

PROCEDURA privind aprobarea accesului la serviciile disponibile în cadrul sistemului informatic PatrimVen

1. Principii

1.1. Dreptul de acces la serviciile sistemului informatic se acordă autorităților/instituțiilor publice, denumite în continuare *A/IP*.

1.2. Dreptul de acces al *A/IP* se exercită de către personalul desemnat în acest scop de către *A/IP* dintre angajații proprii.

1.3. Dreptul de acces se solicită și se înregistrează la Ministerul Finanțelor Publice, respectiv la Agenția Națională de Administrare Fiscală prin organele fiscale teritoriale, conform prezentei proceduri.

1.4. Identificarea persoanelor se face cu certificate digitale calificate, emise de autorități de certificare acreditate, precum și cu certificate digitale necalificate recunoscute de către MFP.

1.5. Identificarea persoanelor se va putea face și cu alte mijloace de identificare, în funcție de evoluția tehnologică și de nivelul de securitate necesar.

1.6. Persoanelor li se atribuie drepturi de acces, denumite *roluri*, în funcție de atribuțiile de serviciu stabilite de către *A/IP*.

1.7. Procesul prin care unei persoane i se atribuie un rol se numește *înrolare*.

1.8. Unul dintre rolurile atribuite cel puțin unei persoane dintr-o *A/IP* este acela de „administrator al drepturilor de acces ale utilizatorilor, pe scurt „administrator de interoperabilitate”.

1.9. Pentru fiecare *A/IP* pot fi acordate maximum două roluri de administrator de interoperabilitate”.

1.10. Procedurile de înrolare a administratorului de interoperabilitate sau a altor categorii de utilizatori pot fi diferite.

1.11. Pentru a putea înrola alte categorii de utilizatori este obligatoriu ca *A/IP* să aibă cel puțin un administrator de interoperabilitate înrolat.

1.12. Pentru a putea înrola alte categorii de utilizatori, de regulă, nu este necesară prezența fizică a persoanei sau prezentarea de documente pe hârtie.

1.13. *A/IP* asigură mijloacele de verificare a accesului la sistemul informatic, bazat pe înscrierea motivului accesării datelor din sistemul informatic, astfel încât din analiza acestora să rezulte dacă datele au fost accesate în conformitate cu legislația în vigoare și pentru îndeplinirea sarcinilor de serviciu sau în alte scopuri.

2. Înrolarea și revocarea administratorului de interoperabilitate

2.1. În vederea înrolării *A/IP* prezintă și depune, după caz, prin persoana nominalizată ca administrator de interoperabilitate la MFP, respectiv ANAF, prin organele fiscale teritoriale la care *A/IP* are conturi deschise, următoarele documente/fișiere:

— prezintă cartea de identitate a persoanei în original;

- depune pe suport electronic fișierul de export al certificatului digital calificat deținut de persoană;

- depune pe suport hârtie Cererea de numire sau revocare administrator de interoperabilitate, pentru gestionarea drepturilor de acces ale utilizatorilor din partea A/IP, semnată și ștampilată de reprezentantul legal al acesteia, conform modelului prevăzut în anexa nr. 3 la ordin.

2.2. Înregistrarea persoanelor cu rol de administrator de interoperabilitate se face de către MFP prin unitățile teritoriale în termen de maximum 3 zile lucrătoare de la depunerea documentelor. Administratorul de interoperabilitate nu poate avea rol și de utilizator PatrimVen.

2.3. Unitatea teritorială a MFP verifică identitatea persoanei, copiază și stochează documentul de identitate, verifică corectitudinea datelor înscrise și stochează documentele depuse pe suport hârtie, specimenul de semnătură al ordonatorului de credite și ștampila instituției. După verificarea documentelor depuse pe suport hârtie, cererile se avizează de către șeful organului fiscal central pentru conformitatea datelor verificate și se introduc în sistem, în baza de date a drepturilor de acces, prin aplicația informatică disponibilă în acest scop.

2.4. Se pot înregistra maximum două persoane cu drept de administrator de interoperabilitate pentru o instituție.

2.5. Revocarea dreptului de administrator de interoperabilitate se face de către A/IP în oricare dintre următoarele situații:

- persoana cu drept de administrator de interoperabilitate nu mai este angajat al instituției;

- certificatul digital utilizat la autentificare de administrator de interoperabilitate a fost pierdut, furat, distrus etc;

- A/IP decide să revoce unei persoane dreptul de administrator de interoperabilitate.

2.6. A/IP are obligația de a anunța imediat revocarea dreptului de administrator de interoperabilitate prin:

- administratorul de interoperabilitate care nu are revocat dreptul de administrator, folosind sistemul informatic sau prin prezentarea pe suport hârtie și depunerea la unitatea teritorială a MFP la care A/IP are conturi deschise a Cererii de numire sau revocare administrator de interoperabilitate, pentru gestionarea drepturilor de acces ale utilizatorilor din partea A/IP, semnată și ștampilată de reprezentantul legal al acesteia, conform modelului prevăzut în anexa nr. 3 la ordin.

2.7. În situația în care a expirat perioada de valabilitate a instrumentului de autentificare deținut de persoana cu drept de administrator de interoperabilitate, reînnoirea certificatului se face prin:

- Introducerea datelor noului certificat, folosind sistemul informatic, de către administratorul de interoperabilitate care nu are revocat dreptul de administrator; sau

- prin prezentarea pe suport electronic și depunerea la unitatea teritorială a MFP la care A/IP are conturi deschise a fișierului de export al noului certificat.

