

Gestionare token de acces pentru integrarea cu serviciile ANAF: E-Factura si E-Transport

Descriere procedura.....	1
1. Inregistrare utilizator pentru API-uri specifice serviciilor ANAF.....	1
1.1. Creare cont nou de utilizator pe portalul ANAF.....	2
1.2. Inregistrare la API-uri cu cont existent pe portalul ANAF.....	3
2. Autentificare utilizator in SPV.....	4
3. Gestionare aplicatii in SPV - sectiunea <Editare profil Oauth>.....	6
3.1. Gestionare aplicatii.....	7
3.1.1. Inregistrare aplicatie in SPV.....	7
3.1.2. Vizualizare aplicatii inregistrate.....	9
3.1.3. Vizualizare detalii pentru obtinerea tokenului de acces aferent un aplicatii inregistrate.....	10
3.1.4. Stergere aplicatie.....	10
4. Gestionare token de acces pentru o aplicatie inregistrata in SPV.....	11
4.1. Obtinere token de acces pentru o aplicatie inregistrata in SPV.....	11
4.2. Regenerare token.....	16
4.3. Testare token.....	16
4.4. Stergere token.....	17
4.5. Modificare mediu pe care se apeleaza serviciile ANAF (Base Endpoint).....	18

Descriere procedura

Aceasta procedura are rolul de a obtine si gestiona un **token de acces ce va fi folosit pentru integrarea cu serviciile ANAF**:

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

Obtinerea tokenului se face prin autentificarea utilizatorului folosind certificate digitale calificate. Pentru acest lucru, trebuie ca utilizatorul sa fie inregistrat pe portalul ANAF cu drept in SPV (Spatiu Privat Virtual). Pe portalul ANAF, in sectiunea SPV, utilizatorul va inregistra o aplicatie, cu datele consolei de administrare, in care se va alege serviciul dorit: **E-Factura** si/sau **E-Transport**. Apoi se va accesa consola de administrare corespunzatoare modulului pe care utilizatorul, si pe baza valorilor obtinute la inregistrarea aplicatiei in SPV, se va autentifica folosind certificatul digital si va obtine token-ul de acces ce va fi folosit in apelul serviciilor ANAF solicitate. Odata obtinut, token-ul de acces va putea fi gestionat: reimprospatat, testat sau sters.

In cele ce urmeaza sunt detaliate pasii necesari pentru obtinerea token-ului de acces.

1. Inregistrare utilizator pentru API-uri specifice serviciilor ANAF

Pentru ca un utilizator sa poate inregistra o aplicatie in SPV, care va folosi serviciile ANAF, trebuie mai intai ca acesta sa se inregistreze pentru accesul la serviciile de tip API. Pentru acest lucru, se acceseaza portalul <https://anaf.ro> si din secțiunea *Servicii Online* -> *Inregistrare utilizatori* -> *Dezvoltatori aplicatii* se selecteaza link-ul **Inregistrare pentru API-uri**.

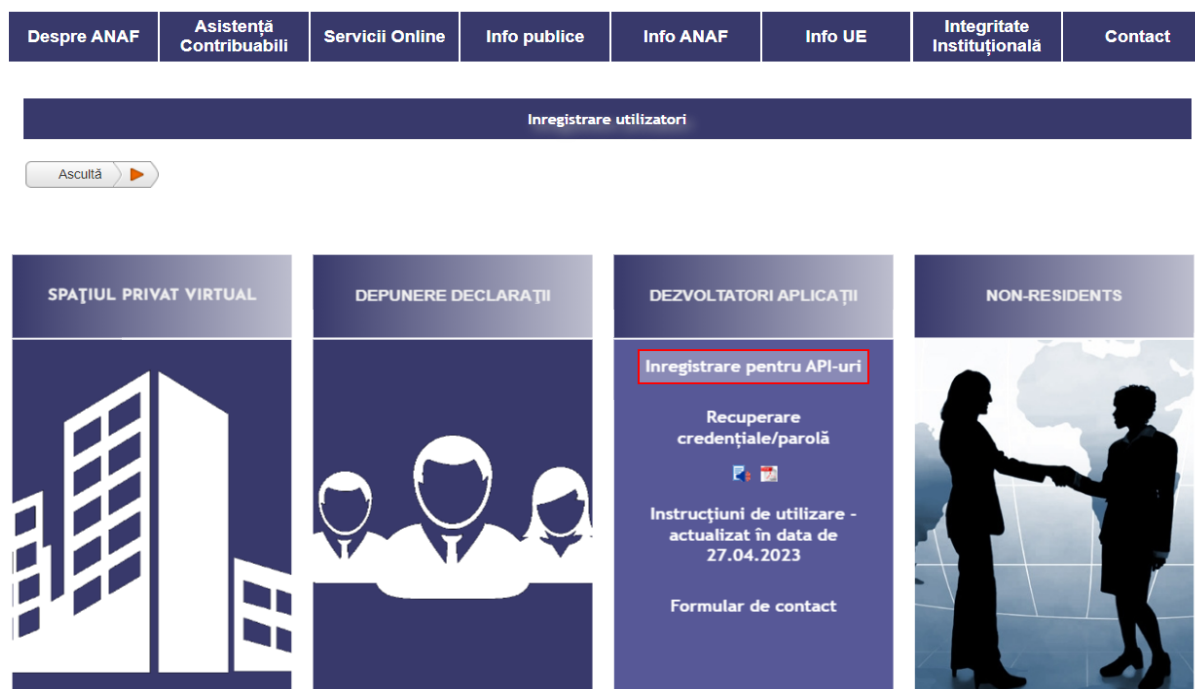


Fig. 1 - Selectie <Inregistrare pentru API-uri>

Se va afisa un formular pentru inregistrarea utilizatorului la API-uri.

În situația în care aveți deja un cont pe portalul ANAF cu username și parolă, pentru a vă înregistra ca dezvoltator de aplicații [click aici](#).

