Paperless webSIGN

Web platform for remote electronic signing

Table of Contents

The Paperless webSIGN signing platform - websign.ro offers the possibility to purchase:

- a **qualified digital certificate for remote signing,**
- **rekey of the qualified digital certificate for remote signing** (i.e. to request the issuance of a new digital certificate for remote signing based on the existing valid qualified digital certificate)
- **reissue of the qualified digital certificate for remote signing.**

The packages available to certSIGN customers are as follows:

Paperless 1 – Qualified electronic signature with qualified certificate valid for 1 year

- Qualified digital certificate –1 year validity
- Access to the Paperless webSIGN signing platform
- 200 transactions (electronic signatures and timestamps)

Paperless 2 – Qualified electronic signature with qualified certificate valid for 2 years

- Qualified digital certificate - valid for 2 years
- Access to the Paperless webSIGN signing platform
- 400 transactions (electronic signatures and timestamps)

Paperless 3 – Qualified electronic signature with qualified certificate valid for 3 years

- Qualified digital certificate – valid for 3 years
- Access to the Paperless webSIGN signing platform
- 600 transactions (electronic signatures and timestamps)

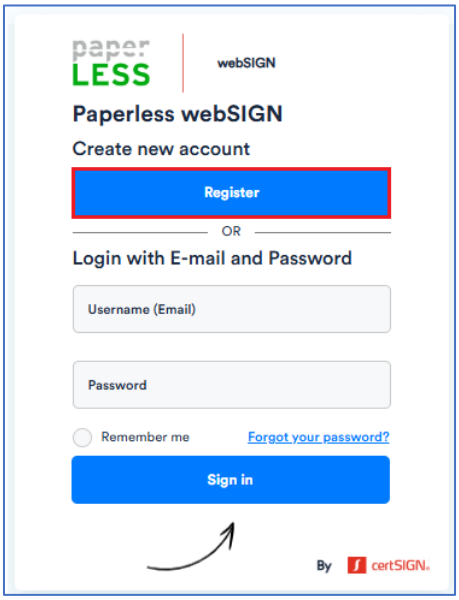
1. Qualified digital certificate for remote signing

To purchase a new certificate, the user (new customer or customer who wants another account) must follow the steps below:

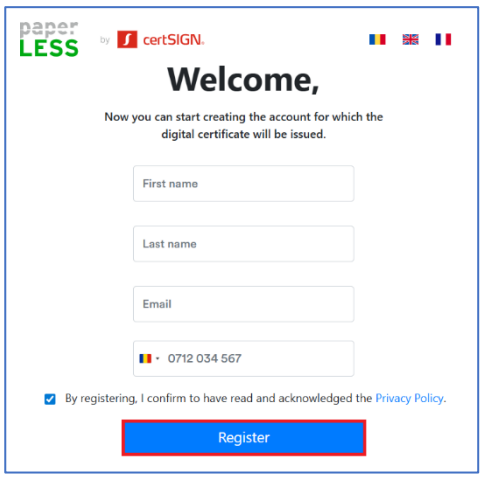
- Enrol user;
- Create an account by setting a username and password;
- Select the package you want, enter your data and pay online;
- Video identification of the future account holder and remote qualified digital certificate;
- Set up the authorisation solution;
- Issuing the remote qualified digital certificate.

1.1. Enrol user

To enrol the user and issue a qualified digital certificate for remote signing, go to the platform https://websign.ro. Press the **Register** button.



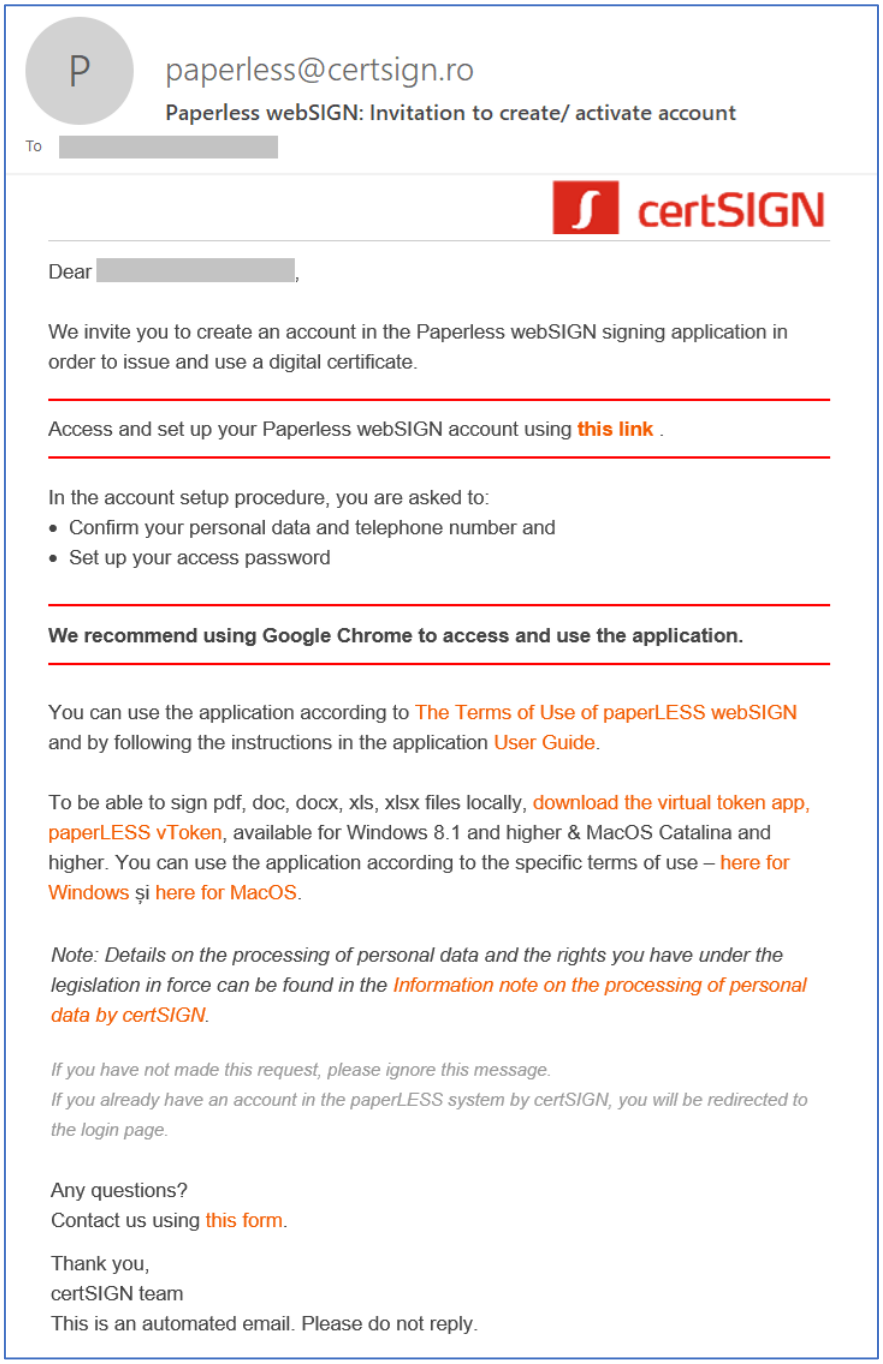
Fill in the requested data (name, surname, e-mail, phone), tick that you agree to the privacy policy data processing and press the **Register** button.



The invitation to create an account in the Paperless webSIGN signing platform will be sent to the e-mail address you provided.

1.2. Create / activate your Paperless webSIGN account

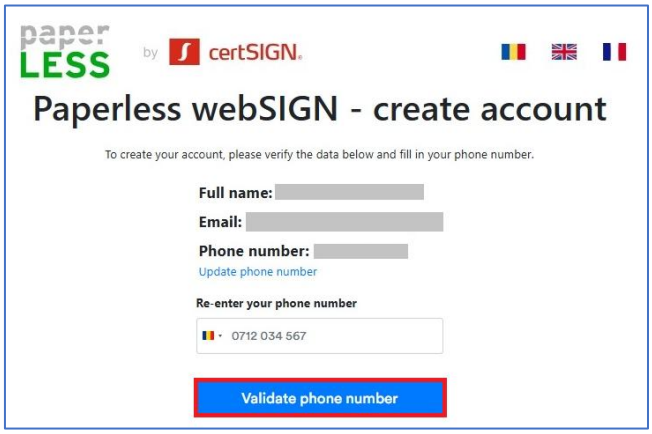
Open the **Paperless webSIGN: Invitation to create/activate account** received via e-mail. To set up your Paperless account, follow **this link** in the email. We recommend using the Google Chrome browser.



The page displayed contains the data you previously filled in. Select the country and enter your phone number again, then press **Validate phone number**. On this number you will receive a SMS form a short number with the label certSIGN.

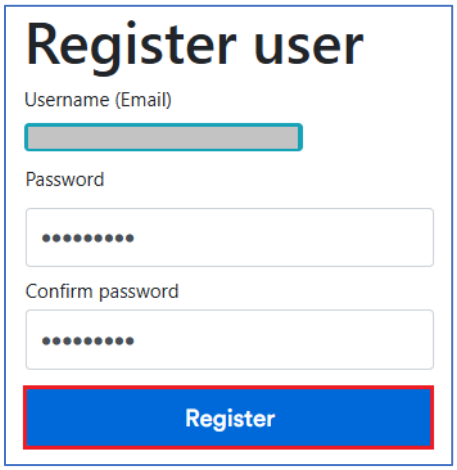
Attention! Please check that you have permission to receive SMS from short numbers.

If you want to change the phone number associated with your account, select **Change phone number** and follow the steps from there.

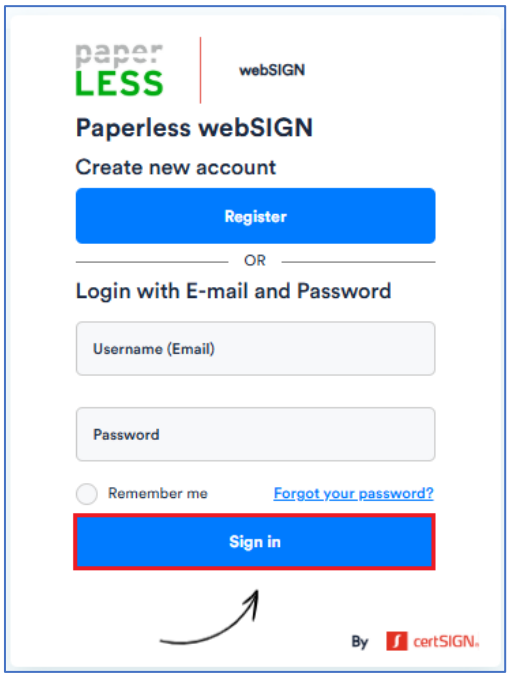


Enter the SMS code in the time displayed on the screen. If you fail to enter the code in time (a code is valid for 10 minutes), the **Resend code** button will appear, so you can request another SMS code for validation, but not before 30 minutes.

Set a complex password for the account you have created, then press the **Register** button.



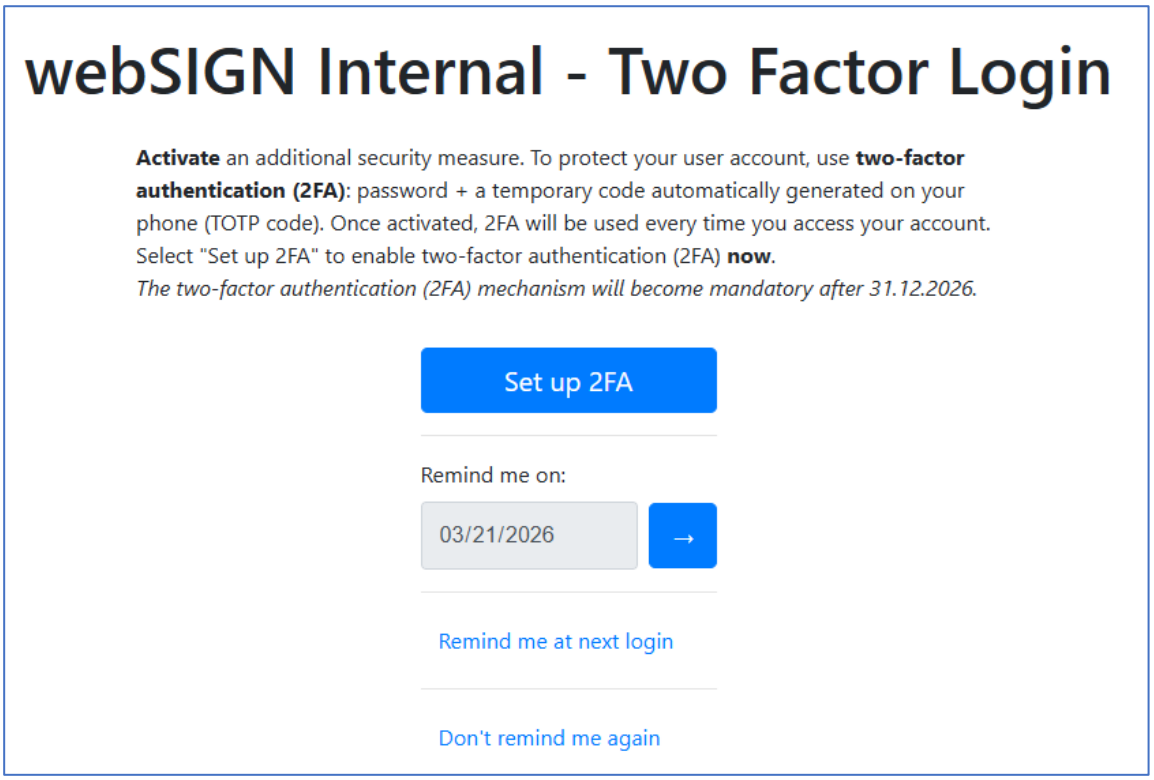
The account login page is displayed. Enter your username (e-mail) and password, then press **Sign in**.



On the next page, you will see a message informing you that you need to set up two-factor authentication (2FA). Two-factor authentication (2FA) adds an extra layer of protection when logging into your account because, in addition to your password, you are also required to enter a code generated on your mobile phone by one of the recommended authorization apps: Google Authenticator or Microsoft Authenticator, which you must pair with your cloud account.

