

Cuprins

DESCRIERE TEHNICA	1
INREGISTRAREA PENTRU API-URI.....	5
Creare cont nou de utilizator	6
Utilizatorul are un cont pe portalul ANAF.....	9
Recuperare credentiale/parola	11
AUTENTIFICARE	12
INREGISTRARE APLICATIE PROFIL OAUTH	14
Prezentare Aplicatie profil OAUTH	14
Gestionare aplicatii	15
Istoric	18
Renuntare OAUTH.....	19
TOKEN OAUTH.....	21
Obtinerea tokenului de acces de tip JWT.....	21
Refresh Token JWT	28
Obtinerea token-ului de access de tip OPAQUE	29
Refresh Token OPAQUE	33
Revocare Token OPAQUE.....	34
LISTA SERVICII DE TIP API DEZVOLTATE DE ANAF PROFIL OAUTH	37
Serviciul web pentru sistemul national privind facture electronica RO e-Factura.....	37
Serviciul web pentru sistemul electronic integrat RO e-Transport	37
Serviciul web de test "TestOauth"	38
ALTE INFORMATII TEHNICE.....	40
Perioada de valabilitate a parametrilor utilizati.....	40
Mesajele care se pot obtine la apelul serviciilor web.....	40
Limite accesari api.anaf.ro	40
ASISTENTA TEHNICA	41

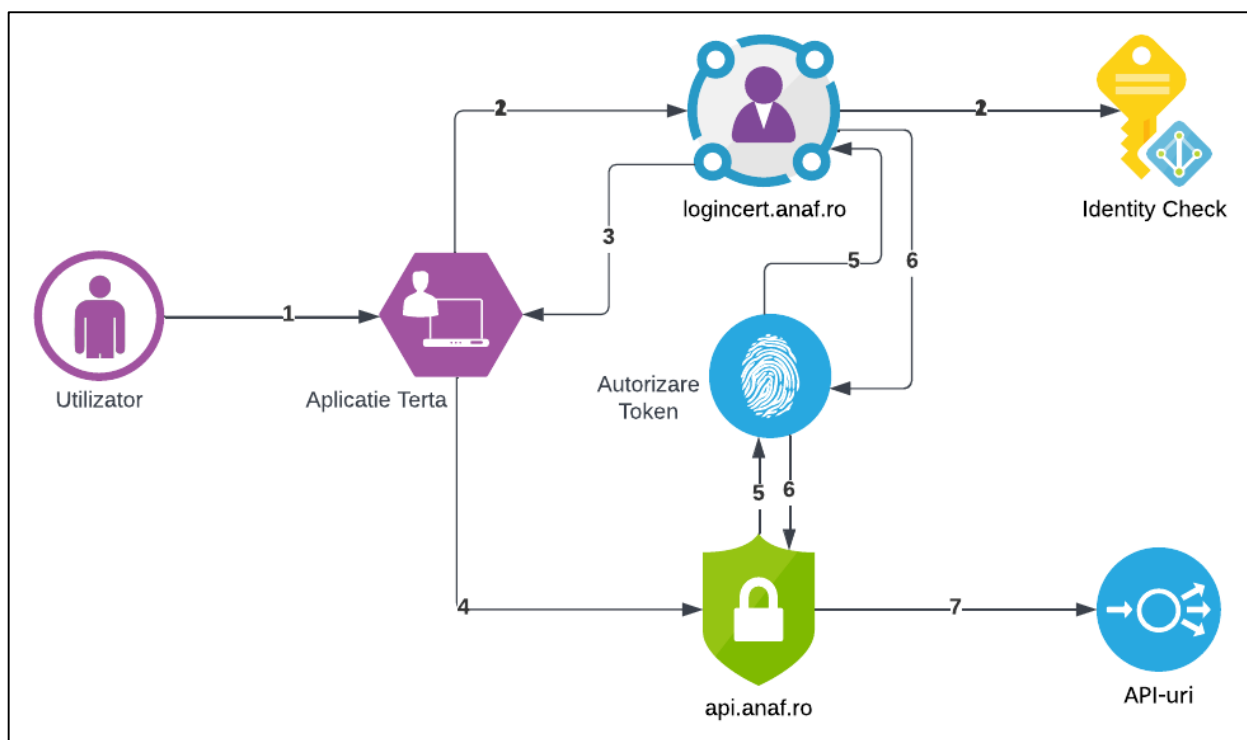
DESCRIERE TEHNICA

Pentru integrarea serviciilor ANAF expuse în Internet, cu aplicații terțe, web/desktop/mobile, s-a implementat o soluție de autorizare a accesului la serviciile de tip API, dezvoltate de ANAF, folosind mecanisme standard bazate pe folosirea protocolului OAUTH. **Această soluție este destinată dezvoltatorilor de aplicații. Sunt necesare cunoștințe de IT și de protocol Oauth 2.0. Este necesară dezvoltarea unei aplicații pentru folosirea acestei soluții.**

Pentru acest lucru s-au definit două servicii expuse în Internet, cu următoarele roluri:

- **logincert.anaf.ro** - serviciu de tip “Identity Provider” - IdP, ce facilitează obținerea unor token-uri de acces folosite pentru autorizarea accesului la servicii de tip API. Obținerea se face prin autentificarea utilizatorului folosind certificate digitale calificate.
- **api.anaf.ro** - serviciu protejat ce expune API-uri care necesită acces autorizat pe bază de token-uri de acces.

Schema după care funcționează soluția este prezentată în figura următoare:



Pașii pentru utilizarea soluției sunt următorii:

- Utilizatorul înregistrat pe portalul ANAF cu certificat digital calificat cu unul din drepturile de SPV PJ (reprezentant legal, reprezentant desemnat, imputernicit) accesează o aplicație terță. Aceasta poate să fie:
 1. o aplicație de tip mobile, nativă Android/IOS,
 2. o aplicație de tip desktop sau
 3. o aplicație de tip web (site web)
- Prin intermediul aplicației terțe utilizatorul este redirecționat către IdP, logincert.anaf.ro, pentru autentificare și obținerea token-ului de autorizare. Autentificarea se face folosind certificatul digital calificat al utilizatorului înregistrat pe portalul ANAF cu unul din drepturile de SPV PJ (reprezentant legal, reprezentant desemnat, imputernicit). Pentru înregistrarea în SPV accesați link-ul: <https://www.anaf.ro/InregPersFizicePublic/#tabs-2>. În pasul de generare al token-ului se iau în considerare două lucruri:
 1. Drepturile de acces ale utilizatorului definite de serialul certificatului înrolat în sistemele ANAF cu unul din drepturile de SPV PJ (reprezentant legal, reprezentant desemnat, imputernicit);
 2. Drepturile de acces ale aplicației terțe către serviciile expuse de ANAF.
- IdP-ul returnează aplicației terțe un token de autorizare pe baza drepturilor aplicației și a utilizatorului
 1. Dacă utilizatorul nu are acces la serviciu dar aplicația terță are, IdP-ul va returna un token care nu-i va permite utilizatorului să acceseze serviciul respectiv;

2. Dacă utilizatorul are acces la serviciu dar aplicația terță nu a fost înrolată la serviciul respectiv, IdP-ul va returna un token care nu-i va permite utilizatorului să acceseze serviciului prin intermediul acelei aplicații;
 3. Dacă utilizatorul are acces la serviciu și aplicația terță a fost înrolată corect pentru serviciul respectiv, IdP-ul va returna un token ce-i permite utilizatorului să acceseze serviciul protejat prin aplicația utilizată;
 4. Orice token furnizat de IdP permite accesul cel puțin spre serviciul de testare de tip “Hello”, denumit TestOAuth. Serviciul “Hello” va fi customizat pe viitor pentru a afișa mai multe informații.
- Aplicația terță accesează o resursă protejată aflată în spatele serviciului api.anaf.ro folosind token-ul obținut la pasul 3;
 - Resursa protejată, api.anaf.ro, autorizează accesul către API-uri folosind un mecanism de validare la IdP al token-ului prezentat;
 - IdP-ul validează token-ul prezentat;
 - Resursa protejată permite accesul către API-ul accesat.

