Paperless webSIGN

Platformă web pentru semnarea electronică la distanță

Cuprins

1. Certificat digital calificat pentru semnare la distanță 4
1.1. Înrolarea utilizatorului 4
1.2. Crearea/activarea contului Paperless webSIGN 5
• Configurarea contului pentru autentificarea cu 2FA 8
• Configurarea contului pentru autentificarea fără 2FA 9
1.3. Selectarea pachetului dorit, introducerea datelor și plata online 11
1.4. Identificarea video a viitorului titular de cont și de certificat digital calificat la distanță 13
1.5. Configurarea autorizării la serviciul Paperless webSIGN pentru autentificarea fără 2FA 15
1.5.1. Instalarea soluției de autorizare pe telefon 15
1.5.2. Împerecherea soluției de autorizare cu contul Paperless webSIGN 15
1.6. Emiterea certificatului digital în platforma Paperless webSIGN 17
2. Rekey – reînnoire certificat digital calificat pentru semnare la distanță 21
2.1. Selectarea pachetului dorit și plata online 25
2.2. Completarea datelor și trimiterea cererii de reinnoire certificat 27
3. Reemiterea după expirare a certificatului digital calificat 31
3.1. Selectarea pachetului dorit și plata online 33
3.2. Identificarea video 36
3.3. Emiterea certificatului digital 37
4. Schimbare parolă 41
4.1. Schimbare parolă cont când se cunoaște parola de logare 41
4.2. Recuperare parolă cont când nu se cunoaște parola de logare 42
5. Schimbare număr de telefon asociat contului 44
6. Reîmperecherea aplicației de telefon cu contul din platforma Paperless webSIGN 47
7. Semnarea cu certificatul digital calificat pentru semnare la distanță 49
7.1. Semnarea în Paperless webSIGN 49
7.2. Semnarea pe stația locală 52
8. Autentificarea cu certificatul digital calificat pentru semnare la distanță pe platformele online 55

În platforma de semnare Paperless webSIGN – websign.ro este pusă la dispoziție posibilitatea de a achiziționa:

- un **certificat digital calificat pentru semnare la distanță ,**
- **rekey certificat digital calificat pentru semnare la distanță** (respectiv de a solicita emiterea unui nou certificat digital pentru semnare la distanță in baza certificatului digital calificat existent valabil)
- **reemitere certificat digital calificat pentru semnare la distanță.**

Pachetele puse la dispoziția clienților certSIGN sunt următoarele:

Paperless 1 – Semnătură electronică calificată cu certificat calificat valabilitate 1 an

- Certificat digital calificat – valabilitate 1 an
- Acces în platforma de semnare Paperless webSIGN
- 200 de tranzacții (semnături electronice și mărci temporale)

Paperless 2 – Semnătură electronică calificată cu certificat calificat valabilitate 2 ani

- Certificat digital calificat – valabilitate 2 ani
- Acces în platforma de semnare Paperless webSIGN
- 400 de tranzacții (semnături electronice și mărci temporale)

Paperless 3 – Semnătură electronică calificată cu certificat calificat valabilitate 3 ani

- Certificat digital calificat – valabilitate 3 ani
- Acces în platforma de semnare Paperless webSIGN
- 600 de tranzacții (semnături electronice și mărci temporale)

1. Certificat digital calificat pentru semnare la distanță

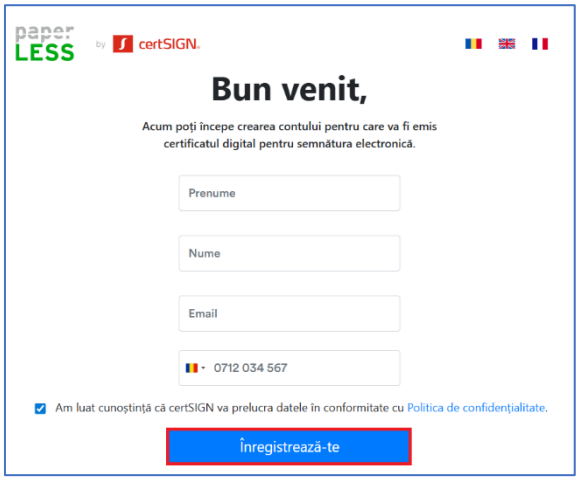
Pentru achiziția unui nou certificat, utilizatorul (client nou sau care dorește încă un cont) trebuie să parcurgă următoarele etape:

- înrolarea utilizatorului;
- crearea contului cu setare de user și parolă;
- selectarea pachetului dorit, introducerea datelor și plata online;
- identificarea video a viitorului titular de cont și de certificat digital calificat la distanță;
- configurarea autorizării;
- emiterea certificatului digital calificat la distanță.

1.1. Înrolarea utilizatorului

Pentru înrolarea utilizatorului și emiterea unui certificat digital calificat pentru semnare la distanță, accesați platforma https://websign.ro. Apăsați butonul **Înregistrează-te**.

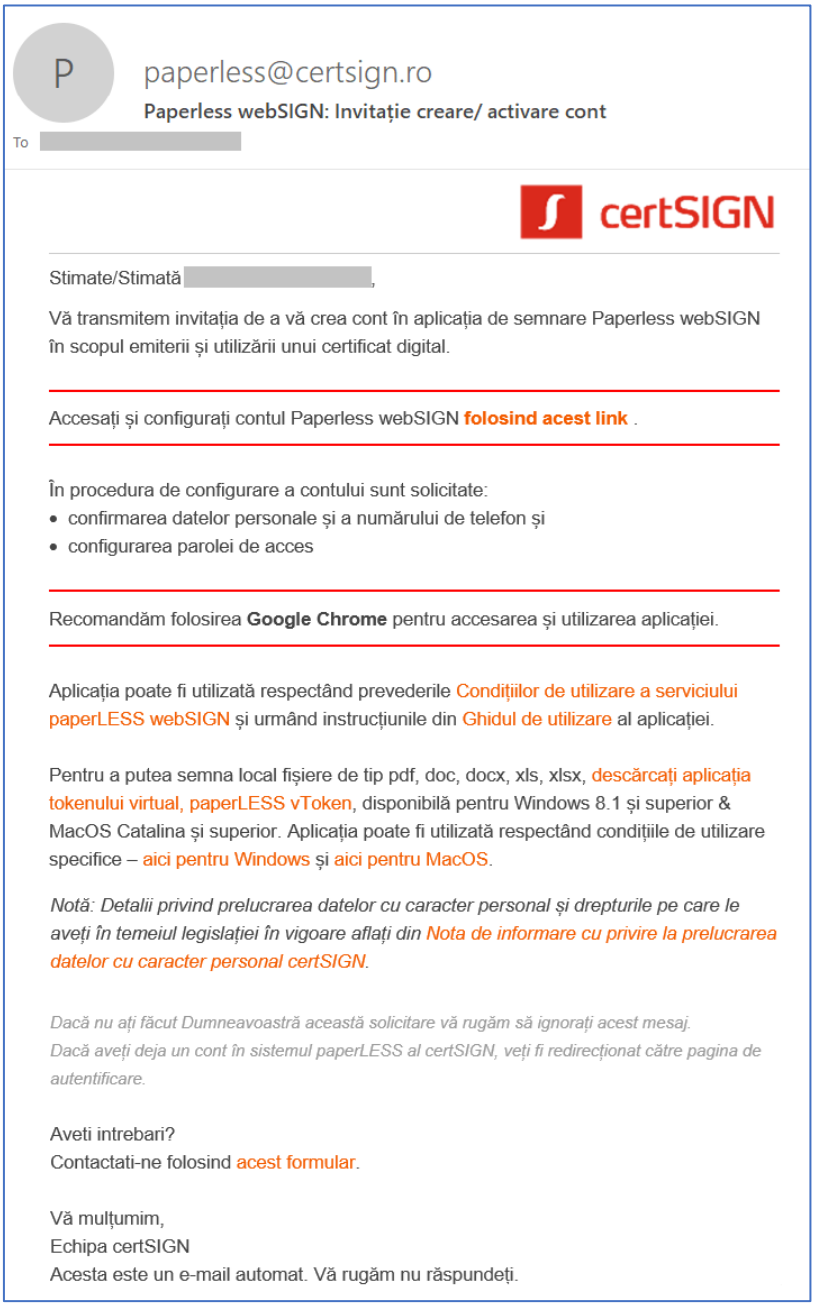
Completați datele solicitate (nume, prenume, e-mail, telefon), bifați că ați luat cunoștință de prelucrarea datelor conform politicii de confidențialitate și apăsați butonul **Înregistrează-te**.



Pe adresa de e-mail completată se va transmite invitația pentru crearea contului în platforma de semnare Paperless webSIGN.

1.2. Crearea/activarea contului Paperless webSIGN

Deschideți invitația **Paperless webSIGN: Invitație creare/activare cont** primită pe e-mail. Pentru a configura contul dvs. Paperless accesați hyperlinkul aflat în textul **folosind acest link**. Folosiți browser-ul Google Chrome.



P paperless@certsign.ro
Paperless webSIGN: Invitație creare/ activare cont
To [redacted]

certSIGN

Stimate/Stimată [redacted],

Vă transmitem invitația de a vă crea cont în aplicația de semnare Paperless webSIGN în scopul emiterii și utilizării unui certificat digital.

Accesați și configurați contul Paperless webSIGN **folosind acest link** .

În procedura de configurare a contului sunt solicitate:
- confirmarea datelor personale și a numărului de telefon și
- configurarea parolei de acces

Recomandăm folosirea **Google Chrome** pentru accesarea și utilizarea aplicației.

Aplicația poate fi utilizată respectând prevederile Condițiilor de utilizare a serviciului paperLESS webSIGN și urmând instrucțiunile din Ghidul de utilizare al aplicației.

Pentru a putea semna local fișiere de tip pdf, doc, docx, xls, xlsx, descărcați aplicația tokenului virtual, paperLESS vToken, disponibilă pentru Windows 8.1 și superior & MacOS Catalina și superior. Aplicația poate fi utilizată respectând condițiile de utilizare specifice – aici pentru Windows și aici pentru MacOS.

Notă: Detalii privind prelucrarea datelor cu caracter personal și drepturile pe care le aveți în temeiul legislației în vigoare aflați din Nota de informare cu privire la prelucrarea datelor cu caracter personal certSIGN.

Dacă nu ați făcut Dumneavoastră această solicitare vă rugăm să ignorați acest mesaj.
Dacă aveți deja un cont în sistemul paperLESS al certSIGN, veți fi redirecționat către pagina de autentificare.

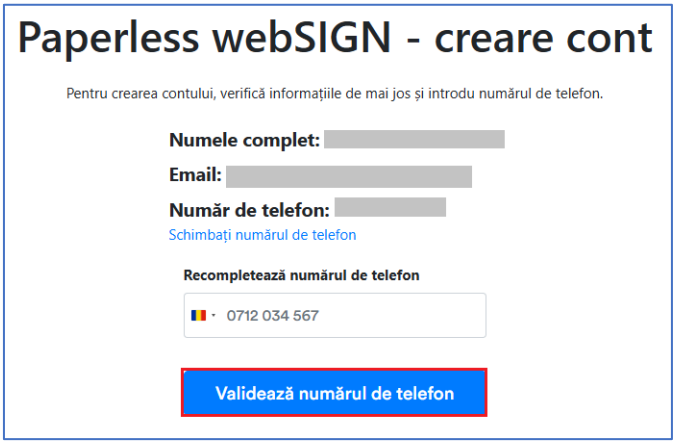
Aveti intrebari?
Contactati-ne folosind acest formular.

Vă mulțumim,
Echipa certSIGN
Acesta este un e-mail automat. Vă rugăm nu răspundeți.

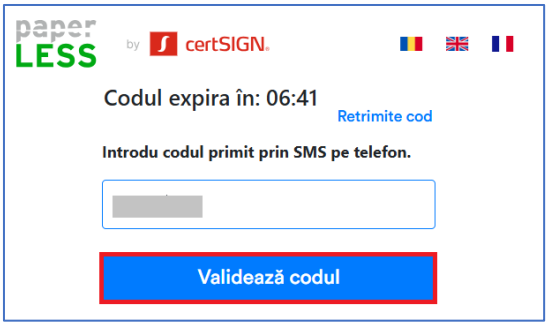
În pagina care se afișează vor fi datele completate de dvs. anterior. Selectați țara și recompletați numărul de telefon, apoi apăsați **Validează numărul de telefon**. Pe numărul de telefon veți primi un SMS de la un număr scurt cu eticheta certSIGN.

Atenție! Verificați să aveți permisă primirea de SMS-uri de la numere scurte.

În cazul în care vreți să modificați numărul de telefon asociat contului dvs., selectați **Schimbați numărul de telefon** și urmați pașii de acolo.



Introduceți codul SMS în timpul afișat pe ecran. Dacă nu reușiți să introduceți în timp util codul SMS (un cod este valabil 10 minute), va apărea butonul **Retrimite cod**, ca să puteți solicita alt cod SMS pentru validare, dar nu înainte de 30 de minute.



Stabiliți o parolă complexă pentru contul pe care l-ați creat, apoi apăsați butonul **Înregistrează-te**.

Se va deschide pagina de logare în cont. Introduceți Numele de utilizator (e-mail) și parola, apoi apăsați **Continuă**.

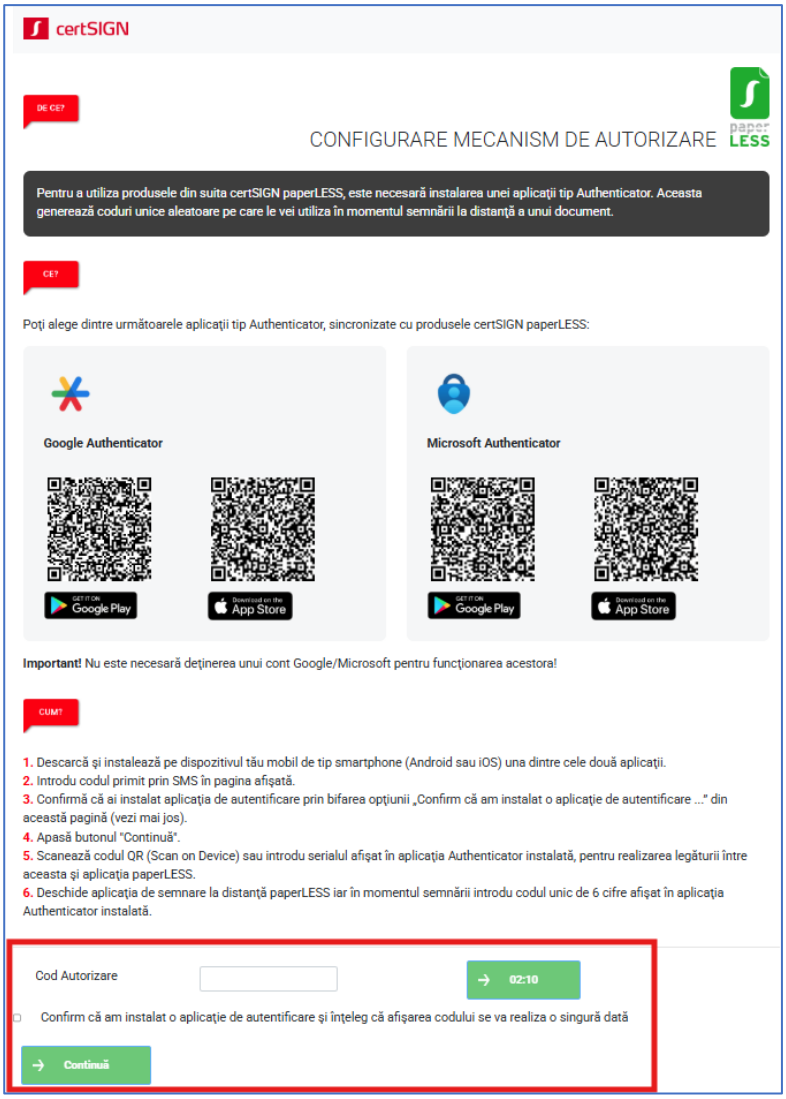
În pagina următoare, apare informarea de necesitate a configurării mecanismului de autentificare cu doi factori (2FA). Autentificare cu doi factori (2FA) adaugă un nivel de protecție suplimentar la logarea în contul dvs. deoarece, în afară de parolă, este solicitată și introducerea unui cod generat pe telefonul mobil de una dintre aplicațiile de autorizare recomandate: Google Authenticator sau Microsoft Authenticator, pe care trebuie să o împerecheați cu contul de cloud.

Dacă doriți să faceți configurarea, apăsați butonul **Configureaza 2FA** și urmați instrucțiunile apărute. Odată configurarea făcută, logarea în cont o veți face prin autentificare cu doi factori (2FA): parolă cont și cod generat de aplicația de autorizare de pe telefon.

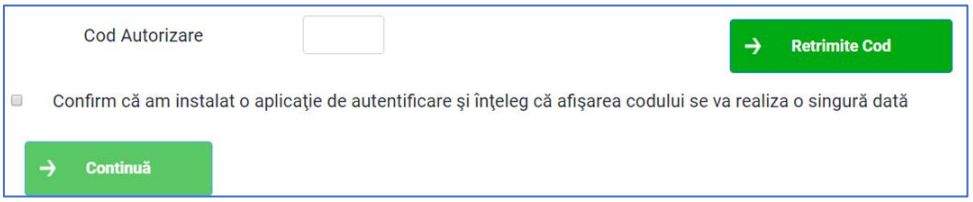
Dacă nu doriți să faceți configurarea, optați pentru unul dintre momentele de reamintire: la o dată aleasă de dvs., la următoarea autentificare sau niciodată. Oricare variantă veți alege, configurarea 2FA poate fi făcută cel târziu până la data de 31.12.2026, când devine obligatorie.

• Configurarea contului pentru autentificarea cu 2FA

1. După ce ați apăsat butonul **Configureaza 2FA** se va deschide o pagină cu informații, iar pe numărul de telefon folosit la înrolare se va trimite prin SMS codul de autorizare pentru continuarea procedurii. Instalați pe telefon una dintre aplicațiile de autorizare Google Authenticator sau Microsoft Authenticator prezentate în informațiile de la secțiunea **CE**? Derulați pagina web afișată până în partea de jos și, în câmpul **Cod Autorizare** de la secțiunea **CUM?**, introduceți, în maxim 10 minute, codul de autorizare primit prin SMS în momentul accesării link-ului.



2. Dacă nu ați reușit introducerea codului în cele 10 minute alocate, la terminarea celor 10 minute, cronometrul din dreptul câmpului **Cod Autorizare** se oprește. Apăsați butonul **Retrimite cod** pentru primirea altui cod prin SMS, dar nu înainte de 30 de minute.



3. Pentru finalizarea configurării autorizării bifați check box-ul de confirmare instalare aplicație Authenticator și apăsați **Continuă** (pașii 3-4 secțiunea **CUM?**). Se va afișa pagina cu codul QR.

