# Cuprins

DESCRIERE TEHNICA
INREGISTRAREA PENTRU API-URI
Creare cont nou de utilizator
Utilizatorul are un cont pe portalul ANAF10
Recuperare credentiale/parola12
AUTENTIFICARE
INREGISTRARE APLICATIE PROFIL OAUTH
Prezentare Aplicatie profil OAUTH16
Gestionare aplicatii16
Istoric19
Renuntare OAUTH
TOKEN OAUTH
Obtinerea tokenului de acces de tip JWT23
Refresh Token JWT
LISTA SERVICII DE TIP API DEZVOLTATE DE ANAF PROFIL OAUTH
Serviciul web pentru sistemul national privind facture electronica RO e-Factura
Serviciul web pentru sistemul electronic integrat RO e-Transport
Serviciul web de test "TestOauth"31
ALTE INFORMATII TEHNICE
Perioada de valabilitate a parametrilor utilizati
Mesajele care se pot obtine la apelul serviciilor web
Limite accesari api.anaf.ro
ASISTENTA TEHNICA

## 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 in 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 linkul: <u>https://www.anaf.ro/InregPersFizicePublic/#tabs-2</u>. În pasul de generare al token-ului se iau în considerare două lucruri:
  - 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 aplicatiei terțe către serviciile expuse de ANAF.
- IdP-ul returnează aplicației terțe un token de autorizare pe baza drepturilor aplicației și a utilizatorului
  - 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 seviciul respectiv;
  - 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;

- 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 valideaza token-ul prezentat;
- Resursa protejată permite accesul către API-ul accesat.

Token-urile emise de către IdP sunt de tip "authorization code", JWT cu o durată de valabilitate mare, care pot fi ulterior folosite de către aplicații terțe. Token-ul JWT poat fi decodat si contine informatii despre aplicatie, utilizator si nivelul de acces pentru utilizator. Responsabilitatea păstrarii 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. 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

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

În contextul OAUTH dezvoltatorul unei aplicații software (mobile/web/desktop) este identificat cu un "client app id". Utilizatorii acelei aplicații sunt identificați în cazul sistemelor e-Factura sau e-Transport prin serialul certificatului digital calificat folosit pentru obținerea token-ului Oauth.

Token-urile, atât cel de acces cât și cel de refresh, sunt generate pentru acel certificat digital, și identifică utilizatorul aplicației, nu aplicația în sine. El este asociat unei aplicații, însă acest lucru nu are nicio relevanță pentru identificarea utilizatorului. Toți utilizatorii ajung în același api.anaf.ro (serviciu protejat ce expune API-uri care necesită acces autorizat pe bază de token-uri de acces), fiecare utilizator este autorizat de un token asociat serialului certificatului folosit și aplicației folosite.

Din punct de vedere al securității este fundamental ca dezvoltatorul software să fie identificat unic printr-un client id și nu utilizatorii. Aplicația disponibilă la URL-ul www.anaf.ro/InregOauth este destinată doar dezvoltatorilor de aplicații. Utilizatorii înregistrați în SPV nu trebuie să își creeze cont prin intermediul acestei aplicații, decât dacă sunt și dezvoltatori software și au de înregistrat o aplicație software ce va folosi serviciile electronice puse la dispoziție în cadrul portalului ANAF.

De asemenea, în interfața disponibilă dezvoltatorilor de aplicații, după autentificare, se vor declara aplicațiile web dezvoltate de către dezvoltatori.

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

5



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 cu username și parolă pe portalul ANAF. In cazul unui cont cu certificat digital urmați instrucțiunile de la pasul 1.

## 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:



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 d	condițiile de utilizare a serviciului. e validare cu cifrele și literele aficate în imaginea de mai
	e validare cu cirrele și literele alișate în îmaginea de mai

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: *	11111111111	
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 cu Vă rugăm să completați codul de	ondițiile de utilizare a serviciului. 2 validare cu cifrele și literele afiș	șate în imaginea de mai jos.
enyne		
Continuă		

Se apasă butonul "Continuă".