3. Obligațiile administratorului de interoperabilitate

3.1. Se prezintă personal la organul teritorial al MFP împreună cu documentele necesare pentru înrolare.

3.2. Semnează și transmite formularul electronic Protocol de aderare la serviciile sistemului informatic MFP, denumit în continuare *PASS*.

3.3. Verifică și certifică realitatea datelor de identificare ale persoanelor pe care le înrolează, precum și a celorlalte date necesare înrolării.

3.4. Înrolează persoane cu rol de utilizator al sistemului informatic, conform deciziei conducătorului A/IP.

3.5. Modifică sau revocă, după caz, drepturile de acces ale utilizatorilor, conform deciziei conducătorului A/IP.

3.6. Notifică revocarea drepturilor de acces ale administratorului de interoperabilitate, dacă:

- persoana cu drept de administrator de interoperabilitate nu mai este angajat al instituției;

- certificatul digital utilizat la autentificare a fost pierdut, furat, distrus etc;

- conducătorul A/IP ia o decizie în acest sens.

3.7. Verifică jurnalul de acces al utilizatorilor la sistemul informatic.

3.8. Asigură salvarea și păstrarea pe termen de minimum 5 ani a jurnalului de acces al utilizatorilor la sistemul informatic.

4. Gestiunea drepturilor administratorului de interoperabilitate

4.1. Dreptul de administrator de interoperabilitate se alocă automat, după verificarea de către unitatea teritorială a MFP a documentelor necesare înrolării și după confirmarea corectitudinii datelor primite de la autoritatea de certificare emitentă a certificatului digital.

4.2. Revocarea dreptului de administrator de interoperabilitate se decide de către conducătorul A/IP și se operează prin sistemul informatic PatrimVen sau de către unitatea teritorială a MFP unde au fost prezentate documentele necesare.

5. Înrolarea și revocarea utilizatorilor

5.1. Înrolarea utilizatorilor din cadrul A/IP se face în scopul accesului la unul sau mai multe dintre serviciile disponibile prin sistemul informatic, necesare îndeplinirii atribuțiilor A/IP. Utilizatorul PatrimVen nu poate avea rol și de administrator de interoperabilitate.

5.2. Înrolarea și revocarea utilizatorilor din cadrul A/IP se fac de către administratorul de interoperabilitate, prin aplicația pusă la dispoziție în acest scop în sistemul informatic, prin completarea informațiilor despre persoane și instrumentele de autentificare deținute de acestea.

5.3. MFP verifică datele furnizate de administratorul de interoperabilitate în procesul de înrolare și revocare a utilizatorilor.

5.4. Datele rezultate din verificări sunt înregistrate și reținute în sistemul informatic.

5.5. Înregistrarea persoanelor cu rol de utilizator se face în termen de maximum o zi lucrătoare de la solicitare.

5.6. Finalizarea procesului de înrolare va fi comunicată prin poșta electronică.

5.7. În cazul în care persoana cu drept de utilizator nu mai este angajat al A/IP sau în cazul pierderii, furtului sau distrugerii certificatului digital utilizat la autentificare sau ori de câte ori A/IP decide astfel, A/IP are obligația de a lua imediat, prin administratorul de interoperabilitate, măsurile necesare în vederea retragerii imediate a dreptului de utilizator persoanei care nu mai îndeplinește condițiile pentru acest rol.

6. Gestiunea drepturilor utilizatorilor — actualizarea datelor în urma procesului de reînnoire a instrumentului de autentificare

6.1. În cazul reînnoirii de către o persoană cu drept de utilizator a instrumentului de autentificare, administratorul de interoperabilitate va trimite datele noului instrument de autentificare, asociat titularului, prin intermediul sistemului informatic.

6.2. MFP verifică datele furnizate de administrator de interoperabilitate în procesul de actualizare.

6.3. Datele rezultate din verificări sunt înregistrate și reținute în sistemul informatic.

6.4. Finalizarea procesului de actualizare a datelor în urma reînnoirii instrumentului de autentificare va fi comunicată prin poșta electronică.

7. Drepturile și responsabilitățile utilizatorilor

7.1. Utilizatorul poate accesa serviciile oferite de sistemul informatic conform drepturilor stabilite de administrator de interoperabilitate.

Utilizatorul răspunde de respectarea regulilor de acces la sistemul informatic în conformitate cu drepturile conferite în sistemul informatic și atribuțiile de serviciu.

8. Funcția de audit

8.1. ANAF poate vizualiza lista accesărilor utilizatorilor, respectiv poate solicita periodic instituției să prezinte, prin sondaj, situații cu corectitudinea interogărilor efectuate de acești utilizatori pentru a verifica dacă au fost utilizate în concordanță cu atribuțiile de serviciu și s-au respectat dispozițiile Legii nr. 677/2001 pentru protecția persoanelor, cu privire la prelucrarea datelor cu caracter personal și liberă circulație a acestor date, cu modificările și completările ulterioare.

(Se completează denumirea autorității sau instituției publice.)

CIF

(Se completează CIF.)

**CERERE
de numire sau
revocare
administrator de
interoperabilitate**

Prin prezenta cerere,

(Se completează denumirea autorității sau instituției
publice.)

cu codul de identificare fiscală, reprezentată prin

.....,

(Se completează CIF.)

(Se completează numele și

prenumele

reprezentantului legal.)

în calitate de, solicităm (se bifează numai una dintre opțiuni):

(Se completează funcția.)

☐ înregistrarea cu rol de administrator de interoperabilitate în scopul
gestionării, din partea noastră,
a drepturilor de acces ale utilizatorilor la sistemului informatic PatrimVen

☐ înregistrarea revocării dreptului de administrator de
interoperabilitate pentru accesul la sistemul
informatic PatrimVen pentru următoarele persoane:

Numele	Prenumele	CNP	Funcția	Telefonul	E-mail

(Se completează funcția.)