Nume: *	<input type="text"/>
Prenume: *	<input type="text"/>
Adresă de email: *	<input type="text"/>
Confirmare adresă de email: *	<input type="text"/>
CNP: *	<input type="text"/>
Tip act de identitate: *	<input type="text" value="Selectati"/>
Serie act identitate: *	<input type="text"/>
Număr act identitate: *	<input type="text"/>
Număr telefon: *	<input type="text"/>
Nume utilizator: *	<input type="text"/>
Parolă: *	<input type="password"/>
Confirmare parolă: *	<input type="password"/>

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.

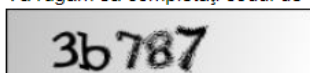


Fig. 2 - Formular <Inregistrare pentru API-uri>

In acest moment, exista 2 situatii:

- Utilizatorul nu are niciun cont pe portalul ANAF
- Utilizatorul are un cont pe portalul ANAF

1.1. Creare cont nou de utilizator pe portalul ANAF

Se completeaza formularul pentru inregistrare cu informatiile necesare utilizatorului si se apasa butonul

Se va afisa o fereastră de confirmare, in care utilizatorul va introduce codul de verificare primit pe adresa de e-mail.

Cod de verificare: 402811 *

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

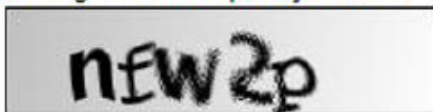


Fig. 3 - Introducere cod de verificare pt cont nou

Se apasa butonul **Continua**. Se va afisa mesajul "Contul a fost creat cu succes". Din acest moment, utilizator are cont creat pe portul ANAF si este inregistrat pentru API-uri.

1.2. Inregistrare la API-uri cu cont existent pe portalul ANAF

In situatia in care utilizatorul are cont pe portalul ANAF, atunci din formularul pentru inregistrare, acesta va selecta optiunea pentru inregistrare cu cont existent:

În situația în care aveți deja un cont pe portalul ANAF cu username și parolă, pentru a vă înregistra ca dezvoltator de aplicații [click aici](#).

Se va afisa un formular pentru verificare cont existent, in care trebuie sa se completeze nume utilizator si adresa de email a utilizatorului.

Nume utilizator: *

Email utilizator: *

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



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

Fig. 4 - Verificare cont existent

Se completeaza informatiile solicitate si se apasa butonul **Continua**. Apoi, se va afisa o fereastra de confirmare, in care utilizatorul va introduce codul de verificare primit pe adresa de e-mail.

Cod de verificare: 402811 *

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

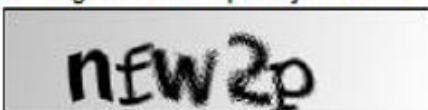


Fig. 5 - Introducere cod de verificare pt cont existent

Se apasa butonul **All**. Se va afisa mesajul "Drepturile au fost actualizate cu succes". Din acest moment, utilizator are cont creat pe portalul ANAF si este inregistrat pentru API-uri.

*Pasul 1 se va executa doar prima data, pentru inregistrarea la API-uri.

2. Autentificare utilizator in SPV

Utilizatorul, ce are cont pe portalul ANAF si care este inregistrat pentru API-uri, poate defini una sau mai multe aplicatii ce vor folosi serviciile ANAF. Pentru acest lucru este necesar ca utilizatorul sa se autentifice in SPV. Din pagina principala a portalului ANAF se selecteaza butonul **Autentificare utilizator**.



Fig. 6 - Buton pentru autentificare utilizator

Se va afisa un formular de autentificare in care se completeaza utilizatorul si parola.

The image shows the user authentication form on the ANAF website. At the top is the ANAF logo and name. Below it, the text 'Autentificare username si parola' is displayed. There are two input fields: 'Utilizator' and 'Parola'. Below the 'Parola' field is an 'Autentificare' button. Below the form, there is a paragraph of text providing instructions for new users and those with digital certificates. At the bottom, there are two links: 'Recuperare credentiale/Parolă' and 'Schimbare adresa de email'.

Fig. 7 - Formular pentru autentificare utilizator

Apoi se apasa butonul **Autentificare**. Se va afisa o fereastra de confirmare, in care utilizatorul va introduce codul de siguranta primit pe adresa de e-mail configurata la crearea contului. Codul de siguranta este valabil doar 5 minute. Se apasa **Autentificare**.



Autentificare username și parolă

Va rugam introduceți codul de siguranță recepționat la adresa de e-mail declarată, de la adresa Autentificare.SpatiuPrivat@anaf.ro.

Acest cod de siguranță expiră după 300 secunde.

Fig. 8 - Confirmare cod de siguranta pentru autentificare utilizator

Utilizatorul este autentificat in portalul ANAF si are acces la Spatiul Privat Virtual. Din acest moment, utilizatorul are disponibil un meniu cu urmatoarele sectiuni:

- **Instructiuni de utilizare** : informatii necesare pentru gestionarea SPV;
- **Editare profil Oauth**: gestionare profil Oauth in care se definesc aplicatiile care folosesc serviciile ANAF;



Fig. 9 - Meniu SPV dupa autentificare

3. Gestionare aplicatii in SPV - sectiunea <Editare profil OAuth>

Se selecteaza sectiunea **Editare profil OAuth**.

Se va afisa interfata pentru gestionarea profilul OAuth, in care se definesc aplicatiile ce vor folosi serviciile ANAF. Aceasta sectiune este constituita din urmatoarele elemente:

- **meniu** cu optiuni pentru gestionarea aplicatiilor si a profilului OAuth;
- **formular pt inregistrare aplicatie**;
- **tabel cu aplicatiile inregistrate** pentru contul utilizatorului;

^ Meniu

Profil OAuth

Denumire aplicatie: *

Callback URL 1: * +

Serviciu: *

Generare Client ID

Client ID-uri OAuth existente pentru contul dvs.

Denumire aplicatie	Client ID	Client Secret

Sterge aplicatia

Valori pentru obtinerea tokenului OAuth pentru aplicatia

Selectati o aplicatie din tabela de mai sus.

