apps?
"Microsoft Edge" is trying to open "Postman".
Yes
No



Token Details Use Token

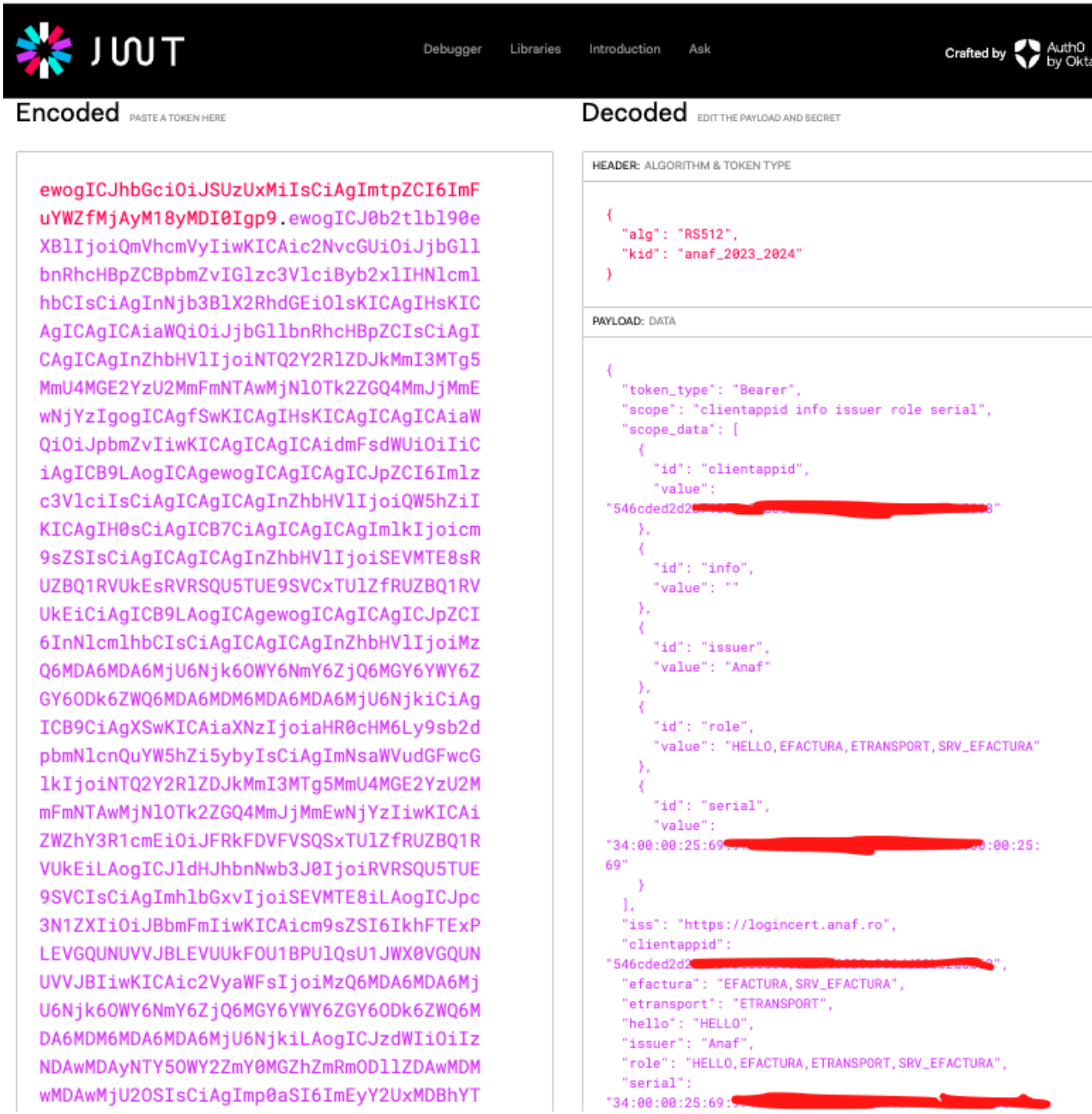
Token Name JWT TOKEN

Access Token

ewogICJhbGciOiJSUzUxMiIsCiAgImtpZCI6ImFuYWZfMjAyM18yMDI
0Igp9.ewogICJ0b2tlbl90eXBlIjoiQmVhcmVyIiwKICAic2NvcGUiOiJjb
GllbnRhcHBpZCBpbmZvIGlzc3VlciByb2xlIHNlcmlhbCIsCiAgInNjb3B
lX2RhdGEiOlsKICAgIHsKICAgICAgICAiaWQiOiJjbGllbnRhcHBpZCIs
CiAgICAgICAgInZhbHVlIjoiNTQ2Y2RlZDJkMmI3MTg5MmU4MGE2
YzU2MmFmNTAwMjNlOTk2ZGQ4MmJjMmEwNjYzIgogICAgfSwKIC
AgIHsKICAgICAgICAiaWQiOiJpbmZvIiwKICAgICAgICAidmFsdWUiO
iliCiAgICB9LAogICAgewogICAgICAgICJpZCI6ImIzc3VlciIsCiAgICAg
ICAgInZhbHVlIjoiQW5hZiIKICAgIH0sCiAgICB7CiAgICAgICAgImlkIjoi
cm9sZSIsCiAgICAgICAgInZhbHVlIjoiSEVMTE8sRUZBQ1RVUkEsRV
RSQU5TUE9SVCxTUlZfRUZBQ1RVUkEiCiAgICB9LAogICAgewogIC
AgICAgICJpZCI6InNlcmlhbCIsCiAgICAgICAgInZhbHVlIjoiMzQ6MDA
6MDA6MjU6Njk6OWY6NmY6ZjQ6MGY6YWY6ZGY6ODk6ZWQ6M
DA6MDM6MDA6MDA6MjU6NjkiCiAgICB9CiAgXSwKICAiaXNzIjoiaH

Se observa ca token-ul obtinut este ca dimensiune mai mare decat un token opaque. Acest lucru se datoreaza faptului ca acesta contine informatia necesara procesarii.

Informatiile din token pot fi verificate folosind orice tool online de decodare a token-urilor de tip JWT, cum ar fi https://jwt.io :



La finalul token-ului se pot vedea si data la care s-a emis token-ul, iss, data de expirare, exp.

Access token-ul JWT este emis pe 90 de zile, refresh token-ul este emis pe 365 de zile. Folosirea refresh token-ului duce la obtinearea unui nou access token JWT.