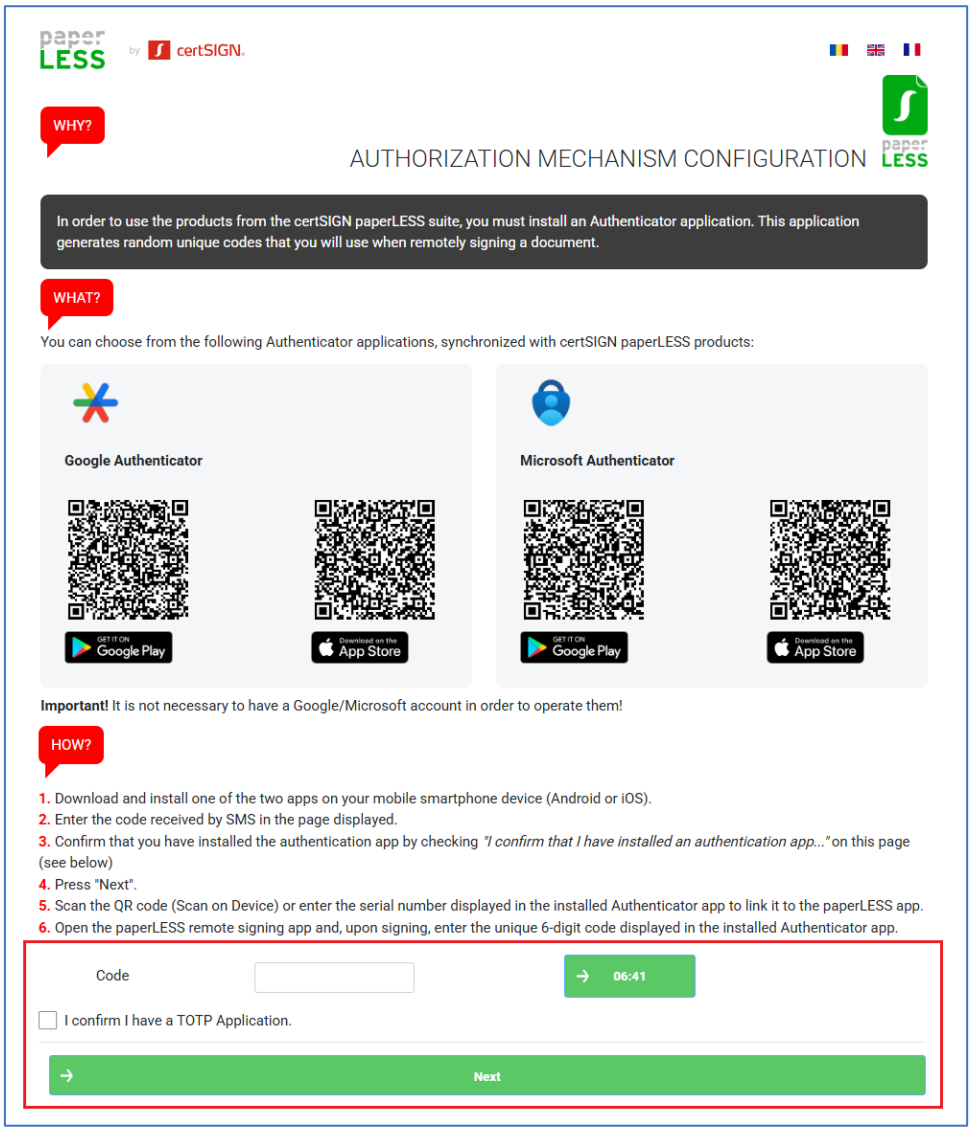
If you want to set it up, press the **Continue** button and follow the instructions displayed. Once set up, you will log in to your account using two-factor authentication (2FA): your account password and the code generated by the authorization app on your phone.

If you do not want to set it up, choose one of the reminder options: on a date of your choice, at the next login, or never. Whichever option you choose, 2FA must be set up by December 31, 2026, at the latest, when it becomes mandatory.

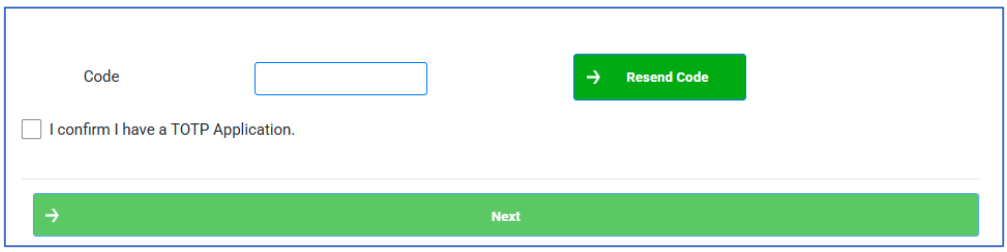


- **Setting up your account for 2FA authentication**

1. After clicking the **Continue** button, an information page will open, and an authorization code will be sent via SMS to the phone number used for registration in order to continue the procedure. Install one of the Google Authenticator or Microsoft Authenticator authorization apps on your phone, as described in the information in the **WHAT**? section. Scroll down to the bottom of the web page and, in the **Authorization Code** field in the **HOW**? section, enter the authorization code you received via text message when you accessed the link within 10 minutes.



2. If you did not manage to enter the code within the allotted 10 minutes allocated, at the end of the 10 minutes, the timer next to the **Authorization Code** field will stop. Press the **Resend Code** button to receive another code via SMS, but not before 30 minutes.

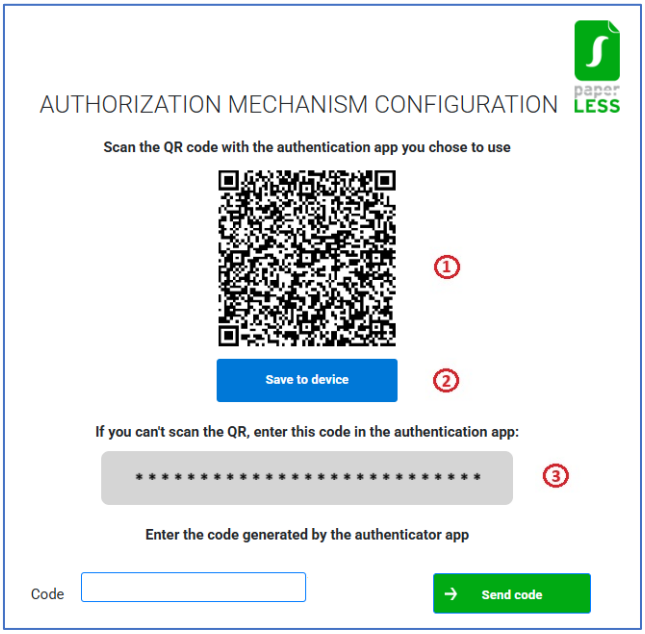


3. To complete the authorization setup, check the box to confirm the installation of the Authenticator app and click **Continue** (steps 3-4 in the **HOW**? section). The page with the QR code will be displayed.

4. To pair the authorization solution on your phone with your Paperless webSIGN account on the Paperless webSIGN signing platform, you must copy or scan the QR code displayed (step 5 in the HOW? section), depending on the device you used to follow the configuration steps:

– if you have the QR code displayed on a device (computer, laptop, tablet, or other phone) other than the one on which you installed the authorization app, open the Authenticator app installed on your phone and scan the QR code as in ①;

– if you have the QR code displayed on the phone on which you installed the authorization app, press the **Save to device** button ② and the QR code will be saved.

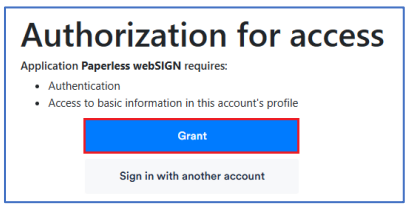


5. After scanning/saving the QR code, the Authenticator app on your phone will generate 6-digit authorization codes that are valid for 30 seconds. To complete the setup, enter a code generated by the authorization app and press **Send Code**. The access authorization window will then appear.

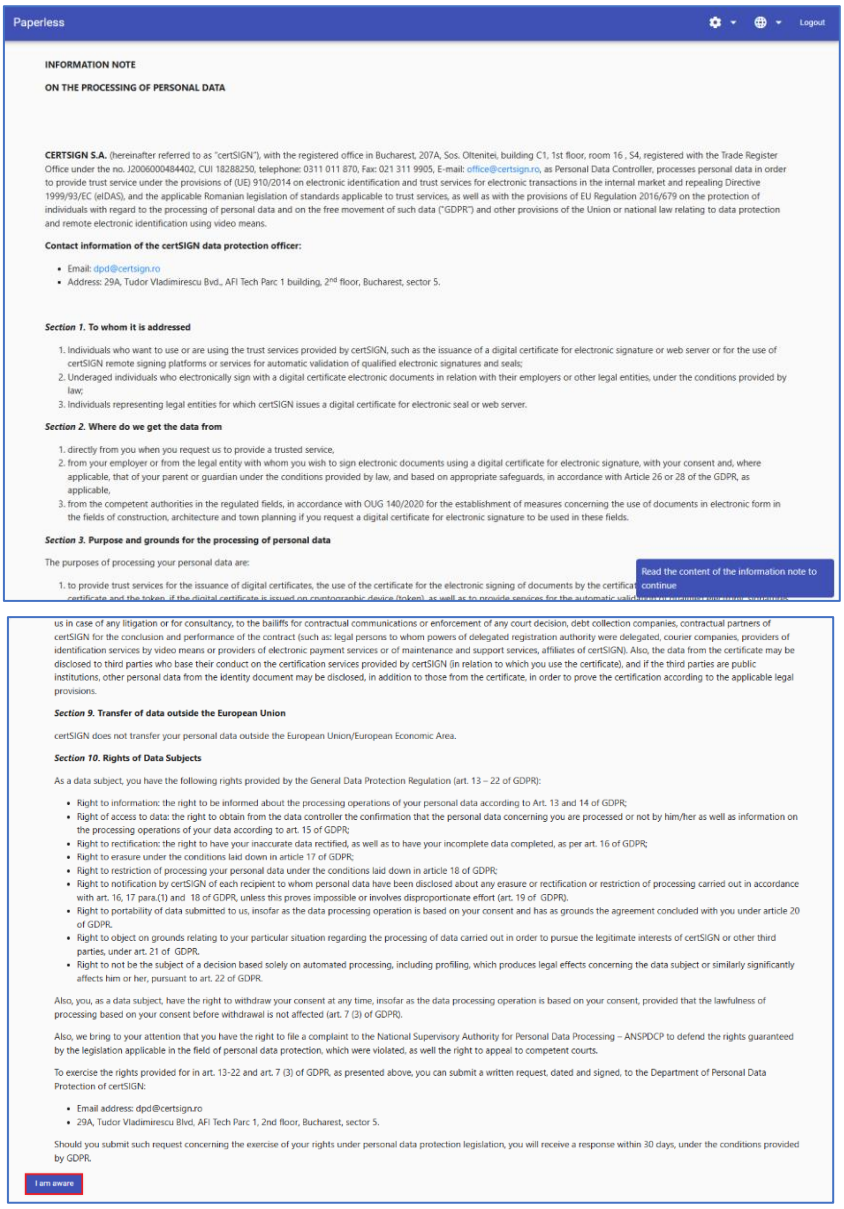
• Setting up your account for authentication without 2FA

After selecting any of the options to postpone setting up two-factor authentication, the access authorization window will appear.

Regardless of the type of authentication you have chosen, with or without 2FA, the application will ask for your consent to access protected resources, as shown in the image below. This screen will only be displayed on your first login. Press the **Grant** button to be able to use the Paperless webSIGN application.

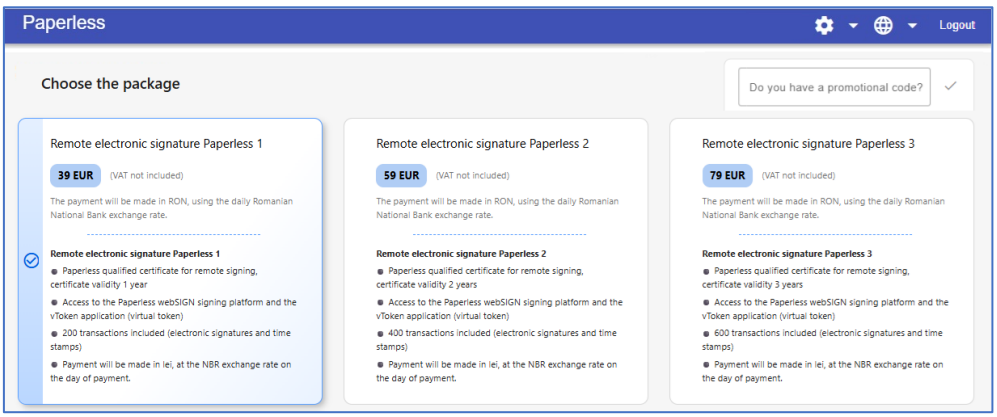


Read the GDPR Information Note on the processing of your data. Press the **I am aware** button to move on.