Fig. 10 - Interfata pt sectiunea <Editare profil OAuth>

Meniul acestei sectiuni este constituit din urmatoarele optiuni:

- **Gestionare aplicatii** - pt aceasta optiune sunt disponibile urmatoarele actiuni: *inregistrare aplicatie / vizualizare aplicatii inregistrate / vizualizare detalii pentru obtinerea tokenului de acces aferent unei aplicatii inregistrate (perechea Client Id - Client Secret) / stergere aplicatie inregistrata*;
- **Istoric**: *vizualizare istoric pentru operatiile efectuate de catre utilizator (aplicatii create / sterse)*;
- **Renuntare OAuth**: optiune in care se **renunta la serviciul OAuth si se anuleaza accesul la sectiunea de profil OAuth**. *Important: aceasta actiune implica stergerea tuturor aplicatiilor inregistrate in sistem, precum si a perechiilor Client Id - Client Secret necesare pentru obtinerea tokenului de acces. De asemenea, token-urile generate vor fi revocate si nu vor mai putea fi folosite; Pentru a putea inregistra noi aplicatii si a solicita token-uri noi de acces, va fi necesar ca utilizatorul sa se inregistreze din nou pentru API-uri.*

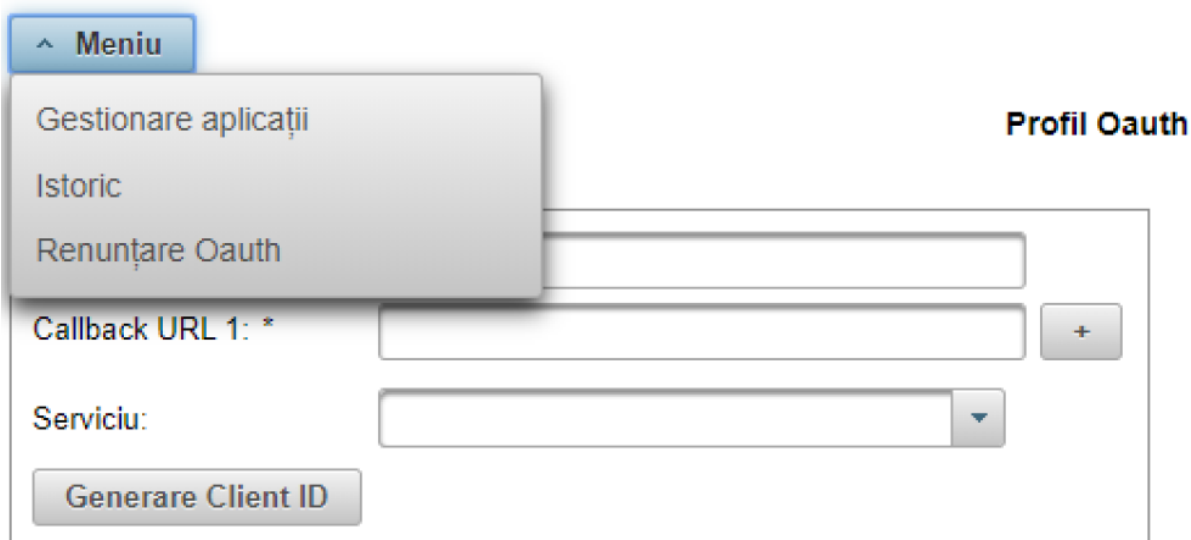


Fig. 11 - Meniu - secțiune <Profil Oauth>

3.1. Gestionare aplicații

În această pagină se gestionează aplicațiile care vor folosi serviciile ANAF. Pentru gestionarea acestora sunt disponibile următoarele acțiuni: *înregistrare aplicație în SPV / vizualizare aplicații înregistrate / vizualizare detalii pentru obținerea tokenului de acces aferent unei aplicații înregistrate (perechea Client Id - Client Secret) / ștergere aplicație înregistrată*;

3.1.1. Înregistrare aplicație în SPV

Pentru înregistrarea unei aplicații în SPV se va folosi formularul din pagina de **Gestionare aplicații**.

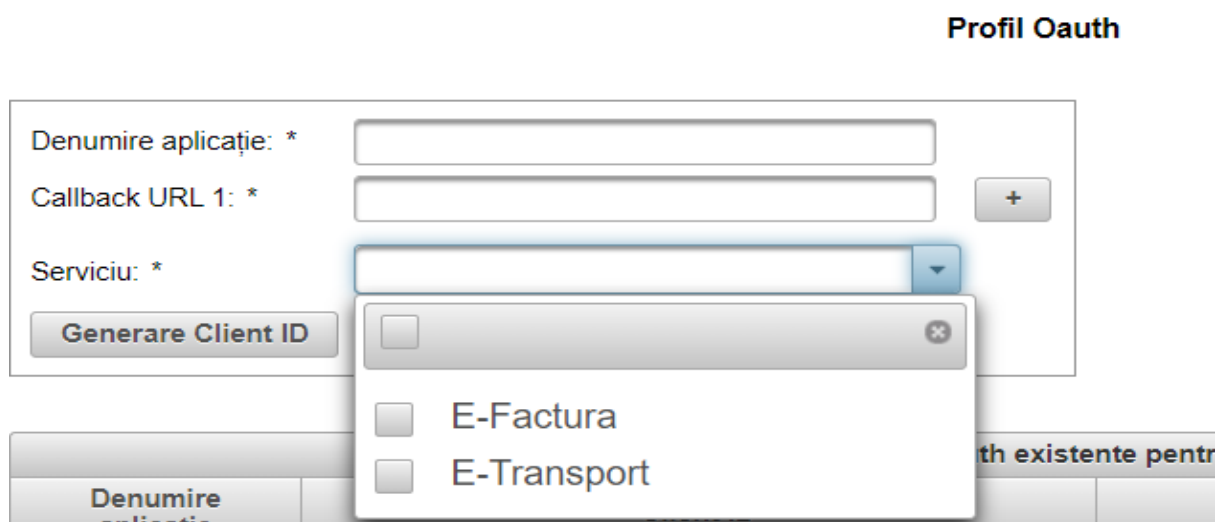


Fig. 12 - Formular pentru înregistrare aplicație în SPV

Se completeaza toate campurile obligatorii din formular, dupa cum urmeaza:

- **Denumire aplicatie:** denumirea aplicatiei ce se va inregistra pt a folosi serviciile ANAF;
- **Callback URL:** URL de redirect care se va folosi in aplicatie pentru a returna codul de autorizare pe baza caruia se va obtine token-ul de acces; URL-ul trebuie sa aiba urmatoarea structura: **<URL_Aplicatie>/<CONSOLA>/EFacturaRedirect.mk**, unde:
 - **<URL_Aplicatie>** reprezinta url-ul aplicatiei - la care se poate accesa consola de administrare. Este obligatoriu ca url-ul sa fie o adresa publica, de tip **https**, deoarece la inrolarea aplicatiei se accepta doar adresa de forma **https**. Acest url trebuie sa fie definit si in consola de adminstrare in sectiunea *Setari Aplicatie* -> tabul *Actiuni* (camp **URL aplicatie**). Exemplu de url aplicatie: **https://testanaf.emsys.ro**



Fig. 13 - Definire url aplicatie in consola de administrare

- **<CONSOLA>** in functie de modulul utilizat se va folosi consola de adminstrare specifica (Ex: pt ERP: **CONSOLE_ERP** / pt utilitati: **CONSOLE_UTI**).
- **EFacturaRedirect.mk** - serviciul, din consola de adminstrare, utilizat pentru a obtine token-ul de acces;

Exemplu de callback URL:

- ERP: **https://testanaf.emsys.ro/CONSOLE_ERP/EFacturaRedirect.mk**
- UTI: **https://testanaf.emsys.ro/CONSOLE_UTI/EFacturaRedirect.mk**
- **Serviciu:** Se selecteaza serviciu oferit de portalul ANAF, dintr-un nomenclator de servicii. Sunt puse la dispozitie urmatoarele 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);

Se poate alege un singur serviciu (aplicatia va folosi doar serviciul ales) sau se pot selecta ambele servicii (aplicatii va avea integrate ambele servicii ANAF);

In figura urmatoare (Fig. 14 - Exemplu completare formular pentru inregistrare aplicatie in SPV) este exemplificat un formular pt o inregistrare de aplicatie in SPV, care va folosi ambele servicii ANAF: **E-Factura** si **E-Transport**. Pentru acest exemplu vom folosi consola de adminstrare pt utilitati.

^ Meniu

Profil Oauth

Denumire aplicație: *

Callback URL 1: * +

Serviciu: * E-Factura x E-Transport x ▾

Generare Client ID

x
 E-Factura
 E-Transport

th existente

Fig. 14 - Exemplu completare formular pentru inregistrare aplicatie in SPV

Dupa completarea informatiilor se apasa pe butonul **Generare Client ID**.

Se va afisa un mesaj informativ in care se specifica faptul ca s-a creat profilul aplicatiei inregistrate. De asemenea, se vor afisa informatii privind *Client Id* si *Client Secret* obtinute.

Dupa inregistrarea aplicatiei, aceasta va aparea in tabelul cu aplicatii existente pentru contul utilizatorului. (Este posibil ca uneori sa fie necesar sa se dea un refresh la pagina, pentru a aparea aplicatia in tabel - datorita unui bug al portalului ANAF);

**Pot fi inregistrate in SPV maximum 5 aplicatii pentru un cont de utilizator.*

3.1.2. Vizualizare aplicatii inregistrate

Aplicatiile inregistrate de catre utilizator in SPV pot fi vizualizate in tabelul din pagina cu **Gestionare aplicatii**.

Client ID-uri Oauth existente pentru contul dvs.		
Denumire aplicație	Client ID	Client Secret
app_efact_etransp	b36c338847d5c6f79cbd43ccb2310023e996dd821654e863	eca5d48a750b09530b99ceb2742aca355aa172712f7d0023e996dd821654e863

Sterge aplicația

Fig. 15 - Tabel cu aplicatii inregistrare in SPV

In tabel trebuie sa se regaseasca si aplicatia inregistrata la pasul anterior.

3.1.3. Vizualizare detalii pentru obtinerea tokenului de acces aferent un aplicatii inregistrate

Pentru a vedea detalii necesare pentru obtinerea token-ului de acces corespunzator unei aplicatii inregistrate, se selecteaza linia dorita din tabelul cu aplicatii. Se vor afisa urmatoarele informatii:

- **Grant Type:** tipul de autorizare folosit pentru obtinerea tokenului (cod de autorizare);
- **Callback URL:** URL-ul folosit la inrolarea aplicatiei in SPV;
- **Auth URL:** URL-uri pentru autorizare, accesare si revocare token;
- **Client ID:** id client - obtinut la inregistrarea aplicatiei;
- **Client Secret:** cheie secreta pt client - obtinuta la inregistrarea aplicatiei;

app_efact_efransp	b36c338847d5c6f79cbd43ccb2310023e996dd821654e663	eca5d48a750b09530b99ceb2742aca355aa1727f2f7d0023e996dd821654e663
<input type="button" value="Șterge aplicația"/>		
Valori pentru obținerea tokenului OAuth pentru aplicația app_efact_efransp		
Grant Type	Authorization Code	
Callback URL	["https://testanaf.emsys.ro/CONSOLE_UTI/EFacturaRedirect.mk"]	
Auth URL	https://logincert.anaf.ro/anaf-oauth2/v1/authorize https://logincert.anaf.ro/anaf-oauth2/v1/token https://logincert.anaf.ro/anaf-oauth2/v1/ revoke	
Client ID	b36c338847d5c6f79cbd43ccb2310023e996dd821654e663	
Client Secret	eca5d48a750b09530b99ceb2742aca355aa1727f2f7d0023e996dd821654e663	

Fig. 16 - Detalii necesare pentru obtinerea token-ului de acces pentru o aplicatie inregistrata in SPV

3.1.4. Stergere aplicatie

Pentru a sterge o aplicatie inregistrata in SPV, se selecteaza aplicatia dorita din tabel si se apasa butonul **Sterge aplicatia**.

app_efact_efransp	b36c338847d5c6f79cbd43ccb2310023e996dd821654e663	eca5d48a750b09530b99ceb2742aca355aa1727f2f7d0023e996dd821654e663
<input type="button" value="Șterge aplicația"/>		

Fig. 17 - Stergere aplicatie din SPV

Se va afisa un mesaj de confirmare pentru stergerea aplicatiei. Daca se selecteaza **DA** atunci aplicatia va fi stearsa din SPV. Se va afisa un mesaj informativ in care se specifica ca profilul aplicatiei a fost sters si ca s-a revocat *Client Id* (token-ul a fost revocat si nu se mai poate folosi);

4. Gestionare token de acces pentru o aplicatie inregistrata in SPV

Dupa ce o aplicatie a fost inregistrata in SPV devin disponibile cateva actiuni pt gestionarea token-ului de acces aferent aplicatiei respective: *obtinere token de acces, regenerare token, testare token si stergere token*). Pentru aceste actiuni se va folosi consola de administrare corespunzatoare modulului pe care opereaza utilizatorul.