4. Pentru împerecherea soluției de autorizare de pe telefon cu contul dvs. Paperless webSIGN din platforma de semnare Paperless webSIGN, trebuie copiat sau scanat codul QR afișat (pasul 5 secțiunea **CUM?**), în funcție de device-ul de pe care ați urmat pașii de configurare:

– dacă aveți afișat codul QR pe alt device (calculator, laptop, tabletă sau alt telefon) decât cel pe care ați instalat aplicația de autorizare, deschideți aplicația Authenticator instalată pe telefon și scanați codul QR ca la ①;

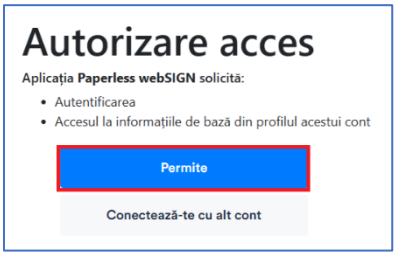
– dacă aveți afișat codul QR pe telefonul pe care ați instalat aplicația de autorizare, apăsați butonul **Salvează pe dispozitiv** ② și codul QR va fi salvat.

5. După scanarea/salvarea codului QR, aplicația Authenticator de pe telefon va genera coduri de autorizare de 6 cifre, valabile 30 de secunde. Pentru finalizarea configurării, introduceți un cod generat de aplicația de autorizare și apăsați **Trimite codul**. Ulterior va apărea fereastra de autorizare a accesului.

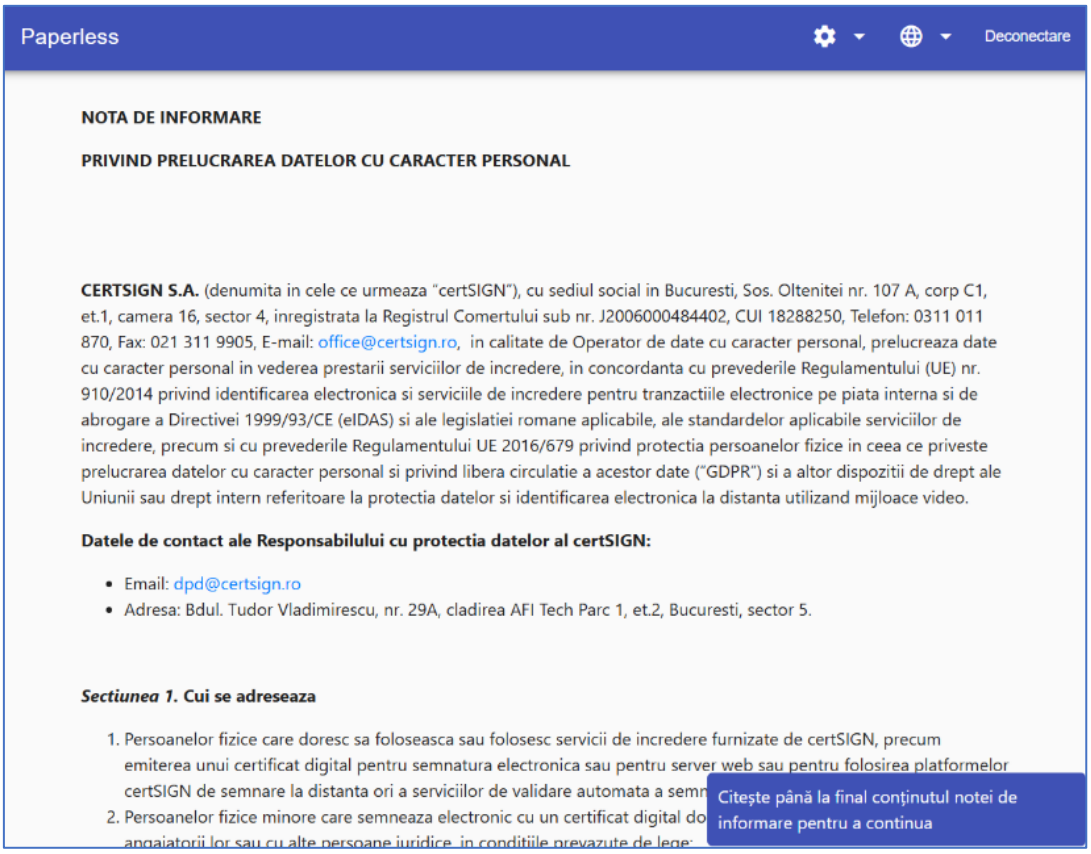
• Configurarea contului pentru autentificarea fără 2FA

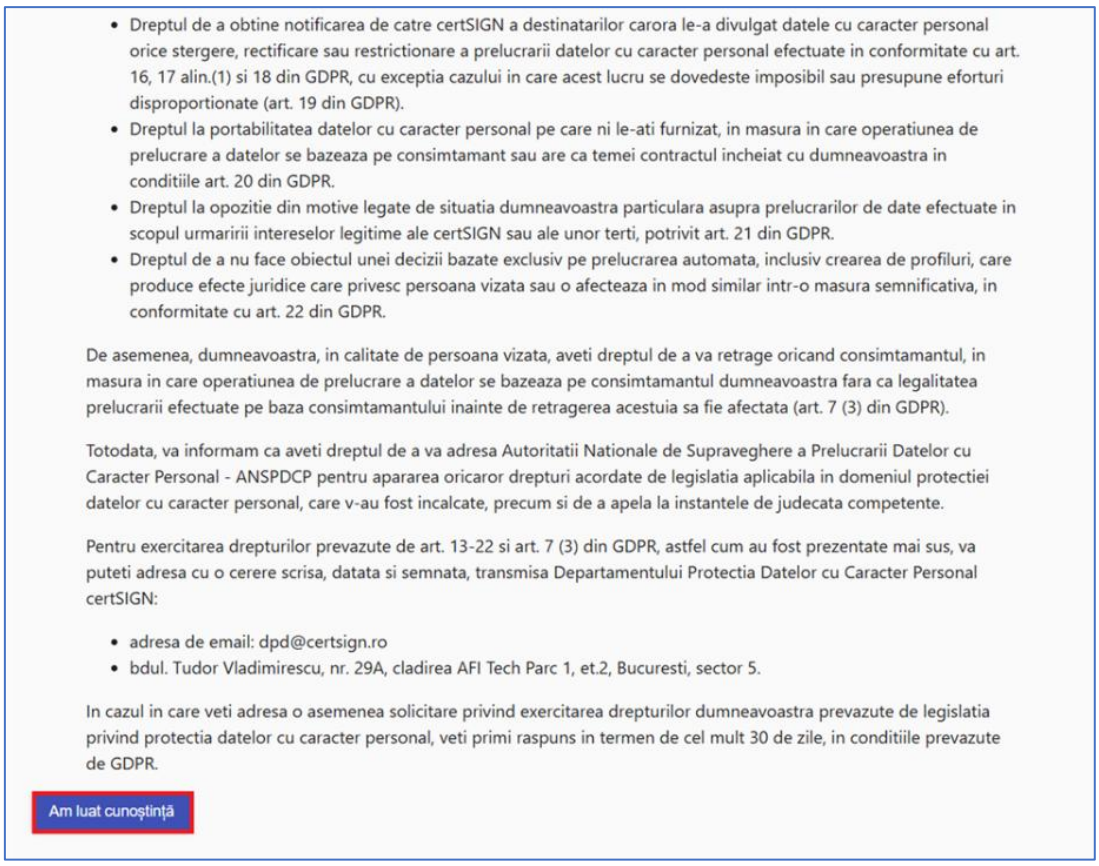
După ce ați selectat oricare dintre variantele de amânare a configurării mecanismului de autentificare cu doi factori, va apărea fereastra de autorizare a accesului.

Orice tip de autentificare ați ales, cu 2FA sau fără 2FA, aplicația vă va solicita acordul pentru accesarea unor resurse protejate, așa cum apare în imaginea de mai jos. Acest ecran va fi afișat doar la prima conectare. Apăsați butonul **Permite** pentru a putea utiliza aplicația Paperless webSIGN.



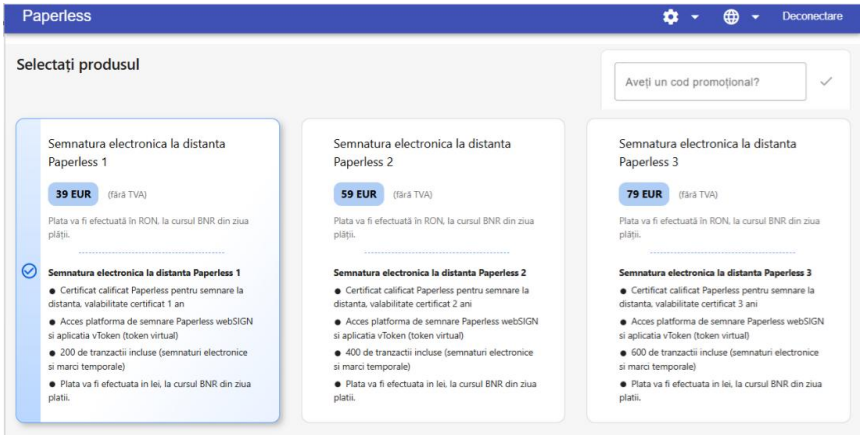
Citiți *Nota de informare privind prelucrarea datelor dvs. conform GDPR*. Apăsați butonul **Am luat cunoștință** pentru a trece mai departe.





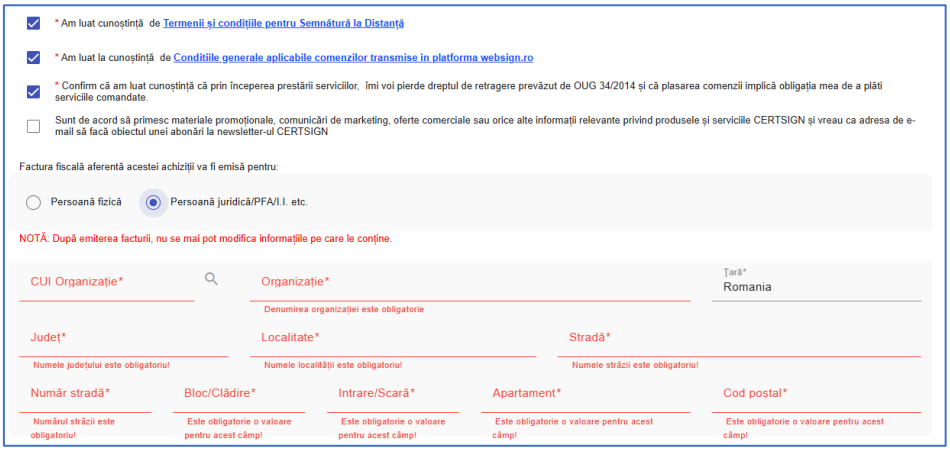
1.3. Selectarea pachetului dorit, introducerea datelor și plata online

Selectați pachetul dorit pentru noul certificat:

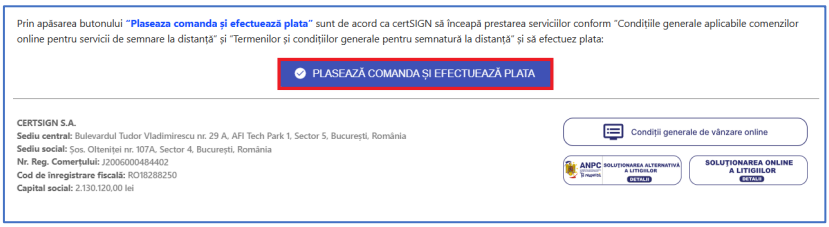


Consultați documentele **Termenii și condițiile pentru Semnătură la Distanță**, respectiv **Condițiile generale aplicabile comenzilor transmise în platforma Paperless**, apoi bifați corespunzător:

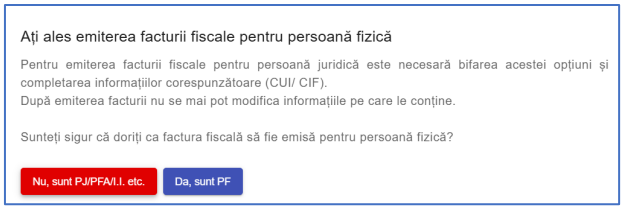
Dacă doriți ca factura fiscală să fie emisă pe numele unei companii, bifați corespunzător și completați datele companiei:



Pentru inițierea plății, apăsați butonul **PLASEAZĂ COMANDA ȘI EFECTUEAZĂ PLATA**:

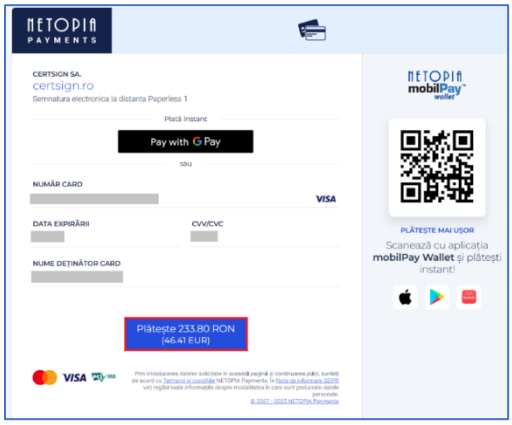


Dacă s-a bifat persoană fizică, va apărea un pop up care să vă informeze că datele din factură nu se pot modifica după emitere și să verificați dacă aveți nevoie totuși de factură pentru persoană juridică. Dacă doriți factura pentru persoană juridică, apăsați butonul **Nu, sunt PJ/PFA/I.I. etc.** și introduceți datele pentru persoană juridică. Dacă doriți factura pentru persoană fizică, apăsați butonul **Da, sunt PF**.



Se va deschide fereastra de plată din aplicația Netopia unde trebuie introdusă adresa de e-mail pentru validarea datelor (numărul de telefon este deja introdus). Pentru continuare apăsați butonul **Continuă**.

Se va plăti suma pentru pachetul ales (euro + TVA) în lei la cursul BNR din ziua plății. După completarea detaliilor solicitate pentru card, apăsați butonul **Plătește** pentru a face plata.



Odată ce plata a fost făcută, pe adresa de e-mail înregistrată primiți confirmarea de plată de la Netopia.

În interfața platformei https://websign.ro, după ce plata a fost confirmată, urmează pasul de identificare video. Aveți nevoie de actul de identitate în original, conexiune bună la internet și acces la camera video și microfon.

1.4. Identificarea video a viitorului titular de cont și de certificat digital calificat la distanță

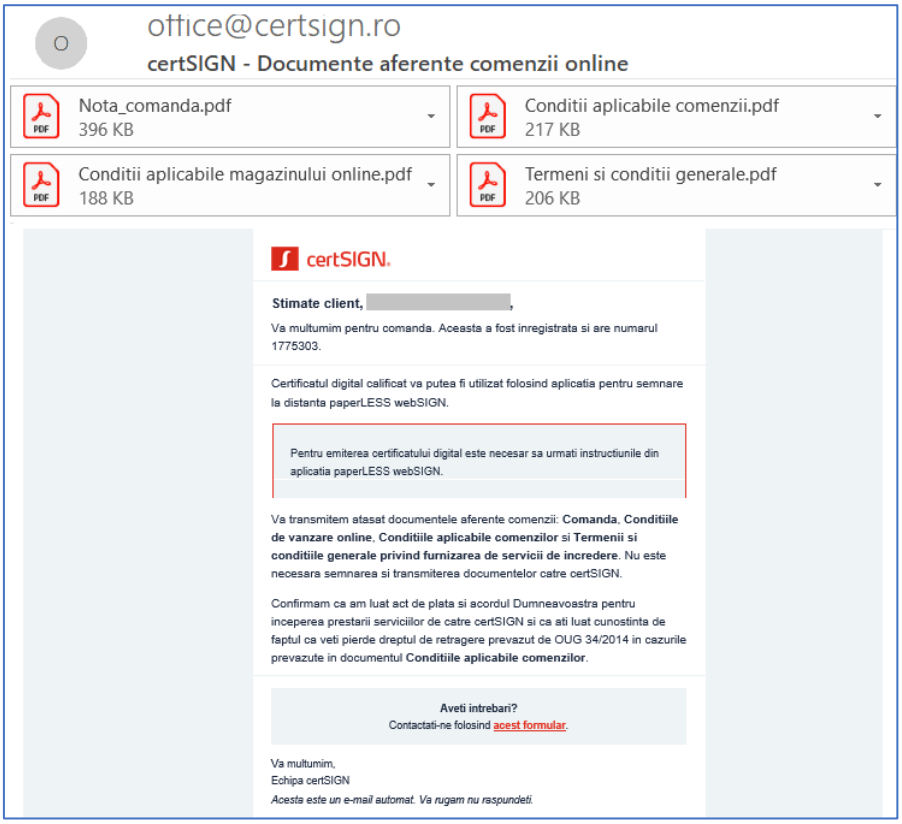
După apăsarea butonului **Continuă** (vezi imaginea anterioară), veți fi redirecționat către platforma de identificare video unde trebuie să selectați tipul actului de identitate cu care vă identificați, să bifați check box-urile și să apăsați butonul roșu **Apasă aici pentru a începe**.

Atenție! Dacă în procesul de identificare video nu primiți SMS sau constatați că numărul de telefon nu este corect, îl puteți schimba. Ulterior, dacă doriți, noul număr de telefon va putea fi asociat contului dvs. de cloud din platforma https://websign.ro.

După finalizarea identificării video, platforma afișează informarea cu privire la durata maximă a procesului de verificare a identității:

După verificarea identificării video, veți primi pe e-mail notificarea cu privire la acceptarea sau respingerea acesteia, precum și a motivelor de respingere, după caz.

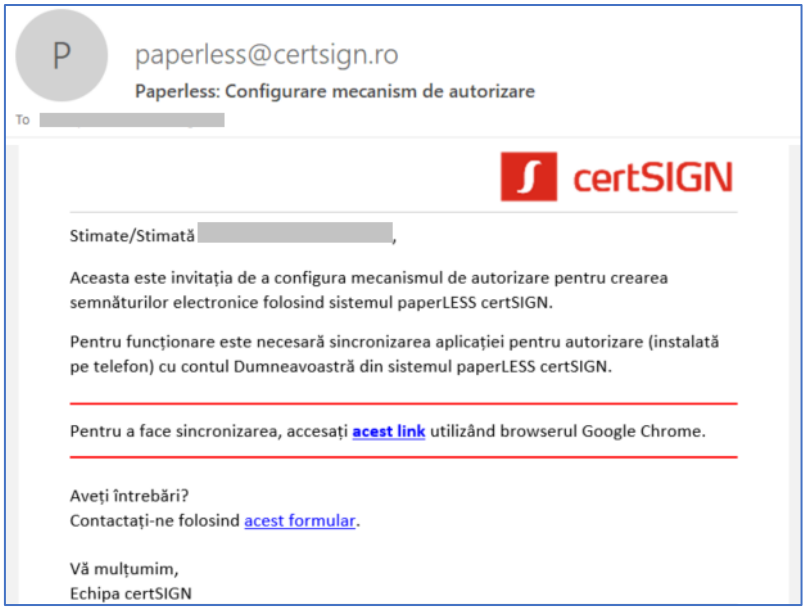
Pe e-mail veți primi și confirmarea acceptării de către certSIGN a comenzii dvs. împreună cu documentele aferente.