(Se completează
numele și
prenumele
reprezentantului
legal.)

Semnătura

Dat

**DOCUMENTE CE TREBUIE DEPUSE
LA GHIȘEELE UNITĂȚILOR FISCALE TERITORIALE,
ÎN VEDEREA ÎNREGISTRĂRII OFITERULUI DE SECURITATE**

- 1. Cartea de identitate a persoanei căreia i se va alocă rol de administrator – copie și original.**
- 2. Împuternicire din partea instituției, semnată și ștampilată de reprezentantul legal al acesteia, conform modelului prevăzut în Anexa 1.A.**
- 3. Fișierul de export al certificatului instalat în prealabil în browser, pe suport electronic.**

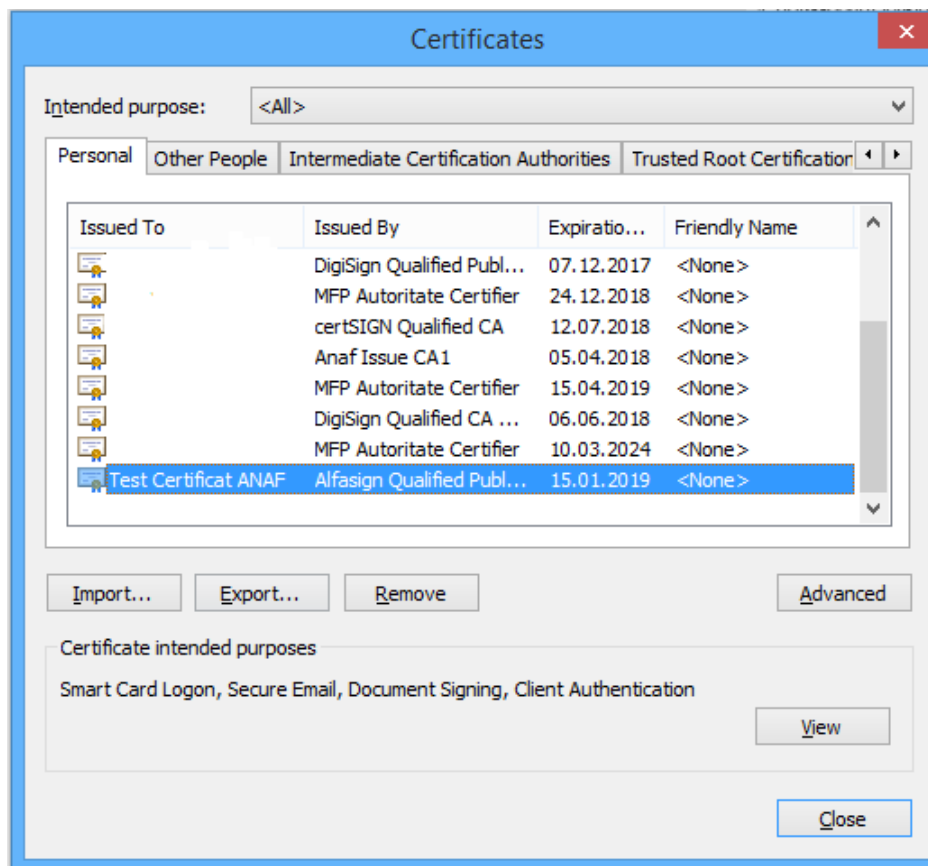
Export certificat

Pentru a obține certificatul digital în format fișier există două modalități:

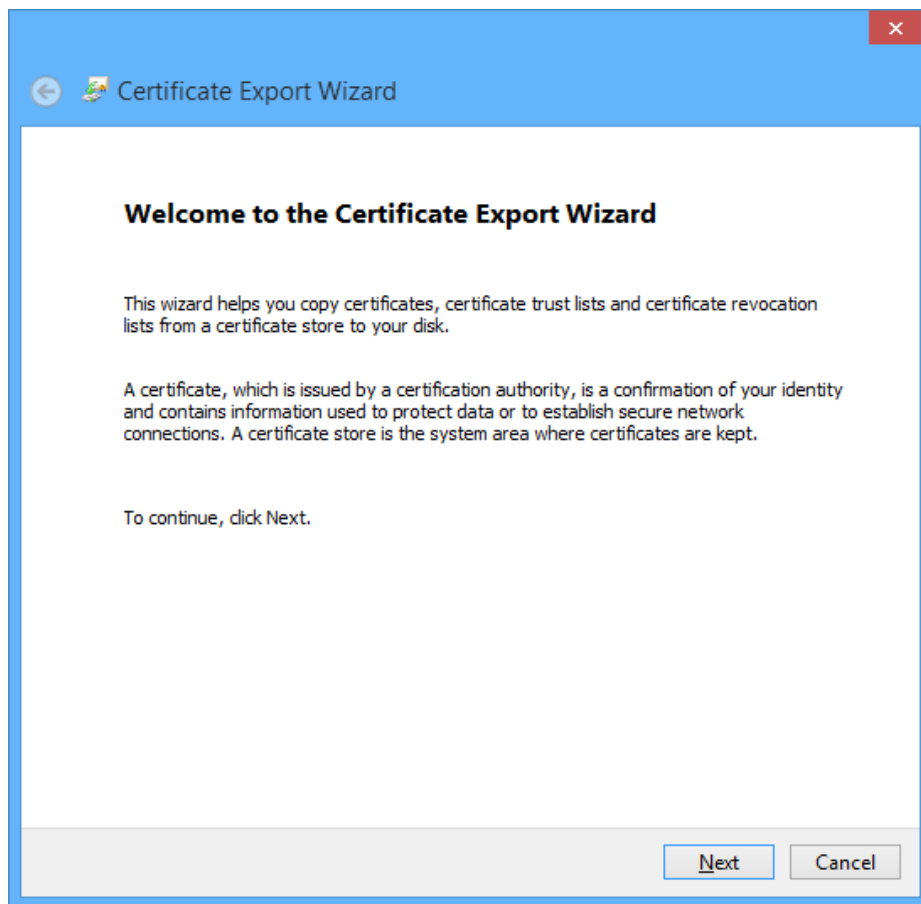
1. Se intră pe site-ul autorității de certificare și se descarcă certificatul.
2. Se face export de certificat din browser-ul utilizat:

Tools -> Internet Options -> Content -> Certificates

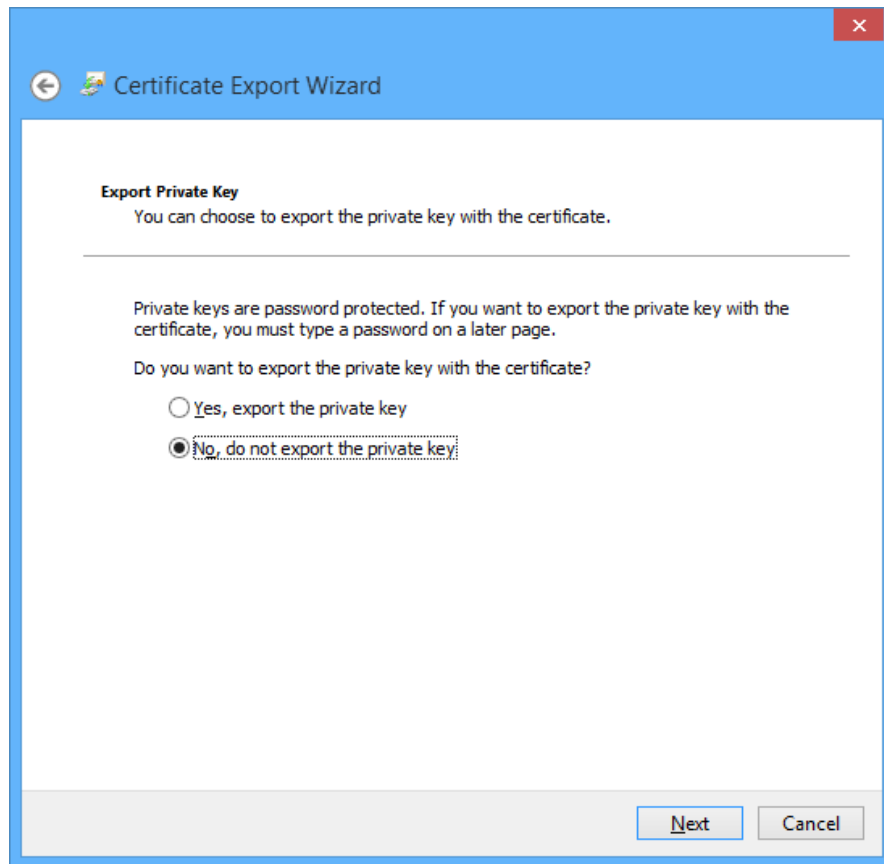
The screenshot displays a web browser window with the ANAF (Agenția Națională de Administrare Fiscală) website. The address bar shows a URL from anaf.ro. The browser's toolbar includes various icons and a search bar. The main content area of the website features the ANAF logo, navigation links, and a search bar. A sidebar on the left contains links to 'NOUTĂȚI' (News) and 'CĂUTARE' (Search). The main content area includes a section for 'ASISTENȚĂ CONTRIBUABILI' (Contributor Assistance) with a call center number, and a section for 'SERVICII ONLINE' (Online Services) with a link to '01 Declarații electronice' (01 Electronic Declarations). The Internet Options dialog box is open, showing the 'Content' tab, which includes sections for 'Certificates', 'AutoComplete', and 'Feeds and Web Slices'. The 'Certificates' section is highlighted, showing options to 'Clear SSL state', 'Certificates', and 'Publishers'. The 'AutoComplete' section shows options to 'Settings' and 'Feeds and Web Slices'. The 'Feeds and Web Slices' section shows options to 'Settings' and 'Feeds and Web Slices'.



Selectare certificat>Export>



Next>



Next >

×

← Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

☒ DER encoded binary X.509 (.CER)

☐ Base-64 encoded X.509 (.CER)

☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☐ Include all certificates in the certification path if possible

☐ Personal Information Exchange - PKCS #12 (.PFX)

☐ Include all certificates in the certification path if possible

☐ Delete the private key if the export is successful

☐ Export all extended properties

☐ Microsoft Serialized Certificate Store (.SST)