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



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



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 p	Inregistrare pentru API-uri		
Pentru înregistrare cu un cont exist	ent de Portal/SPV <u>click aici</u> .		
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.

Inregistrare pentru API-uri				
Nume utilizator: * andrei9786 Email utilizator: * test@test.test				
Vă rugăm să completați codul de validare cu cifrele și literele afișate în imaginea de mai jos.           pdgxm				
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@mfinante.ro

către eu 💌

Codul de validare al emailului 474873

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

Cod de verificare: * 474873	
Vă rugăm să completați codul	e validare cu cifrele și literele afișate în imaginea de mai jos.
wg3m6	
Continuă	

Se apasă butonul "Continuă".

Utilizatorul va primi mesajul de succes:

Inregistrare pentru API-uri

Drepturile au fost actualizate cu succes . Nume de utilizator: andrei9786

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 daca 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 :

Continuă

Cnp: *		
Email utilizator: '	k	

AUTENTIFICARE



## Se introduc numele și parola:



#### Autentificare username si parola

Utilizator	
test factura	
Parola	
Autentificare	

Dacă nu sunteți înregistrat ca utilizator al SPV iată <u>instrucțiunile</u> necesare înrolării. Dacă dispuneți de un certificat digital calificat înregistrat pe portalul ANAF (<u>https://www.anaf.ro</u>), vă recomandăm să accesați <u>aplicația</u> "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 (<u>https://www.anaf.ro</u>), vă recomandăm să accesați <u>aplicația</u> "Înregistrare utilizatori declarații persoane fizice", pentru a vă putea abona ca utilizator la SPV.

<u>Parolă pierdută</u> <u>Recuperare credențiale</u> <u>Schimbare adresa de email</u>

Click pe butonul "Autentificare">

	Spațiul Privat Virtual	Deconectare	
	Instrucțiuni de utilizare	Editare profil Oauth	ۍ ا
	Instrucțiuni de v	Silizare GAUTH	
	• 🗟 🔀 Instrucțiuni de utilizare OAUTH		
副			
	O Agenția Națională de Administrare Fiscală - CNEF-	Conținului acestui portal este proprietalea Agenției Naționale de Administrare Faculă	

Click pe meniul "Editare profil Oauth" Se ajunge în aplicația "Editare profil Oauth">

Valori pentru obți

Selectati o aplicatje din tabela de mai su



rea tokenului Oauth pentru aplicația

## INREGISTRARE APLICATIE PROFIL OAUTH

## Prezentare Aplicatie profil OAUTH

#### Aplicația are disponibile următoarele servicii:

^ Meniu	
Gestionare aplicații	Profil Oauth
Istoric	
Renunțare Oauth	
Callback URL 1: *	+
Serviciu:	•
Generare Client ID	

- Gestionare aplicații
- Istoric
- Renuntare Oauth

## Gestionare aplicatii

Se completează datele în formularul web care se afișează:

- 1. Denumirea aplicației ce se va înregistra;
- 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
Moniu				
* meniu		Profil Oauth		
Denumire aplicație: *				
Callback URL 1: *		+		
Serviciu: *	<b></b>			
Generare Client ID				
	E-Factura			
Denumire aplicație	E-Transport	uri Oauth existen	te pentru contu	Il dvs. Client Secret

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

↑ Meniu	Profil Oauth
Denumire aplicație: *	EFactura
Callback URL 1: *	Url-ul aplicatiei +
Serviciu: *	E-Factura ×
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 obțin	erea tokenului Oauth pentru a	plicația		
Nu au fost găsite înregistrări.				