1.5. Configurarea autorizării la serviciul Paperless webSIGN pentru autentificarea fără 2FA

În cazul în care ați optat pentru autentificarea cu 2FA, continuați cu pasul 1.6 deoarece configurarea mecanismului de autorizare a fost făcută deja la crearea contului.

În cazul în care ați optat pentru autentificarea fără 2FA (ca să o realizați mai târziu), pe e-mail veți primi invitația pentru configurarea mecanismului de autorizare. Parcurgeți pașii de configurare din browserul Google Chrome.



Pentru configurarea autorizării de semnare prin serviciul Paperless webSIGN trebuie să parcurgeți două etape:

– instalarea soluției de autorizare pe telefon;

– împerecherea soluției de autorizare cu contul Paperless webSIGN.

1.5.1. Instalarea soluției de autorizare pe telefon

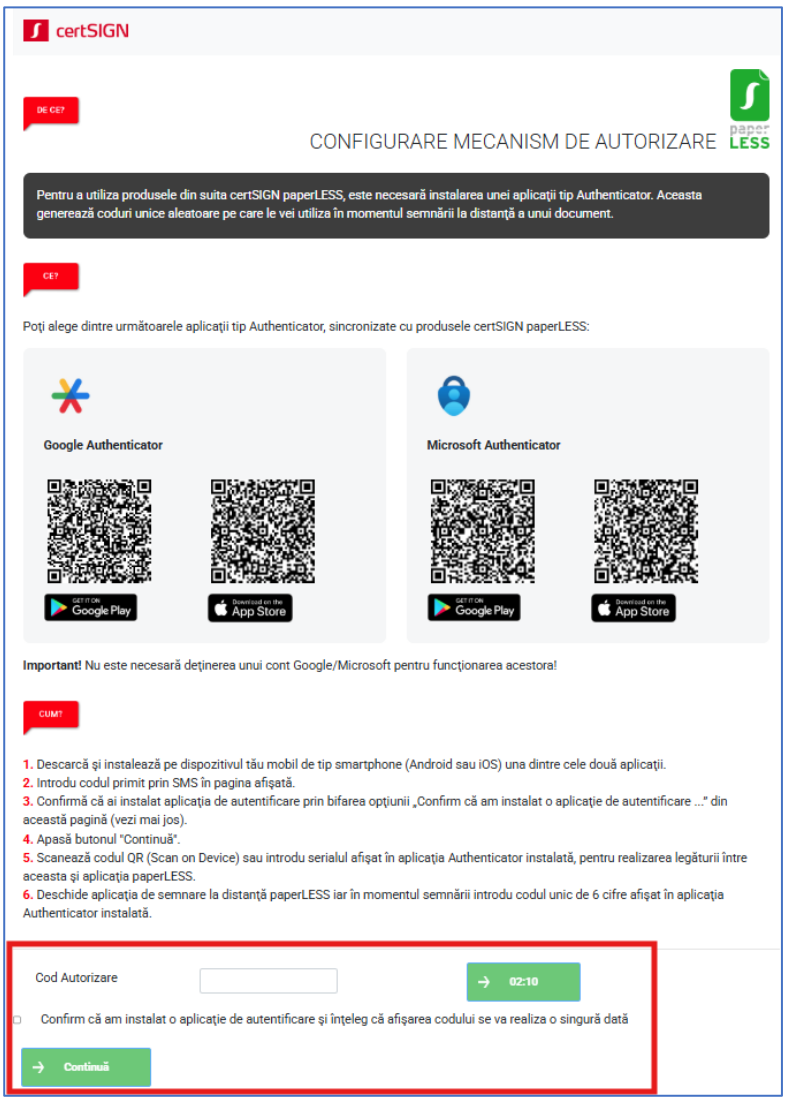
Pentru autorizarea de pe telefon se poate folosi varianta instalării uneia dintre aplicațiile **Google Authenticator** sau **Microsoft Authenticator**. Ambele se descarcă din magazinul de aplicații al telefonului. Aplicația este compatibilă cu Android și iPhone.

1.5.2. Împerecherea soluției de autorizare cu contul Paperless webSIGN

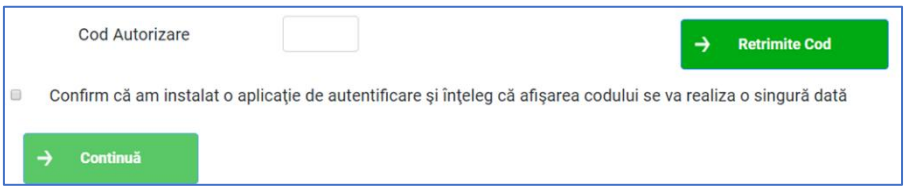
După instalarea soluției de autorizare, pe adresa de e-mail pe care ați făcut înrolarea, căutați e-mail-ul **Paperless: Configurare mecanism de autorizare** de la paperless@certsign.ro. E-mail-ul reprezintă invitația de configurare a mecanismului de autorizare.

În vederea autorizării utilizării serviciului Paperless webSIGN parcurgeți pașii de mai jos:

1. Apăsați cuvintele **acest link** și deschideți hiperlink-ul în browser-ul Google Chrome. La accesarea link-ului, pe numărul de telefon folosit la înrolare se va trimite prin SMS codul de autorizare pentru continuarea procedurii. Derulați pagina web afișată până în partea de jos și, în câmpul **Cod Autorizare** de la secțiunea **CUM?**, introduceți, în maxim 10 minute, codul de autorizare primit prin SMS în momentul accesării link-ului.



2. Dacă nu ați reușit introducerea codului în cele 10 minute alocate, la terminarea celor 10 minute, cronometrul din dreptul câmpului **Cod Autorizare** se oprește. Apăsați butonul **Retrimite cod** pentru primirea altui cod prin SMS, dar nu înainte de 30 de minute.



3. Pentru finalizarea configurării autorizării bifați check box-ul de confirmare instalare aplicație Authenticator și apăsați Continuă (pașii 3-4 secțiunea CUM?). Se va afișa pagina cu codul QR.

4. Pentru împerecherea soluției de autorizare de pe telefon cu contul dvs. Paperless webSIGN din platforma de semnare Paperless webSIGN, trebuie copiat sau scanat codul QR afișat (pasul 5 secțiunea CUM?), în funcție de device-ul de pe care ați urmat pașii de împerechere:

– dacă aveți afișat codul QR pe alt device (calculator, laptop, tabletă sau alt telefon) decât cel pe care ați instalat aplicația de autorizare, deschideți aplicația Authenticator instalată pe telefon și scanați codul QR ca la ①;

– dacă aveți afișat codul QR pe telefonul pe care ați instalat aplicația de autorizare, apăsați butonul **Salvează pe dispozitiv** ② și codul QR va fi salvat.

5. După scanarea/salvarea codului QR, aplicația Authenticator de pe telefon va genera coduri de autorizare de 6 cifre, valabile 30 de secunde. Pentru finalizarea împerecherii, introduceți un cod generat de aplicația de autorizare și apăsați **Trimite**. Se va afișa mesajul că ați configurat cu succes mecanismul de autorizare.

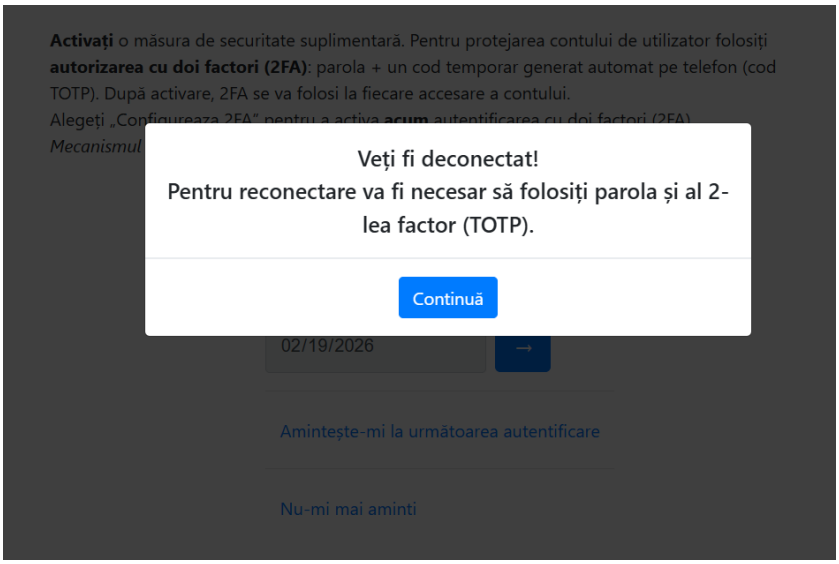
1.6. Emiterea certificatului digital în platforma Paperless webSIGN

Pentru emiterea certificatului digital accesați platforma https://websign.ro cu e-mail-ul și parola cu care v-ați înrolat. Emiterea se poate face atât de pe calculator cu Windows sau macOS, cât și de pe telefon Android sau iPhone.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA, dar doriți să o faceți acum, apăsați butonul **Configureaza 2FA**.

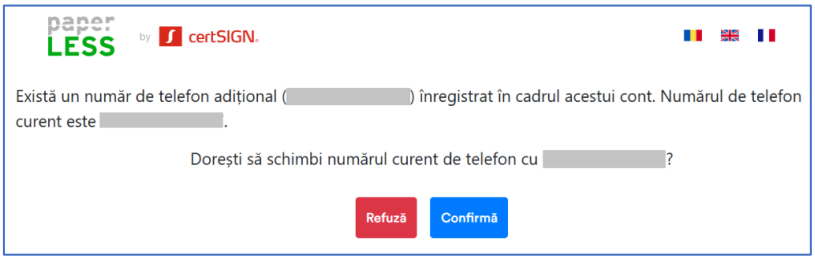
Se va afișa un pop-up cu un mesaj de informare că veți fi deconectat și că la reconectare, după introducerea userului și parolei, trebuie să introduceți un cod de autorizare din aplicația Authenticator pe care o aveți deja configurată pe telefon. Apăsați butonul **Continuă**.



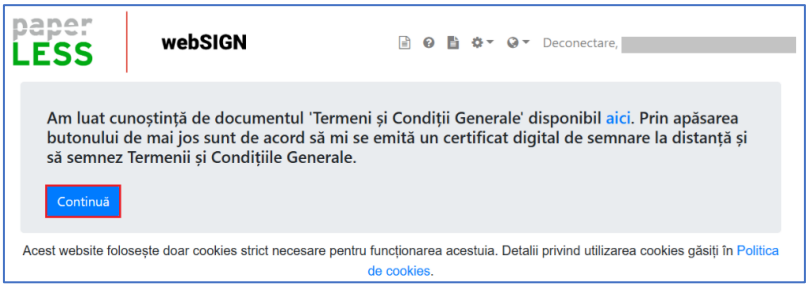
După logare cu parola contului, în fereastra care apare, introduceți codul de autorizare afișat de aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA și nu doriți să o faceți acum, alegeți una dintre opțiunile de amânare.

În cazul în care, în etapa de identificare video, ați optat pentru modificarea numărului de telefon în scopul primirii SMS-ului, aveți posibilitatea să asociați acest număr cu contul de cloud din platforma https://websign.ro. Dacă doriți să aveți asociat cu contul de cloud acest număr de telefon, apăsați butonul **Confirmă**. Dacă doriți să rămână numărul care este deja asociat, apăsați butonul **Refuză**.

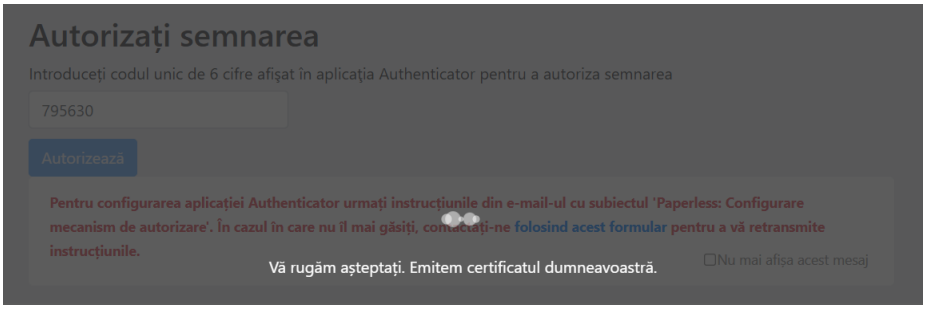


Consultați termenii și condițiile specifice procesului de emitere pentru noul certificat și, dacă sunteți de acord, apăsați butonul **Continuă** pentru a semna termenii și a se emite certificatul.

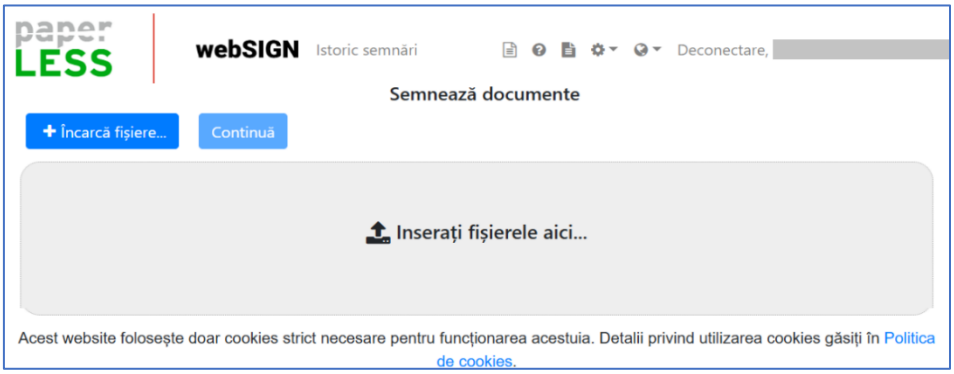


La apăsarea butonului **Continuă** se va deschide pagina de autorizare, ce conține un câmp în care se solicită un cod de autorizare generat de aplicația de autorizare de pe telefon, Microsoft Authenticator sau Google Authenticator.

După ce se va introduce codul de autorizare, se va emite certificatul calificat care va fi folosit la semnare pe parcursul perioadei sale de valabilitate.



După generarea certificatului, va apărea pagina principală din platforma Paperless webSIGN unde se pot încărca documentele pentru a fi semnate.



2. Rekey – reînnoire certificat digital calificat pentru semnare la distanță

Cu 45 de zile înainte de expirarea certificatului valabil deținut deja (sau cu 15 zile daca nu s-a facut rekey-ul), utilizatorul primește pe e-mail o notificare, cu link către platforma Paperless webSIGN, pentru actualizarea datelor în vederea reînnoirii certificatului.

office@certsign.ro
certSIGN - Notificare expirare certificat pentru semnare la distanta
To

Stimate client ********** ,

Certificatul tău digital cu serialul nr. ********** expiră la ********** .

Pentru emiterea unui nou certificat:

1. autentifică-te în contul tău din aplicația **websign.ro** și apăsa butonul **"Începe procesul"**,

2. alege produsul cu valabilitatea dorită pentru noul certificat,

3. citește și bifează mențiunile afișate în pagină,

4. achită contravaloarea produsului selectat,

5. completează datele cerute în pasul următor, încarcă o copie a documentului tău de identitate și trimite și semnează cererea pentru noul certificat prin apăsarea butonului **"Înregistrare"**.

După validarea cererii, cu cel mult 3 zile înainte de expirarea certificatului actual, certSIGN va emite noul certificat, iar prin e-mail ți se va trimite o notificare în acest sens.

IMPORTANT!

Cererea pentru noul certificat trebuie transmisă cel mai tarziu cu 3 zile înainte de data expirării. Transmiterea întârziată a cererii nu garantează reînnoirea online certificatului.

Daca certificatul expiră vă rugăm să ne contactați la datele de mai jos.

Pentru mai multe informatii, nu ezitati sa ne contactati la adresa office@certsign.ro sau sa apelati la 031 101 18 70.

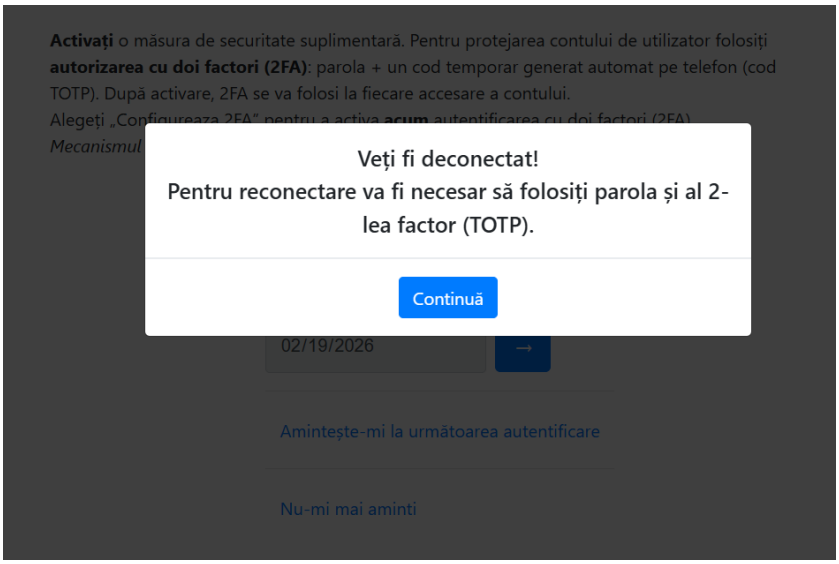
Îți mulțumim,
Echipa certSIGN

La accesarea link-ului https://websign.ro, utilizatorul este redirectat către ecranul de autentificare în platformă.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA, dar doriți să o faceți acum, apăsați butonul **Configureaza 2FA**.

Se va afișa un pop-up cu un mesaj de informare că veți fi deconectat și că la reconectare, după introducerea userului și parolei, trebuie să introduceți un cod de autorizare din aplicația Authenticator pe care o aveți deja configurată pe telefon. Apăsați butonul **Continuă**.