4.1. Obtinere token de acces pentru o aplicatie inregistrata in SPV

In momentul in care aplicatia a fost inregistrata in SPV de catre utilizator si s-au obtinut informatiile necesare se poate trece la generarea token-ului de acces corespunzator acestei aplicatii. Pentru acest lucru se va accesa consola de administrare corespunzatoare modulului pe care opereaza utilizatorul (pt ERP: **consola de ERP** / pt utilitati: **consola de utilitati**). Consola de administrare trebuie sa poata fi accesata la url-ul aplicatiei folosit pt campul *Callback URL* la inrolarea in SPV - de tip https (descrie la pasul 3.1.1. - Ex: https://testanaf.emsys.ro/CONSOLE_UTI).

Se autentifica in consola de administrare si se selecteaza tab-ul **Servicii Anaf**.



Fig. 18 - Selectie tab <Servicii Anaf> din consola de administrare

Se afiseaza intertafa pentru gestionare informatii pentru token-ul de acces, ce este constituita din urmatoarele elemente:

- **combo pt selectie Tip token** - reprezinta tipul de serviciu folosit la inregistrarea aplicatiei. Valori posibile *E-Factura, E-Transport, Toate (E-Factura si E-Transport)*; Implicit este selectata valoarea *E-Factura*;
- **buton Generare token** - la selectia acestui buton se va lansa un popup in care se pot efectua urmatoarele operatiuni: obtinere informatii token, regenerare token, testare token;

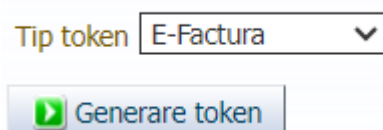


Fig. 19 - Interfata tab <Servicii Anaf>

Se selecteaza *tipul de token corespunzator cu serviciul ales la inregistrarea aplicatiei in SPV*, deoarece aplicatia va avea acces doar la serviciul solicitat la inrolarea aplicatiei. Selectia se va face astfel:

- pt serviciul *E-Factura* se va selecta **Tip token = E-Factura**;
- pt serviciul *E-Transport* se va selecta **Tip token = E-Transport**;
- pt ambele servicii (*E-Factura* si *E-Transport*) se va selecta **Tip token = Toate** (token-ul va putea fi folosit pt ambele servicii *E-Factura* si *E-Transport*);

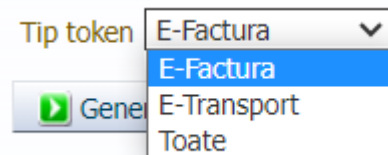
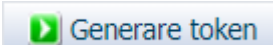


Fig. 20 - Selectie tip token

Apoi se apasa pe butonul 

Se va lansa un popup care va contine un formular ce trebuie completat cu informatiile obtinute la inregistrarea aplicatiei in SPV. Este necesar ca valorile completate in formular sa fie identice cu cele obtinute in SPV pentru a putea genera token-ul de acces. Campurile din formular sunt obligatorii de completat si acestea se completeaza dupa cum urmeaza:

- **ANAF Authorization Endpoint:** reprezinta URL-ul pentru obtinerea codului de autorizare. Este propus implicit cu valoarea standard pt mecanismul OAuth - <https://logincert.anaf.ro/anaf-oauth2/v1/authorize> ;
- **ANAF Token Issuance Endpoint:** reprezinta URL-ul folosit in obtinerea token-ului de acces pe baza codului de autorizare. Este propus implicit cu valoarea standard pt mecanismul OAuth - <https://logincert.anaf.ro/anaf-oauth2/v1/token> ;
- **ANAF Token Revoke Endpoint:** reprezinta URL-ul pentru revocarea token-ului. Este propus implicit cu valoarea standard pt mecanismul OAuth - <https://logincert.anaf.ro/anaf-oauth2/v1/revoke> ;
- **Client Id:** se completeaza cu id-ul de client obtinut la inregistrarea aplicatiei in SPV;
- **Client Secret:** se completeaza cu cheia secreta obtinuta la inregistrarea aplicatiei in SPV;
- **Callback URL:** se completeaza cu URL-ul folosit la inrolarea aplicatiei in SPV. Acesta se foloseste pentru a accesa serviciul care va obtine token-ul de acces. Campul va fi propus initial cu valoarea completata la inregistrare. Structura acestui URL trebuie sa fie `<URL_Aplicatie>/<CONSOLA>/EFacturaRedirect.mk` (vezi pasul 3.1.1. - campul *Callback URL*);
- **Base Endpoint:** reprezinta mediul pe care se vor apela serviciile ANAF. Sunt disponibile 2 medii: *productie* si *test*. Implicit este propus cu URL-ul pt mediul de *productie*: <https://api.anaf.ro/prod>. Daca se doreste mediul de *test*, atunci se va completa cu URL-ul: <https://api.anaf.ro/test> ;

The screenshot shows a web form titled "Generare token" with the following fields and values:

- ANAF Authorization Endpoint: `https://logincert.anaf.ro/anaf-oauth2/v1/authorize`
- ANAF Token Issuance Endpoint: `https://logincert.anaf.ro/anaf-oauth2/v1/token`
- ANAF Token Revoke Endpoint: `https://logincert.anaf.ro/anaf-oauth2/v1/revoke`
- Client Id: (empty)
- Client Secret: (empty)
- Callback URL: `https://testanaf.emsys.ro/CONSOLE_UTI/EFacturaRedirect.mk`
- Base Endpoint: `https://api.anaf.ro/prod`
- Data expirare token: (empty)

Buttons: "Reincarcare date" (refresh) and "Initializare token cu semnatura digitala" (initialize token with digital signature).