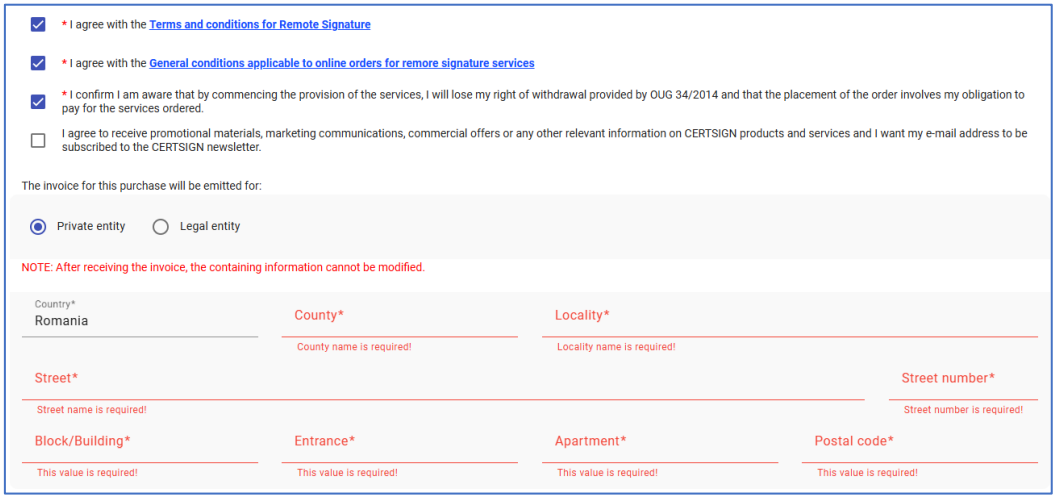


1.3. Select the package, enter your data and pay online

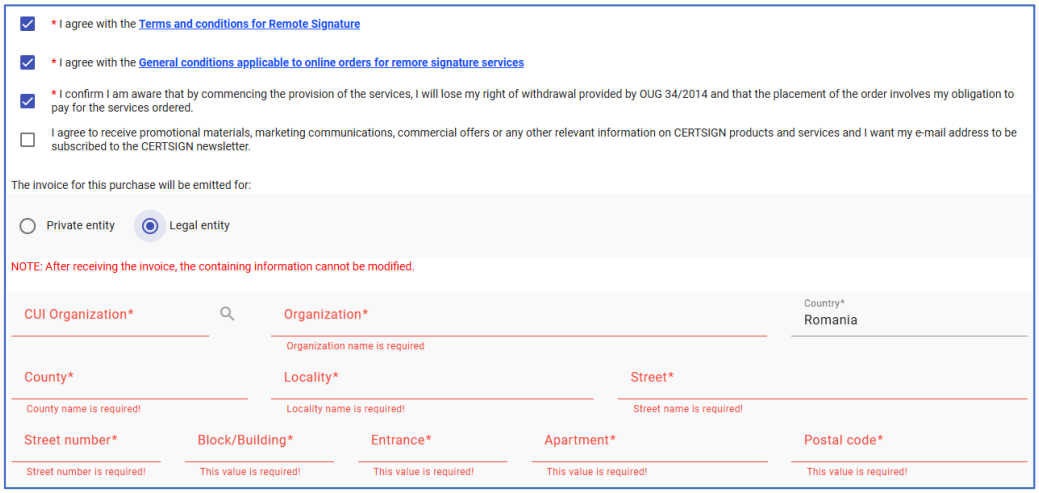
Select the desired package for the new certificate:



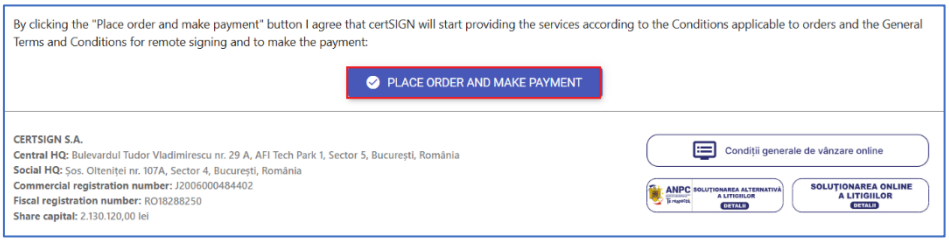
Read the **Terms and conditions for remote signing**, respectively the **General Terms and Conditions applicable to orders submitted on the Paperless platform**, then tick as appropriate:



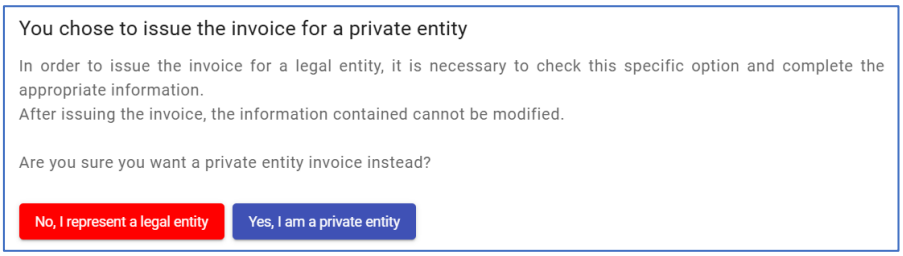
If you want the invoice to be issued in the name of a company, check the appropriate box and fill in the company details:



To start the payment, press the **PLACE ORDER AND MAKE PAYMENT**:

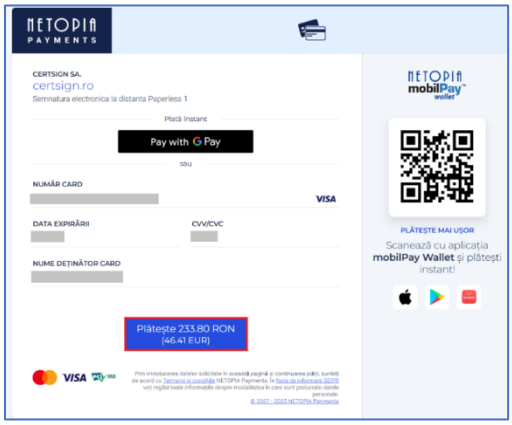


If you selected the private entity for the invoice, a pop up will appear informing you that the data on the invoice cannot be changed after issue and asking you to check if you still need the invoice for the legal entity. If you want the invoice for a legal entity, click the **No, I am private entity/Legal entity/Certified private entity/Individual enterprise.** etc. button and enter the data for the legal entity. If you want the invoice for a private entity, press the **Yes, I am a private entity** button.



You are redirected to the payment window in the Netopia application where you need to enter your e-mail address to validate your data (phone number is already entered). To continue press the **Next/Continua** button.

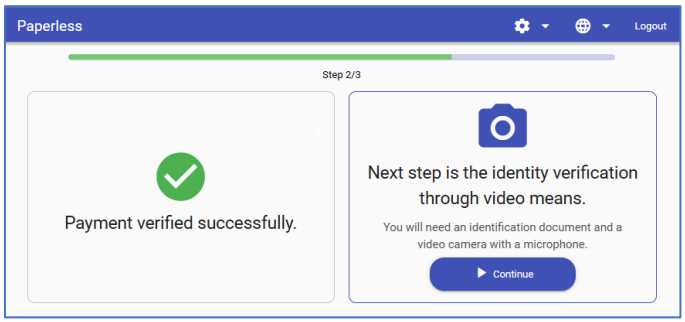
The amount for the selected package (euro + VAT) will be paid in lei at the NBR exchange rate on the day of payment. After filling in the required card details, press the **Pay** button to make the payment.



Once the payment has been made, you will receive a payment confirmation from Netopia on your registered e-mail address.

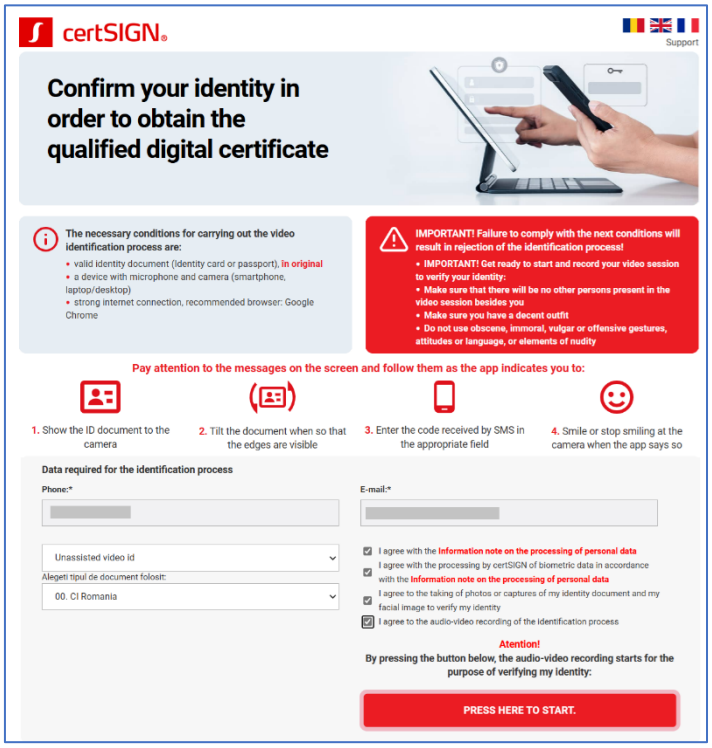
c

Once the payment has been confirmed, follow the video identification step on https://websign.ro platform. You need your ID card in original, a good internet connection and access to a video camera with microphone.



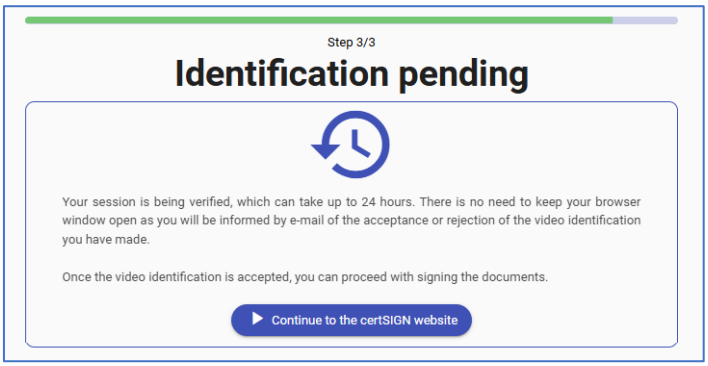
1.4. Video identification of the future account holder and of the remote qualified digital certificate

After pressing the **Continue** button (see the previous print screen), you will be redirected to the video identification platform where you need to select the type of ID you are identifying yourself with, tick the check boxes and press the red **Press here to start** button.

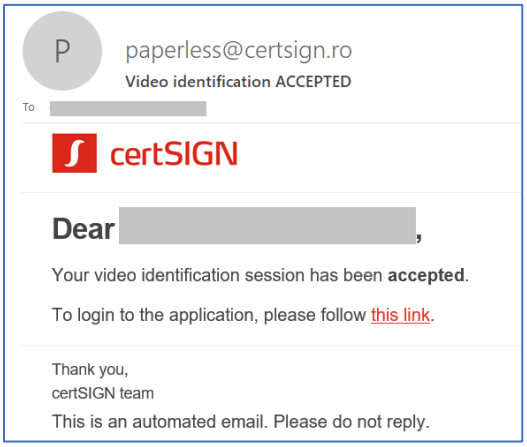


Please note! If you do not receive an SMS during the video identification process or find that the phone number is incorrect, you can change it. Subsequently, if you wish, the new phone number can be linked to your cloud account on the https://websign.ro platform.

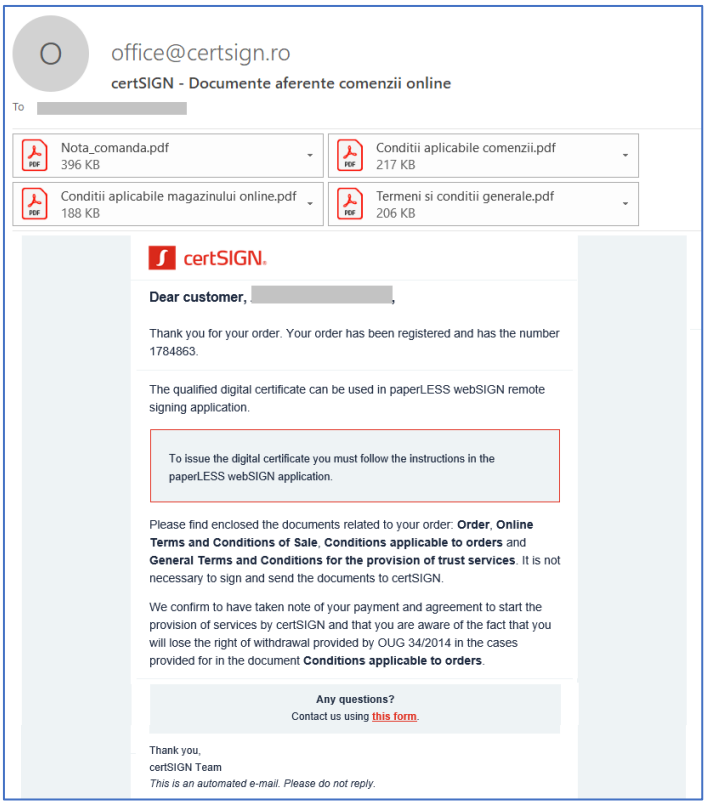
Once the video identification is completed, the platform displays information on the maximum duration of the identity verification process:



Once your video identification has been verified, you will receive an e-mail notification of acceptance or rejection and the reasons for rejection, if applicable.



By e-mail you will receive confirmation that certSIGN has accepted your order together with the related documents.



1.5. Setting up the Paperless webSIGN authorisation solution for authentication without 2FA

If you have opted for 2FA authentication, proceed to step 1.6, as the authorization mechanism has already been configured when you created your account.

If you have opted for authentication without 2FA (to do it later), you will receive an invitation to set up the authorization mechanism by email. Follow the setup steps in the Google Chrome browser.

To set up the authorization for signing using the Paperless webSIGN service, you must follow these two steps:

- install the authorisation solution on your phone;

– Pair the authorisation solution with your Paperless webSIGN account.