Se apasă butonul "Generare Client ID">

^ Meniu		
	P	rofil Oauth
Denumire aplicație: *	EFactura	
Callback URL 1: *	Url-ul aplicatiei	+
Serviciu: *	E-Factura ×	•
Generare Client ID		

Client Id Client So S-a crea	ecret: t profilui aplicației EFactura	×
	Client ID	uri Oauth existente pentru contul dvs.
Denumire aplicație	Client ID	Client Secret
EFactura	7d ·	e88t
		Șterge aplicația

Valori pentru obținerea tokenului Oauth>

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

Denumire aplicație: *	EFactura	
Callback URL 1: *	Url-ul aplicatiei	+
Serviciu: *	E-Factura ×	
Generare Client ID		

	Client ID-uri Oauth	existente pentru contul dvs.	
Denumire aplicație	Client ID	Client Secret	
EFactura			
	Şte	ge aplicația	
	Valori pentru obținerea tokenului Oauth pentru a	plicația 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			

Se afișează informațiile referitoare la câmpurile:

Grant Type:

Callback URL:

Auth URL:

Client ID:

**Client Secret:** 

## Istoric

Pentru a vedea istoricul operatiunilor efectuate, din meniu se selectează serviciul "lstoric":

^ Meniu	
Gestionare aplicații	Profil Oauth
Istoric	
Renunțare Oauth	
Callback URL 1: *	+
Serviciu:	•
Generare Client ID	

## Istoric

Meniu

Istoric operații

Operații efectuate - ștergere sau creare de aplicații				
(1 of 1) III << 1 >> >> 15 ¥				
Denumire aplicație	Client ID	Operație	Serviciu	Data operație
EFactura		Creare	E-Factura	26.01.2022 12:34
Efactura		Ştergere		26.01.2022 12:31
Efactura		Creare		17.01.2022 08:21
EFactura		Ştergere		17.01.2022 08:13
EFactura		Creare		14.01.2022 09:18
(1 of 1) 14 <4 1 P> P1 15 ¥				

## Renuntare OAUTH

În situația în care se dorește renuntarea la serviciul Oauth, din meniu se selectează serviciul "Renunțare Oauth":

^ Meniu	
Gestionare aplicații	Profil Oauth
Istoric	
Renunțare Oauth	
Callback URL 1: *	+
Serviciu:	•
Generare Client ID	

## Renunțare Oauth

^ Meniu
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.
Renunțare Oauth

## Se selectează aplicația care se dorește a se șterge:

	П			
	Client ID-uri Oauth exist	ente pentru contul dvs.		
Denumire aplicație	Client ID	Client Secret		
EFactura	24			
Şterge aplicația				
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				
	Şter	je aplicația		
	Valori pentru obținerea tokenului Oauth pentru aj	licația 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 ×	;
^ Sunteţi sigur că doriţi ştergerea aplicaţiei EFactura?	
Da Nu	

## Mesajul de succes>

^ Meniu			
	Profil	Oauth	
Denumire aplicație: * Callback URL 1: * Serviciu: Generare Client ID	•		
<ul> <li>S-a şters profilul aplicației EFactura</li> <li>S-a revocat Client ld pentru aplicația EFac</li> </ul>	tura		
			)
Client ID-uri Oau	th existente pentru contul	dvs.	
Denumire aplicație	Client ID	Client Secret	
Nu au fost găsite înregistrări.			
Ş	terge aplicația		

## 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: <u>https://logincert.anaf.ro/anaf-oauth2/v1/authorize</u>
- 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.

Configure New Token		
Token Name	se trece denumirea token-ului	
Grant Type	Authorization Code	~
Callback URL 🖲	https://oauth.pstmn.io/v1/callback	
	<ul> <li>Authorize using browser</li> </ul>	
Auth URL ④	https://logincert.anaf.ro/anaf- oauth2/v1/authorize	
Access Token URL ③	https://logincert.anaf.ro/anaf- oauth2/v1/token	
Client ID 🛞	se trece client id-ul obtinut	۵
Client Secret (3)	se trece client secret-ul obtinut	۵
Scope ①	e.g. read:org	
State ③	State	
Client Authentication ④	Send as Basic Auth header	$\sim$
> 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