Next

Cancel

Next>

×

← Certificate Export Wizard

File to Export
Specify the name of the file you want to export

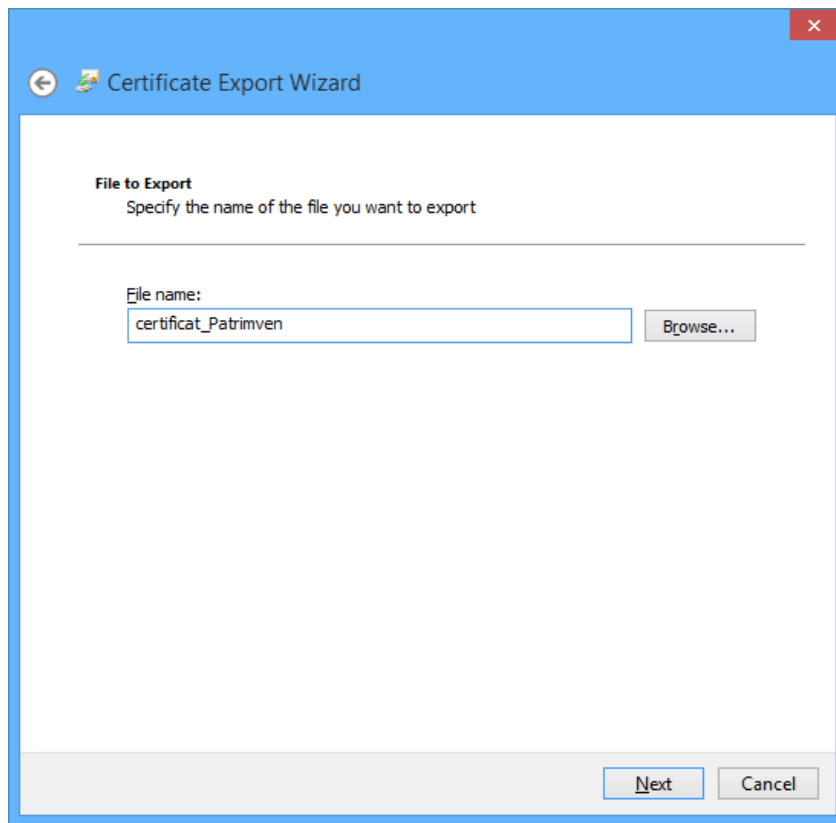
File name:

Browse...

Next

Cancel

Introduceți numele cu care doriți să fie salvat certificatul>



The screenshot shows the 'File to Export' step of the Certificate Export Wizard. The window has a blue title bar with a back arrow, a certificate icon, and the text 'Certificate Export Wizard'. The main area is white with the heading 'File to Export' and the instruction 'Specify the name of the file you want to export'. Below this is a text box labeled 'File name:' containing the text 'certificat_Patrimven'. To the right of the text box is a 'Browse...' button. At the bottom right of the window are 'Next' and 'Cancel' buttons.

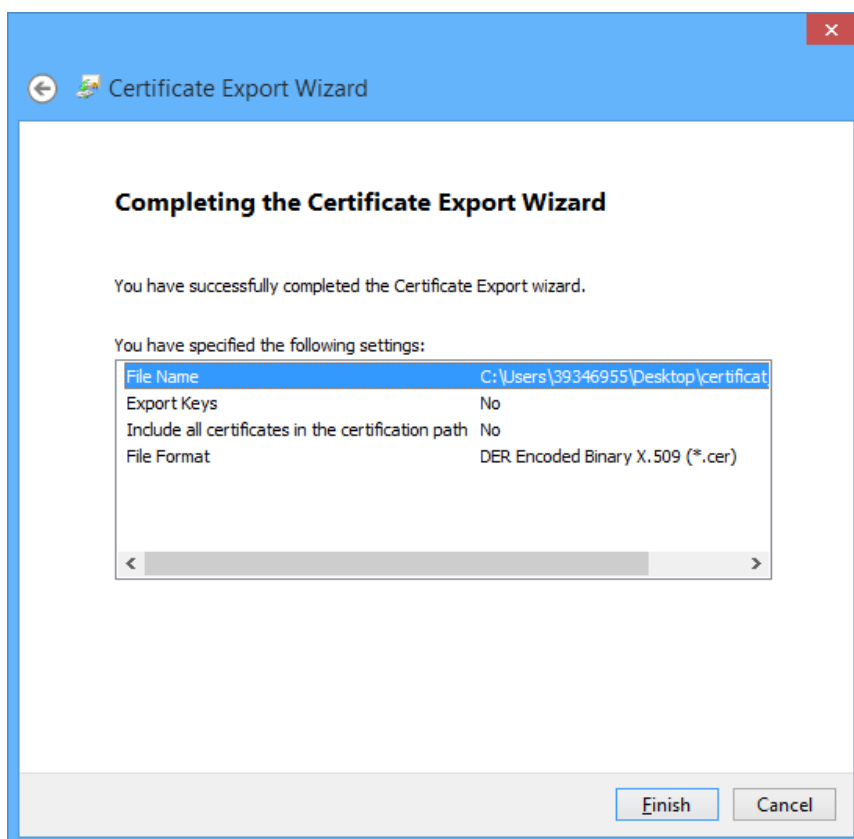
File to Export
Specify the name of the file you want to export

File name:
certificat_Patrimven

Browse...

Next Cancel

Next>



The screenshot shows the 'Completing the Certificate Export Wizard' screen. The window has a blue title bar with a back arrow, a certificate icon, and the text 'Certificate Export Wizard'. The main area is white with the heading 'Completing the Certificate Export Wizard'. Below this is the text 'You have successfully completed the Certificate Export wizard.' and 'You have specified the following settings:'. A table lists the settings: File Name (C:\Users\39346955\Desktop\certificat), Export Keys (No), Include all certificates in the certification path (No), and File Format (DER Encoded Binary X.509 (*.cer)). At the bottom right of the window are 'Finish' and 'Cancel' buttons.