1.5.1. Install the authorisation solution on your phone

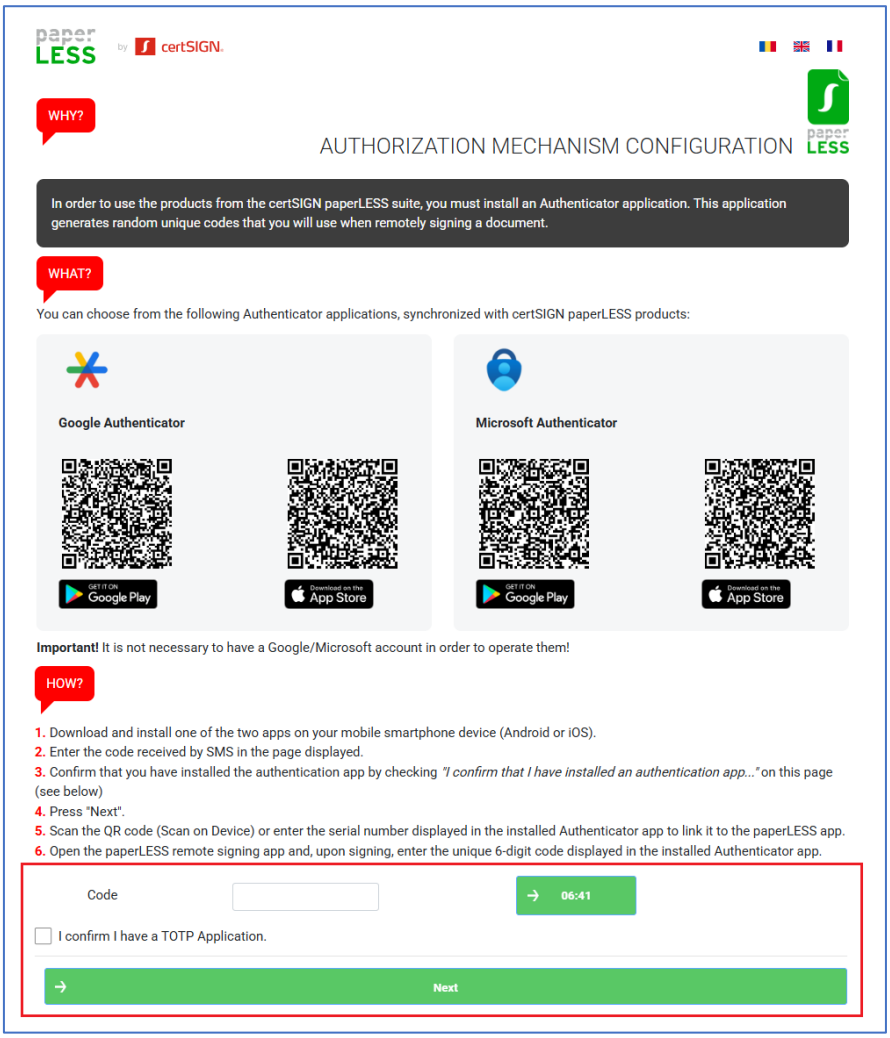
You can use one of the **Google Authenticator** or **Microsoft Authenticator** applications for authorisation from your phone. Both can be downloaded from your phone's app store. The app is compatible with Android and iPhone.

1.5.2. Pair the auth solution with your Paperless webSIGN account

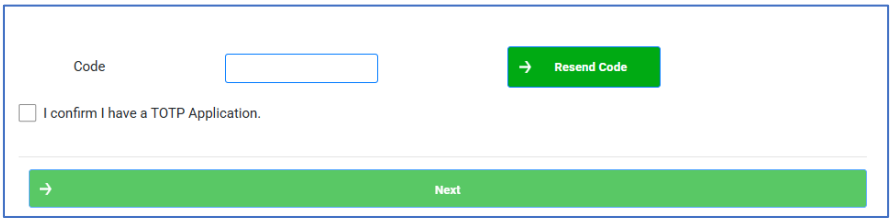
After installing the authorization solution, on the e-mail address provided to certSIGN, look for the e-mail from **Paperless**: **Set up the auth mechanism** from paperless@certsign.ro. The e-mail is the invitation to configure the authorisation mechanism.

In order to authorise the use of Paperless webSIGN please follow the steps below:

1. Click **this link** and open the hyperlink in Google Chrome. When you click on the link, the authorisation code to continue the procedure will be sent by SMS to the phone number used for enrolment. Scroll down to the bottom of the web page and, in the **Authorisation Code** field in the **HOW TO?** section, enter the authorisation code received by SMS, within 10 minutes.



2. If you failed to enter the code within the allotted 10 minutes, at the end of the 10 minutes, the timer next to the **Authorisation Code** field stops. Press the **Resend code** button to receive another code by SMS, but not before 30 minutes.

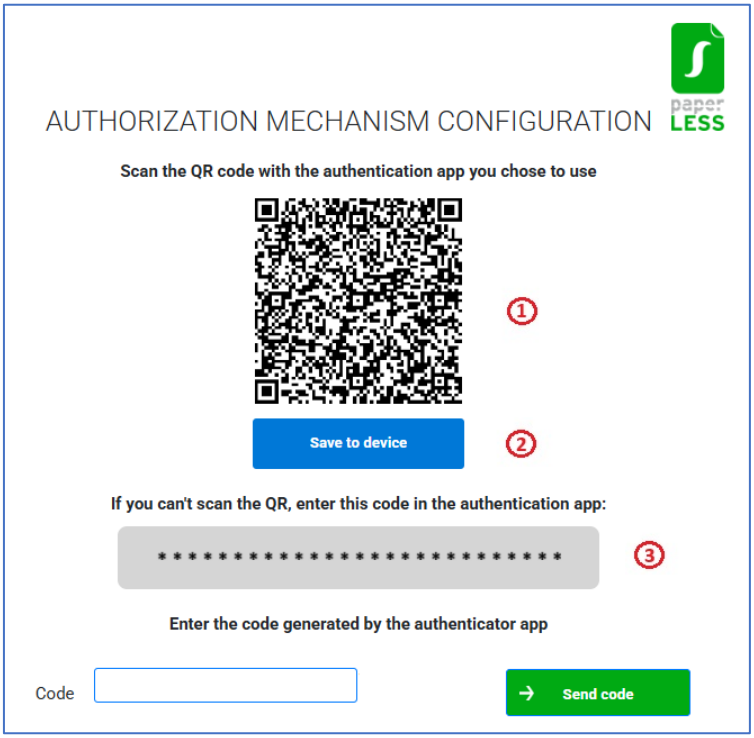


3. To complete the authorisation setup, tick the Authenticator app installation confirmation check box and press **Continue** (steps 3 and 4 in the **How to** section). The QR code page will be displayed.

4. To pair the authorisation solution on your phone with your account Paperless webSIGN authorisation solution from the Paperless webSIGN signing platform, you need to copy or scan the QR code displayed (step 5 HOW TO? section), depending on the device from which you followed the pairing steps:

– if you accessed the pairing link from a device (computer, laptop, tablet or other phone) other than the one on which you installed the authorisation app, open the Authenticator app installed on your phone and scan the QR code that appears on the ①;

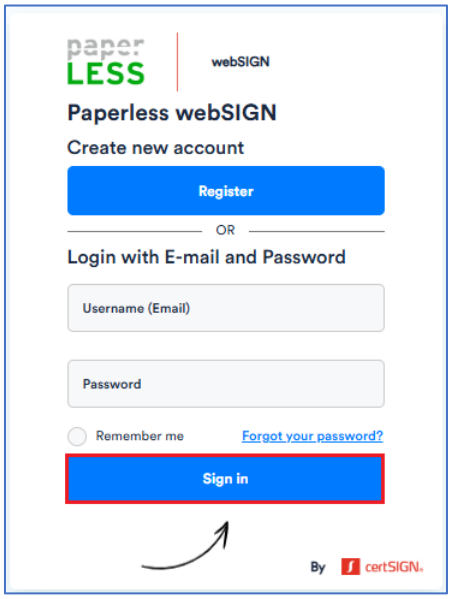
– if you accessed the pairing link from the phone where you installed the authorisation app, press the **Save to device** button ② and the QR will be saved.



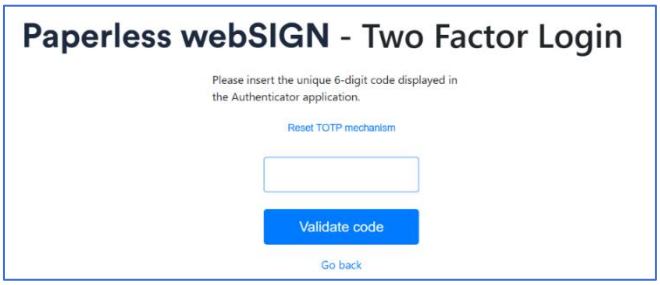
5. After scanning/saving the QR code, the Authenticator app on your phone will generate 6-digit authorisation codes valid for 30 seconds. To complete the pairing, enter a code generated by the authorisation app and press **Send**. The message that you have successfully set up the authorisation mechanism will be displayed.

1.6. Issuing the digital certificate in the Paperless webSIGN platform

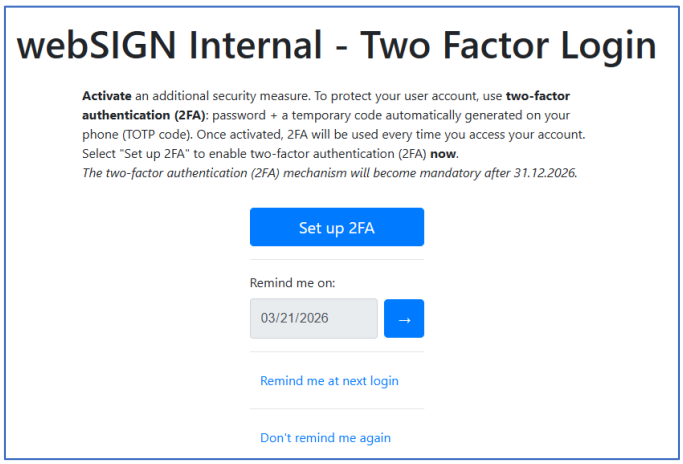
To issue your digital certificate, go to https://websign.ro using the e-mail address and password you registered with. Issuing can be done both from a Windows or macOS computer and from an Android or iPhone mobile phone.



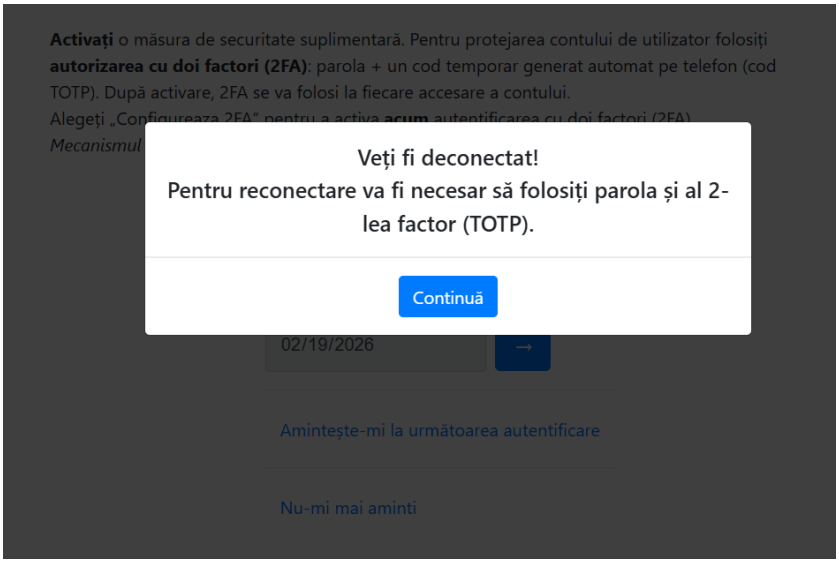
If you have enabled 2FA authentication, an additional window will appear requesting an authorization code from the Authenticator app on your phone.



If you haven't activated 2FA authentication but want to do so now, press Set up 2FA.

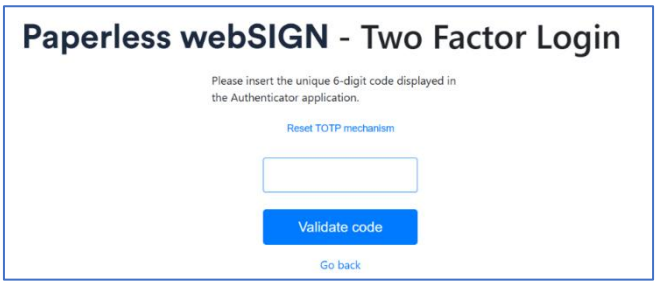


A pop-up will appear with a message informing you that you will be logged out and that when you log back in, after entering your username and password, you will need to enter an authorization code from the Authenticator app that you have already set up on your phone. Press the **Continua/Next** button.



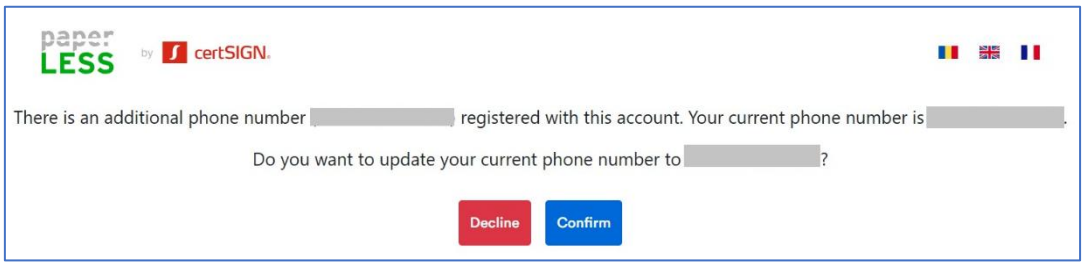
After entering your account password, you will be prompted to enter the authorization code displayed by the Authenticator app on your phone.

.

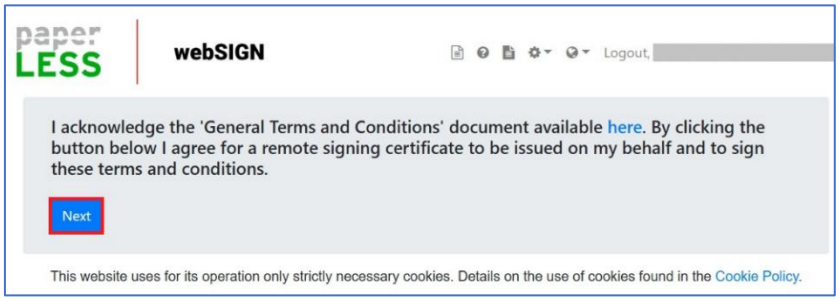


If you haven't set the 2FA and don't want to do so now, choose one of the deferral options.

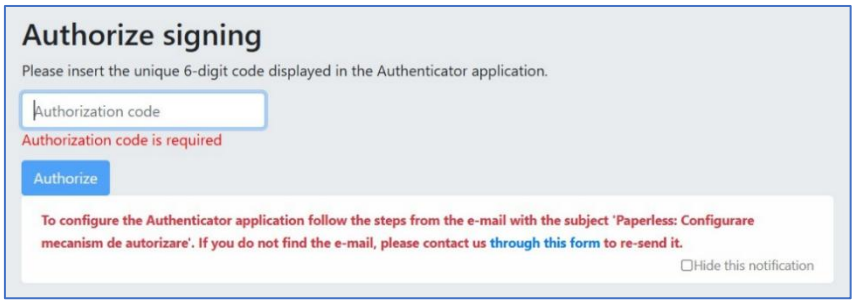
If, during the video identification stage, you chose to change your phone number for the purpose of receiving the SMS, you can associate this number with your cloud account on the https://websign.ro platform. If you want to associate this phone number with your cloud account, press the **Confirm** button. If you want to keep the number that is already associated, press the **Decline** button.