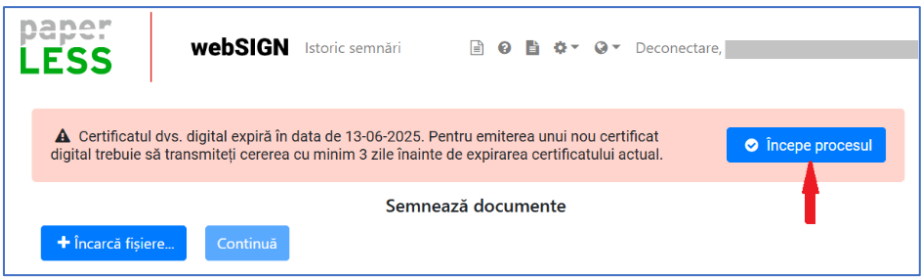
După logare cu parola contului, în fereastra care apare, introduceți codul de autorizare afișat de aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA și nu doriți să o faceți acum, alegeți una dintre opțiunile de amânare.

După autentificare în interfața platformei Paperless webSIGN, în partea de sus a ecranului principal utilizatorul va avea afișat un banner cu detaliile privind expirarea certificatului, pe toată perioada în care se poate face rekey. Cu 3 zile (72 ore) înainte de expirarea certificatului deținut se încheie perioada de rekey și NU se mai poate parcurge această procedură pentru reînnoirea certificatului.

Atenție! Procedura de reînnoire certificat poate fi parcursă până cu maxim 3 zile (= 72 ore) înainte de expirare. În cazul în care certificatul are mai puțin de 72 de ore până la expirare sau a expirat, va fi necesar să faceți o nouă achiziție după expirarea certificatului actual. Achiziția presupune plata și identificarea video a utilizatorului. Plata efectuată pentru rekey va fi restituită în contul Dvs.

Pentru a iniția procesul de reînnoire a certificatului se va apăsa butonul **Începe procesul**:



Citiți Nota de informare privind prelucrarea datelor dvs. conform GDPR. Apăsați butonul **Confirmă** pentru a vă exprima acordul și a trece mai departe.

Acord GDPR

NOTA DE INFORMARE

PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

CERTSIGN S.A. (denumita in cele ce urmeaza "certSIGN"), cu sediul social in Bucuresti, Sos. Oltenitei nr. 107 A, corp C1, et.1, camera 16, sector 4, inregistrata la Registrul Comertului sub nr. J2006000484402, CUI 18288250, Telefon: 0311 011 870, Fax: 021 311 9905, E-mail: office@certsign.ro, in calitate de Operator de date cu caracter personal, prelucreaza date cu caracter personal in vederea prestarii serviciilor de incredere, in concordanta cu prevederile Regulamentului (UE) nr. 910/2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna si de abrogare a Directivei 1999/93/CE (eIDAS) si ale legislatiei romane aplicabile, ale standardelor aplicabile serviciilor de incredere, precum si cu prevederile Regulamentului UE 2016/679 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date ("GDPR") si a altor dispozitii de drept ale Uniunii sau drept intern referitoare la protectia datelor si identificarea electronica la distanta utilizand mijloace video.

Datele de contact ale Responsabilului cu protectia datelor al certSIGN:

- Email: dpd@certsign.ro
- Adresa: Bdul. Tudor Vladimirescu, nr. 29A, cladirea AFI Tech Parc 1, et.2, Bucuresti, sector 5.

Sectiunea 1. **Cui se adreseaza**

1. Persoanelor fizice care doresc sa foloseasca sau folosesc servicii de incredere furnizate de certSIGN, precum emiterea unui certificat digital pentru semnatura electronica sau pentru server web sau pentru folosirea platformelor certSIGN de semnare la distanta ori a serviciilor de validare automata a semnaturilor si sigiliilor electronice calificate;

Renunță | Confirmă

Acord GDPR

disproportionate (art. 19 din GDPR).

- Dreptul la portabilitatea datelor cu caracter personal pe care ni le-ati furnizat, in masura in care operatiunea de prelucrare a datelor se bazeaza pe consimtamant sau are ca temei contractul incheiat cu dumneavoastra in conditiile art. 20 din GDPR.
- Dreptul la opozitie din motive legate de situatia dumneavoastra particulara asupra prelucrarilor de date efectuate in scopul urmaririi intereselor legitime ale certSIGN sau ale unor terti, potrivit art. 21 din GDPR.
- Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automata, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizata sau o afecteaza in mod similar intr-o masura semnificativa, in conformitate cu art. 22 din GDPR.

De asemenea, dumneavoastra, in calitate de persoana vizata, aveti dreptul de a va retrage oricand consimtamantul, in masura in care operatiunea de prelucrare a datelor se bazeaza pe consimtamantul dumneavoastra fara ca legalitatea prelucrarii efectuate pe baza consimtamantului inainte de retragerea acestuia sa fie afectata (art. 7 (3) din GDPR).

Totodata, va informam ca aveti dreptul de a va adresa Autoritatii Nationale de Supraveghere a Prelucrarii Datelor cu Caracter Personal - ANSPDCP pentru apararea oricaror drepturi acordate de legislatia aplicabila in domeniul protectiei datelor cu caracter personal, care v-au fost incalcate, precum si de a apela la instantele de judecata competente.

Pentru exercitarea drepturilor prevazute de art. 13-22 si art. 7 (3) din GDPR, astfel cum au fost prezentate mai sus, va puteti adresa cu o cerere scrisa, datata si semnata, transmisa Departamentului Protectia Datelor cu Caracter Personal certSIGN:

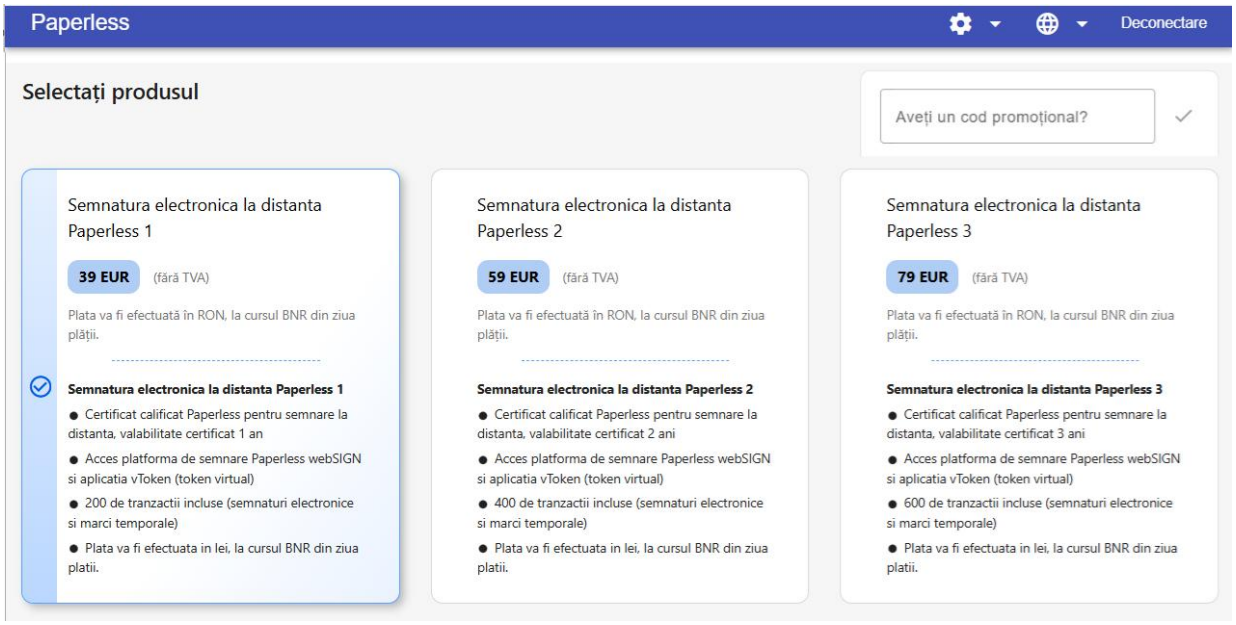
- adresa de email: dpd@certsign.ro
- bdul. Tudor Vladimirescu, nr. 29A, cladirea AFI Tech Parc 1, et.2, Bucuresti, sector 5.

In cazul in care veti adresa o asemenea solicitare privind exercitarea drepturilor dumneavoastra prevazute de legislatia privind protectia datelor cu caracter personal, veti primi raspuns in termen de cel mult 30 de zile, in conditiile prevazute de GDPR.

Renunță | Confirmă

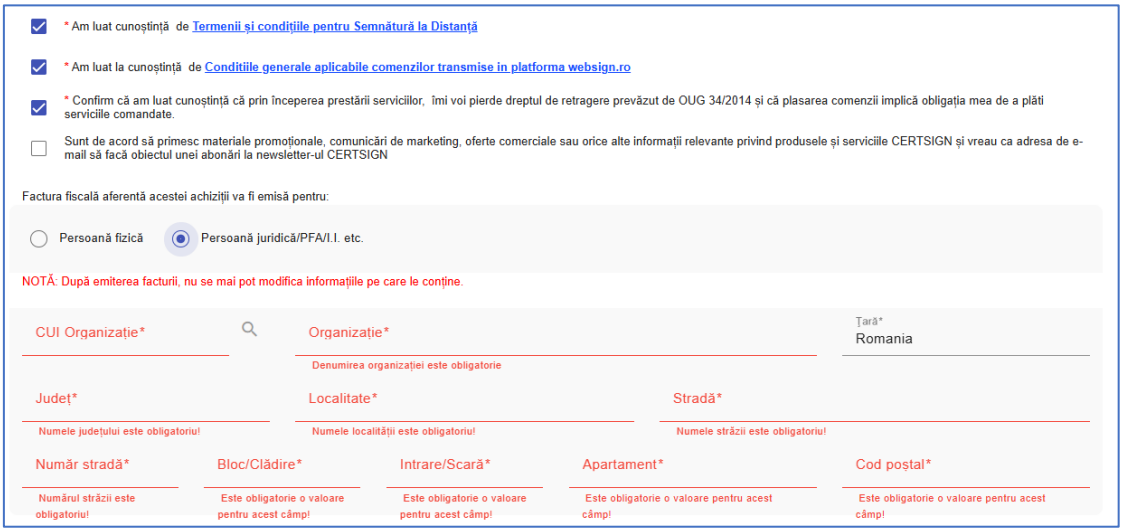
2.1. Selectarea pachetului dorit și plata online

Selectați pachetul dorit pentru noul certificat:

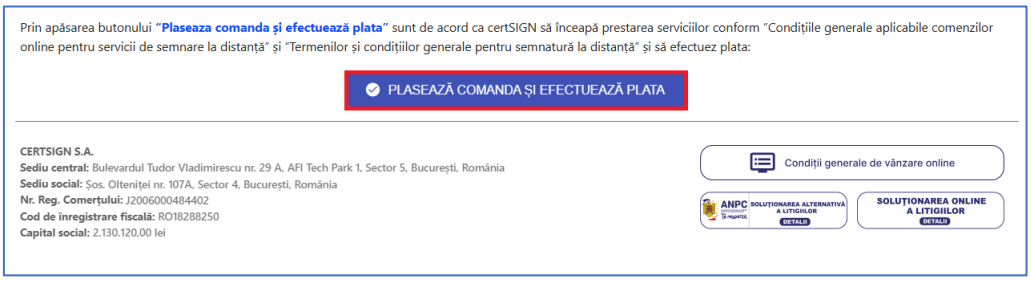


Consultați documentele **Termenii și condițiile pentru Semnătură la Distanță**, respectiv **Condițiile generale aplicabile comenzilor transmise în platforma Paperless**, apoi bifati corespunzator:

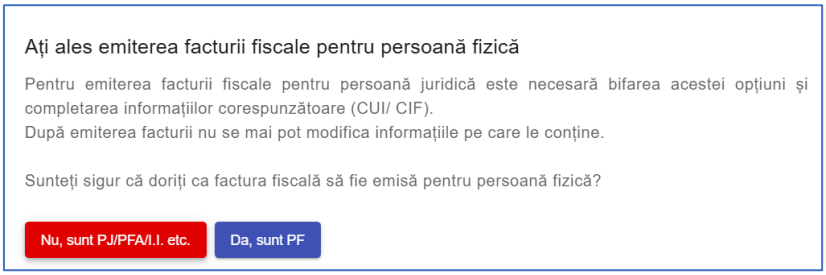
Dacă se dorește ca factura fiscală să fie emisă pe numele unei companii, se pune bifa corespunzătoare și se completează datele companiei:



Pentru inițierea plății, se va apăsa butonul **PLASEAZĂ COMANDA ȘI EFECTUEAZĂ PLATA**:

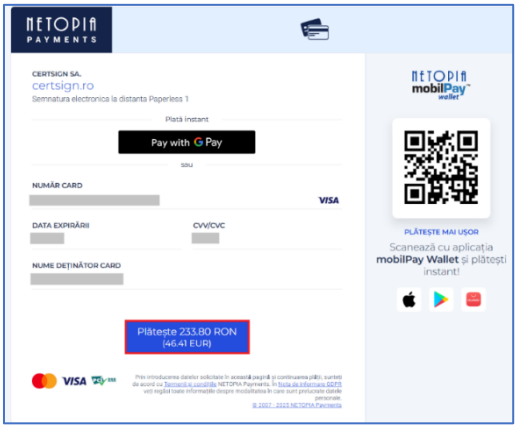


Dacă s-a bifat persoană fizică, va apărea un pop up care să vă informeze că datele din factură nu se pot modifica după emitere și să verificați dacă aveți nevoie totuși de factură pentru persoană juridică. Dacă doriți factura pentru persoană juridică, apăsați butonul **Nu, sunt PJ/PFA/I.I. etc.** și introduceți datele pentru persoană juridică. Dacă doriți factura pentru persoană fizică, apăsați butonul **Da, sunt PF**.



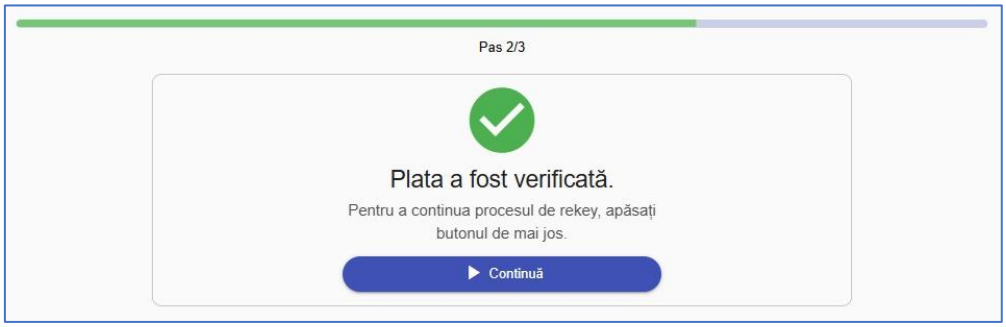
Se va deschide fereastra de plată din aplicația Netopia unde trebuie introdusă adresa de e-mail pentru validarea datelor (numărul de telefon este deja introdus). Pentru continuare se apasă butonul **Continuă**.

Se va plăti suma pentru produsul ales (euro + TVA) în lei la cursul BNR din ziua plății. După completarea detaliilor solicitate pentru card, se apasă butonul **Plătește** pentru a face plata.



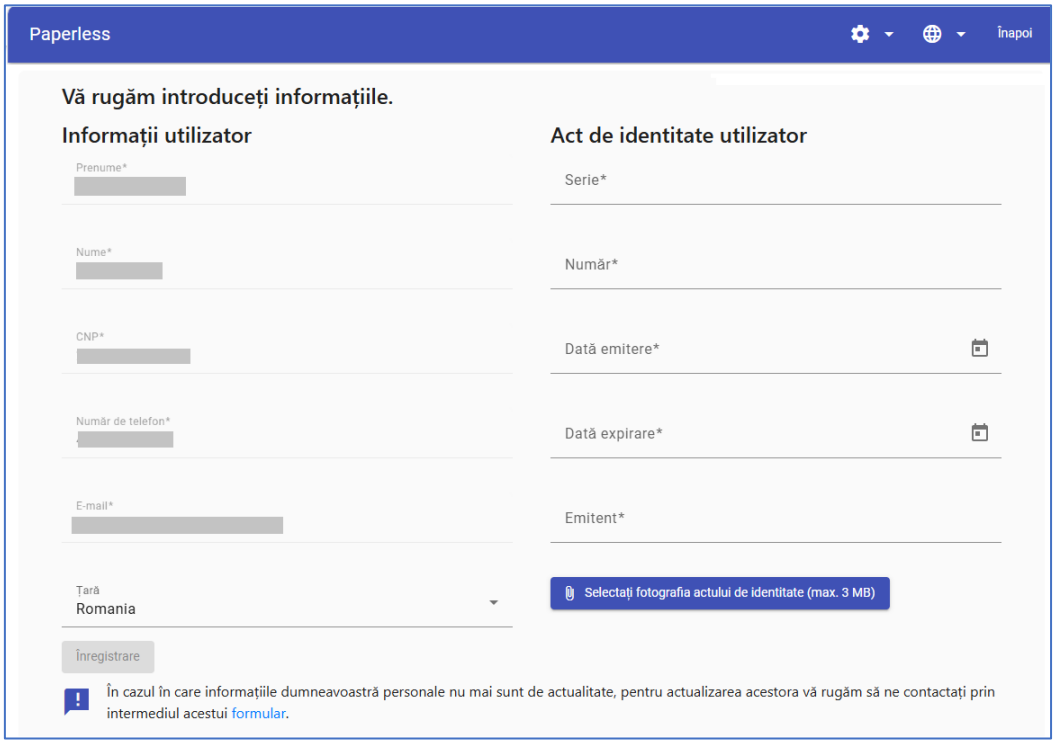
Odată ce plata a fost făcută, pe adresa de e-mail înregistrată primiți confirmarea de plată de la Netopia.

După realizarea plății, aceasta va fi confirmată în platforma websign.ro. Apăsați butonul **Continuă** pentru a trece la completarea datelor.

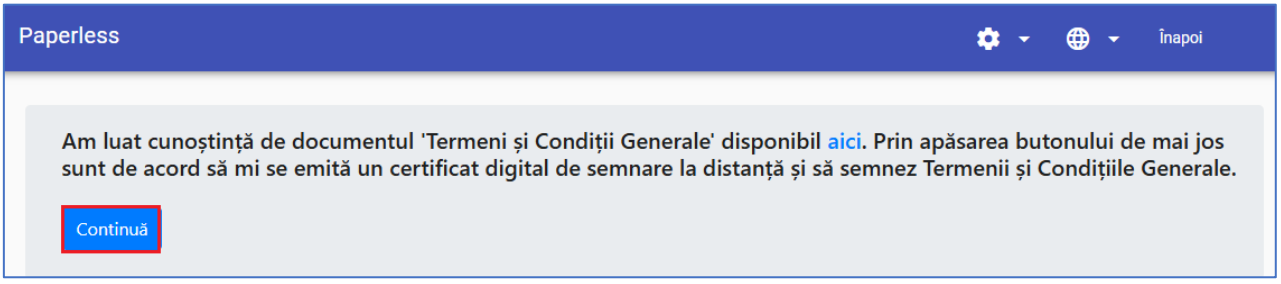


2.2. Completarea datelor și trimiterea cererii de reinnoire certificat

După validarea plății, se vor completa datele în vederea trimiterii cererii de reinnoire certificat. Datele din zona ”**Informații utilizator**” nu sunt editabile. Datele din zona ”**Act de identitate utilizator**” sunt editabile și trebuie verificate. Sunt acceptate doar acte de identitate aflate în perioada de valabilitate la data emiterii noului certificat. După verificarea / completarea câmpurilor și încărcarea copiei documentului de identitate, se activează butonul **Înregistrare**.