Completing the Certificate Export Wizard

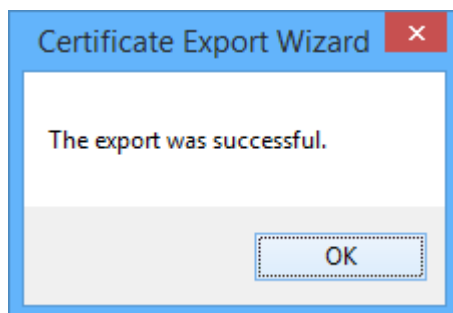
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\39346955\Desktop\certificat
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

Finish Cancel

Finish>



Certificatul va fi salvat automat pe desktop cu extensia .cer.

9. Servicii informatice disponibile

Pentru a accesa sistemul informatic, este necesară autentificarea pe pagina web de la adresa: <https://epatrim.fiscnet.ro>



După autentificarea în sistem, în funcție de serviciile la care ați aderat, puteți vizualiza unul sau mai multe servicii.

Lista tuturor serviciilor disponibile în cadrul sistemului PATRIMVEN este prezentată în imaginea de mai jos:

Servicii oferite:**Comunicare raspunsuri la solicitarile transmise****

Browser address bar: <https://www.fiscnet.ro/patrimven/Cautare.faces>

File Edit View Favorites Tools Help

Icons: [https://epatrimtest.fiscnet](#), IBM Sites, Tabs, Acasa, Dictionar Englez Roman - ..., Google, IBM Content Manager, ileana.neagaionescu - Yah..., Web Slice Gallery, Yahoo!, WebSphere



PatrimVen

Agencia Națională de Administrare Fiscală

[Inapoi](#)
[Deconectare](#)

Utilizator: ILEANA NEAGA-IONESCU

Motiv accesare informatii: Numar cerere/dosar*: din data*:

CNP/CUI/NIF: NUME, PRENUME, DENUMIRE:

ADRESA:

[BANI](#)
[CONTRIBUTII \(D 112\)](#)
[VENITURI](#)
[VEHICULE](#)
[CLADIRI](#)
[TERENURI](#)

© Agentia Nationala de Administrare Fiscala - DGTI Continutul acestui site este proprietatea Agentiei Nationale de Administrare Fiscala. Modificarea neautorizata a acestui site web constituie infractiune si se pedepseste conform prevederilor Legii nr. 8/1996 si ale Legii nr. 161/2003 Titlul 3

9.1.1. Accesarea informațiilor, în alte situații decât cele prevăzute de dispozițiile art. 5 al. 2 din Legea nr. 677/2001, se va putea face doar ca urmare a depunerii, de către cetățean, a unei cereri sau dosar, pentru soluționarea căruia își va da acordul de consultare a datelor cu caracter personal.

9.1.2. Funcționarii care accesează aceste informații vor trebui să respecte prevederile legislative în vigoare, cu privire la confidențialitatea datelor cu caracter personal.

9.1.3. Câmpurile „Motiv accesare informații”, „număr cerere/dosar”, „din data”, „CNP/CUI” sunt obligatorii. Pe baza acestor înregistrări se va face verificarea corectitudinii acceselor la informații.

9.1.4. Verificarea se face punctual, pentru fiecare contribuabil în parte, accesând serviciile disponibile în funcție de atribuțiile de serviciu.

9.2. Administrare drepturi

9.2.1. Activitatea de administrare drepturi presupune activități de administrare a drepturilor de acces la Sistemul Informatic al MFP-ANAF, ale personalului instituțiilor, înregistrate în vederea accesării informațiilor:

- Înregistrare utilizatori

Meniu

- Adaugare utilizator
- Administrare roluri
- Gestionare certificat
- Audit
- Editare utilizator
- Revocare utilizator

Înregistrare utilizatori

Pentru înregistrarea utilizatorilor aveți la dispoziție următoarele servicii disponibile în meniul aplicației

- Adaugare utilizator – va permite să adăugați un utilizator nou în sistem
- Administrare roluri – va permite să atribuiți/revocați roluri utilizatorilor.

Nota: După adăugarea unui utilizator în sistem trebuie să i se asigneze și roluri pentru a putea accesa serviciile.

Meniul Audit va permite să vizualizați toate operațiunile efectuate de către utilizatorii înregistrați.

- Administrare roluri utilizatori (alocare/revocare drepturi utilizatori înregistrați)

Meniu

- Adaugare utilizator
- Administrare roluri
- Gestionare certificat
- Audit
- Editare utilizator
- Revocare utilizator

Adminstrare roluri utilizator

Utilizator:

Adminstrare roluri utilizator

Acasa | Deconectare

EDUARD-ANDREI COSMA, Comuna Albac, Albac

Meniu

- Adaugare utilizator
- Administrare roluri
- Audit

Adminstrare roluri utilizator

Utilizator:

Roluri disponibile		Roluri asignate
banci	→	
contributii	←	
venituri	↔	
creante	←	
vehicule	→	
cladiri	↔	
terenuri	→	
asistentia	↔	

ROLURILE DISPONIBILE ÎN APLICAȚIE

Rolurile vor fi alocate de către persoana cu rol de administrator, în funcție de atribuțiile de serviciu ale utilizatorilor.

- BĂNCI cu posibilitate de vizualizare a datelor despre băncile la care contribuabilul are deschise conturi;
- CONTRIBUȚII cu posibilitatea vizualizării informațiilor declarate în D112;
- VENIT cu posibilitatea vizualizării veniturilor din alte surse decât cele salariale;
- CLĂDIRI cu posibilitatea vizualizării clădirilor deținute;
- VEHICULE cu posibilitatea vizualizării vehiculelor deținute;

- TERENURI cu posibilitatea vizualizării terenurilor deținute;
- ADMINISTRATOR cu posibilitate de acordare și administrare roluri, vizualizarea și listarea jurnalului de accese. Poate fi acordat doar utilizatorului cu atribuții de administrator.