Access token-ul JWT este semnat digital, validarea lui la procesare se face prin verificarea criptografica a semnaturii. Manipularea token-ului duce la invalidarea acestuia si imposibilitatea utilizarii lui in continuare. Utilizatorii sunt responsabili de manipularea in mod securizat a token-urilor si de eventuala pierdere sau interceptare a lor de catre utilizatori neautorizati.

Token-ul obținut este folosit pentru autorizarea în serviciile API puse la dispoziție pentru care s-a solicitat înregistrarea aplicației.

Cu token-ul generat se acceseaza serviciul web aferent.

Refresh Token JWT

Pentru obtinrea unui access token folosind doar refresh token-ul se poate fie utiliza functia automata de refresh din POSTMAN sau se executa un call de tip POST catre https://logincert.anaf.ro/anaf-oauth2/v1/token cu urmatoarele caracteristici:

- Basic Authentication completat cu client id si client secret folosit
- Requestul trimis sub forma x-www-form-urlencoded cu doi parametrii completati:
    - refresh_token cu valoarea refresh token-ului obtinut în urma solicitării tokenului de acces pentru care se face refresh. Valoarea refresh token-ului se poate gasi în sectiunea Available Tokens – Manage Tokens din Postman.
    - grant_type cu valoarea refresh_token

Clientul este responsabil de gestionarea token-urilor JWT si de a se asigura ca nu sunt accesibile personelor care nu au nevoie de acces la ele.

In cazul unei probleme de securitate la client in care token-urile folosite sunt compromise e nevoie ca ele sa fie trimise ANAF-ului pentru a bloca accesul lor in sistem.

Urmare a apelului, se obține rezultatul 200 OK. În Body se găsesc valorile noi pentru access_token și în refresh_token. Acestea trebuiesc salvate pentru a putea fi folosite in continuare.