Token-urile emise de către IdP sunt de tip “authorization code”, opaque sau **JWT** cu o durată de valabilitate mare, care pot fi ulterior folosite de către aplicații terțe. Token-ul Opaque nu transportă nici o informație despre aplicații sau utilizatori, acesta autorizează accesul utilizatorului la serviciile la care este înrolat, token-ul JWT poate fi decodat și conține informații despre aplicație, utilizator și nivelul de acces pentru utilizator. Responsabilitatea păstrării în mod securizat a token-urilor revine dezvoltatorilor de aplicații care folosesc acest mecanism.

Aplicația terță poate să stocheze în mod securizat token-ul obținut de utilizator pentru refolosiri ulterioare, sau poate să revoce token-ul respectiv instruind IdP-ul să revoce acel token. Odată revocat un token, acesta nu va mai fi validat și autorizat pentru acces. Modul în care se tratează managementul token-urilor depinde de fiecare aplicație în parte și de modul în care a fost construită. Managementul token-urilor se face folosind mecanismele standard puse la dispoziție de OAuth2.0. URL-urile de management sunt:

Authorization Endpoint	https://logincert.anaf.ro/anaf-oauth2/v1/authorize
Token Issuance Endpoint	https://logincert.anaf.ro/anaf-oauth2/v1/token
Token Revocation Endpoint	https://logincert.anaf.ro/anaf-oauth2/v1/revoke

Ldap-ul returnează un set format din două token-uri, unul de autorizare (Authorizarion Token) si unul de refresh (Refresh Token). Refresh token-ul poate fi folosit pentru obținerea unui nou Authorization Token. Ambele pot fi reutilizate.

Pentru folosirea soluției de autorizare a accesului la serviciile de tip API, dezvoltate de ANAF, folosind mecanisme standard bazate pe folosirea protocolului OAUTH, dezvoltatorii de aplicații au la dispoziție un mecanism de înrolare a aplicațiilor în sistemele ANAF. Utilizatorii aplicațiilor trebuie să fie înregistrați și înrolați în sistemele ANAF, cu drepturi de acces către diverse servicii furnizate de portalul ANAF.

INREGISTRAREA PENTRU API-URI

Pentru înregistrarea utilizatorilor care vor înregistra la rândul lor aplicații ce vor folosi soluția de autorizare a accesului la serviciile de tip API disponibile pe portalului ANAF, se accesează portalul <https://anaf.ro>, secțiunea: Servicii Online>Inregistrare utilizatori>DEZVOLTATORI APLICAȚII



Această secțiune pune la dispoziție două servicii:

- Înregistrare pentru API-uri
- Instrucțiuni de utilizare

Pentru înregistrarea utilizatorilor ce vor înregistra la rândul lor aplicațiile ce vor utiliza soluția de autorizare a accesului la serviciile de tip API, dezvoltate de ANAF, folosind mecanisme standard bazate pe folosirea protocolului OAUTH, se accesează link-ul “Înregistrare pentru API-uri”>

Aici exista două situații:

1. Utilizatorul nu are niciun cont pe portalul ANAF
2. Utilizatorul are un cont pe portalul ANAF

Creare cont nou de utilizator

Pentru înregistrarea unui cont nou de utilizator se selectează secțiunea “Înregistrare pentru API-uri” în formularul web care se afișează:

The screenshot displays the ANAF website's navigation menu and a grid of service tiles. The navigation menu at the top includes: Despre ANAF, Asistență Contribuabili, Servicii Online, Info publice, Info ANAF, Info UE, and Contact. Below the menu is a dark blue banner with the text "Inregistrare utilizatori". Underneath the banner is a button labeled "Ascultă" with a play icon. A large red arrow points down to the "DEZVOLTATORI APLICAȚII" tile in the grid. This tile contains the following text: "Inregistrare pentru API-uri", "Recuperare credențiale/parolă" (with a small icon), "Instrucțiuni de utilizare - actualizat în data de 23.06.2022", and "Formular de contact". The other tiles in the grid are: "SPAȚIUL PRIVAT VIRTUAL" (with a building icon), "DEPUNERE DECLARAȚII" (with an icon of three people), and "NON-RESIDENTS" (with an icon of two people shaking hands over a globe).

Inregistrare pentru API-uri

Pentru înregistrare cu un cont existent de Portal/SPV [click aici](#).

Nume: *	
Prenume: *	
Adresă de email: *	
Confirmare adresă de email: *	
CNP: *	
Tip act de identitate: *	Selectati
Serie act identitate: *	
Număr act identitate: *	
Număr telefon: *	
Nume utilizator: *	
Parolă: *	
Confirmare parolă: *	

☐ Sunt de acord cu [Termenii și condițiile de utilizare a serviciului](#).

Vă rugăm să completați codul de validare cu cifrele și literele afișate în imaginea de mai jos.



Se completează datele aferente utilizatorului în formularul web care se afișează.

Nume: *	Test E-Factura
Prenume: *	API
Adresă de email: *	test@gmail.com
Confirmare adresă de email: *	test@gmail.com
CNP: *	111111111111
Tip act de identitate: *	Selectati
Serie act identitate: *	AB
Număr act identitate: *	123456
Număr telefon: *	0712345678
Nume utilizator: *	test factura
Parolă: *	****
Confirmare parolă: *	****

☒ Sunt de acord cu [Termenii și condițiile de utilizare a serviciului.](#)

Vă rugăm să completați codul de validare cu cifrele și literele afișate în imaginea de mai jos.

Continuă

Se apasă butonul „Continuă”.

Utilizatorul va primi pe e-mail codul de verificare a adresei de e-mail.



Cod verificare email API ANAF
autoritate.MFP to:

Codul de validare al emailului 402811

La „Cod de verificare” se va introduce codul primit pe e-mail.

Cod de verificare: 402811 *

Vă rugăm să completați codul de validare cu cifrele și literele afișate în imaginea de mai jos.

Se apasă butonul „Continuă”.

Utilizatorul va primi mesajul de succes:

Contul a fost creat cu succes .
Nume de utilizator : test factura

Utilizatorul are un cont pe portalul ANAF

În situația în care utilizatorul are un cont de utilizator pe portalul ANAF, procedează în felul următor: accesează și completează informațiile din macheta de mai jos.

Înregistrare cu un cont existent de portal/SPV:

Inregistrare pentru API-uri



Pentru înregistrare cu un cont existent de Portal/SPV [click aici](#).

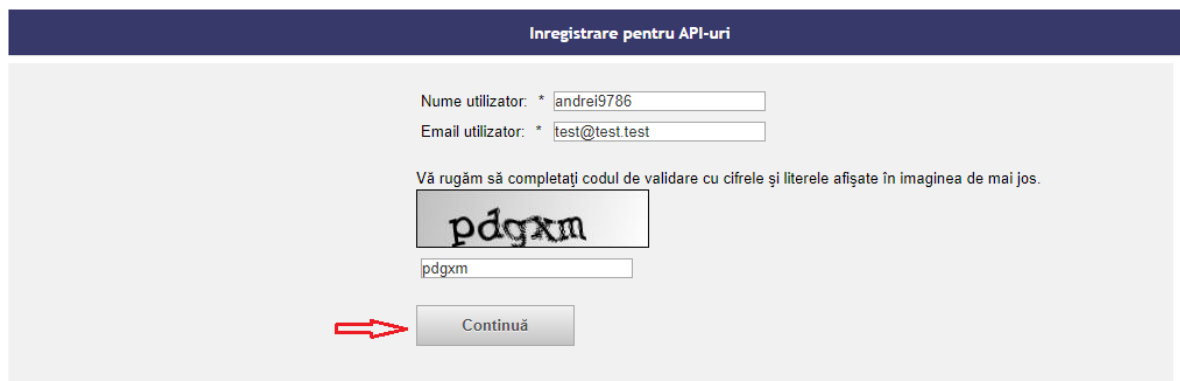
Nume: *	
Prenume: *	
Adresă de email: *	
Confirmare adresă de email: *	
CNP: *	
Tip act de identitate: *	Selectati
Serie act identitate: *	
Număr act identitate: *	
Număr telefon: *	
Nume utilizator: *	
Parolă: *	
Confirmare parolă: *	

☐ Sunt de acord cu [Termenii și condițiile de utilizare a serviciului](#).