- Audit (Jurnalizare operații)

9.2.2. Funcționarul cu rol de administrator sau alt reprezentant al instituției, desemnat de conducătorul acesteia, are obligația să verifice corectitudinea acceselor la informații și să raporteze neregulile sesizate.

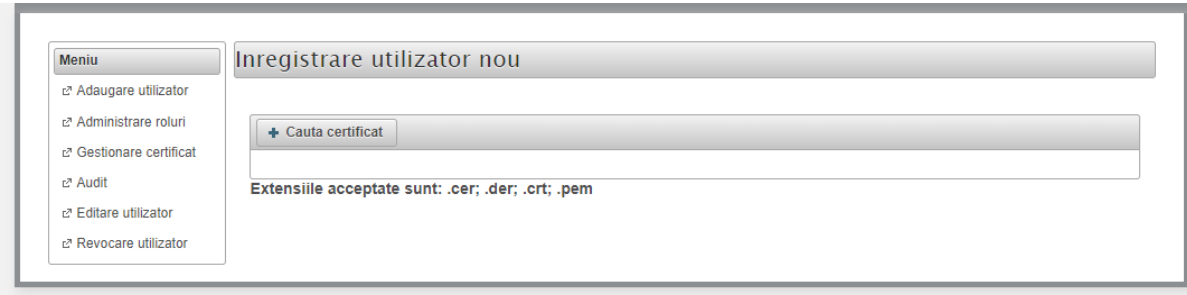
9.2.3. Atribuția de administrator presupune listarea și consultarea/punerea la dispoziția reprezentantului desemnat a jurnalului de accese periodic.

DATE CE TREBUIE COMPLETATE ONLINE
ÎN SISTEMUL INFORMATIC PATRIMVEN
ÎN VEDEREA ÎNREGISTRĂRII UTILIZATORILOR COMUNI
(de către administratorul/ofițerul de securitate desemnat)

1. CNP utilizator
2. E-mail al utilizatorului
3. Funcția deținută în cadrul instituției
4. Departamentul în care își desfășoară activitatea
5. Instituția în care utilizatorul își desfășoară activitatea
6. **Informațiile ce se preiau din fișierul de export al certificatului digital**

Pentru preluarea informațiilor din fișierul de export al certificatului se parcurg următorii pași:

- se selectează butonul caută certificat pentru încărcarea certificatului exportat



Meniu

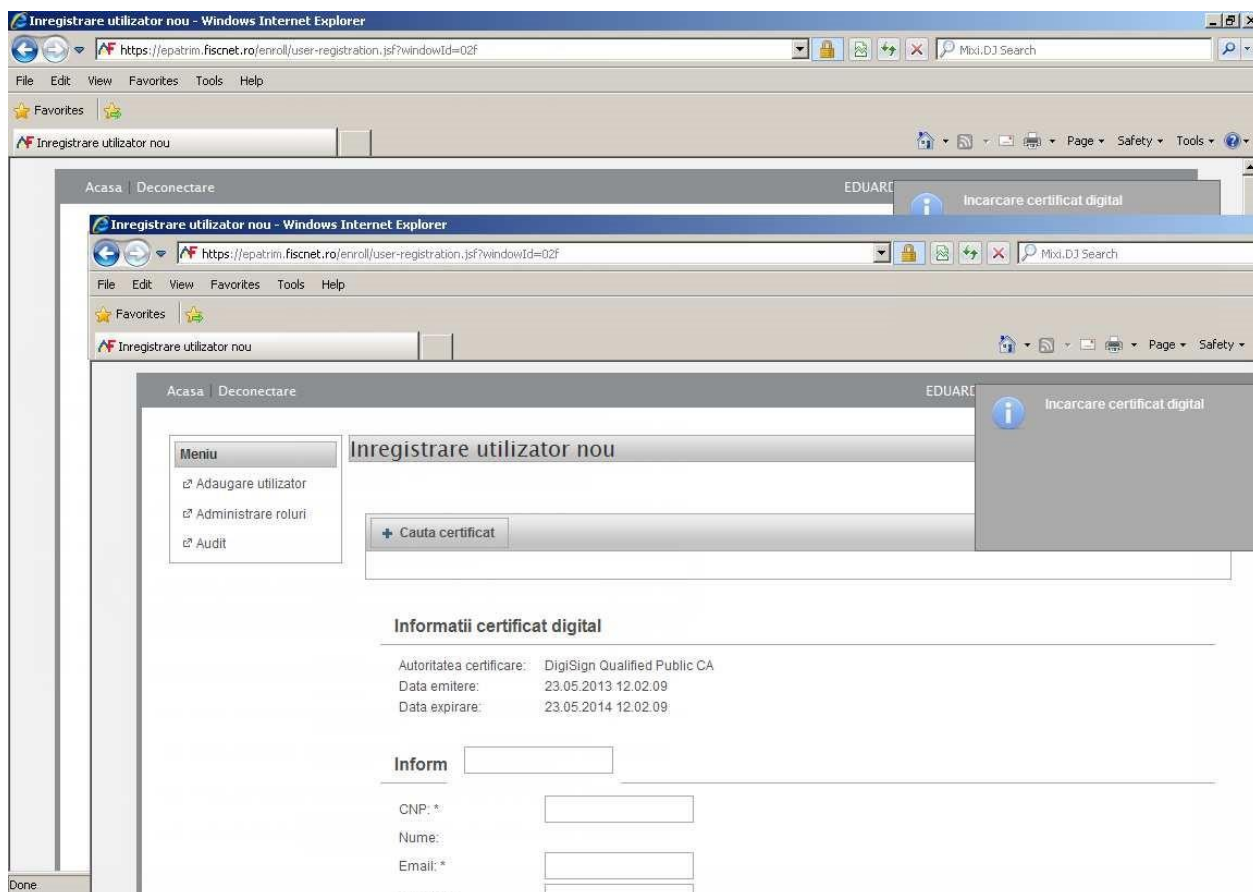
- Adaugare utilizator
- Administrare roluri
- Gestionare certificat
- Audit
- Editare utilizator
- Revocare utilizator