Fig. 21 - Formular cu valori propuse pentru obtinere token

Practic trebuie complete doar **Client Id** si **Client Secret**, restul campurilor fiind deja propuse, inasa este recomandat sa se verifice ca informatiile completate in formular sa fie identice cu valorile aplicatiei din SPV.

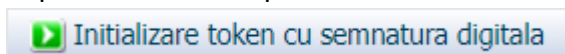
The screenshot shows the same "Generare token" form, but with the following fields filled:

- Client Id: `b36c338847d5c6f79cbd43ccb2310023e996dd821654e663`
- Client Secret: `eca5d48a750b09530b99ceb2742aca355aa1727f2f7d0023e996dd821654e663`

The "Initializare token cu semnatura digitala" button is highlighted with a green arrow.

Fig. 22 - Formular cu toate campurile completate

Apoi se cupleaza la statia de lucru stick-ul USB care contine semnatura digitala autorizata. Dupa ce a fost cuplat si instalat stick-ul USB cu semnatura digitala, se apasa butonul



Se va deschide automat o fereastra in care se solicita sa se selecteze certificatul pentru semnatura digitala.

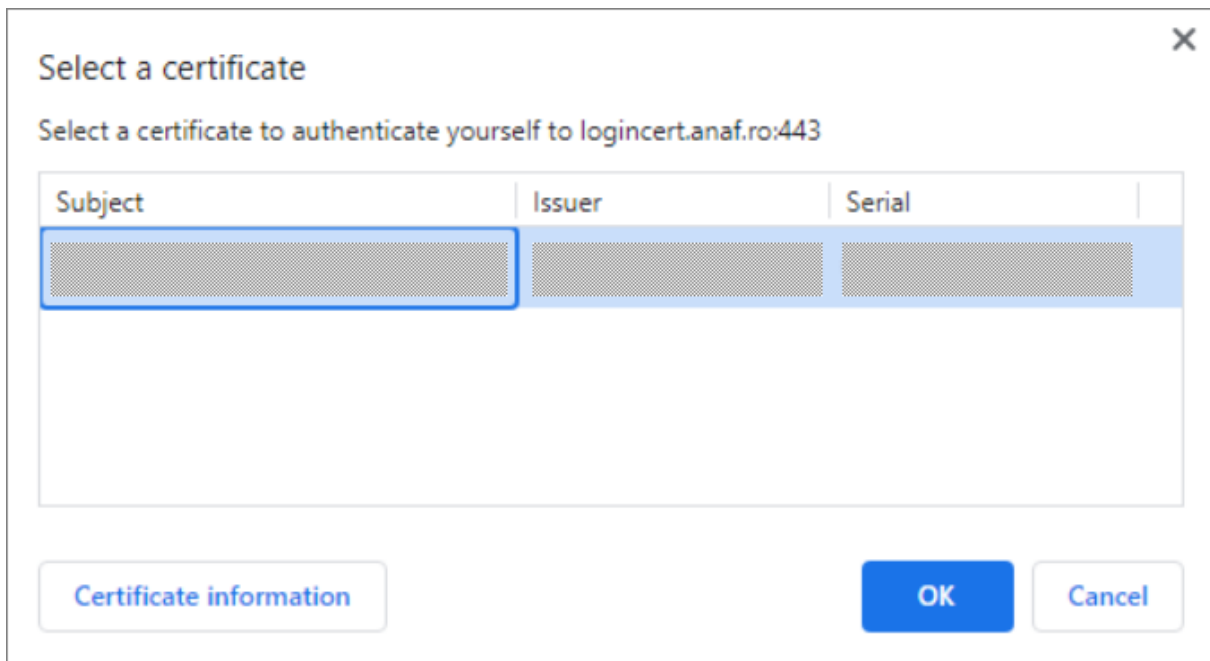


Fig. 23 - Selectie certificat pentru semnatura digitala

Dupa selectia certificatului se va deschide o alta fereastra in care trebuie sa se completeze codul PIN pentru certificatul ales.