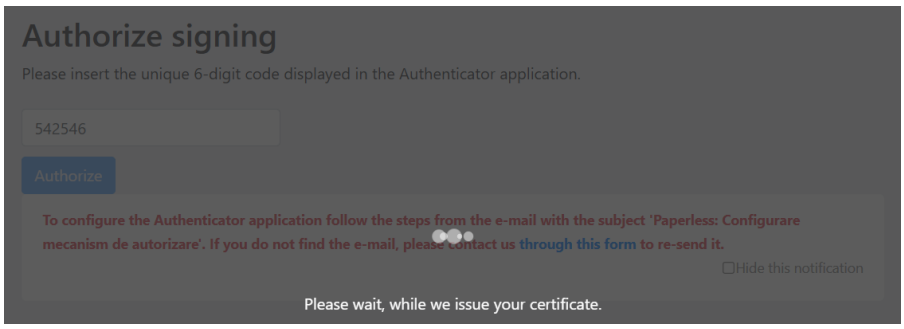
Read the terms and conditions specific to the issuance process for the new certificate and, if you agree, click **Next** to sign the terms and the certificate will be issued.



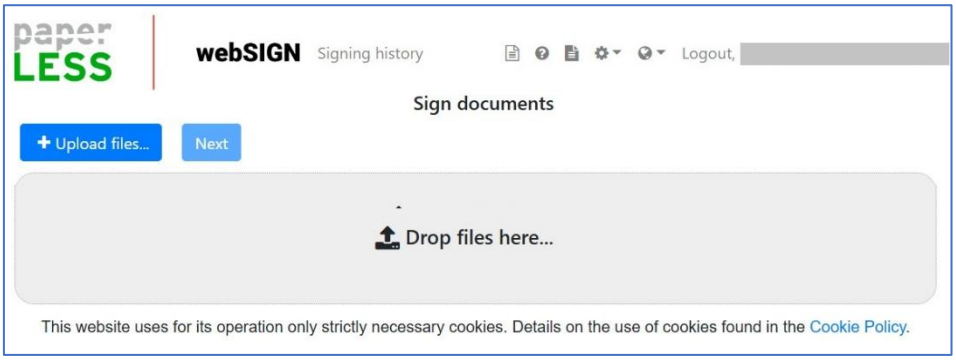
Clicking **Next** opens the authorisation page with a field requiring the authorisation code generated by the authorisation app on your phone, Microsoft Authenticator or Google Authenticator.



Once the authorisation code has been entered, the qualified certificate will be issued and will be used for signing during its period of validity.

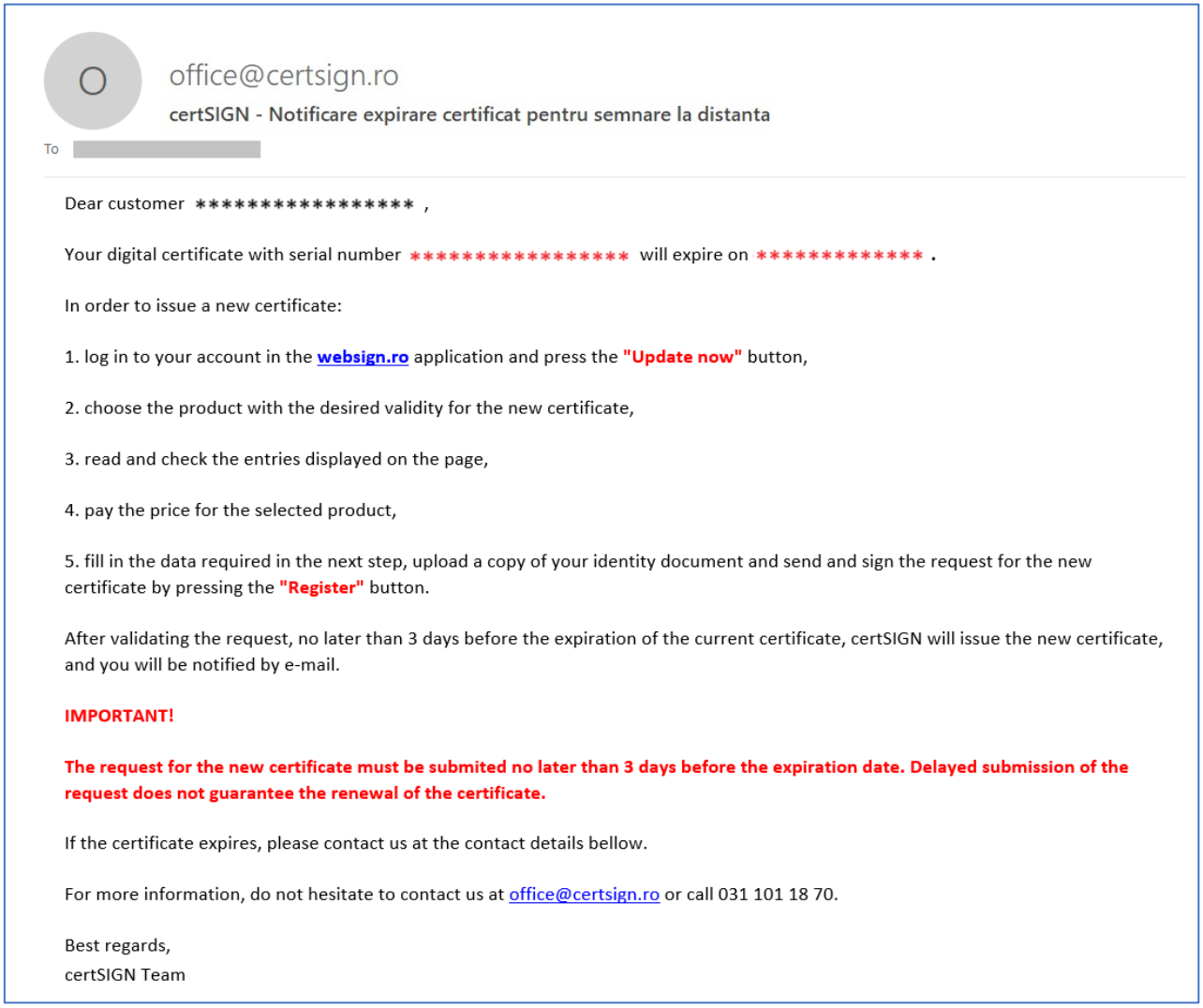


Once the certificate has been generated, you will be redirected to the main page of the Paperless webSIGN platform, where you can upload documents for signing.



2. Rekey – renewal of qualified digital certificates for remote signing

45 days before the expiry date of a valid certificate (or 15 days if the re-key has not been performed), users will receive an email notification with a link to the Paperless webSIGN platform. This allows them to update their data in order to renew their certificate. When they access the link, they are redirected to the application's login screen.



office@certsign.ro

certSIGN - Notificare expirare certificat pentru semnare la distanta

To

Dear customer ********** ,

Your digital certificate with serial number ********** will expire on ********** .

In order to issue a new certificate:

1. log in to your account in the **websign.ro** application and press the **"Update now"** button,

2. choose the product with the desired validity for the new certificate,

3. read and check the entries displayed on the page,

4. pay the price for the selected product,

5. fill in the data required in the next step, upload a copy of your identity document and send and sign the request for the new certificate by pressing the **"Register"** button.

After validating the request, no later than 3 days before the expiration of the current certificate, certSIGN will issue the new certificate, and you will be notified by e-mail.

IMPORTANT!

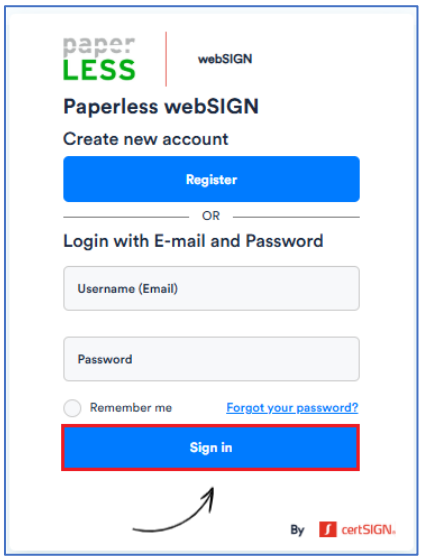
The request for the new certificate must be submited no later than 3 days before the expiration date. Delayed submission of the request does not guarantee the renewal of the certificate.

If the certificate expires, please contact us at the contact details bellow.

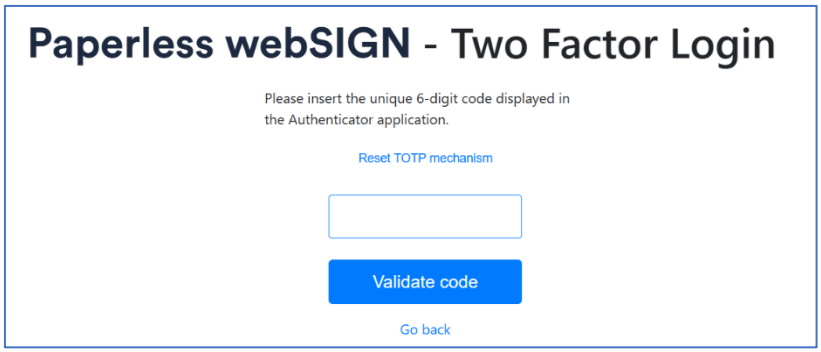
For more information, do not hesitate to contact us at office@certsign.ro or call 031 101 18 70.

Best regards,
certSIGN Team

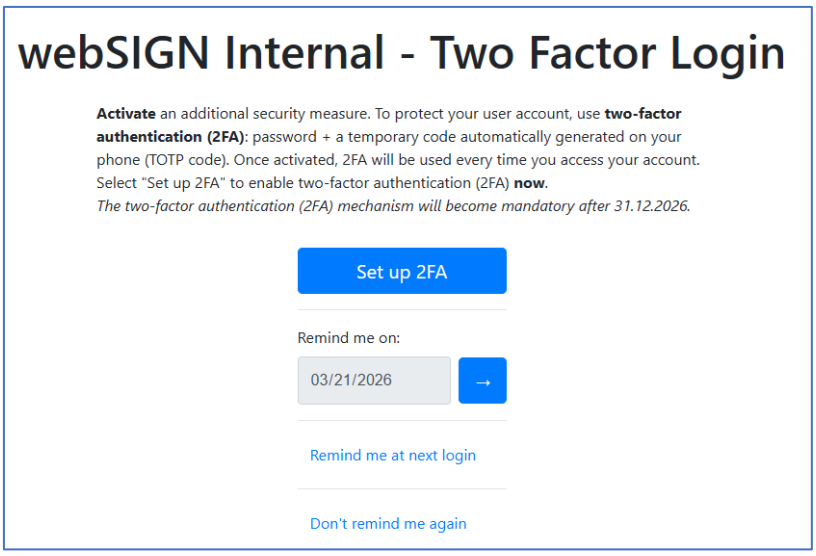
When accessing the link https://websign.ro, the user is redirected to the platform login screen.



If you have enabled 2FA authentication, an additional window will appear requesting an authorization code from the Authenticator app on your phone.

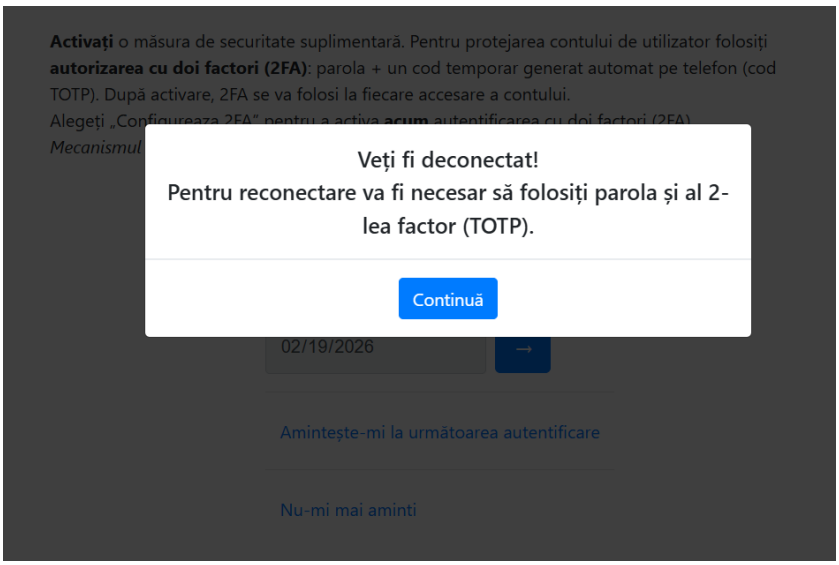


If you haven't set the 2FA authentication but want to do so now, press **Set up 2FA.**



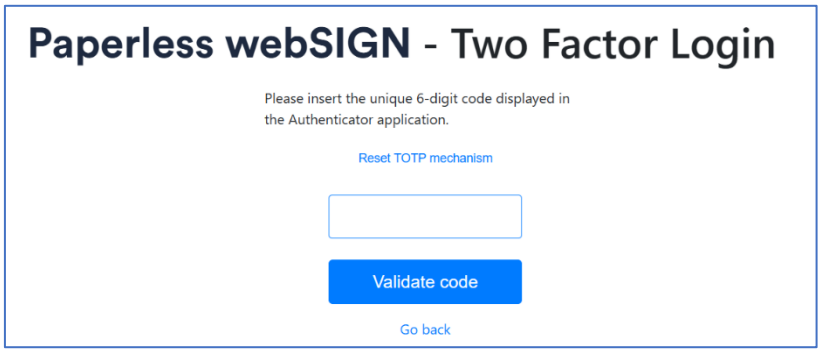
A pop-up will appear with a message informing you that you will be logged out and that when you log back in, after entering your username and password, you will need to enter an authorization code from the Authenticator app that you have already set up on your phone. Press the **Continua/Next** button.

.



After logging in with your account password, you will be prompted to enter the authorization code displayed by the Authenticator app on your phone.