Vă rugăm să completați codul de validare cu cifrele și literele afișate în imaginea de mai jos.



Se completează datele aferente utilizatorului în formularul web care se afișează.



Se apasă butonul „Continuă”.

Utilizatorul va primi pe e-mail, codul de verificare a adresei de e-mail.

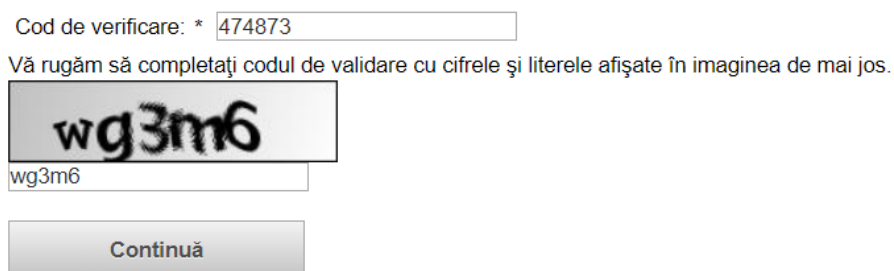
Cod verificare email API ANAF

autoritate.MFP@mfinante.ro

către eu ▼

Codul de validare al emailului 474873

La „Cod de verificare” se va introduce codul primit pe e-mail.



Se apasă butonul „Continuă”.

Utilizatorul va primi mesajul de succes:



După parcurgerea pașilor de înregistrare ce au ca scop final înregistrarea aplicațiilor terțe ce vor folosi soluția de autorizare a accesului la serviciile de tip API disponibile pe portalului ANAF, pași diferențiați în funcție de situația dacă utilizatorul are sau nu cont pe portalul ANAF, se accesează butonul "Autentificare utilizator":

Autentificare utilizator

[Recuperare credentiale/parola](#)

În situația în care utilizatorul dorește recuperarea credențialelor/parolei procedează în felul următor: accesează secțiunea "Recuperare credențiale/parolă" și completează informațiile din macheta de mai jos.

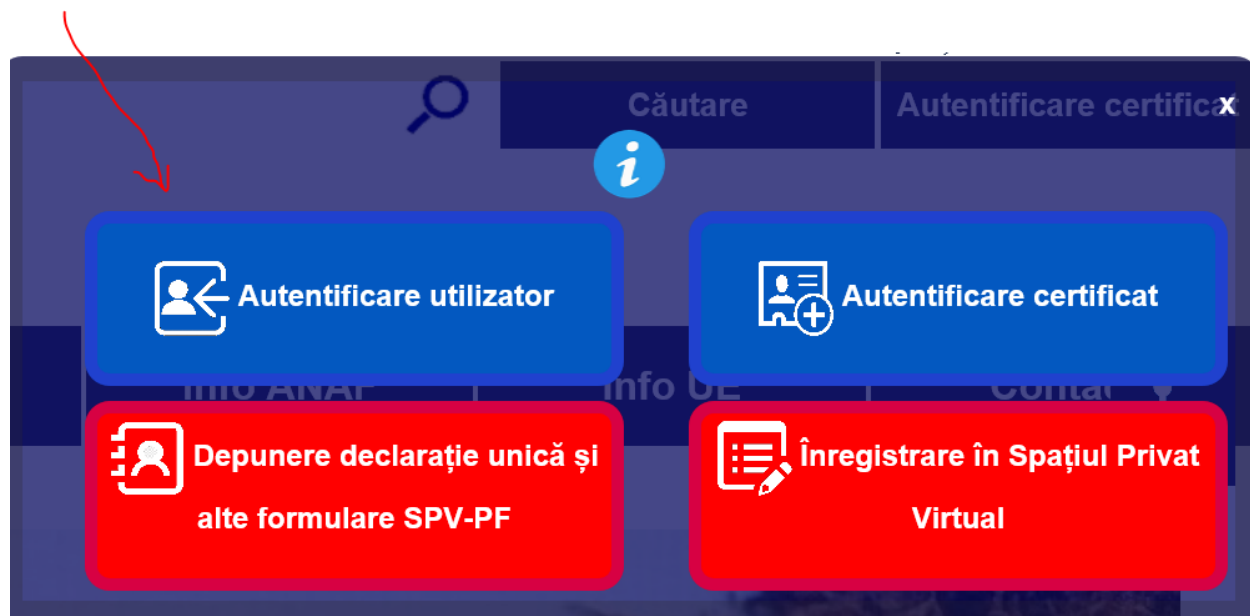


Se completează CNP și email utilizator :

Cnp : *

Email utilizator: *

AUTENTIFICARE



Se introduc numele și parola:



Autentificare username si parola

Utilizator
test factura

Parola

Autentificare

Dacă nu sunteți înregistrat ca utilizator al SPV iată [instrucțiunile](#) necesare înrolării.
Dacă dispuneți de un certificat digital calificat înregistrat pe portalul ANAF (<https://www.anaf.ro>),
vă recomandăm să accesați [aplicația](#) "Abonare/Editare - Spațiul Privat Virtual - Persoane Fizice" pentru a deveni utilizator SPV.
Dacă dispuneți de un certificat digital calificat și nu sunteți înregistrat pe portalul ANAF (<https://www.anaf.ro>),
vă recomandăm să accesați [aplicația](#) "Înregistrare utilizatori declarații persoane fizice", pentru a vă putea abona ca utilizator la SPV.

[Parolă pierdută](#)
[Recuperare credențiale](#)
[Schimbare adresa de email](#)

Click pe butonul „Autentificare”>

Click pe meniul “Editare profil OAuth”

Se ajunge în aplicația „Editare profil OAuth”>

SPV
Spațiul Privat Virtual

SPV > Editare profil OAuth

Deconectare

Instrucțiuni de utilizare Editare profil OAuth

Profil OAuth

Denumire aplicație: *

Callback URL 1: *

Serviciu: * E-Factura

Generare Client ID

Există servicii existente pentru contul dvs.

Denumire aplicație	Client ID	Client Secret

Salvează aplicația

Valori pentru obținerea tokenului OAuth pentru aplicația

Selectați o aplicație din tabela de mai sus.

INREGISTRARE APLICATIE PROFIL OAUTH

Prezentare Aplicatie profil OAUTH

Aplicația are disponibile următoarele servicii:

^ Meniu

Gestionare aplicații

Istoric

Renunțare OAuth

Profil OAuth

Callback URL 1: *

Serviciu:

Generare Client ID

- Gestionare aplicații
- Istoric
- Renunțare OAuth

Gestionare aplicatii

Se completează datele în formularul web care se afișează:

1. Denumirea aplicației ce se va înregistra;
2. Se selectează serviciul oferit de portalul ANAF, dintr-un nomenclator de servicii.

Sunt puse la dispoziție următoarele servicii:

- **E-Factura** (Servicii web pentru Sistemul national privind factura electronica
RO e-Factura)
- **E-Transport** (Servicii web pentru Sistemul electronic integrat RO e-Transport)

Instrucțiuni de utilizare	Editare profil OAuth
---------------------------	----------------------

^ Meniu

Profil OAuth

Denumire aplicație: *
Callback URL 1: * +
Serviciu: *

☐ ☐ ☐

☐ ☐ ☐

Generare Client ID

Denumire aplicație

Client Secret

Mai jos exemplificăm pentru serviciul de factură electronică, cu mențiunea că în același fel se procedează și pentru restul serviciilor ce există în cadrul acestui nomenclator, dacă se dorește utilizarea acestora.