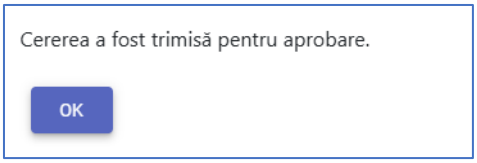


La apăsarea butonului **Înregistrare** se afișează un ecran în care se pot consulta *Termenii și Condițiile Generale* pentru semnătură la distanță. Consultați termenii și condițiile specifice procesului de emitere pentru noul certificat și, dacă sunteți de acord, apăsați butonul **Continuă** pentru a semna termenii și a se emite certificatul.



La apăsarea butonului **Continuă** se va deschide un câmp în care se va solicita un cod de autorizare generat de aplicația Authenticator pentru aplicarea semnăturii pe documentul *Termeni și condiții Generale*. După ce se va introduce codul, datele vor fi transmise către certSIGN.

După transmitere, se afișează un mesaj de confirmare că datele au fost transmise automat către certSIGN pentru validare. Utilizatorul apasă **OK**.

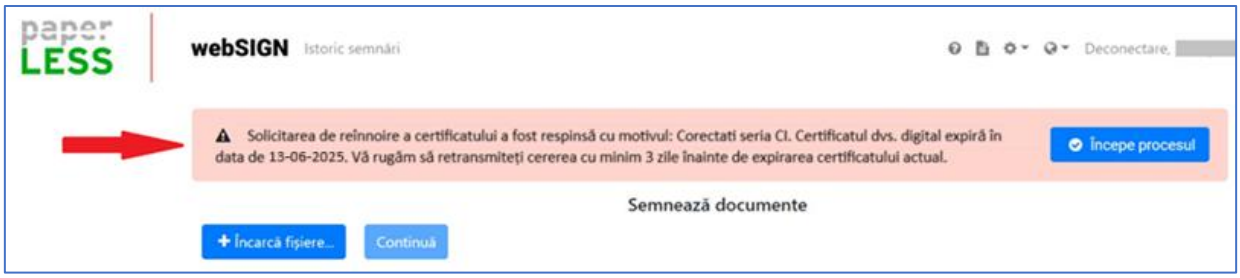


Utilizatorul este redirectat spre ecranul principal al aplicației și poate utiliza în continuare platforma online Paperless webSIGN. În ecran nu va mai fi afișată atenționarea privind actualizarea datelor atât timp cât acestea se află în proces de validare de către certSIGN.

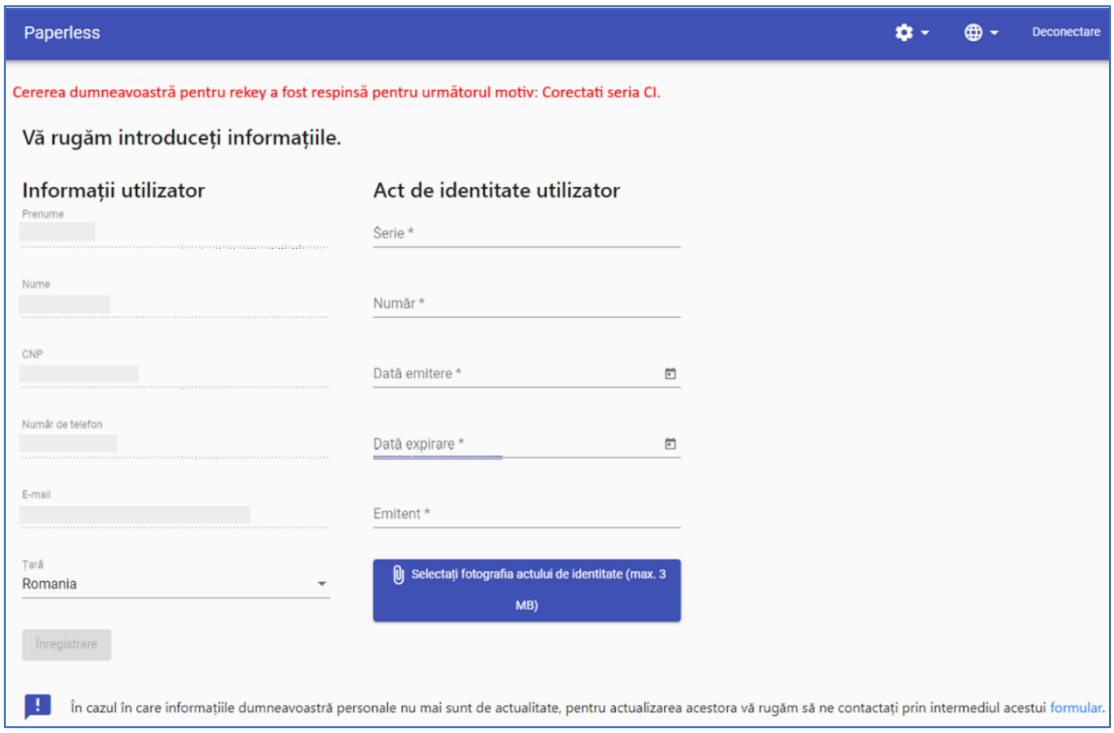
Datele completate de utilizator sunt validate de certSIGN:

● Dacă datele transmise **corespund** cu cele din actul de identitate încărcat, utilizatorul va fi notificat prin e-mail că i-a fost aprobată solicitarea de reînnoire certificat. Certificatul va fi emis automat cu 3 zile înaintea expirării certificatului actual.

● Dacă datele transmise **NU corespund** cu cele din actul de identitate încărcat, utilizatorul va fi notificat prin e-mail ca i-a fost respinsă solicitarea de reînnoire certificat, fiind precizat și motivul respingerii. Utilizatorul va trebui să reia procesul de reînnoire a certificatului înainte cu 3 zile de expirarea certificatului deținut deja. În contul său din platforma online Paperless webSIGN, după autentificare, utilizatorul va avea afișat în partea de sus a ecranului principal un banner cu un mesaj de atenționare. Utilizatorul trebuie să apese butonul **Începe procesul** pentru a relua procedura de reînnoire.

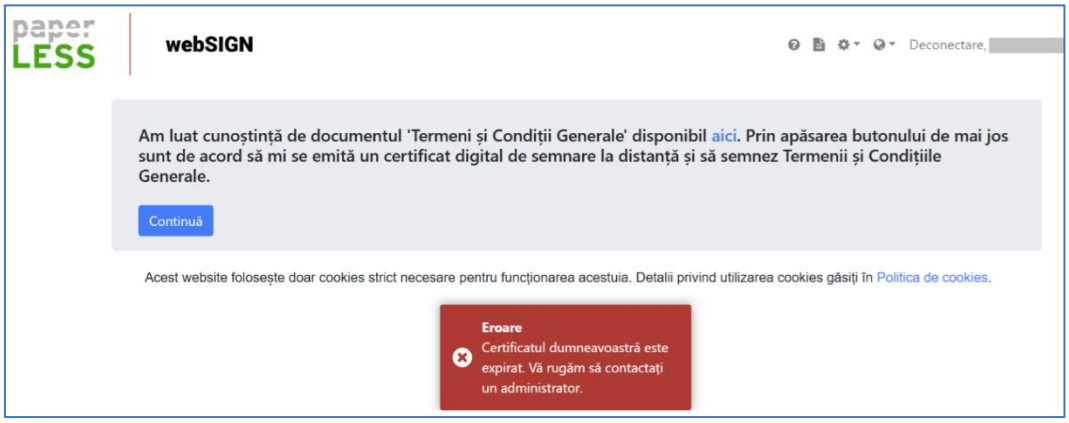


În banner, utilizatorul va putea vizualiza motivul pentru care NU i-au fost validate datele transmise anterior. În funcție de motiv, completează corect toate datele despre actul de identitate actual, apoi apasă butonul **Înregistrare**. Procesul se reia cu semnarea termenilor și condițiilor de către utilizator.



Observație:

Dacă utilizatorul a rămas logat în platformă și a expirat certificatul între timp, la încercarea de semnare se va primi mesajul de informare: *"Certificatul dumneavoastră este expirat. Vă rugăm să contactați un administrator"*. Reluați logarea și alegeți **Vreau certificat nou** (vedeți subcapitolul 3).


paper LESS
webSIGN
Deconectare,
Am luat cunoștință de documentul 'Termeni și Condiții Generale' disponibil aici. Prin apăsarea butonului de mai jos sunt de acord să mi se emită un certificat digital de semnare la distanță și să semnez Termenii și Condițiile Generale.
Continuă
Acest website folosește doar cookies strict necesare pentru funcționarea acestuia. Detalii privind utilizarea cookies găsiți în Politica de cookies.
Eroare
Certificatul dumneavoastră este expirat. Vă rugăm să contactați un administrator.

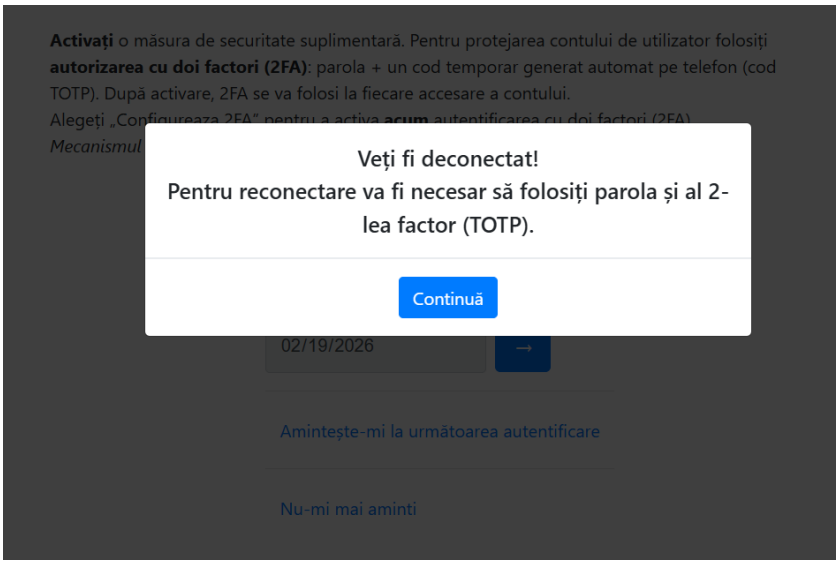
3. Reemiterea după expirare a certificatului digital calificat

Dacă certificatul dvs. a expirat, puteți solicita emiterea unui nou certificat. Pentru aceasta, accesați platforma https://websign.ro și introduceți userul și parola pentru autentificare.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA, dar doriți să o faceți acum, apăsați butonul **Configureaza 2FA**.

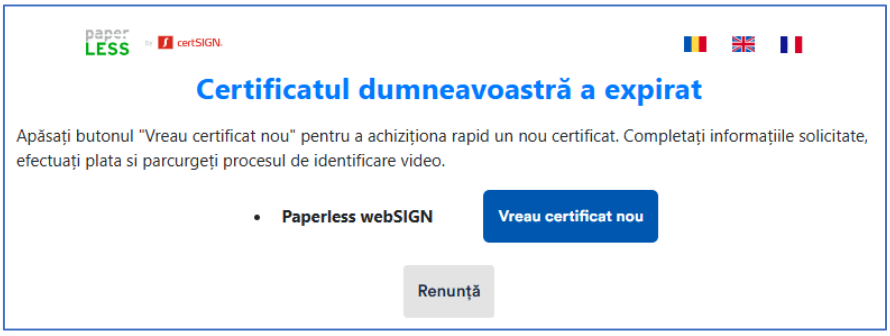
Se va afișa un pop-up cu un mesaj de informare că veți fi deconectat și că la reconectare, după introducerea userului și parolei, trebuie să introduceți un cod de autorizare din aplicația Authenticator pe care o aveți deja configurată pe telefon. Apăsați butonul **Continuă**.



După logare cu parola contului, în fereastra care apare, introduceți codul de autorizare afișat de aplicația Authenticator de pe telefon.

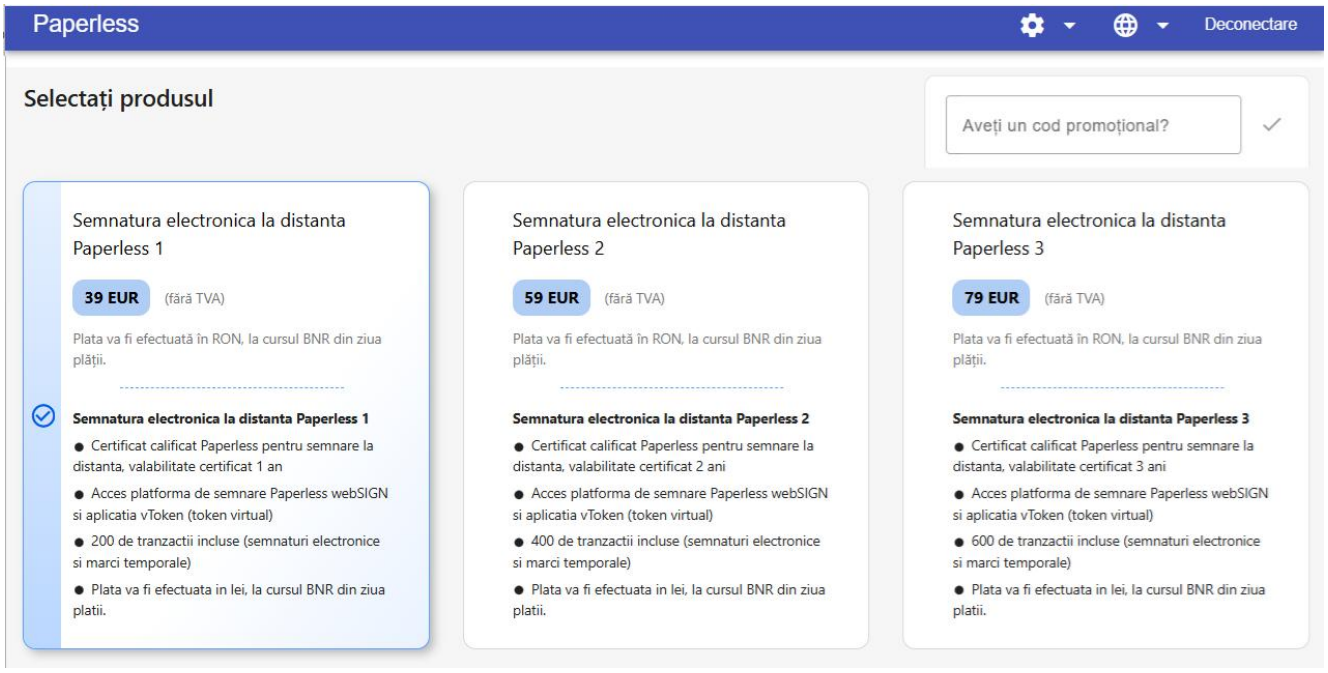
Dacă nu ați activat autentificarea 2FA și nu doriți să o faceți acum, alegeți una dintre opțiunile de amânare.

După autentificare în interfața platformei Paperless webSIGN, va apărea informarea că certificatul dvs. a expirat. Pentru emiterea unui nou certificat apăsați butonul **Vreau certificat nou**.



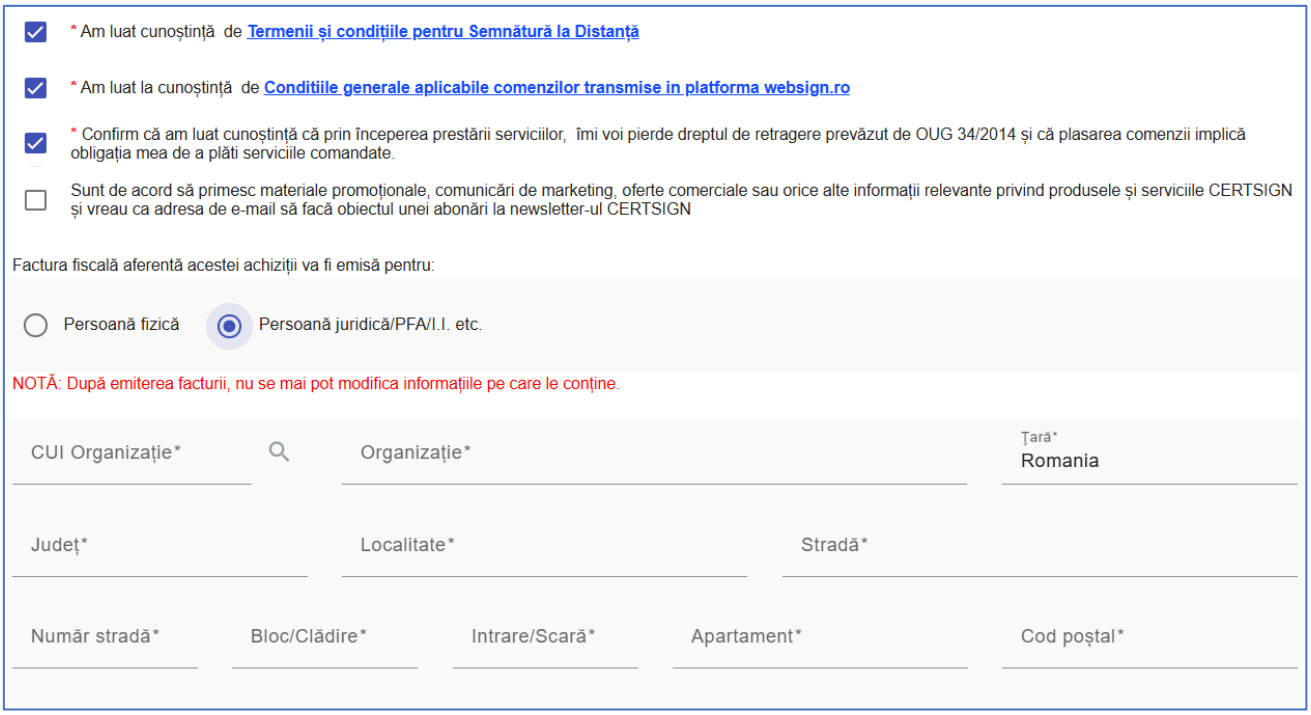
3.1. Selectarea pachetului dorit și plata online

Selectați pachetul dorit pentru noul certificat:

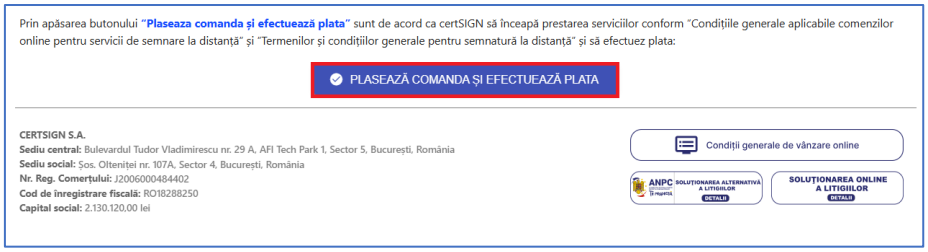


Consultați documentele **Termenii și condițiile pentru Semnătură la Distanță**, respectiv **Condițiile generale aplicabile comenzilor transmise în platforma Paperless**, apoi bifați corespunzător:

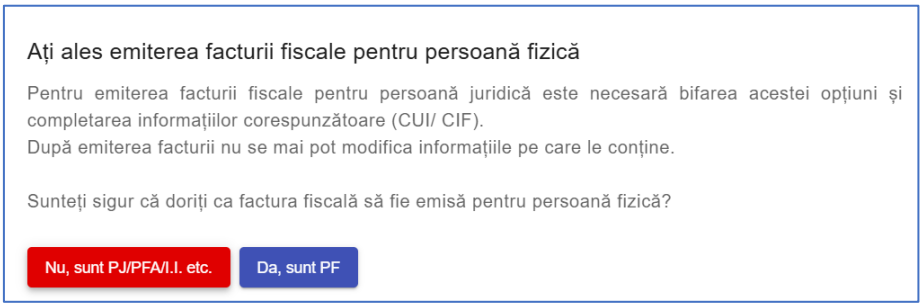
Dacă se dorește ca factura fiscală să fie emisă pe numele unei companii, se pune bifa corespunzătoare și se completează datele companiei:



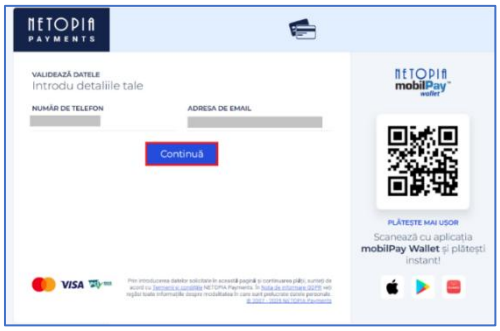
Pentru inițierea plății, se va apăsa butonul **PLASEAZĂ COMANDA ȘI EFECTUEAZĂ PLATA**:



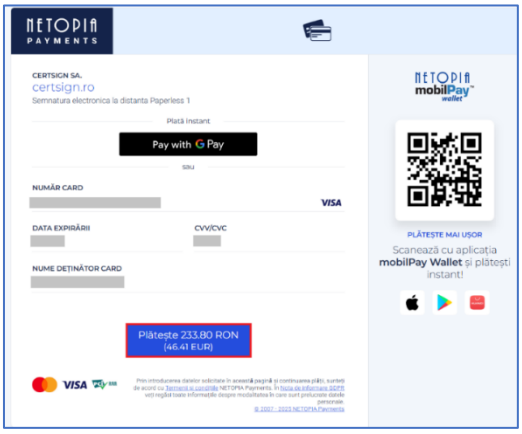
Dacă s-a bifat persoană fizică, va apărea un pop up care să vă informeze că datele din factură nu se pot modifica după emitere și să verificați dacă aveți nevoie totuși de factură pentru persoană juridică. Dacă doriți factura pentru persoană juridică, apăsați butonul **Nu, sunt PJ/PFA/I.I. etc.** și introduceți datele pentru persoană juridică. Dacă doriți factura pentru persoană fizică, apăsați butonul **Da, sunt PF**.



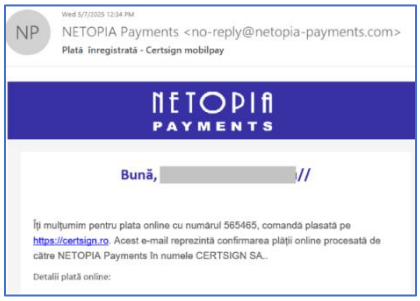
Se va deschide fereastra de plată din aplicația Netopia unde trebuie introdusă adresa de e-mail pentru validarea datelor (numărul de telefon este deja introdus). Pentru continuare se apasă butonul **Continuă**.



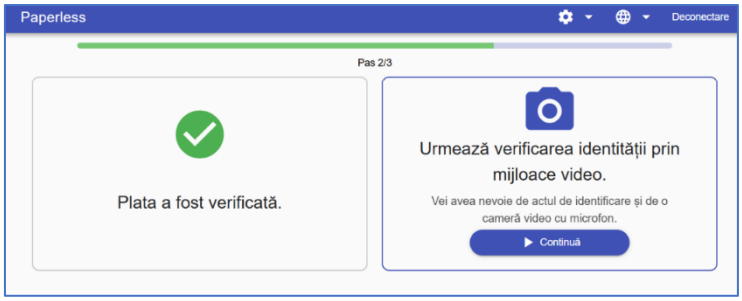
Se va plăti suma pentru produsul ales (euro + TVA) în lei la cursul BNR din ziua plății. După completarea detaliilor solicitate pentru card, se apasă butonul **Plătește** pentru a face plata.



Odată ce plata a fost făcută, pe adresa de e-mail înregistrată primiți confirmarea de plată de la Netopia.



În interfața platformei https://websign.ro, după ce plata a fost confirmată, urmează pasul de identificarea video. Aveți nevoie de actul de identitate în original, conexiune bună la internet și de acces la camera video și microfon.

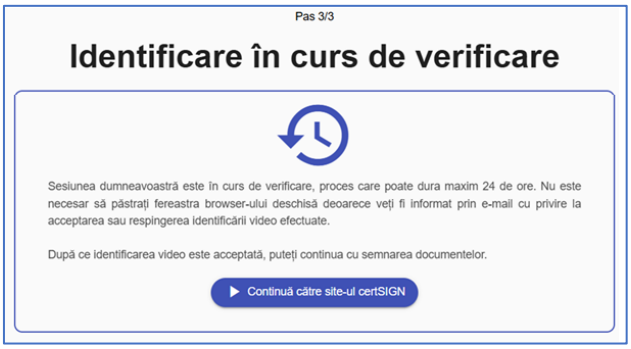


3.2. Identificarea video

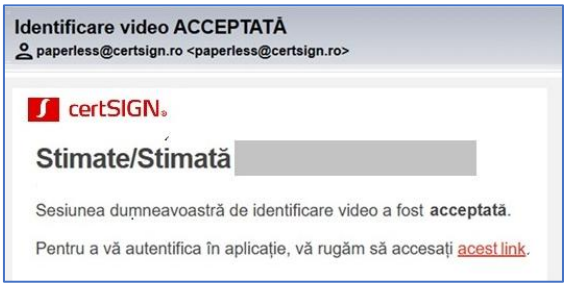
După apăsarea butonului **Continuă** (cel din imaginea de mai sus), veți fi redirecționat către platforma de identificare video unde trebuie să selectați tipul de act de identitate cu care va identificați, să bifați check box-urile din dreapta apoi apăsați butonul roșu **Apasă aici pentru a începe**.

Atenție! Dacă în procesul de identificare video nu primiți SMS sau constatați că numărul de telefon nu este corect, îl puteți schimba. Ulterior, dacă doriți, noul număr de telefon va putea fi asociat contului dvs. de cloud din platforma https://websign.ro.

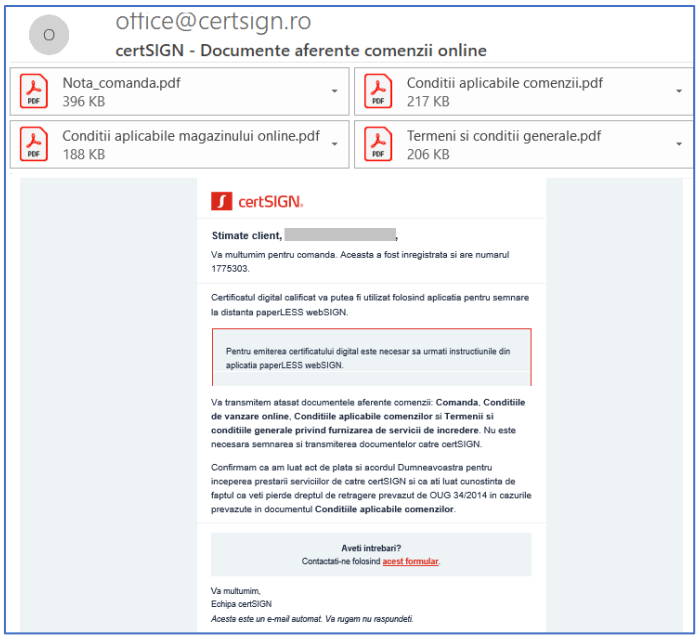
După finalizarea identificării video, platforma afișează informarea cu privire la durata maximă a procesului de verificare a identității:



După verificarea procesului de identificare video, veți primi pe e-mail notificarea cu privire la acceptarea sau respingerea procesului de identificare, precum și a motivelor de respingere, după caz.



Tot pe e-mail veți primi confirmarea acceptării de către certSIGN a comenzii dvs. împreună cu documentele aferente.



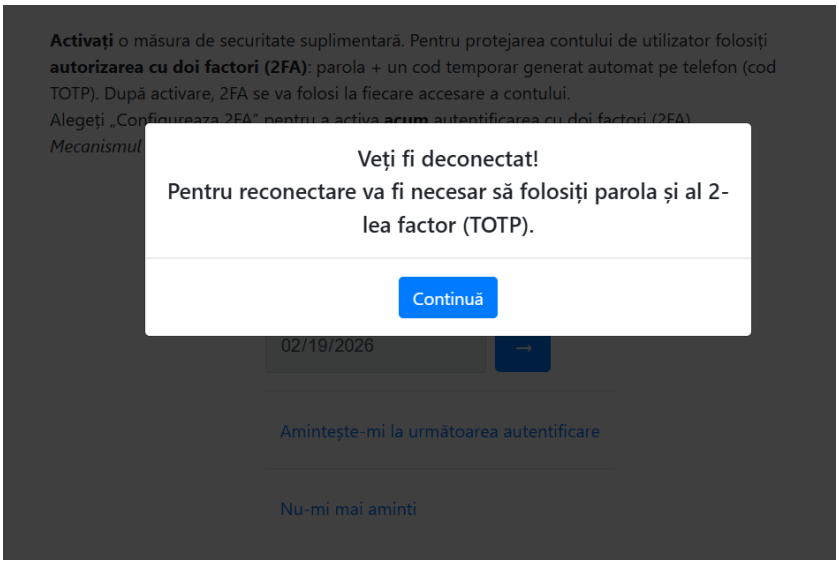
3.3. Emiterea certificatului digital

Pentru emiterea certificatului digital accesați platforma https://websign.ro cu e-mail-ul și parola pe care le folosiți. Emiterea se poate face atât de pe calculator cu Windows sau macOS, cât și de pe telefon Android sau iPhone.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA, dar doriți să o faceți acum, apăsați butonul **Configureaza 2FA**.

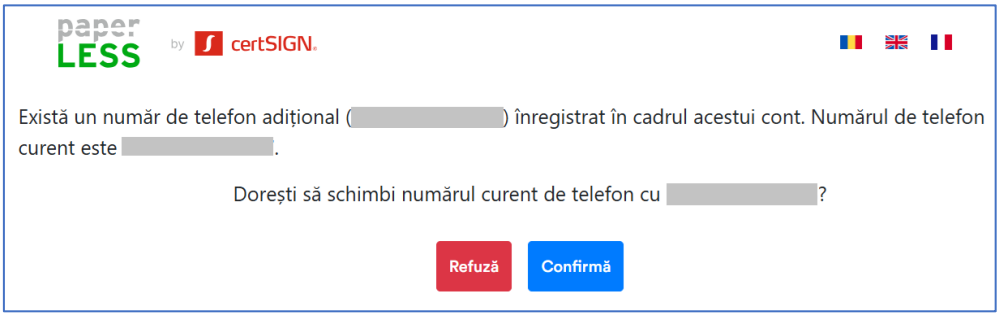
Se va afișa un pop-up cu un mesaj de informare că veți fi deconectat și că la reconectare, după introducerea userului și parolei, trebuie să introduceți un cod de autorizare din aplicația Authenticator pe care o aveți deja configurată pe telefon. Apăsați butonul **Continuă**.



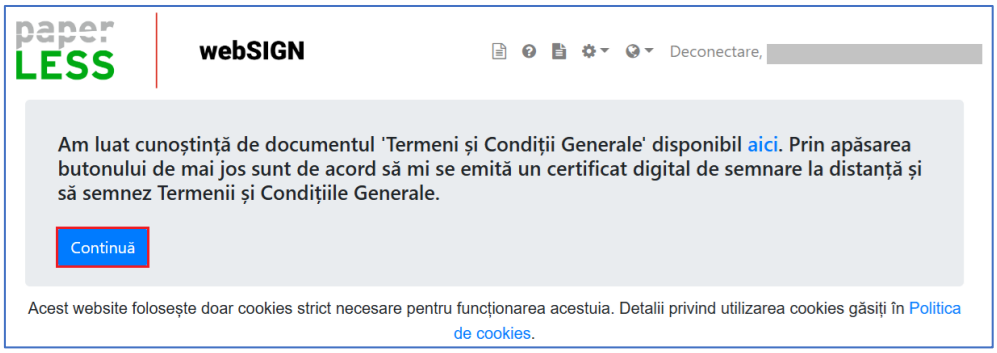
După logare cu parola contului, în fereastra care apare, introduceți codul de autorizare afișat de aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA și nu doriți să o faceți acum, alegeți una dintre opțiunile de amânare.

În cazul în care, în etapa de identificare video, ați optat pentru modificarea numărului de telefon în scopul primirii SMS-ului, aveți posibilitatea să asociați acest număr cu contul de cloud din platforma https://websign.ro. Dacă doriți să aveți asociat cu contul de cloud acest număr de telefon, apăsați butonul **Confirmă**. Dacă doriți să rămână numărul care este deja asociat, apăsați butonul **Refuză**.

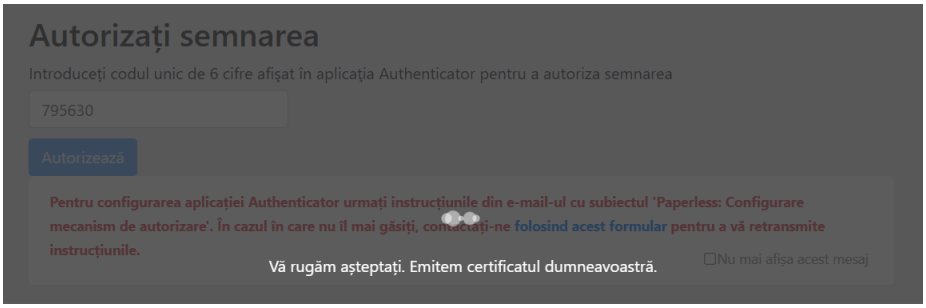


Consultați termenii și condițiile specifice procesului de emitere pentru noul certificat și, dacă sunteți de acord, apăsați butonul **Continuă** pentru a semna termenii și a se emite certificatul.

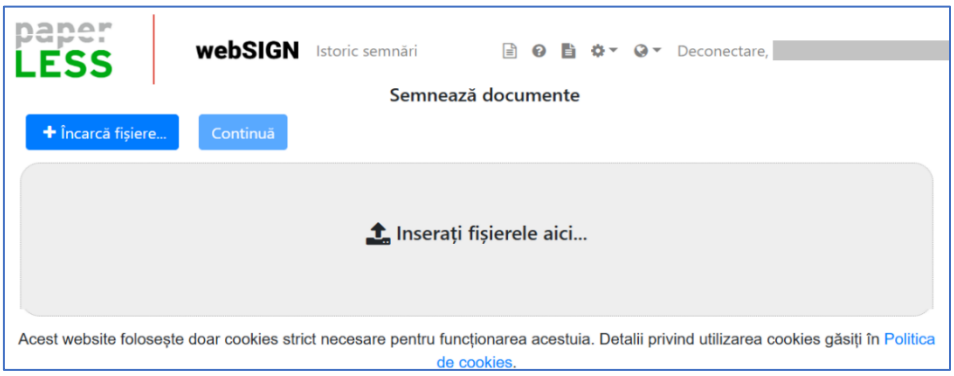


La apăsarea butonului **Continuă** se va deschide pagina de autorizare, care conține un câmp în care se solicită un cod de autorizare generat de aplicația de autorizare de pe telefon, Microsoft Authenticator sau Google Authenticator.

După ce se va introduce codul de autorizare, se va emite certificatul calificat care va fi folosit la semnare pe parcursul perioadei sale de valabilitate.



După generarea certificatului, va apărea pagina principală din platforma Paperless webSIGN unde se pot încărca documentele pentru a fi semnate.



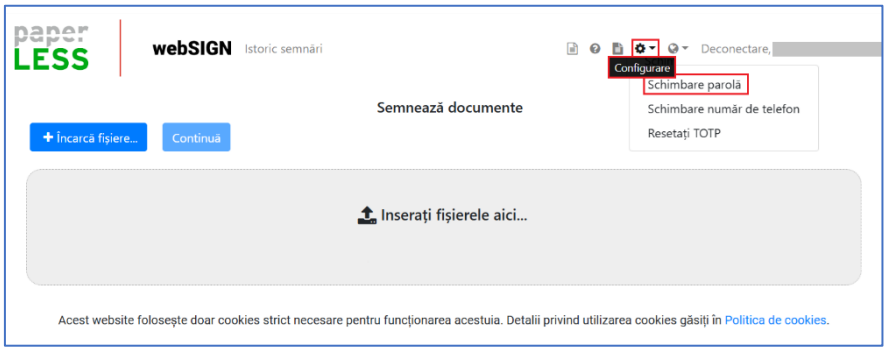
4. Schimbare parolă

4.1. Schimbare parolă cont când se cunoaște parola de logare

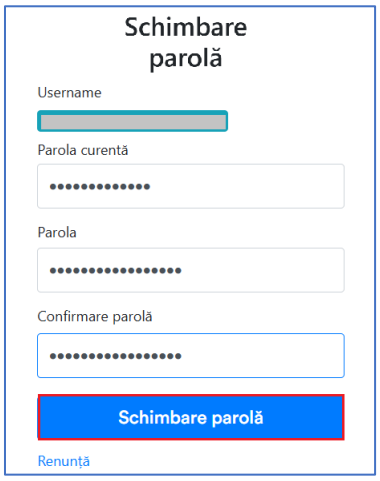
Dacă doriți să schimbați parola contului dvs. Paperless webSIGN, accesați platforma https://websign.ro cu e-mail-ul și parola cu care v-ați înrolat.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

Accesați butonul **Configurări** și selectați opțiunea **Schimbare parolă**.