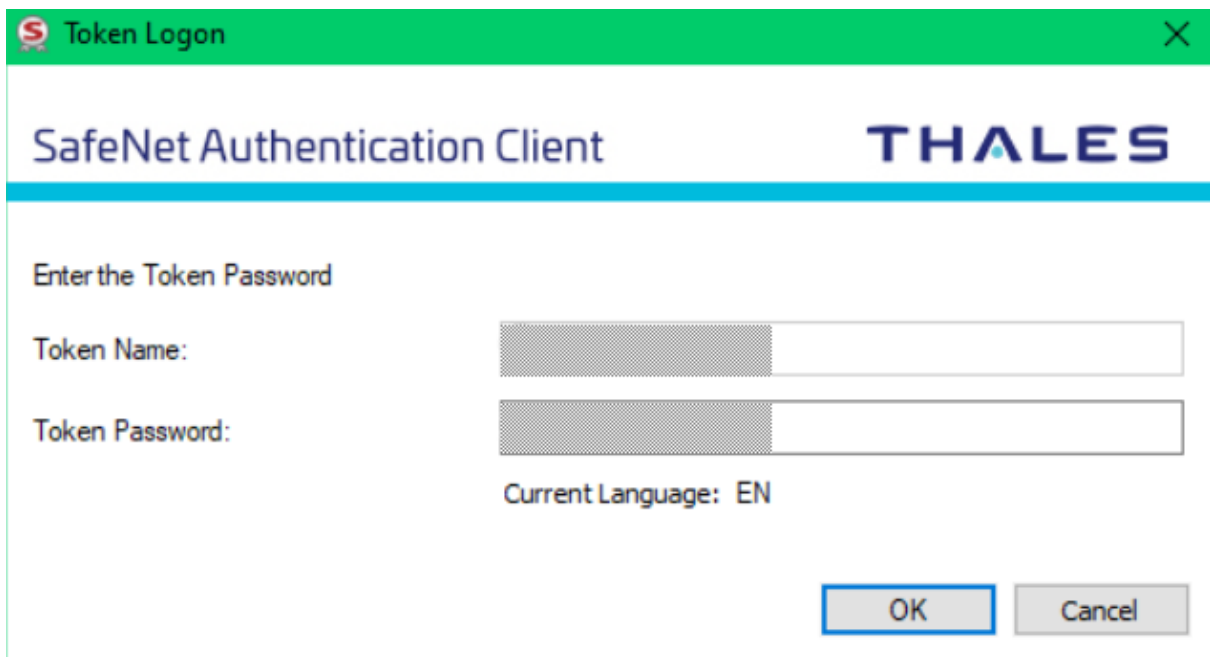


Fig. 24 - Completare PIN pentru certificatul ales

Dupa introducerea codului PIN se va afisa o fereastra in care se specifica faptul ca autentificarea s-a efectuat cu succes si se solicita sa se reimprospateze ecranul principal pentru a actualiza datele obtinute. In acest moment s-a obtinut token-ul de acces pentru aplicatia inregistrata in SPV si informatiile au fost salvate in sistem. Token-ul obtinut este valabil pe o perioada de 3 luni.

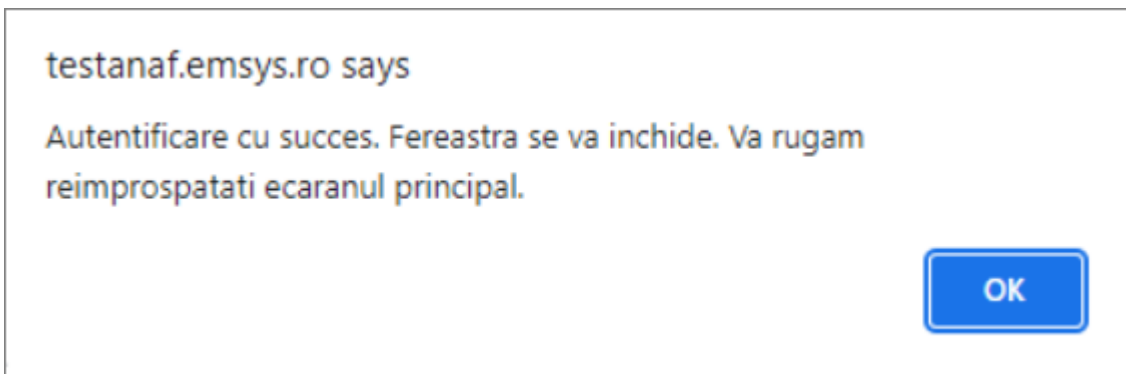
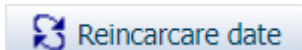


Fig. 25 - Mesaj pentru autentificare cu succes (token obtinut)

Se inchide aceasta fereastra si se reintoarce in ecranul principal in care se apasa pe butonul



Se observa ca datele au fost actualizate, astfel incat pe interfata din ecranul principal s-au inactivat campurile si butonul de initializare token, a fost completata *data de expirare a token-ului* si au aparut butoane pentru gestionarea token-ului obtinut:

- **Regenerare token** - prin actiunea acestui buton se reimprospateaza token-ul;
- **Test token** - se verifica daca token-ul obtinut este generat corect;

Token-ul obtinut are o valabilitate de 3 luni. Din acest moment, se poate extrage stick-ul USB cu semnatura digitala deoarece acesta nu mai este necesar. Este recomandat ca inainte de expirarea token-ului sa se efectueze o reimprospatare a acestuia. La reimprospatare token-ului se va prelungi valabilitatea acestuia cu inca 3 luni (pt aceasta actiune nu este nevoie de stick-ul cu semnatura digitala);

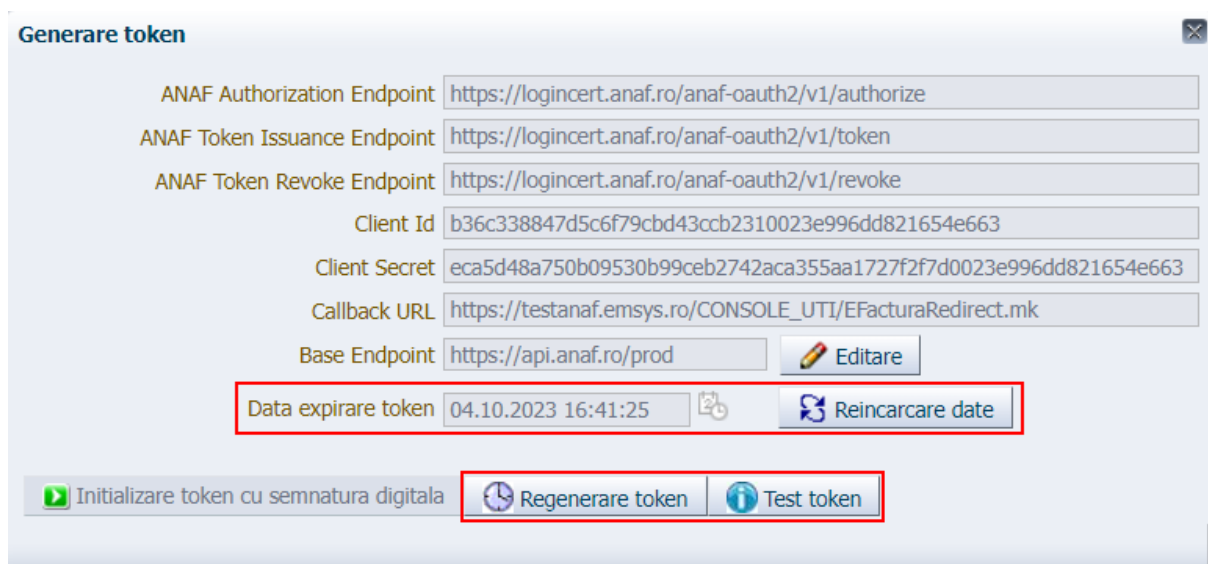
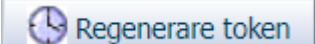


Fig. 26 - Interfata dupa obtinera tokenului de acces

4.2. Regenerare token

Regenerarea token-ului are rolul de a prelungi valabilitatea acestuia cu 3 luni din momentul in care se actioneaza. Aceasta actiune se poate efectua fara a fi nevoie ca stick-ul USB cu semnatura digitala sa fie introdus.