^ Meniu

Profil OAuth

Denumire aplicație: *
Callback URL 1: * +
Serviciu: *

☐ ☐ ☒

☐ ☐ ☒

Generare Client ID

* În cazul în care folosiți utilitarul POSTMAN, se va trece Url-ul <https://oauth.pstmn.io/v1/callback> (Url folosit pentru autentificarea cu browserul)

Client ID-uri OAuth existente pentru contul dvs.		
Denumire aplicație	Client ID	Client Secret
Nu au fost găsite înregistrări.		
Șterge aplicația		

Valori pentru obținerea tokenului OAuth pentru aplicația	
Nu au fost găsite înregistrări.	

Se apasă butonul „Generare Client ID”>

^ Meniu

Profil OAuth

Denumire aplicație: *

Callback URL 1: * +

Serviciu: * E-Factura x ▼

i Client Id:
Client Secret:
S-a creat profilul aplicației E-Factura x

Client ID-uri OAuth existente pentru contul dvs.		
Denumire aplicație	Client ID	Client Secret
EFactura	7d1...	e88k...

Valori pentru obținerea tokenului OAuth>

Pentru a vedea detaliile aferente valorilor pentru obținerea tokenului OAuth se dă click pe înregistrarea aferentă aplicației înregistrată:

Denumire aplicație: *

Callback URL 1: * +

Serviciu: * E-Factura x ▼

Client ID-uri OAuth existente pentru contul dvs.		
Denumire aplicație	Client ID	Client Secret
EFactura		

[Șterge aplicația](#)

Valori pentru obținerea tokenului OAuth pentru aplicația EFactura	
Grant Type	Authorization Code
Callback URL	Url-ul aplicației
Auth URL	https://loginapi.fiscnet.ro/f5-oauth2/v1/authorize https://loginapi.fiscnet.ro/f5-oauth2/v1/token https://loginapi.fiscnet.ro/f5-oauth2/v1/revoke
Client ID	
Client Secret	

Se afișează informațiile referitoare la câmpurile:

Grant Type:

Callback URL:

Auth URL:

Client ID:

Client Secret:

Istoric

Pentru a vedea istoricul operațiunilor efectuate, din meniu se selectează serviciul „Istoric”:

^ Meniu

Gestionare aplicații
Istoric
Renunțare OAuth

Profil OAuth

Callback URL 1: * [+](#)

Serviciu: ▼

Generare Client ID

Istoric

^ Menu

Istoric operații

Operații efectuate - ștergere sau creare de aplicații				
(1 of 1) 1 15				
Denumire aplicație	Client ID	Operație	Serviciu	Data operație
EFactura		Creare	E-Factura	26.01.2022 12:34
Efactura		Ștergere		26.01.2022 12:31
Efactura		Creare		17.01.2022 08:21
EFactura		Ștergere		17.01.2022 08:13
EFactura		Creare		14.01.2022 09:18
(1 of 1) 1 15				

Renuntare OAuth

În situația în care se dorește renunțarea la serviciul OAuth, din meniu se selectează serviciul „Renunțare OAuth”:

^ Meniu

Gestionare aplicații
Istoric
Renunțare OAuth

Profil OAuth

Callback URL 1: *

+

Serviciu:

▼

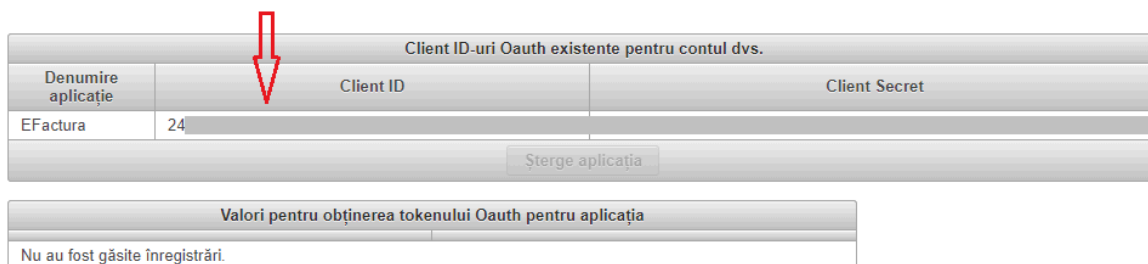
Generare Client ID

Renunțare Oauth

Renunțare OAuth

Renunțarea la serviciul OAuth implică ștergerea tuturor aplicațiilor și implicit a perechilor client ID - client secret, precum și anularea accesului la aplicația Profil OAuth. Accesul aplicațiilor client care folosesc tokenurile asociate perechilor client ID - client secret va fi de asemenea anulat. Pentru a putea solicita tokenuri de acces noi va trebui să vă înregistrați din nou.

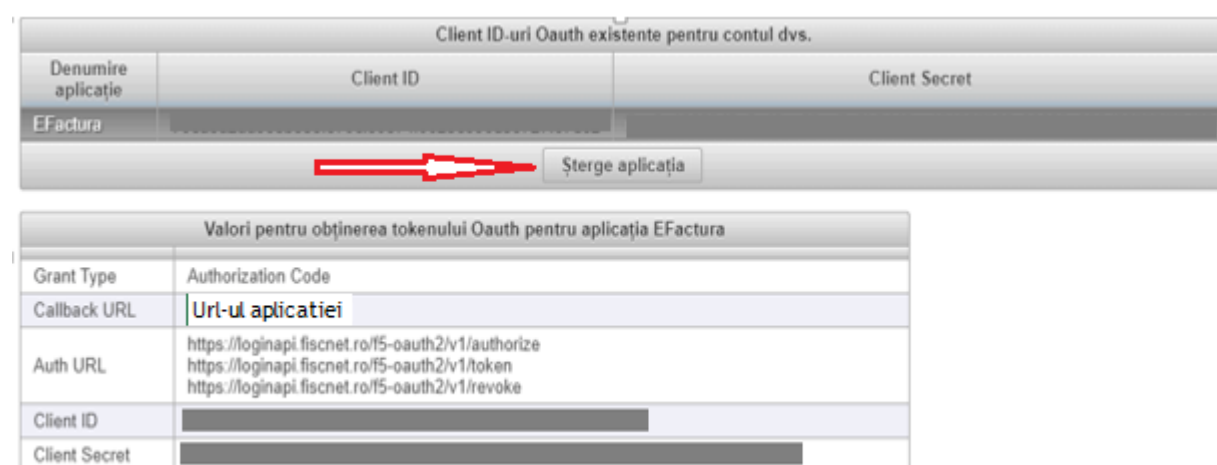
Se selectează aplicația care se dorește a se șterge:



Client ID-uri OAuth existente pentru contul dvs.		
Denumire aplicație	Client ID	Client Secret
EFactura	24	

Valori pentru obținerea tokenului OAuth pentru aplicația	
Nu au fost găsite înregistrări.	

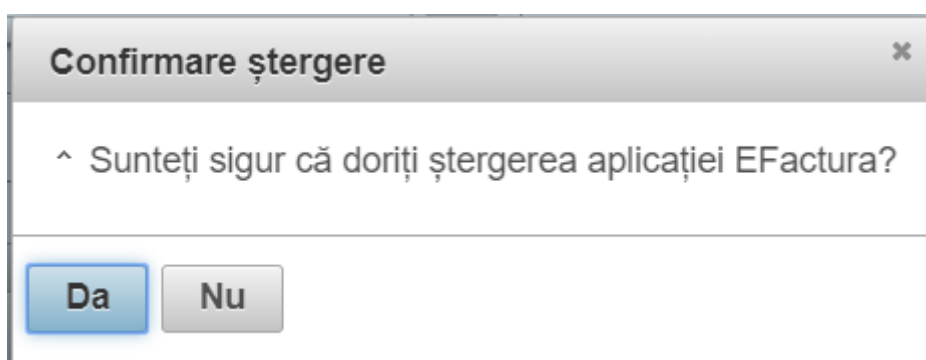
Se apasă butonul “Șterge aplicația”>



Client ID-uri OAuth existente pentru contul dvs.		
Denumire aplicație	Client ID	Client Secret
EFactura		

Valori pentru obținerea tokenului OAuth pentru aplicația EFactura	
Grant Type	Authorization Code
Callback URL	Url-ul aplicatiei
Auth URL	https://loginapi.fiscnet.ro/f5-oauth2/v1/authorize https://loginapi.fiscnet.ro/f5-oauth2/v1/token https://loginapi.fiscnet.ro/f5-oauth2/v1/revoke
Client ID	
Client Secret	

Confirmare ștergere>



Confirmare ștergere ×

^ Sunteți sigur că doriți ștergerea aplicației EFactura?