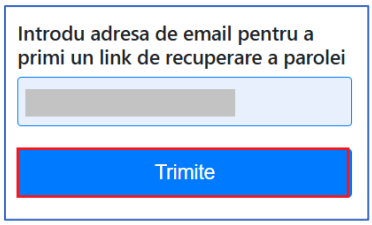
Alegeți noua parolă, apoi apăsați butonul **Schimbare parolă**.



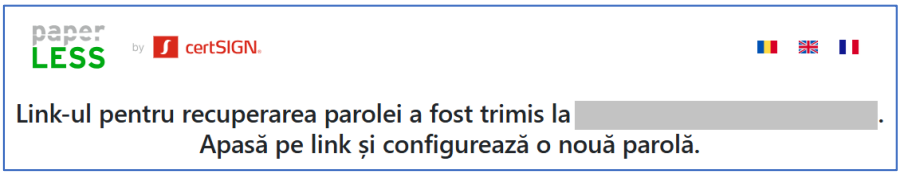
4.2. Recuperare parolă cont când nu se cunoaște parola de logare

Dacă nu mai știți parola contului dvs. Paperless webSIGN, accesați platforma https://websign.ro și apăsați butonul **Ați uitat parola?**

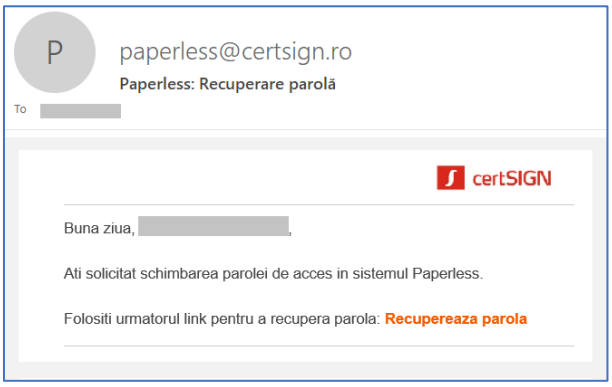
Introduceți adresa de e-mail asociată contului dvs. din platforma Paperless webSIGN și apăsați butonul **Trimite**.



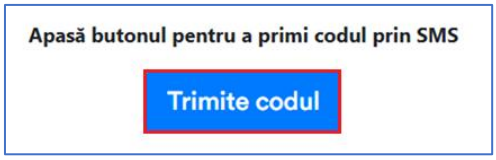
Pe adresa de e-mail asociată contului dvs. din platforma Paperless webSIGN veți primi un e-mail de recuperare parolă.



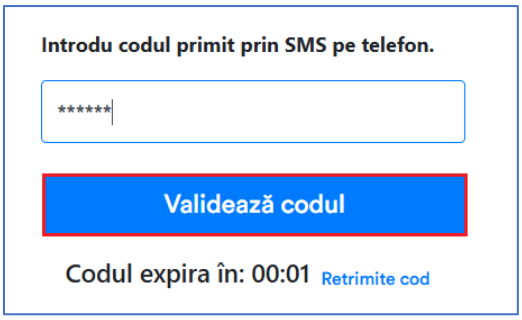
Deschideți e-mail-ul și accesați link-ul **Recupereaza parola**.



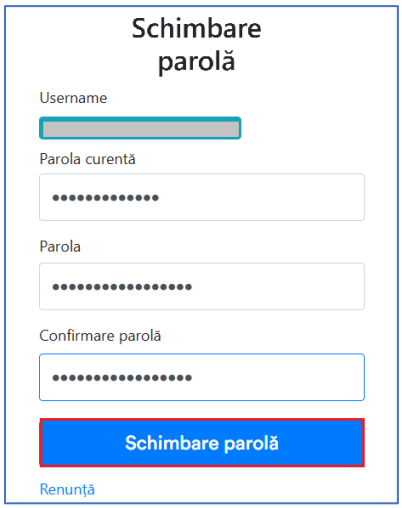
Apăsați butonul **Trimite codul** pentru a primi un cod prin SMS pe numărul de telefon asociat contului dvs. Paperless webSIGN.



Introduceți codul primit prin SMS pe telefon și apăsați butonul **Validează codul**. Dacă nu ați reușit introducerea codului în cele 10 minute alocate, aproape de terminarea celor 10 minute, se activează opțiunea de a solicita încă un cod. Apăsați butonul **Retrimite cod** pentru primirea altui cod prin SMS, dar nu înainte de 30 de minute.



Alegeți noua parolă, apoi apăsați butonul **Schimbare parolă**.

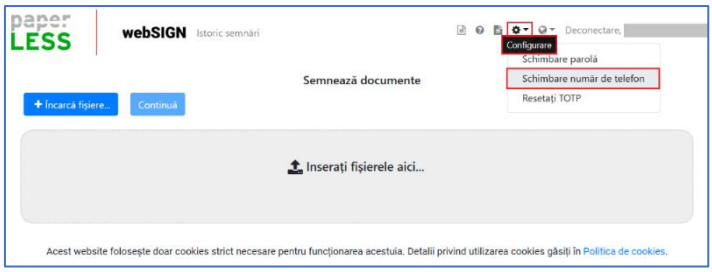


5. Schimbare număr de telefon asociat contului

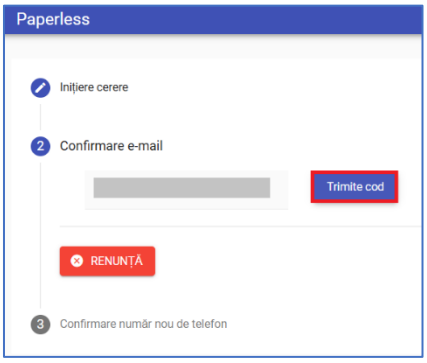
Dacă doriți să schimbați numărul de telefon asociat contului dvs. din platforma Paperless webSIGN, accesați platforma https://websign.ro cu e-mail-ul și parola cu care v-ați înrolat.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

Accesați butonul **Configurări** și selectați opțiunea **Schimbare număr de telefon**.

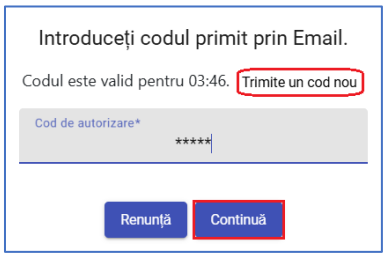


Trebuie să confirmați că aveți acces la adresa de e-mail asociată contului din platforma Paperless webSIGN. Apăsați butonul **Trimite cod** pentru a se transmite pe e-mail codul de autorizare.

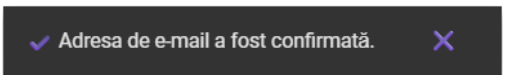


Deschideți e-mail-ul **Ați primit un cod de autorizare** și copiați codul.

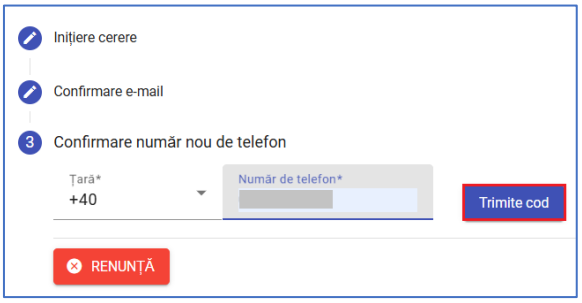
Introduceți codul de autorizare primit pe e-mail și apăsați butonul **Continuă**. Dacă nu ați reușit introducerea codului în cele 5 minute alocate, apăsați butonul **Trimite un cod nou** pentru primirea altui e-mail cu un cod de autorizare, dar nu înainte de 30 de minute.



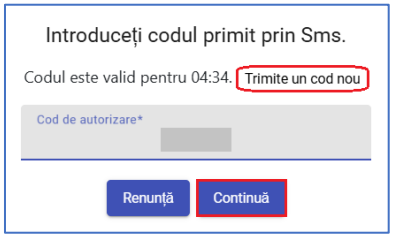
În partea de jos a platformei va apărea informarea că adresa de e-mail a fost confirmată.



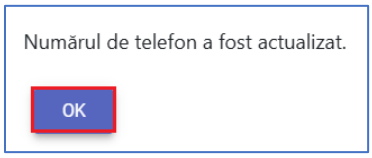
Selectați prefixul de țară și introduceți numărul de telefon pe care vreți să îl asociați cu contul dvs. Paperless webSIGN și apăsați butonul **Trimite cod**.



Introduceți codul de autorizare primit prin SMS și apăsați butonul **Continuă**. Dacă nu ați reușit introducerea codului în cele 5 minute alocate, apăsați butonul **Trimite un cod nou** pentru primirea altui SMS cu un cod de autorizare, dar nu înainte de 30 minute.



Va apărea un pop up cu informarea că numărul de telefon a fost actualizat. Apăsați butonul **OK** pentru a închide informarea.



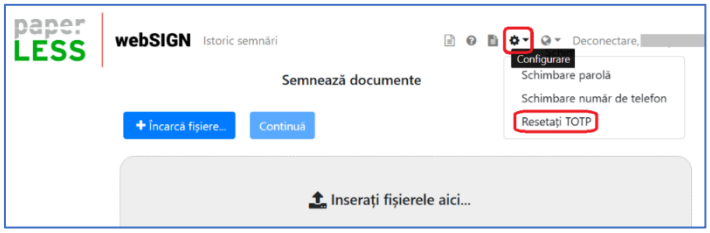
Veți fi redirectat către pagina de deschidere a platformei https://websign.ro, unde trebuie să vă logați cu e-mail-ul cu care v-ați înrolat și parola corespunzătoare.

Pe adresa de e-mail asociată contului dvs. Paperless webSIGN veți primi un e-mail de confirmare a schimbării numărului de telefon.

6. Reîmperecherea aplicației de telefon cu contul din platforma Paperless webSIGN

În cazul în care codul de autorizare nu mai este acceptat (s-a blocat împerecherea ori ați schimbat telefonul) puteți să reîmperecheați aplicația de pe telefon cu contul Paperless webSIGN solicitând resetarea chiar din platformă.

1. Deschideți platforma Paperless webSIGN în browser-ul Google Chrome. Accesați opțiunea **Configurare** și alegați opțiunea **Resetați TOTP**.

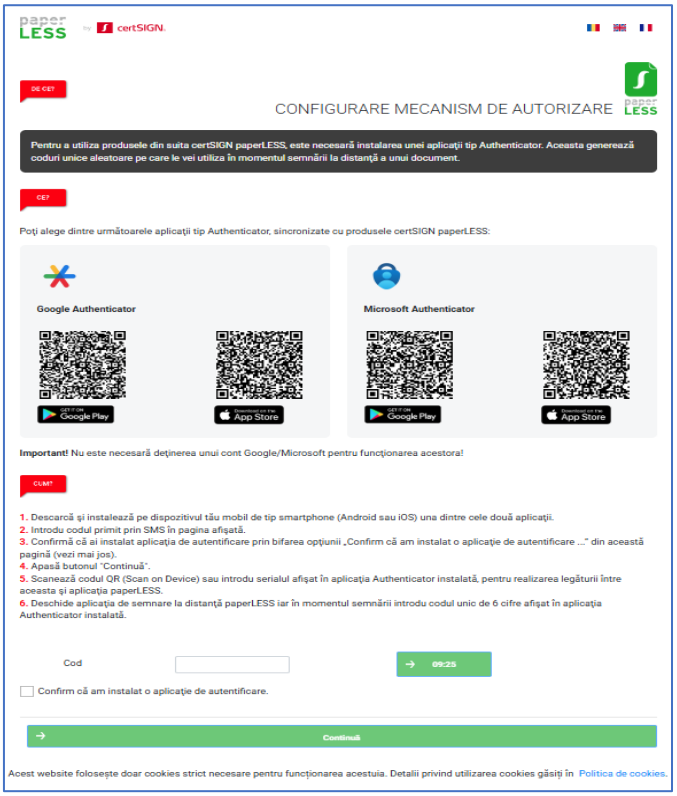


2. Apăsați butonul **Resetați mecanismul TOTP** și se va deschide pagina de împerechere.

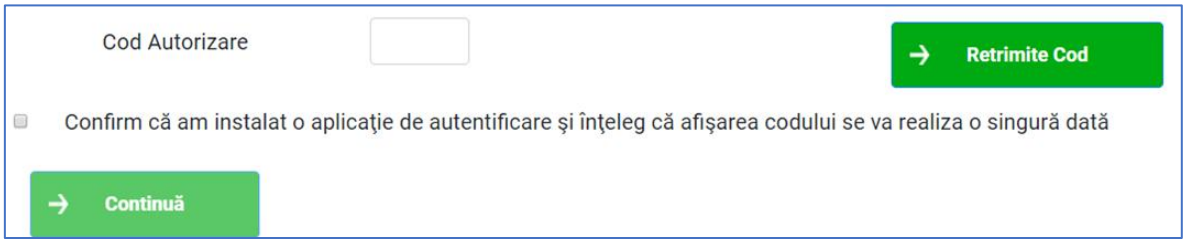
3. Derulați pagina până jos, introduceți codul primit prin SMS la solicitarea resetării mecanismului TOTP, bifați că aveți instalată aplicația de autorizare și apăsați **Continuă**.

Dacă nu aveți niciuna dintre aplicațiile de autorizare instalată pe telefon, atunci instalați una dintre versiuni.

Dacă aveți deja una instalată, ștergeți contul anterior certSIGN Paperless.



4. Dacă nu ați reușit introducerea codului în cele 10 minute alocate, la terminarea celor 10 minute, cronometrul din dreptul câmpului **Cod Autorizare** se oprește. Apăsați butonul **Retrimite cod** pentru primirea altui cod prin SMS, dar nu mai devreme de 30 minute.



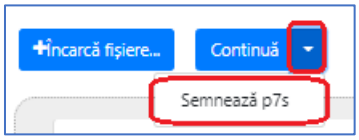
5. Scanați codul QR cu aplicația de autorizare de pe telefon, apoi introduceți în câmpul de sub codul QR unul dintre codurile de autorizare apărute pe telefon și apăsați **Trimite codul**.

Se va reîmperechea mecanismul și veți fi redirectat către platforma de semnare unde să încărcați documentele.

7. Semnarea cu certificatul digital calificat pentru semnare la distanță

7.1. Semnarea în Paperless webSIGN

Platforma Paperless webSIGN acceptă pentru semnare online, pe Windows și macOS, documente .pdf și non-.pdf needitabile, neblocate și fără parolă. Documentele în format .pdf vor avea semnatură interioară, putând fi verificate și vizualizate cu aplicația gratuită Adobe Acrobat Reader DC furnizată de Adobe. Documentele în format non-.pdf (diferit de .pdf) vor fi semnate ca .p7s, putând fi verificate și vizualizate cu aplicația clickSIGN furnizată de certSIGN. Dacă doriți să semnați cu extensia .p7s și fișiere .pdf, apăsați săgeata de lângă butonul **Continuă**.

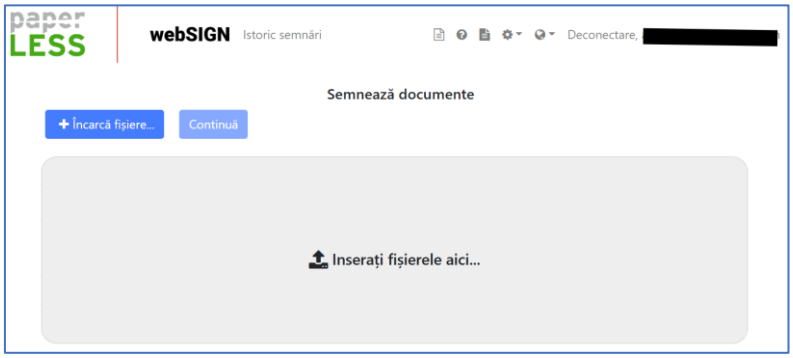


Atenție! Documentele Smart pdf (cum sunt formularele și declarațiile ANAF) NU se semnează în platforma Paperless webSIGN, putând fi semnate doar local, pe Windows sau macOS, folosind aplicația Adobe Acrobat Reader DC, după importarea locală a certificatului prin aplicația tokenului virtual, Paperless vToken.

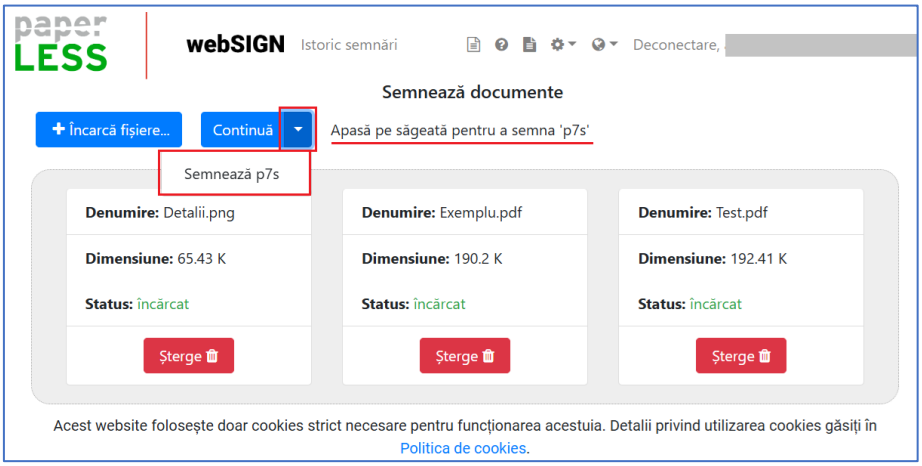
1. Pentru a semna în platforma Paperless webSIGN trebuie să fiți logat, cu user-ul și parola create anterior, în pagina web Paperless webSIGN de la adresa furnizată la achiziție:

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

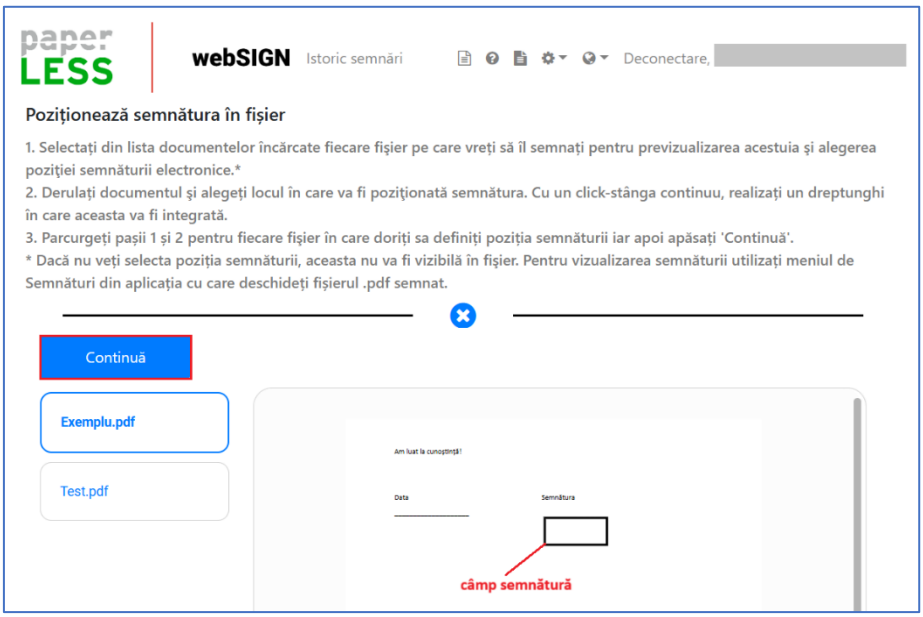
2. Apăsați butonul **Încarcă fișiere** sau trageți fișierele (drag & drop) pentru a le încărca.