∽ Adva	nced					
٩	You can add more specific cu more about <u>configuration</u> #	istomizations to y	our OAuth2	requests here. Learn	×	
Refresh	Refresh Token URL ④			https://logincert.anaf.ro/anaf-oauth2/v1/toker		
Auth Re	quest (j)					
	Кеу		Value			
~	token_content_type		jwt			
	Create parameter		Value			
Token R	Token Request ④					
	Key Value		Send In			
<b>~</b>	token_content_type	jwt		Request Body $\sim$		
	Create parameter	Value				
Refresh	Request ③					
	Key	Value		Send In		
	Create parameter	Value				
🛞 Cle Get Ne	ar cookies () ew Access Token					

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

Windows Security       X         Select a Certificate         Site logincert.anaf.ro needs your credentials:         isite set         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 X + V	
> 🕐 🏠 https://oauth.pstmn.io/v1/callback?code=26e70aee33e5db0def7b495029817a84575dc4fd27b36dc402a38fc5e6d31844	
Your call is authenticated A new windor Did you mean to switch apps? Did you mean to switch apps? Yes No	op-ups.

JAUTH Prod /	vermeare Gail		
GET	GET NEW ACCESS TOKEN	×	
arams • A			anal.rojan 1094a878af
he authorizatio enerated wher earn more abo	Authentication complete This dialogue will automatically close in 3		31b2dcde75
)	Proceed		
			ith header
	Ciear cookies		

#### Token Details

Token Name

JWT TOKEN 💉

Access Token ewoglCJhbGciOiJSUzUxMilsCiAgImtpZCl6lmFuYWZfMjAyM18yMDI Olgp9.ewoglCJ0b2tlbl90eXBlljoiQmVhcmVyliwKlCAic2NvcGUiOiJjb GllbnRhcHBpZCBpbmZvIGlzc3VlciByb2xllHNlcmlhbClsCiAgInNjb3B IX2RhdGEiOIsKICAgIHsKlCAgICAgICAiaWQiOiJjbGllbnRhcHBpZCIs CiAgICAgICAgInZhbHVlljoiNTQ2Y2RIZDJkMml3MTg5MmU4MGE2 YzU2MmFmNTAwMjNIOTk2ZGQ4MmJjMmEwNjYzlgoglCAgfSwKIC AgIHsKICAgICAgICAiaWQiOiJpbmZvliwKlCAgICAgICAgICAgfSwKIC AgIHsKICAgICAgICAgewoglCAgICAgICJpZCl6lmlzc3VlcilsCiAgICAg ICAgInZhbHVlljoiQW5hZilKlCAgIH0sCiAgICB7CiAgICAgICAgImlkljoi cm9sZSIsCiAgICAgICAgInZhbHVlljoiSEVMTE8sRUZBQ1RVUkEsRV RSQU5TUE9SVCxTUIZfRUZBQ1RVUkEiCiAgICB9LAogICAgewogIC AgICAgICJpZCl6lnNlcmlhbClsCiAgICAgInZhbHVlljoiMzQ6MDA 6MDA6MjU6Njk6OWY6NmY6ZjQ6MGY6YWY6ZGY6ODk6ZWQ6M DA6MDM6MDA6MDA6MJ06NjkiCiAgICB9CiAgXSwKICAiaXNzljoiaH

Use Token

Token-ul de tip JWT 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 <u>https://jwt.io</u>:



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 <u>https://logincert.anaf.ro/anaf-oauth2/v1/token</u>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 tokenului 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.

## 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 si 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!"

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 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 depăşeşte limita maximă de apeluri. Limita este setata la 1000 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.

## ASISTENTA TEHNICA

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



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 <u>Spațiul</u> <u>Privat Virtual.</u>

#### (câmpurile marcate cu steluță sunt obligatorii)

Alegeți categoria solicitării: Asistență tehnică servicii informatice				T	0	
Alegeți subcategoria: *	OAUTH	۲	8			
Nume: *		?				
Cod de identificare fiscal	á (CUI/CNP/NIF): *			8		