Mesajul de succes>

^ Meniu

Profil OAuth

Denumire aplicație: *

Callback URL 1: *

Serviciu:

Generare Client ID

S-a șters profilul aplicației EFactura
S-a revocat Client id pentru aplicația EFactura

Client ID-uri OAuth existente pentru contul dvs.

Denumire aplicație	Client ID	Client Secret
Nu au fost găsite înregistrări.		

Șterge aplicația

TOKEN OAUTH

Obținerea 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 obținerea 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: obținut de client la înrolarea aplicației

- 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.

Configure New Token

Token Name	se trece denumirea token-ului
Grant Type	Authorization Code
Callback URL ⓘ	https://oauth.pstmn.io/v1/callback
	☒ Authorize using browser
Auth URL ⓘ	https://logincert.anaf.ro/anaf-oauth2/v1/authorize
Access Token URL ⓘ	https://logincert.anaf.ro/anaf-oauth2/v1/token

Client ID ⓘ	se trece client id-ul obtinut ⓘ
Client Secret ⓘ	se trece client secret-ul obtinut ⓘ
Scope ⓘ	e.g. read:org
State ⓘ	State
Client Authentication ⓘ	Send as Basic Auth header ▼
> Advanced	
 Clear cookies ⓘ	
Get New Access Token	

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

▼ Advanced

① You can add more specific customizations to your OAuth2 requests here. [Learn more about configuration](#) ➤

Refresh Token URL ⓘ

<https://logincert.anaf.ro/anaf-oauth2/v1/toker>

Auth Request ⓘ

	Key	Value
☒	token_content_type	jwt
	Create parameter	Value

Token Request ⓘ

	Key	Value	Send In
☒	token_content_type	jwt	Request Body 
	Create parameter	Value	

Refresh Request ④

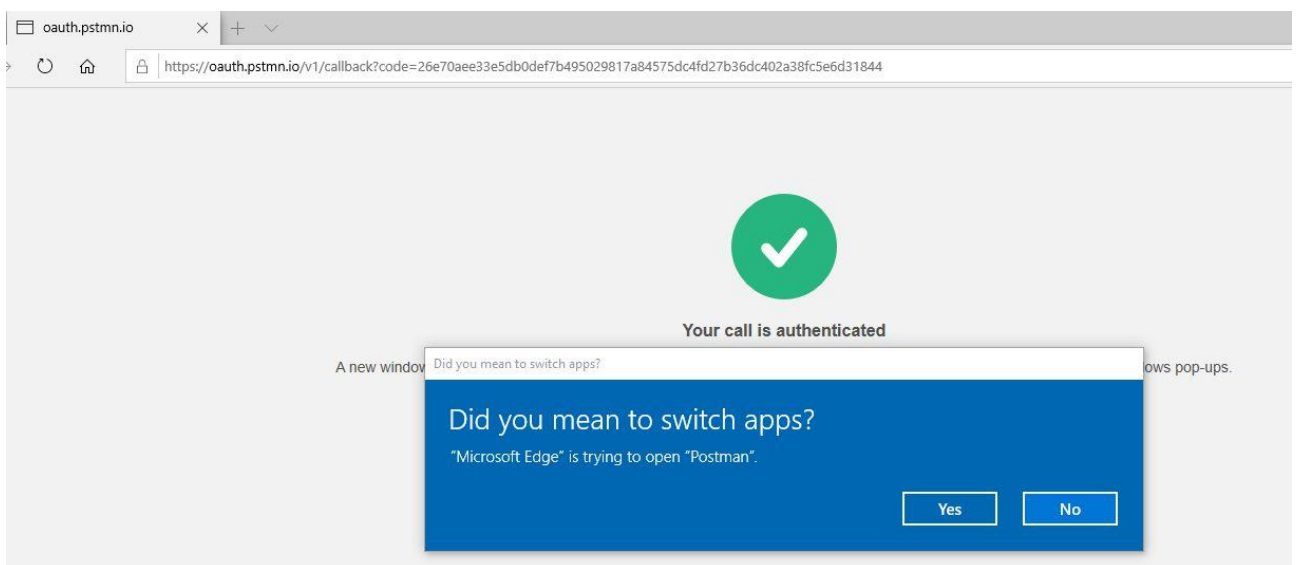
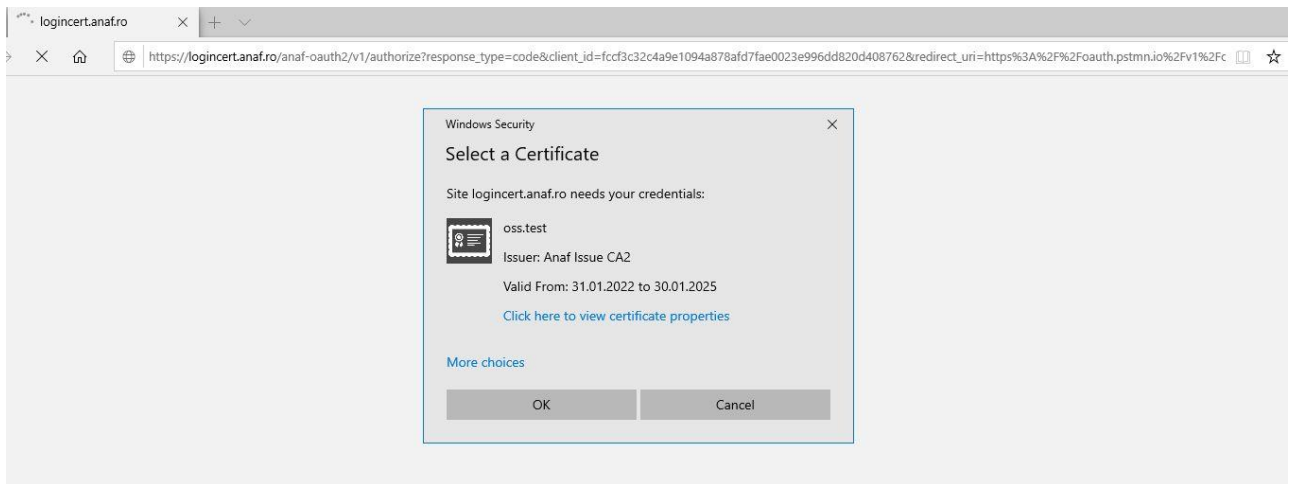
	Key	Value	Send In
	Create parameter	Value	

 Clear cookies 

[Get New Access Token](#)

Cei doi parametrii `token_content_type=jwt` se trimit odata pe Query pentru requestul de Autorizare 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



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

[illegible]

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

```
"iat": 1697733635,
"exp": 1705509635,
"nbf": 1697733335
```

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 obtinerea 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 obtinut 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 obtinerea 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:
 - o 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.
 - o grant_type cu valoarea refresh_token

Clientul este responsabil de gestionarea token-urilor JWT si de a se asigura ca nu sunt accesibile persoanelor 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.

Obținerea token-ului de access de tip OPAQUE

Token-urile de tip OPAQUE vor putea fi folosite pana la data de 15.04.2024. Începând de la acea dată, toți utilizatorii vor folosi doar token-uri de tip JWT. Această implementare are ca scop asigurarea unei bune stabilități a sistemul de autorizare OAUTH, și redundanța acestuia, pentru toate serviciile oferite prin intermediul acestui mecanism de autorizare.