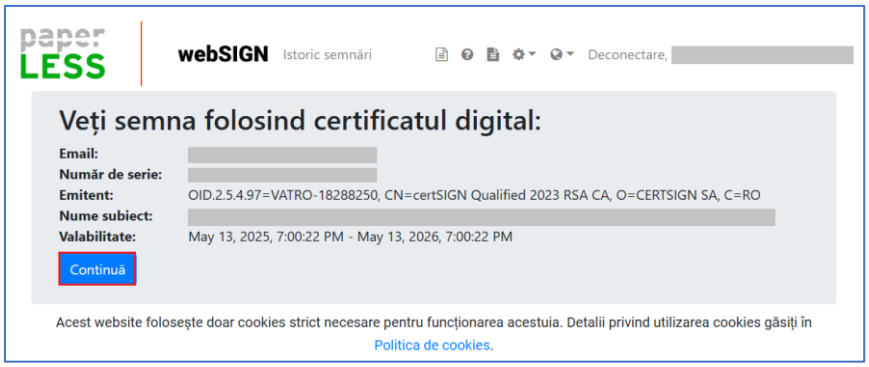
3. După încărcare, se va afișa pagina cu documentele. În cazul în care ați încărcat un document pe care nu doriți să-l semnați, apăsați butonul **Șterge**. Pentru a trece în etapa de semnare, apăsați butonul **Continuă** (pentru a păstra documentele .pdf în același format .pdf) sau pentru a semna toate documentele sub forma .p7s.



4. Pentru a crea semnătură vizibilă pe documentele .pdf, selectați fiecare document în parte, trasați câte un chenar în locul în care doriți să apară semnătura și apăsați butonul **Continuă**. Dacă doriți semnătură invizibilă, apăsați **Continuă** fără a seta acest chenar.

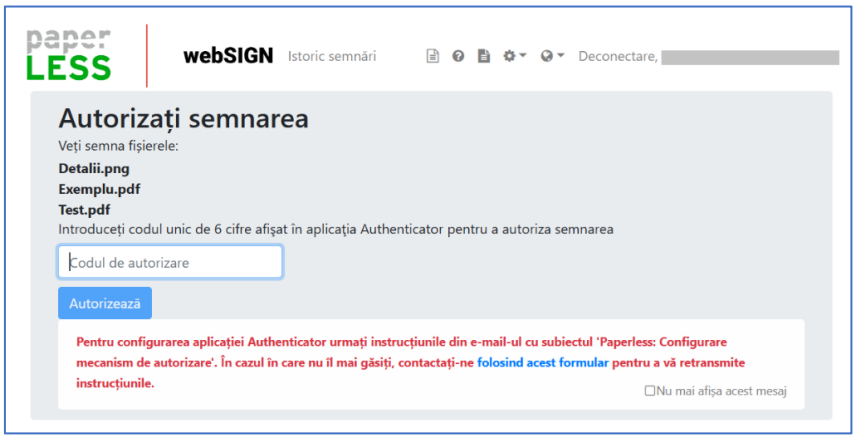


5. După încărcarea documentelor vor apărea detaliile certificatului digital care se va folosi la semnare. Apăsați butonul **Continuă** pentru a continua semnarea cu certificatul prezentat.

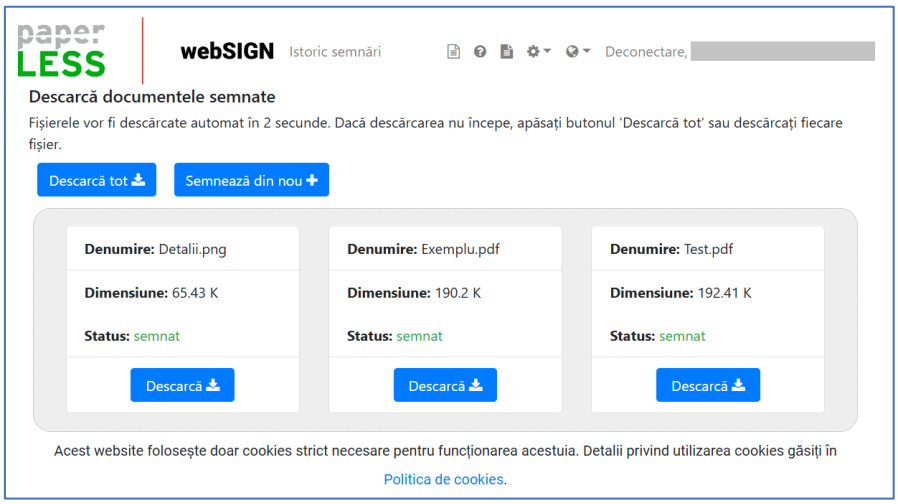


6. Pentru autorizarea semnării documentelor trebuie să introduceți codul afișat de extensia de autorizare din browser. Un cod este valabil 30 secunde de la apariția sa. După introducere, apăsați butonul **Autorizează**.

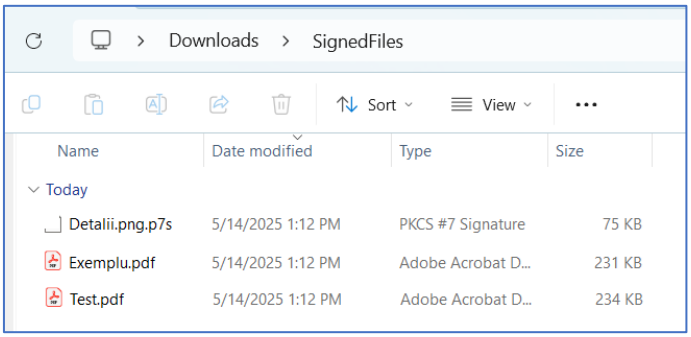
Observație: Dacă nu ați configurat aplicația de autorizare, consultați informațiile din capitoul 1 din acest document. În cazul în care aveți aceste configurări făcute, puteți bifa check box-ul **Nu mai afișa acest mesaj** ca la următoarea semnare să nu mai apară mesajul respectiv.



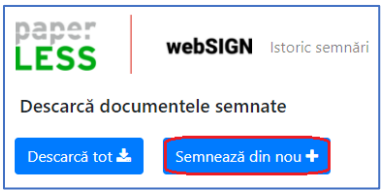
7. După semnarea documentelor se va afișa pagina de descărcare, iar arhiva zip cu acestea se va descărca automat cu denumirea **SignedFiles.zip** în folderul destinat descărcărilor (Downloads, de regulă). Puteți descărca și individual documentele prin apăsarea butonului **Descarcă** de sub fiecare document.



8. După semnare, documentele .pdf își vor păstra extensia și vor fi semnate în interior, iar cele cu altă extensie (non-.pdf) vor fi semnate cu semnătură .p7s.



9. Dacă doriți să continuați semnarea altor documente, accesați **Semnează din nou**.



7.2. Semnarea pe stația locală

După emiterea certificatului digital în platforma Paperless webSIGN, puteți să semnați local diverse tipuri de documente: .pdf (folosind Adobe Reader), respectiv .doc, .docx, .xls, .xlsx (folosind clickSIGN), atât pe Windows, cât și pe macOS, utilizând acest certificat digital și aplicația tokenului virtual, **Paperless vToken**. Aplicația este compatibilă cu sistemele de operare Windows de la 10 în sus și macOS de la Catalina în sus.

Pentru instalarea aplicației Paperless vToken parcurgeți pașii de mai jos:

1. Descărcați aplicația Paperless vToken de pe unul dintre link-urile următoare, în funcție de sistemul de operare deținut:

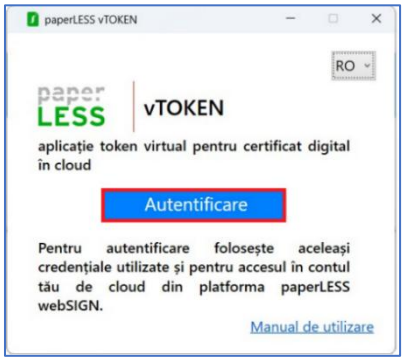
https://www.certsign.ro/vToken/vToken-Launcher.exe – pentru Windows

https://apps.apple.com/ro/app/paperless-vtoken/id6667100978?mt=12 – pentru macOS

Pentru Windows, după descărcare, trebuie să instalați aplicația.

Pentru macOS, aplicația se descărca și își face update-urile doar din App Store.

2. Deschideți aplicația Paperless vToken de la shortcut-ul creat pe Desktop la instalare, apoi apăsați butonul **Autentificare**.



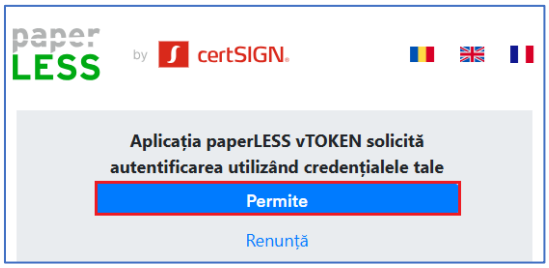
3. În pagina de browser care se deschide introduceți e-mail-ul asociat contului dvs. Paperless webSIGN și apăsați butonul **Continuă**.

4. Introduceți parola cu care accesați contul Paperless webSIGN și apăsați butonul **Continuă**.

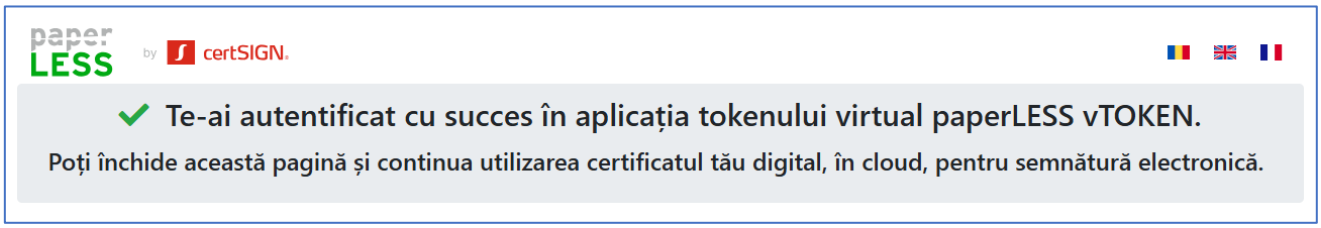
În cazul în care adresa de e-mail pe care ați scris-o nu este cea corectă, apăsați butonul **Renunță** și reluați pasul de introducere a adresei de e-mail cu adresa corectă.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

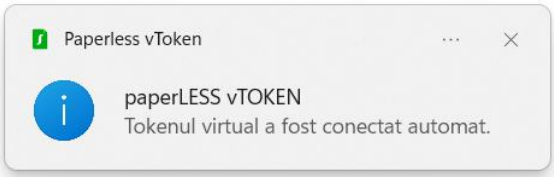
5. Aplicația va solicita să-i acordați permisiunea să facă autentificarea cu credențialele introduse anterior. Apăsați butonul **Permite** pentru a continua accesul.



6. Se va deschide o pagină care vă informează că v-ați autentificat cu succes în aplicația tokenului virtual Paperless vToken.



7. Aplicația se va deschide și în secțiunea Sistem Tray. La deschidere, certificatul digital calificat pentru semnare la distanță va fi importat automat în store-ul de certificate al sistemului de operare și va putea fi folosit la semnare documente .pdf, .doc, .docx, .xls, .xlsx.



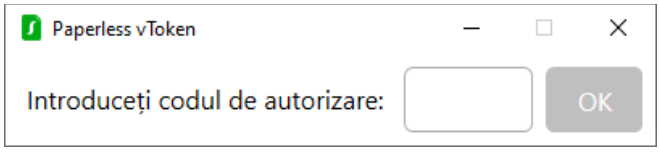
8. Pentru semnarea documentelor .pdf, .doc, .docx, .xls, .xlsx se folosesc tool-urile de semnare integrate în aplicațiile destinate acestor tipuri de fișiere, respectiv:

– Adobe Reader pentru documente .pdf;

– Word pentru documente .doc, .docx;

– Excel pentru documente .xls, .xlsx.

Pentru autorizarea semnării trebuie să introduceți codul de autorizare din aplicația de autorizare configurată anterior.



8. Autentificarea cu certificatul digital calificat pentru semnare la distanță pe platformele online

După emiterea certificatului digital în platforma Paperless webSIGN, puteți să accesați diverse platforme web care necesită autentificare cu certificat digital, atât pe Windows, cât și pe macOS, utilizând acest certificat digital și aplicația tokenului virtual, **Paperless vToken**. Aplicația este compatibilă cu sistemele de operare Windows de la 10 în sus și macOS de la Catalina în sus.

Pentru instalarea aplicației Paperless vToken parcurgeți pașii de mai jos:

1. Descărcați aplicația Paperless vToken de pe unul dintre link-urile următoare, în funcție de sistemul de operare deținut:

https://www.certsign.ro/vToken/vToken-Launcher.exe – pentru Windows

https://apps.apple.com/ro/app/paperless-vtoken/id6667100978?mt=12 – pentru macOS

Pentru Windows, după descărcare, trebuie să instalați aplicația.

Pentru macOS, aplicația se descărca și își face update-urile doar din App Store.

2. Deschideți aplicația Paperless vToken de la shortcut-ul creat pe Desktop la instalare, apoi apăsați butonul **Autentificare**.

3. În pagina de browser care se deschide introduceți e-mail-ul asociat contului dvs. Paperless webSIGN și apăsați butonul **Continuă**.

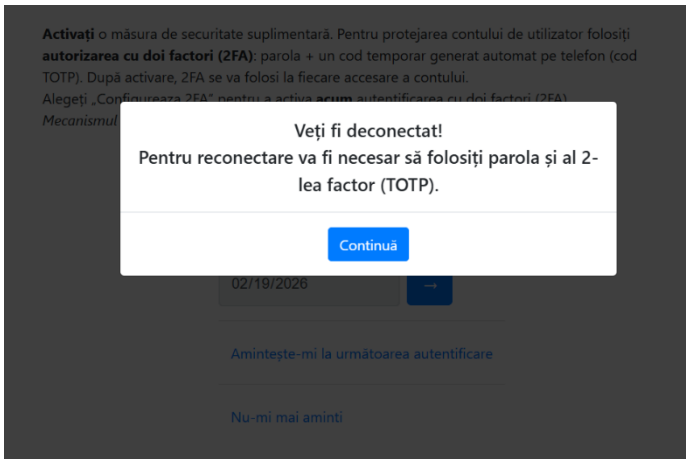
4. Introduceți parola cu care accesați contul Paperless webSIGN și apăsați butonul **Continuă**.

În cazul în care adresa de e-mail pe care ați scris-o nu este cea corectă, apăsați butonul **Renunță** și reluați pasul de introducere a adresei de e-mail cu adresa corectă.

Dacă ați activat autentificarea 2FA, atunci va apărea și fereastra suplimentară de solicitare cod de autorizare din aplicația Authenticator de pe telefon.

Dacă nu ați activat autentificarea 2FA, dar doriți să o faceți acum, apăsați butonul **Configureaza 2FA**.

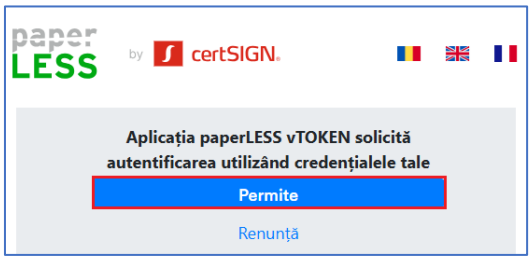
Se va afișa un pop-up cu un mesaj de informare că veți fi deconectat și că la reconectare, după introducerea userului și parolei, trebuie să introduceți un cod de autorizare din aplicația Authenticator pe care o aveți deja configurată pe telefon. Apăsați butonul **Continuă**.



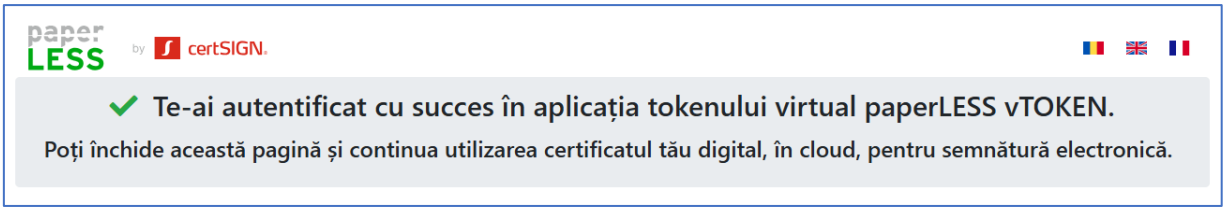
În fereasta care apare, introduceți codul de autorizare afișat de aplicația Authenticator de pe telefon

Dacă nu ați activat autentificarea 2FA și nu doriți să o faceți acum, alegeți una dintre opțiunile de amânare.

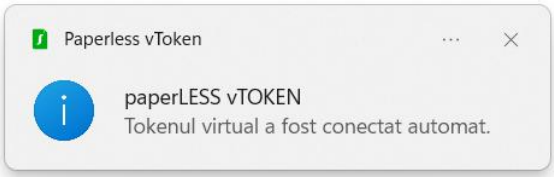
5. Aplicația va solicita să-i acordați permisiunea să facă autentificarea cu credențialele introduse anterior. Apăsați butonul **Permite** pentru a continua accesul.



6. Se va deschide o pagină care vă informează că v-ați autentificat cu succes în aplicația tokenului virtual Paperless vToken.



7. Aplicația se va deschide și în secțiunea Sistem Tray. La deschidere, certificatul digital calificat pentru semnare la distanță va fi importat automat în store-ul de certificate al sistemului de operare și va putea fi folosit la autentificare pe diverse platforme web care necesită certificat digital calificat.



8. Pentru autentificare, deschideți platforma web dorită, selectați certificatul digital calificat care apare la prezentare, apoi introduceți codul de autorizare (din aplicația de autorizare configurată pe telefon) ca să autorizați autentificarea.