Inregistrare utilizator nou

+ Cauta certificat

Extensiile acceptate sunt: .cer; .der; .crt; .pem

- se extrag datele din certificat:
- Autoritatea de certificare
 - Data emitere
 - Data expirare



- se completează secțiunea Informații personale:

- CNP
- Nume (se completează automat după introducerea CNP-ului)
- E-mail
- Funcția
- Departament
- Instituția

- se apasă butonul *Înregistrează*, pentru înregistrarea utilizatorului în sistem.

MENIURILE DISPONIBILE IN ECRANUL DE CONSULTARE
pentru autoritățile sau instituțiile publice

In funcție de rolurile alocate, utilizatorii pot accesa unul sau mai multe meniuri, din cele disponibile:

- BĂNCI
- CONTRIBUȚII (D112)
- VENITURI
- VEHICULE
- CLĂDIRI
- TERENURI

După introducerea datelor în câmpurile obligatorii, în cazul în care CNP-ul solicitat este valid, se activează meniul disponibil:



1. Persoanele care desfășoară activități de asistentă socială vor putea accesa informații primite din diverse surse, disponibile prin serviciul informatic PATRIMVEN, prin alegerea opțiunii „Asistență socială”, corespunzătoare câmpului „Motiv accesare informații”.
2. Persoanele care desfășoară activități de administrare fiscală vor putea accesa informații primite din diverse surse, disponibile prin serviciile informatice, prin alegerea opțiunii „Măsuri de executare silită”, „Inspecție fiscală” sau „Verificare date contribuabil”, corespunzătoare câmpului „Motiv accesare informații”.
3. Pentru demararea unor acțiuni globale, de exemplu înființarea în masă a popririlor pentru toți debitorii pentru care s-a început executarea silită, se va putea cere doar de către administrator un raport pe baza unui Excel exportat, conținând nume și prenume /denumire, CNP/CUI, banca/angajator (doar pentru cei care au conturi active).

Gestionare certificat

Reînnoirea certificatelor se efectuează în secțiunea Gestionare certificate (administratorii au și posibilitatea de ștergere certificat introdus eronat sau expirat).

Meniu

- Adaugare utilizator
- Administrare roluri
- Gestionare certificat**
- Audit
- Ediție utilizator
- Revocare utilizator

Gestionare certificat

Utilizator: Selectati un utilizator ▼

EDUARD-ANDREI COSMA

Gestionare certificat

Utilizator: COSMA V. EDUARD-ANDREI CUI:4221306 ▼

+ Incarca certificat

Extensiile acceptate sunt: .cer; .der; .crt; .pem

✓ Modifica

Certificate Digitale Disponibile					
	Id	Serialul certificatului	Issuer	Data înregistrare certificat	Data expirare certificat
☐	1102350	65fb2bca000000001451	ALFASIGN QUALIFIED CA	23.10.2015 09:51:27	01.06.2016 10:33:46
☐	1102300	65fb2bca000000001451	ALFASIGN QUALIFIED CA	21.10.2015 12:50:08	01.06.2016 10:33:46

✓ Sterge certificat

Se selectează utilizatorul pentru care se dorește efectuarea reînnoirii certificatului, se selectează certificatul nou și se apasă butonul “Modifică/ Adaugă certificatul”.

Pentru a șterge certificatul, se selectează certificatul care se dorește să se șteargă.

EDUARD-ANDREI COSMA, COM.IDECIUL DE JOS, București

Gestionare certificat

Utilizator: NEAGA-IONESCU M. ILEANA CUI:4591449 ▼

+ Incarca certificat

Extensiile acceptate sunt: .cer; .der; .crt; .pem

✓ Modifica

Certificate Digitale Disponibile					
	Id	Serialul certificatului	Issuer	Data înregistrare certificat	Data expirare certificat
☒	9235371	2011042091030404A0AE	Cert Digital Qualified CA Class 3	18.11.2015 15:22:10	20.10.2016 15:04:07

✓ Sterge certificat

Pentru deconectarea din aplicație se va selecta butonul “Deconectare”. În caz contrar, sesiunea va rămâne deschisă și la următoarea accesare veți primi mesaj de eroare.

După deconectare, mesajul pe care-l veți primi, trebuie să fie “Sesiune terminată cu succes!”.



PatrimVen

[Acasă](#)[Verificare stare recipisă](#)[Legislație](#)[Specificații tehnice](#)[Contact](#)

Sesiune terminată cu succes!

Pentru a iniția o nouă sesiune, vă rugăm închideți și redeschideți browser-ul.

Pentru asistență tehnică, vă rugăm să folosiți [Formularul de contact](#), alegând categoria "Asistență tehnică servicii informatice".

© Agenția Națională de Administrare Fiscală - DGTI Conținutul acestui site este proprietatea Agenției Naționale de Administrare Fiscală. Modificarea neautorizată a acestui site web constituie infracțiune și se pedepsește conform prevederilor Legii nr. 8/1996 și ale Legii nr. 161/2003 Titlul 3