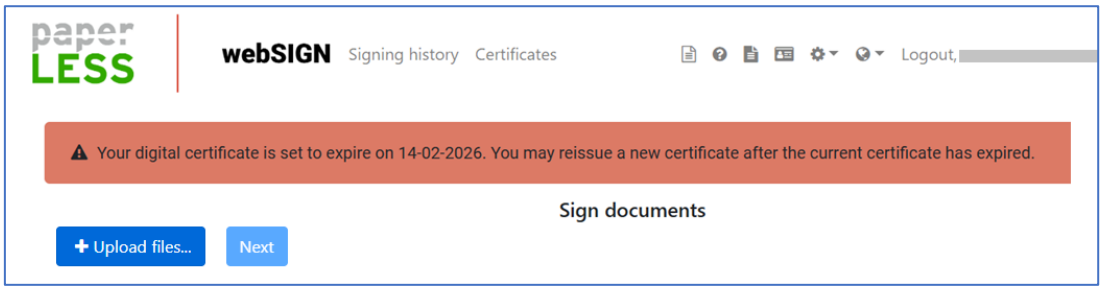
.

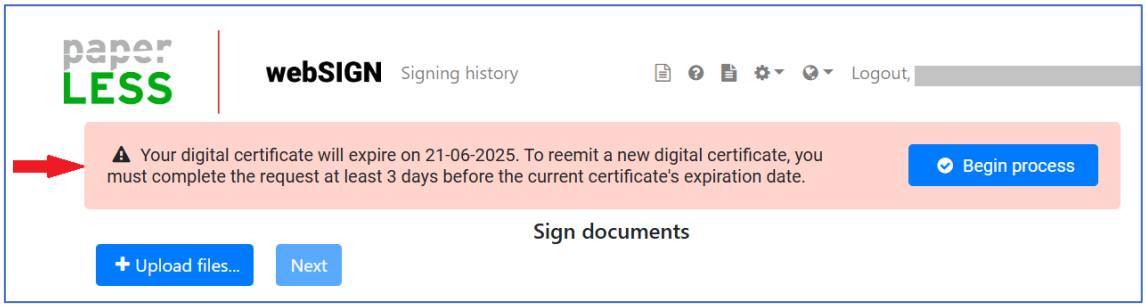


If you haven't set the 2FA and don't want to do so now, choose one of the deferral options.

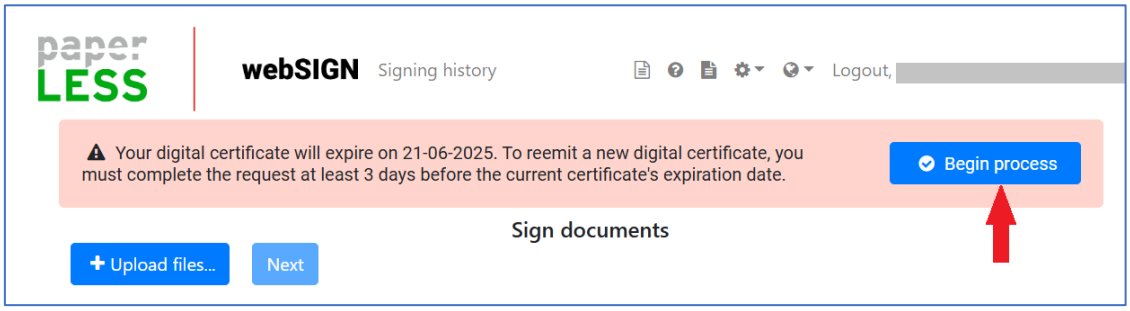
After logging into the Paperless webSIGN platform, a banner will be displayed at the top of the main screen with details of the certificate expiry and the period during which rekeying can be performed. Three days (72 hours) before the certificate expires, the rekey period ends and it will no longer be possible to perform this procedure to renew the certificate.

Please note! You can complete the certificate renewal procedure up to 3 days (72 hours) before the certificate expires. If your certificate is due to expire in fewer than 72 hours, a banner will appear after you log in to the platform informing you that you need to make a new purchase once the current certificate has expired. This purchase requires payment and video identification of the user. If you have paid for the re-key but have not completed the process, the amount will be refunded to your account.

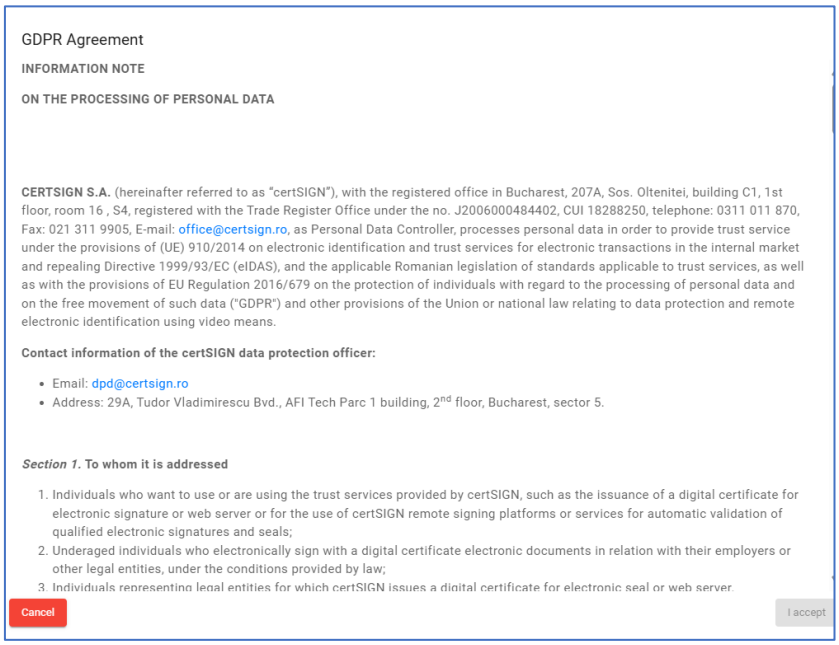


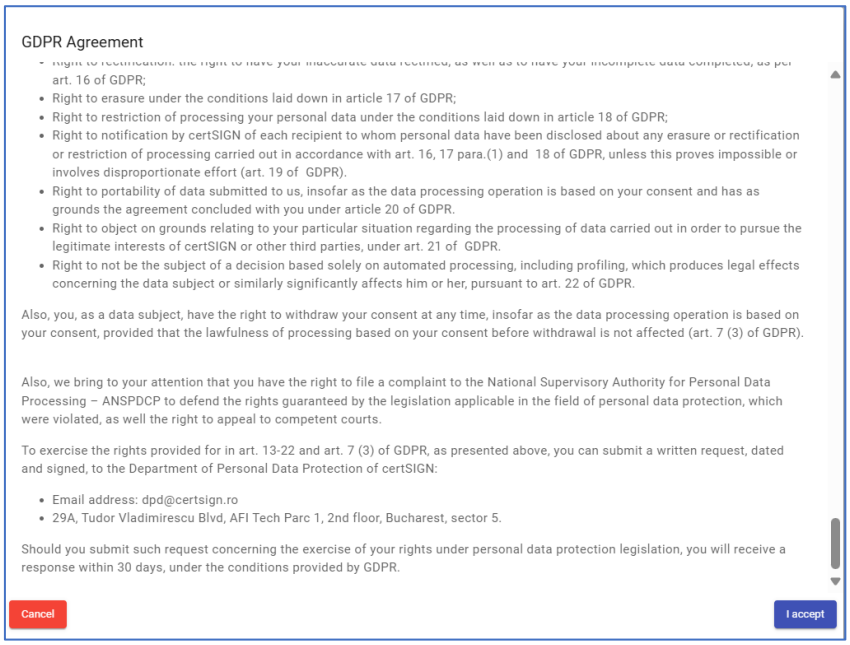


To start the certificate renewal process, click **Begin process**:



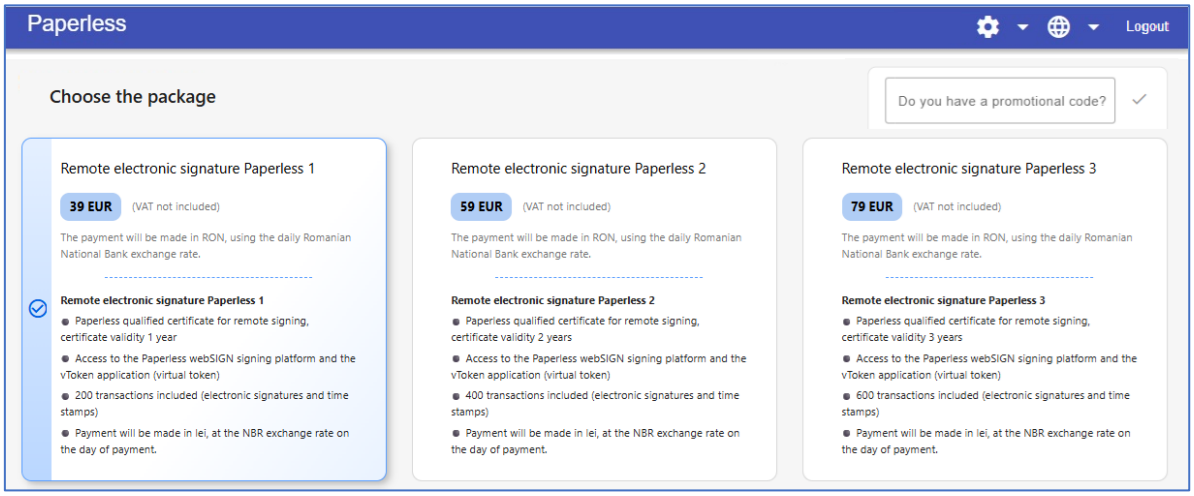
Read the GDPR Information Note on the processing of your data. Press the **I accept** button to agree and move on.



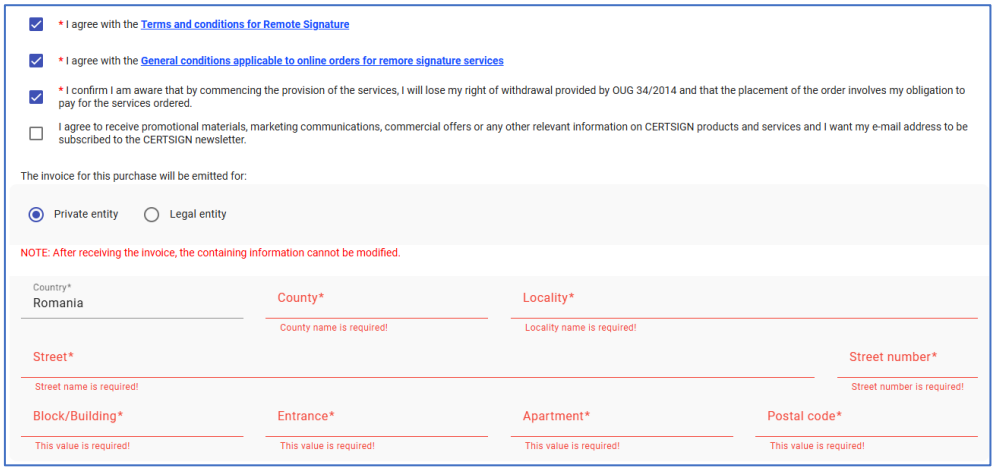


2.1. Select your package and pay online

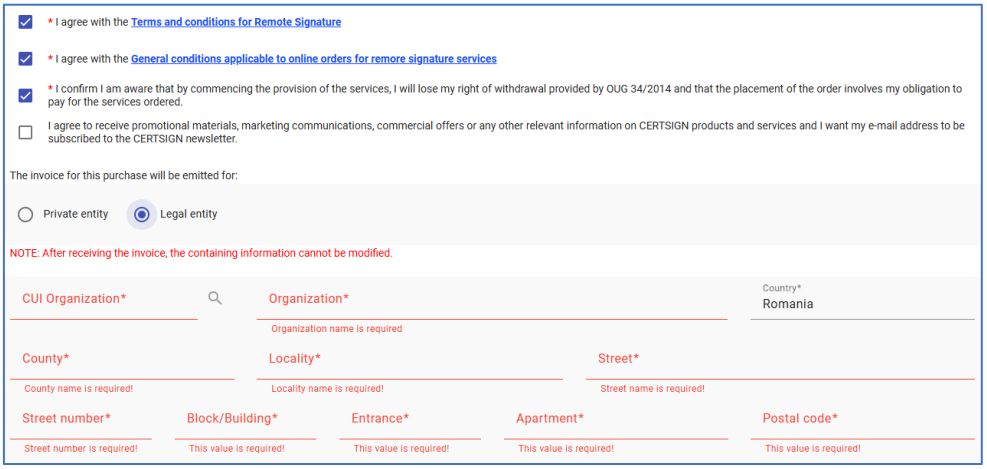
Select the desired package for the new certificate:



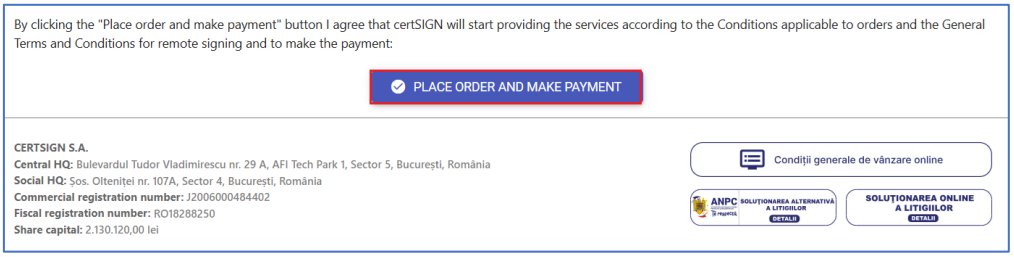
Read the **Terms and Conditions for Remote Signing** and the **General Terms and Conditions for orders placed in the Paperless platform**, and check the appropriate boxes:



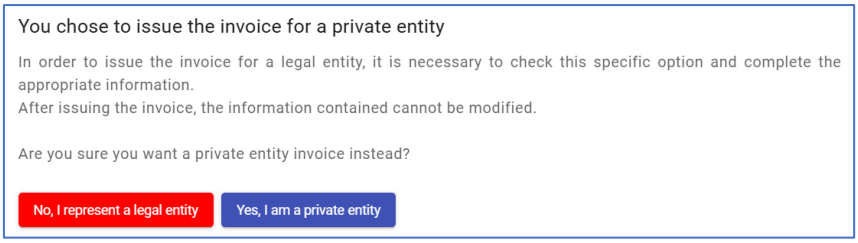
If you want the invoice to be issued in the name of a company, check the appropriate box and fill in the company details:



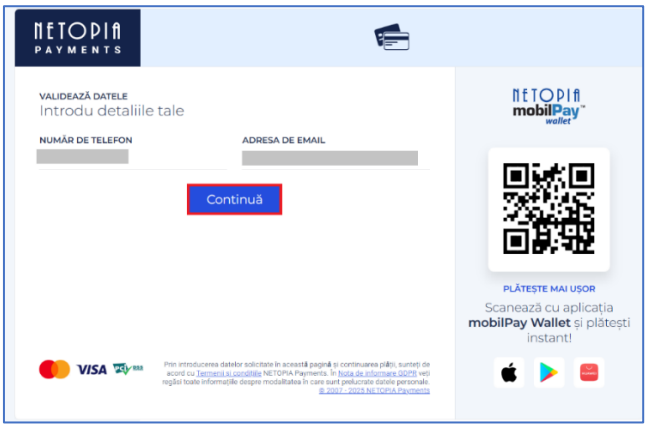
To start the payment, press the **PLACE ORDER AND PAYMENT** button:



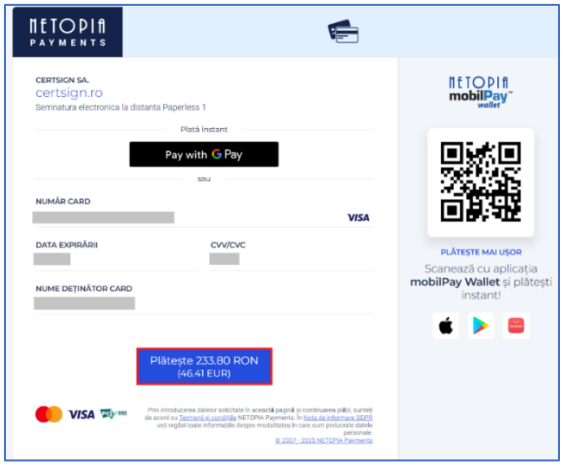
If you selected the private entity for the invoice, a pop up will appear informing you that the data on the invoice cannot be changed after issue and asking you to check if you still need the invoice for the legal entity. If you want the invoice for a legal entity, click the **No, I am private entity/Legal entity/Certified private entity/Individual enterprise.** etc. button and enter the data for the legal entity. If you want the invoice for a private entity, press the **Yes, I am a private entity** button.



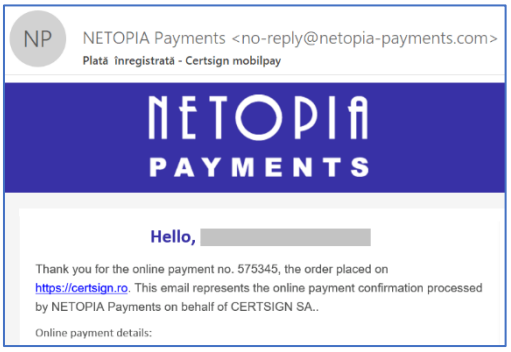
You are redirected to the payment window in the Netopia application where you need to enter your e-mail address to validate your data (phone number is already entered). To continue press the **Next/Continua** button.



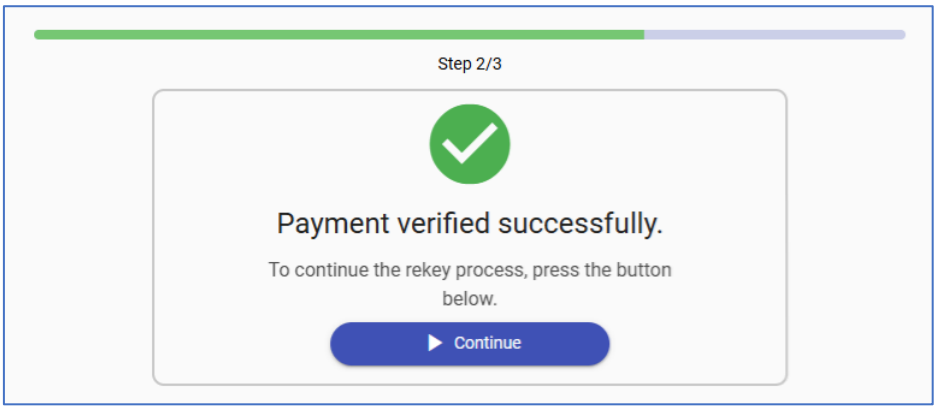
The amount for the selected package (euro + VAT) will be paid in lei at the NBR exchange rate on the day of payment. After filling in the required card details, press the **Pay** button to make the payment.



Once the payment has been made, you will receive a payment confirmation from Netopia on your registered e-mail address.



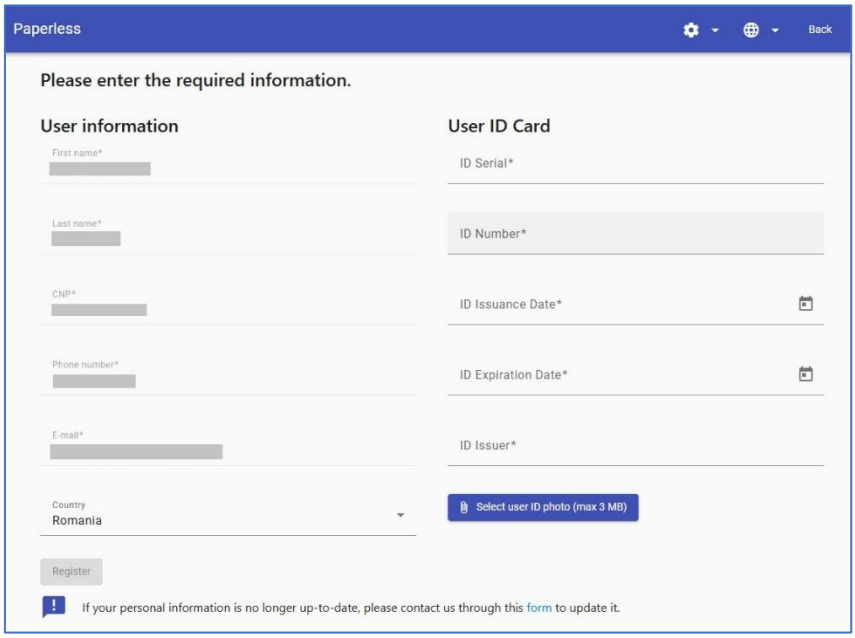
The payment will also be confirmed in the https://websign.ro platform. Press the **Continue** button to proceed and fill in your details.



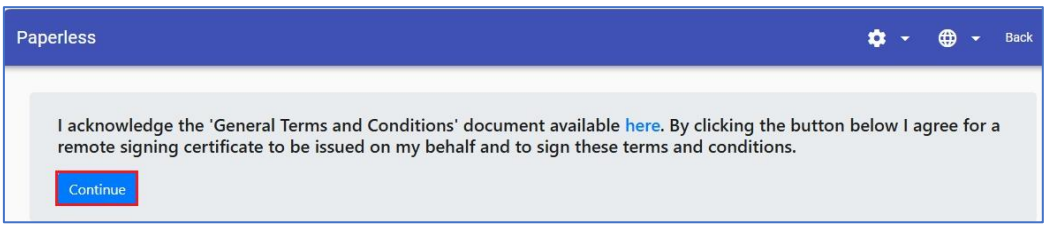
2.2. Fill in the details and submit your certificate application

Once the payment has been validated, the data will be filled in in order to send the certificate request. The data in the **'User information'** area are not editable. The data in the **'User ID'** area are editable and must be verified.

Only identity documents that are valid on the date of issue of the new certificate are accepted. After checking/completing the fields and uploading a copy of the identity document, the **Register** button is enabled.

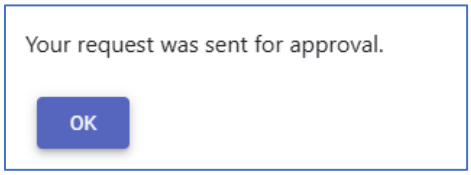


Pressing the **Register** button brings up a screen where you can view the Terms and Conditions for remote signing. Sign the terms by pressing the **Continue** button.



Pressing the **Continue** button will open a field requesting an authorisation code generated by the Authenticator application for applying the signature to the Terms and Conditions document. After entering the code, the data will be transmitted to certSIGN.

After transmission, a message is displayed confirming that the data has been automatically transmitted to certSIGN for validation. The user presses **OK**.

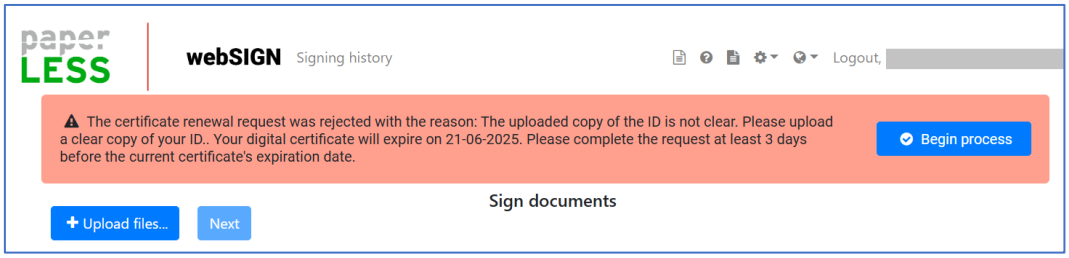


The user is redirected to the main application screen and can still use the Paperless webSIGN online platform. The screen will no longer display the reminder to update the data while it is in the process of being validated by certSIGN.

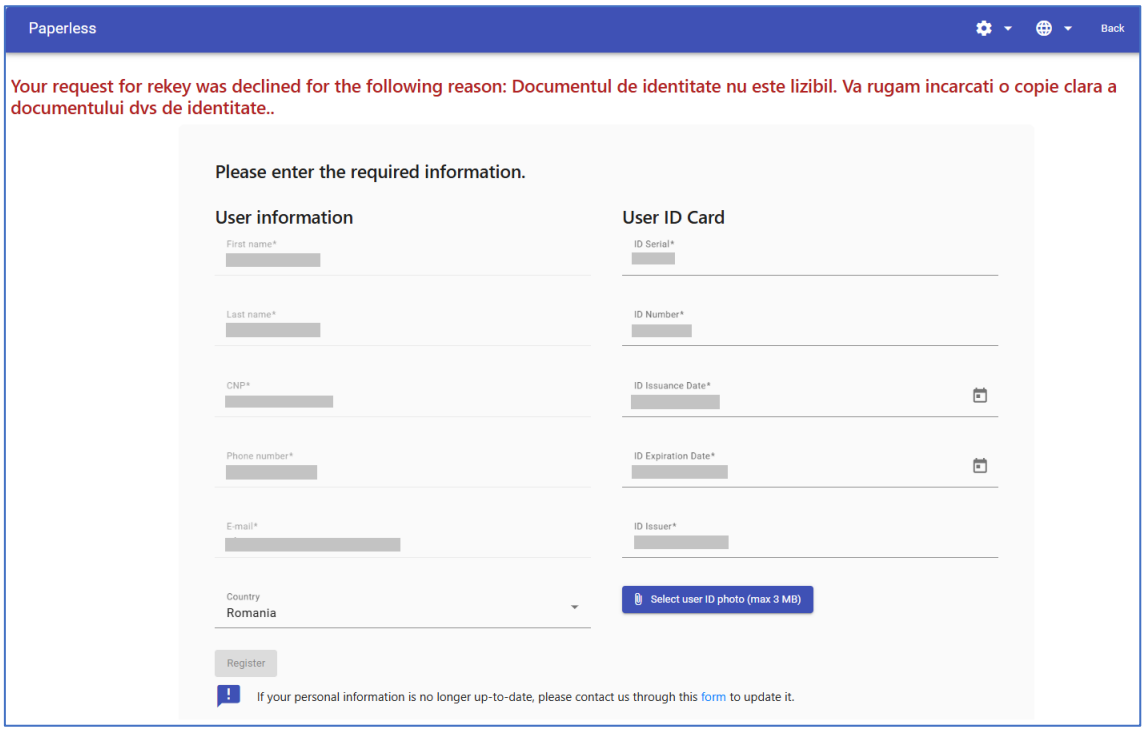
Data filled in by the user is validated by certSIGN:

- If the submitted data **matches** the data in the identity document, the user will be notified by e-mail that their certificate renewal request has been approved. The certificate will be issued automatically 3 days before the current certificate expires.

- If the data submitted **does NOT** correspond to the data in the identity document, the user will be notified by e-mail that the certificate renewal request has been rejected, and the reason for rejection will be stated. The user will have to restart the certificate renewal process within 3 days before the expiry of the certificate already held. In his account in the Paperless webSIGN online platform, after logging in, the user will have a banner with a warning message displayed at the top of the main screen. The user has to press the **Begin process** button to resume the renewal procedure.

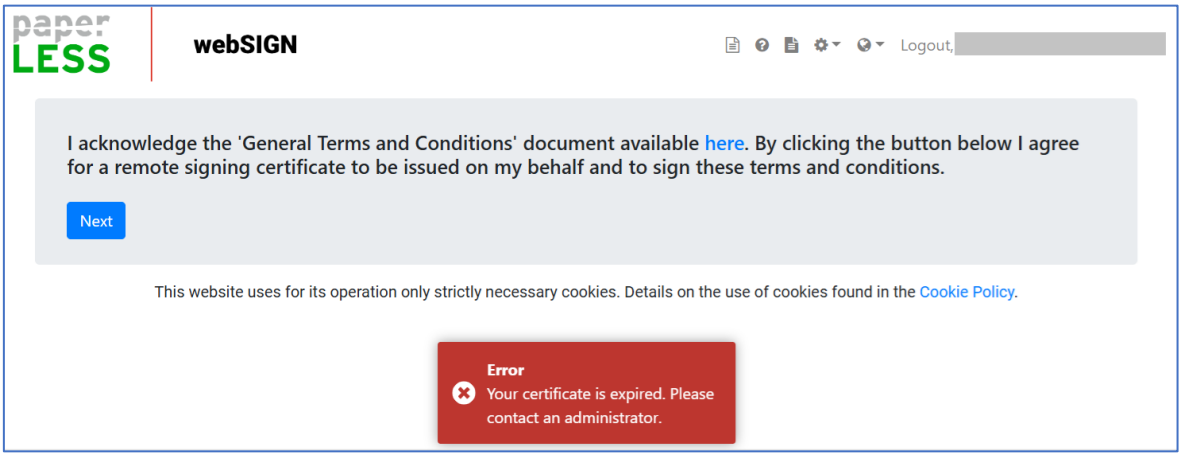


The user will be able to see the reason why his previously submitted data was NOT validated. Depending on the reason, fill in all the data about the current ID correctly, then press the **Register** button. The process resumes with the user signing the terms and conditions.