Este necesar ca regenerarea token-ului sa se efectueze inainte ca acesta sa expire, deoarece pentru cazul in care token-ul este expirat, aceasta actiune nu se va mai putea efectua si va fi nevoie de o generare noua de token.

Pt a reimprospata token-ul, se deschide popup-ul pentru Generare token si se apasa pe butonul 

Se va afisa un mesaj de informare in care se specifica faptul ca regenerarea token-ului s-a efectuat cu succes.



Fig. 27 -Mesaj regenerare token

Pe ecran va fi actualizata noua data de expirare a token-ului.

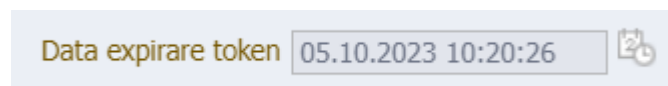
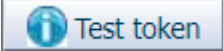


Fig. 28 - Mesaj regenerare token

4.3. Testare token

Aceasta actiune are rolul de a verifica daca token-ul este generat corect.

Pt a verifica token-ul, se deschide popup-ul pentru Generare token si se apasa pe butonul 

Se va afisa un mesaj de informare in care se specifica faptul ca token-ul este corect.

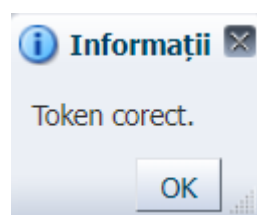


Fig. 29 -Mesaj testare token

4.4. Stergere token

Aceasta actiune are rolul de a revoca si sterge token-ul din sistem. Dupa stergere, token-ul nu va mai putea fi folosit.

Pentru a sterge un token din sistem, se acceseaza pagina initiala a tabului *Servicii Anaf*, in care se selecteaza **tipul de token** si se actioneaza butonul **Stergere token**. Butonul de stergere este disponibil daca in sistem exista informatiile de autentificare pentru token-ul respectiv (la prima lansare a popup-ului pentru generare token se salveaza in sistem parametrii pt autentificare, indiferent daca se genereaza sau nu token-ul - pt a nu mai fi nevoie ca acestia sa se completeze de fiecare data);

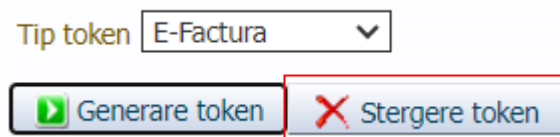


Fig. 30 -Buton pt Stergere token

La actionarea butonul de stergere se va afisa un mesaj in care utilizatorul este rugat sa confirme ca este sigur ca doreste stergerea token-ului cu tipul selectat.

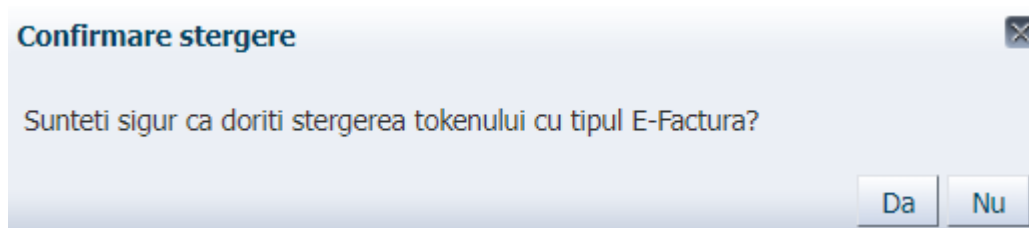


Fig. 31 -Confirmare stergere token

Daca se alege *Da*, atunci se va afisa un mesaj informativ in care se specifica faptul ca a fost sters token-ul cu tipul selectat.

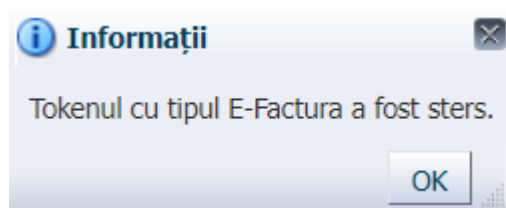


Fig. 32 - Mesaj pt token sters

La stergerea token-ului sunt 2 cazuri:

- pt tipul de token selectat a existat token generat -> se va revoca tokenul si acesta va fi sters din sistem;
- pt tipul de token au existat doar informatiile de autentificare, fara sa existe token generat -> se vor sterge aceste informatii din sistem (la o noua lansare de popup pt generare token cu acest tip va fi necesar sa se completeze parametrii);

4.5. Modificare mediu pe care se apeleaza serviciile ANAF (Base Endpoint)

Pentru apelul serviciilor ANAF, mecanismul Oauth pune la dispozitie doua medii:

- **productie**: https://api.anaf.ro/prod
- **test**: https://api.anaf.ro/prod

Implicit, la obtinerea token-ului, se propune mediul de productie pentru apelul serviciilor ANAF.

Pt a modifica mediul, se deschide popup-ul pentru Generare token si se apasa pe butonul **Editare** (butonul este langa campul specific ce se va modifca - **Base Endpoint**).

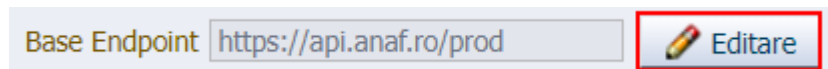


Fig. 33 - Buton pt modificare mediu pt apel servicii ANAF

Campul va devine activ si langa acesta vor aparea urmatoarele butoane: **Ok** (pt salvare modificari) si **Renunt** (renuntare la modificare).

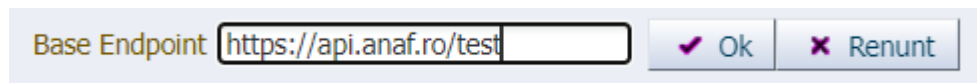


Fig. 34 - Modificare mediu pt apel servicii ANAF

Se modifica acest camp cu mediul dorit (test sau productie) si se apasa **Ok**. Modificarile se salveaza in sistem, iar apelurile serviciilor ANAF se vor efectua pe mediul setat.