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

Se vor avea în vedere următoarele configurări/setari pentru obținerea 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: obținut de client la inrolarea aplicatiei
- Client Secret: obținut 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.

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

Current Token

This access token is only available to you. Sync the token to let collaborators on this request use it.

Access Token

Available Tokens



[Redacted token value]



Header Prefix ⓘ

Bearer

Configure New Token

Configuration Options ●

Advanced Options

Token Name

se trece denumirea tokenului

Grant Type

Authorization Code



Callback URL ⓘ

https://oauth.pstmn.io/v1/callback ...



Authorize using browser

Auth URL ⓘ

https://logincert.anaf.ro/anaf-
oauth2/v1/authorize

Access Token URL ⓘ

https://logincert.anaf.ro/anaf-
pauth2/v1/token

Client ID ⓘ

se trece Client ID-ul obtinut



Client Secret ⓘ

se trece Client Secret obtinut



Scope ⓘ

e.g. read:org

State ⓘ

State

Client Authentication

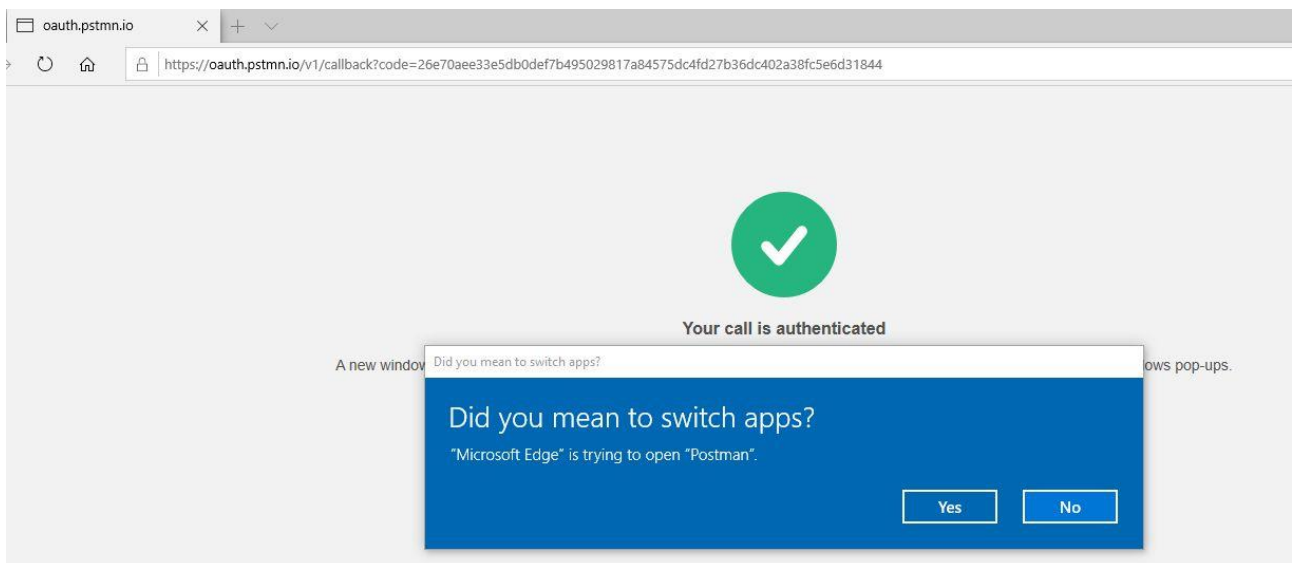
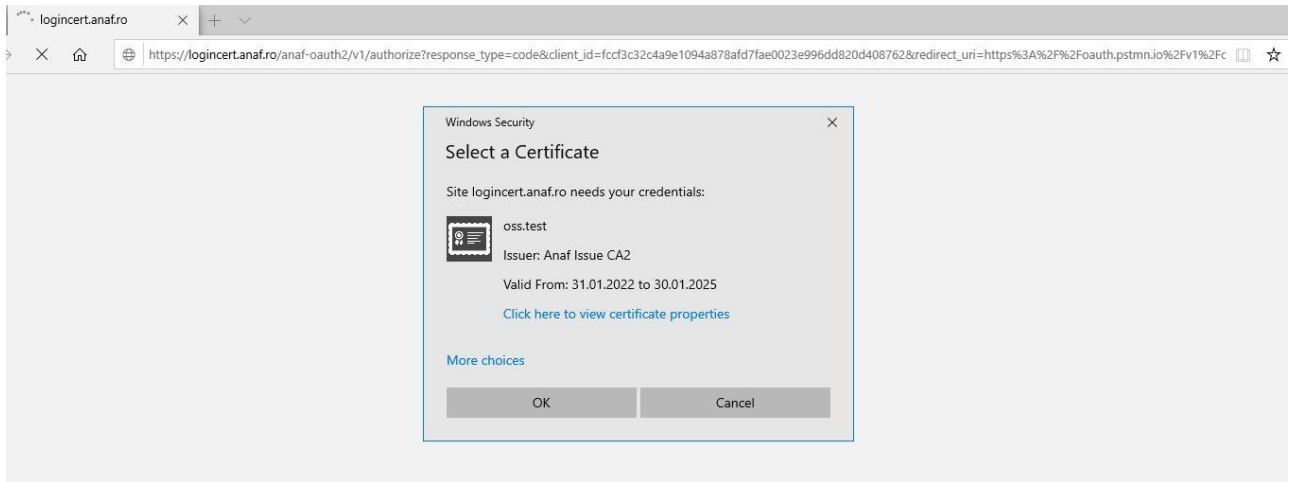
Send as Basic Auth header

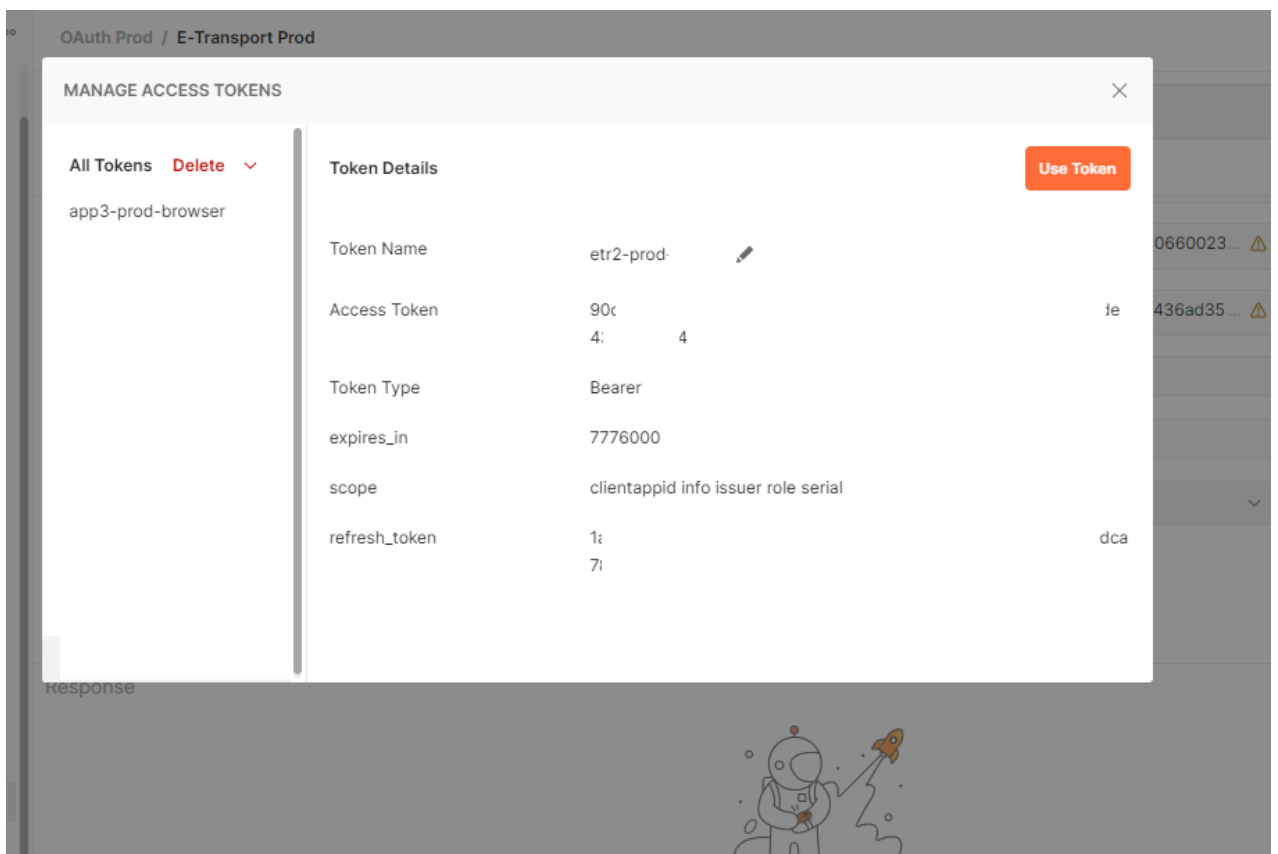
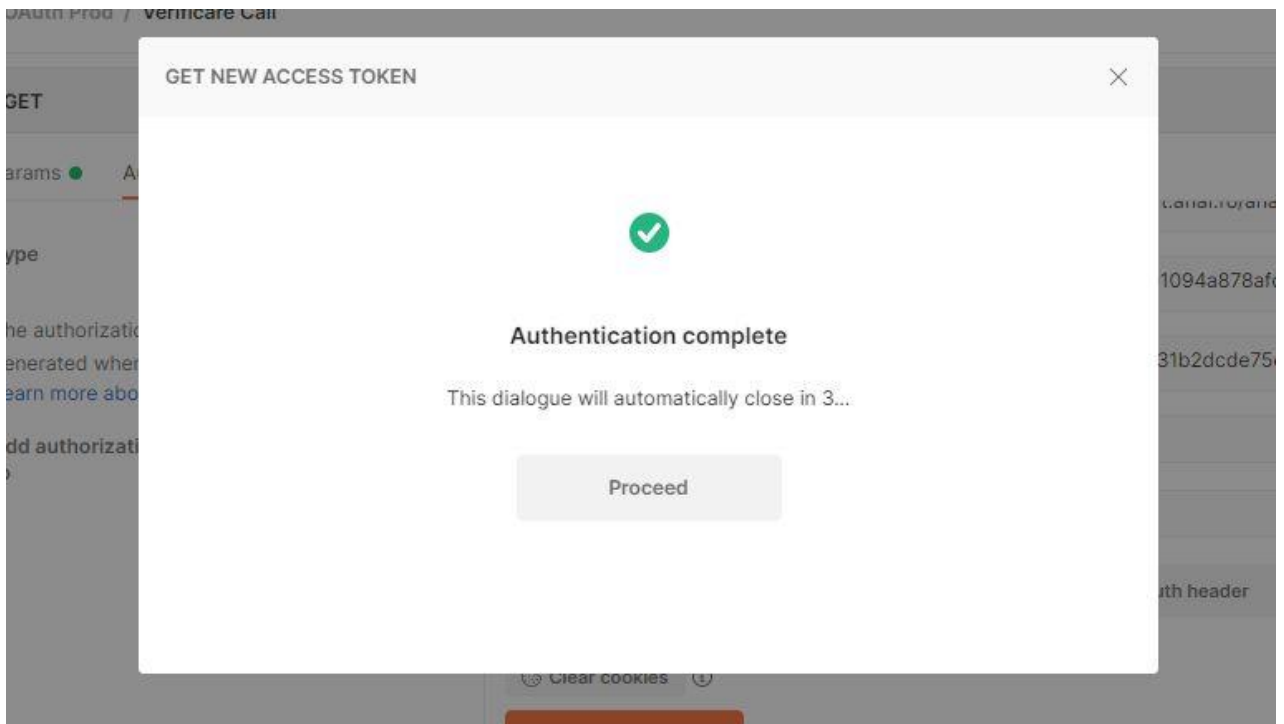


Clear cookies ⓘ

Get New Access Token

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





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 OPAQUE

1. Se execută un call de tip **POST** catre <https://logincert.anaf.ro/anaf-oauth2/v1/token>
2. Se setează Authorization type cu valoarea **OAUTH2 2.0**,
3. Se seteaza Add Authorization Data cu valoarea **Request Headers**
4. Se selectează token-ul folosit
5. In secțiunea Body se bifează si se completează următoarele câmpuri:
6. x-www-form-urlencoded,
7. client_id,
8. client_secret
9. refresh_token
10. grant_type cu valoarea refresh_token.

În imaginea de mai jos exemplificăm pentru apelul aferent prelungirii valabilității token-ului de acces:

The screenshot displays a REST client interface for a POST request to `https://logincert.anaf.ro/anaf-oauth2/v1/token`. The request is configured with the following parameters:

KEY	VALUE	DESCRIPTION
☒ client_id	25a6d1ad263cacb...	
☒ client_secret	966e00081ca20d5f...	
☒ refresh_token	b12c61174565929b...	
☒ grant_type	refresh_token	
Key	Value	Description

The response status is **200 OK** with a time of 106 ms and a size of 421 B. The response body is shown in JSON format:

```
1 {
2   "access_token": "ecc",
3   "expires_in": 7776000,
4   "token_type": "Bearer",
5   "scope": "clientappid info issuer role serial",
6   "refresh_token": "b12"
7 }
```

Urmare a apelului call-ului exemplificat în ecranele de mai sus, se obține rezultatul 200 OK. In Body se găsesc valorile noi pentru access_token și în refresh_token. Acestea trebuie salvate pentru a putea fi folosite in continuare.

Call-ul rulat în Postman are următoarea sintaxă:

POST: https://logincert.anaf.ro/anaf-oauth2/v1/token?client_id=myclientid&client_secret=myclientsecret&refresh_token=mysecretrefreshtoken&grant_type=refresh_token

Perioadele de valabilitate pentru token-urile refresh sunt:

- Refresh Token Lifetime: 1576800 minute = 1095 zile
- Refresh Token Reuse Limit: 64

Revocare Token OPAQUE

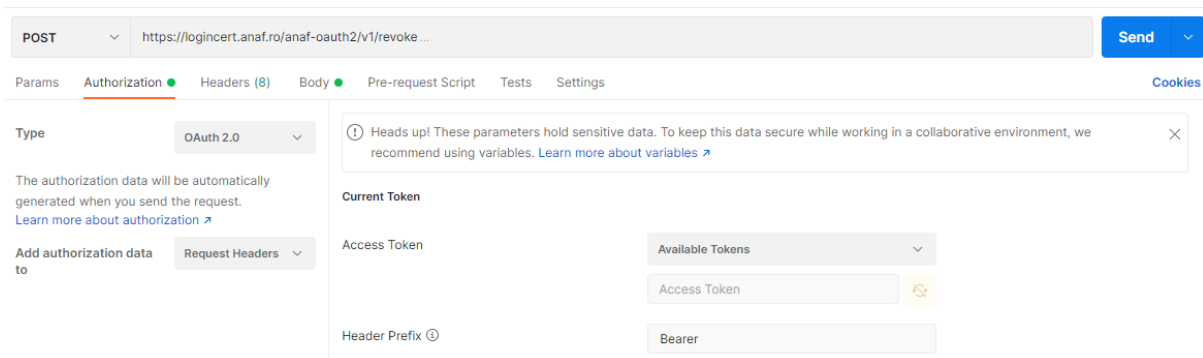
La generarea unui token se obțin două elemente: access token si refresh token.

Pentru revocarea tokenului se folosesc următoarele elemente:

- acces token sau refresh token (se pot folosi oricare din cele doua elemente)
- client ID
- client secret

Pașii pentru revocarea token-ului sunt următorii:

1. Se execută un call de tip **POST** către <https://logincert.anaf.ro/anaf-oauth2/v1/revoke>
2. Se setează Authorization type cu valoarea **OAUTH2 2.0**,
3. Se seteaza Add Authorization Data cu valoarea **Request Headers**
4. Se selectează token-ul ce se dorește a se revoca



5. În secțiunea Body se bifează și se completează următoarele câmpuri:

- a. x-www-form-urlencoded,
- b. client_id,
- c. client_secret
- d. refresh_token sau access_token (oricare funcționează)

În imaginea de mai jos exemplificăm pentru apelul cu folosirea access token-ului:

The screenshot shows a Postman interface for a POST request to `https://logincert.anaf.ro/anaf-oauth2/v1/revoke`. The 'Body' tab is selected, and the 'x-www-form-urlencoded' format is chosen. The body contains three key-value pairs:

KEY	VALUE	DESCRIPTION
☒ client_id	590e5dd...	
☒ client_secret	64a4242...	
☒ access_token	1d4d6db...	

sau:

- a. x-www-form-urlencoded,
- b. client_id,
- c. client_secret
- d. refresh_token

În imaginea de mai jos exemplificăm pentru apelul cu folosirea refresh token-ului:

The screenshot shows a Postman interface for a POST request to `https://logincert.anaf.ro/anaf-oauth2/v1/revoke`. The 'Body' tab is selected, and the 'x-www-form-urlencoded' format is chosen. The body contains three key-value pairs:

KEY	VALUE	DESCRIPTION
☒ client_id	590e5dd...	
☒ client_secret	64a4242...	
☒ refresh_token	542sd84...	

Urmare a apelului celor două call-uri exemplificate în ecranele de mai sus, se obține rezultatul 200 OK, ceea ce înseamnă că token-ul a fost revocat.

Call-ul de tip x-www-form-urlencoded rulat în Postman are următoarea sintaxă:

a. În cazul în care se folosește **acces token**:

POST: https://logincert.anaf.ro/anafoauth2/v1/revoke?client_id=myclientid&client_secret=myclientsecret&access_token=mysecretaccesstoken

sau:

b. În cazul în care se folosește **refresh token**:

POST:

https://logincert.anaf.ro/anafoauth2/v1/revoke?client_id=myclientid&client_secret=myclientsecret&refresh_token=mysecretrefreshtoken

LISTA SERVICII DE TIP API DEZVOLTATE DE ANAF PROFIL OAUTH

Serviciul web pentru sistemul national privind facture electronica RO e-Factura

Mediul de test:

Pentru detalii tehnice, accesați URL-ul:

<https://mfinante.gov.ro/static/10/eFactura/prezentare%20api%20efactura.pdf>

disponibil în cadrul paginii web:

<https://mfinante.gov.ro/ro/web/efactura/informatii-tehnice>

Mediul de producție:

Pentru detalii tehnice, accesați URL-ul:

<https://mfinante.gov.ro/static/10/eFactura/prezentare%20api%20efactura.pdf>

disponibil în cadrul paginii web:

<https://mfinante.gov.ro/ro/web/efactura/informatii-tehnice>

Serviciul web pentru sistemul electronic integrat RO e-Transport

Mediul de test:

<https://api.anaf.ro/test/ETRANSPORT/ws/v1/upload/{val1}/{val2}>

unde:

- *val1* - valoare de tip String - “ETRANSPORT”
- *val2* - CIF

<https://api.anaf.ro/test/ETRANSPORT/ws/v1/stareMesaj/{val1}>

unde:

- *val1* - *id_incarcare* (cod unic de identificare de tip numeric. Se obține din lista de răspunsuri furnizată de api Upload)

<https://api.anaf.ro/test/ETRANSPORT/ws/v1/lista/{val1}/{val2}>

unde:

- *val1* - zile (valorile acceptate sunt între 1 și 60)
- *val2* - CIF

<https://api.anaf.ro/test/ETRANSPORT/ws/v1/descarcare/{val1}>

unde:

- val1 - id (cod unic de identificare de tip numeric. Se obține din lista de răspunsuri furnizată de api Lista)

Mediul de producție:

Pentru detalii tehnice, accesați pagina:

<https://mfinante.gov.ro/ro/web/etransport/informatii-tehnice>

Serviciul web de test "TestOAuth"

De asemenea, pentru verificarea aplicației dezvoltată puteți folosi un serviciu de test „TestOAuth” pus la dispoziție în acest sens:

<https://api.anaf.ro/TestOAuth/jaxrs/hello?name=valoare>

[https://api.anaf.ro/TestOAuth/jaxrs/hello?name="Test Hello App!"](https://api.anaf.ro/TestOAuth/jaxrs/hello?name=)

Acesta returnează cu titlu de exemplu, valorile de mai jos:

Hello, "Test Hello App!"

headers=key=Accept

val=[*/*]

key=Accept-Encoding

val=[gzip, deflate, br]

key=Authorization

val=[Bearer 97.....3]

key=Cache-Control

val=[no-cache]

key=Connection

val=[keep-alive]

key=Host

val=[api.anaf.ro]

key=issuer

val=[Anaf]

key=Postman-Token

val=[.....]

key=serial_certificate

```
val=[.....]  
key=session-id  
val=[.....]  
key=session-key  
val=[.....]  
key=User-Agent
```

ALTE INFORMATII TEHNICE

Perioada de valabilitate a parametrilor utilizati

TOKEN:

- 60 de secunde interval de obținere a unui token valid. După 60 de secunde se resetează conexiunea.

ACCES TOKEN Opaque:

- 129600 minute (24h*60min*90zile), aproximativ 3 luni.

REFRESH TOKEN Opaque: 1576800 minute = 1095 zile

Refresh Token Opaque Reuse Limit: 64

ACCES TOKEN JWT: 129600 minute = 90 zile.

REFRESH TOKEN JWT: 525600 minute = 365 zile

Mesajele care se pot obtine la apelul serviciilor web

- Status code 403 Forbidden - reprezintă un request neautorizat la URL-urile aferente serviciului web de factură.
- 200 OK - reprezintă faptul că autentificarea și autorizarea s-au realizat cu succes, iar serviciul web va returna mesajele aferente de succes sau de eroare în funcție de request-urile care se fac, drepturile certificatului, cui-urile pe care le reprezintă certificatul, informațiile cerute, informațiile încărcate.
- 429 Too Many Requests - reprezintă codul de eroare care apare în momentul în care se depășește limita maximă de apeluri. Limita este setata la 100 de apeluri pe minut.

Limite accesari api.anaf.ro

- 1000 Requests pe 1 minut

Limitele se pot defini si ajusta pe viitor, independent, pentru fiecare serviciu in parte.

ASISTENȚA TEHNICĂ

Pentru asistență tehnică, vă rugăm să folosiți Formularul de contact, alegând categoria "Asistență tehnică servicii informatice", subcategoria "OAUTH".

Despre ANAF	Asistență Contribuabili	Servicii Online	Info publice	Info ANAF	Info UE	Contact
-------------	-------------------------	-----------------	--------------	-----------	---------	---------

Inregistrare utilizatori

Ascultă ▶

SPAȚIUL PRIVAT VIRTUAL


DEPUNERE DECLARAȚII


DEZVOLTATORI APLICAȚII
Inregistrare pentru API-uri
Recuperare credențiale/parolă

Instrucțiuni de utilizare - actualizat în data de 23.06.2022
Formular de contact

NON-RESIDENTS


 Activează asistență vocală

FORMULAR DE CONTACT

Informații cu privire la situația fiscală proprie, supuse secretului fiscal, se pot obține prin intermediul Formularului de contact din cadrul serviciului [Spațiul Privat Virtual](#).

(câmpurile marcate cu steluță sunt obligatorii)

Alegeți categoria solicitării: Asistență tehnică servicii informatice ?

Alegeți subcategoria: * OAUTH ?

Nume: * ?

Cod de identificare fiscală (CUI/CNP/NIF): * ?