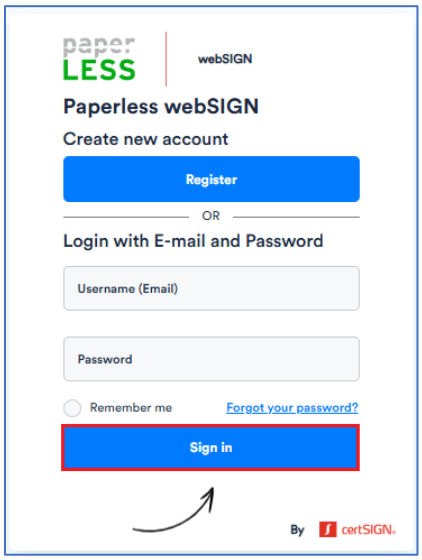
Note:

If a user remains logged in to the platform and their certificate expires in the meantime, the following message will appear when they attempt to sign: 'Your certificate has expired. Please contact an administrator.' Log in again and select 'I want a new certificate' (see subchapter 3).

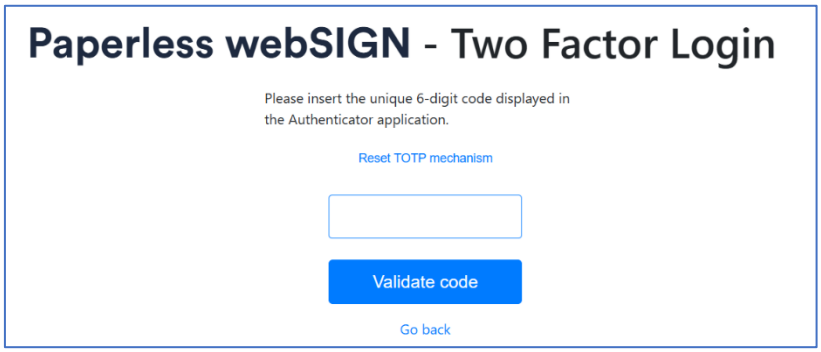


3. Re-issuing a qualified digital certificate for remote signing

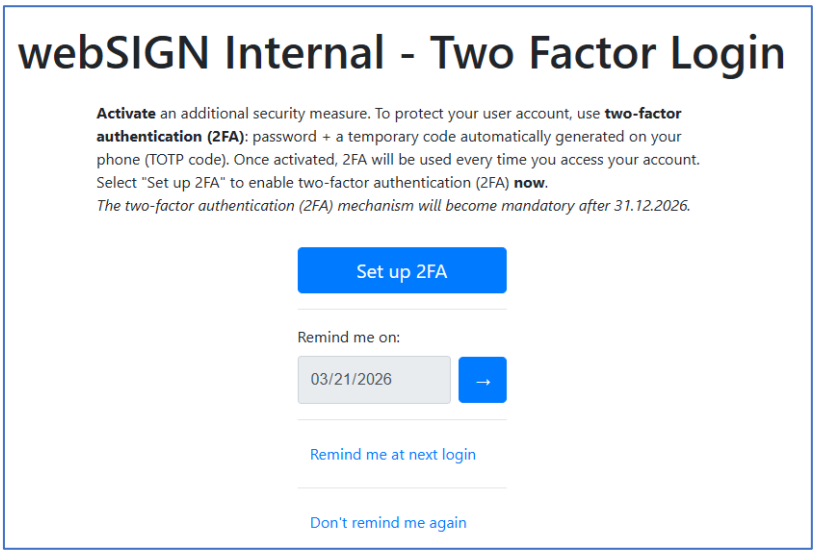
If your certificate has expired, you can apply for a new certificate. To do this go to https://websign.ro and log in with your username and password.



If you have set the 2FA authentication, you will be prompted to enter an authorisation code from the Authenticator app on your phone.

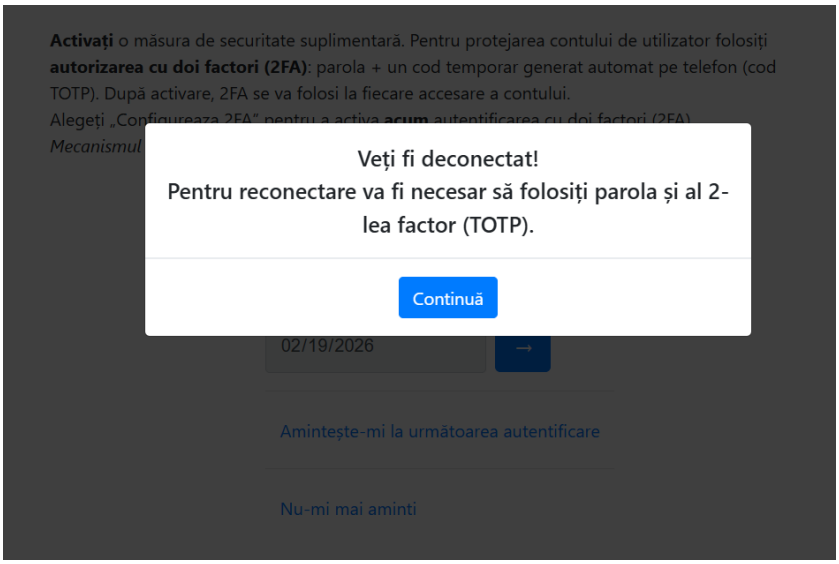


If you haven't set the 2FA authentication but want to do so now, press **Set up 2FA.**

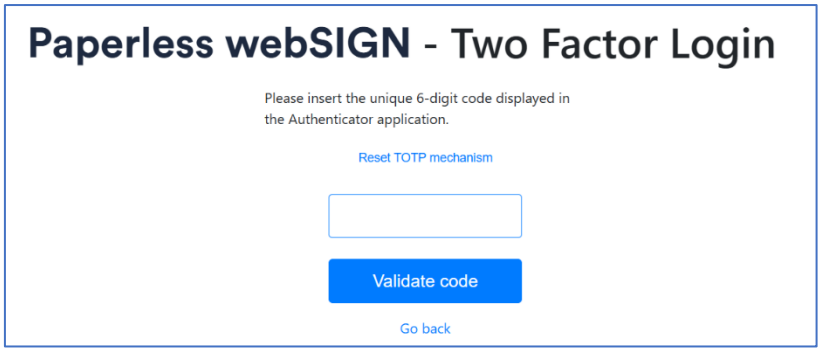


A pop-up message will appear to inform you that you will be logged out. When you log back in, you will need to enter an authorisation code from the Authenticator app that you have already set up on your phone, after entering your username and password. Press the 'Continua/Next' button.

.



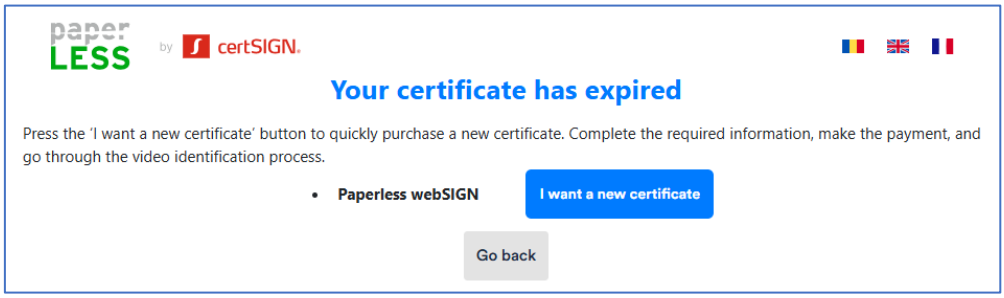
After logging in with your account password, you will be prompted to enter the authorization code displayed by the Authenticator app on your phone. .



If you haven't set the 2FA and don't want to do so now, choose one of the deferral options.

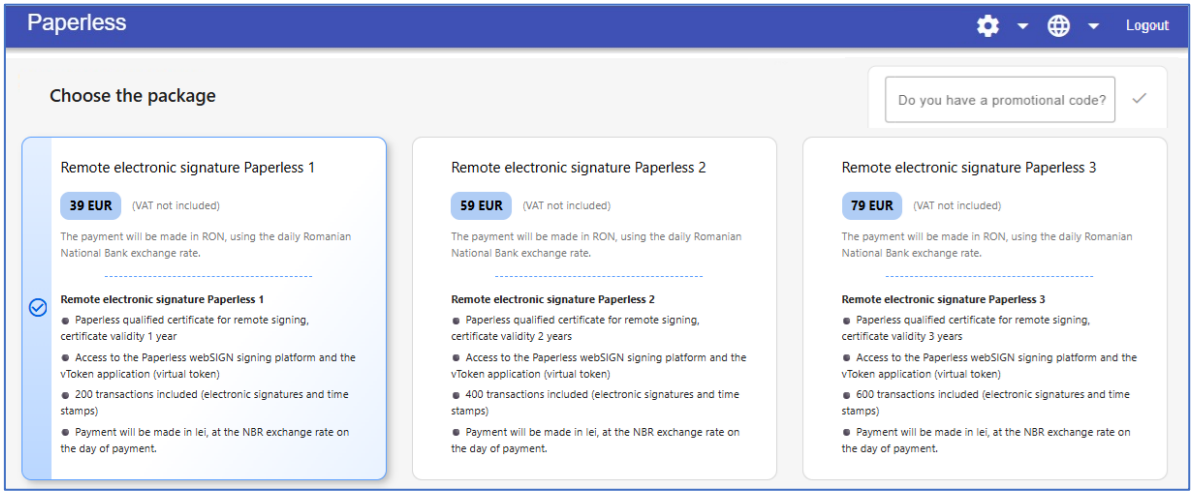
After logging into the Paperless webSIGN platform interface, a message will appear informing you that your certificate has expired. To issue a new certificate, click the **I want a new certificate** button.

.

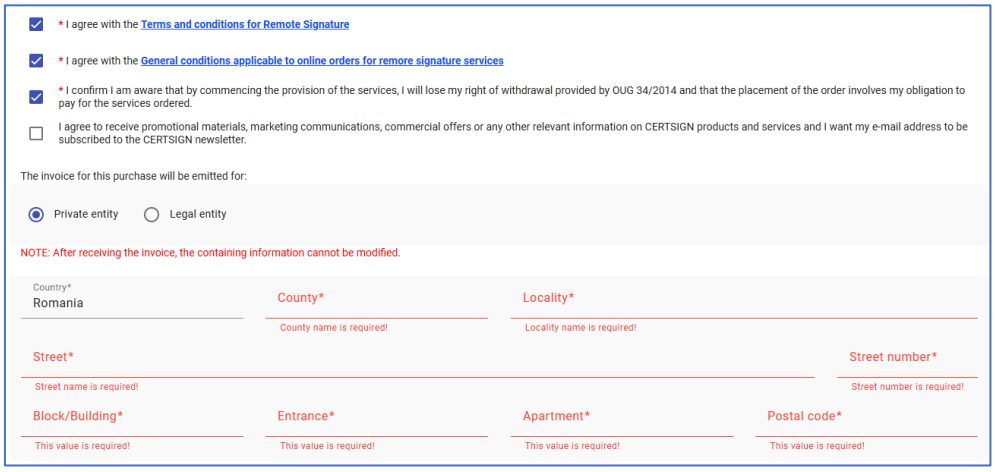


3.1. Select your package and pay online

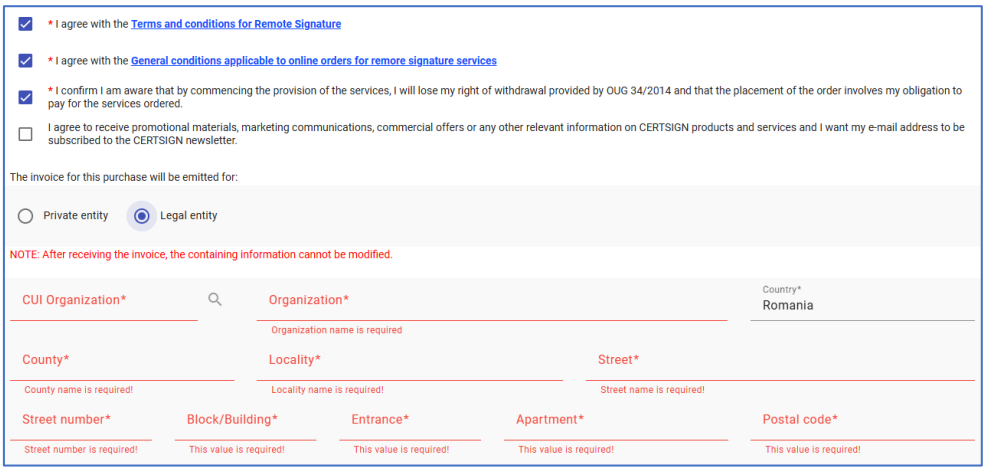
Select the package for the new certificate:



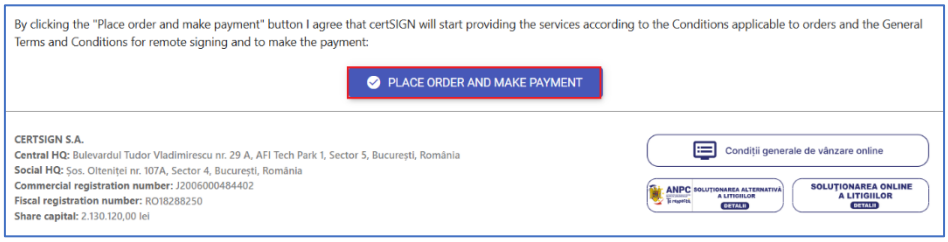
Read the **Terms and Conditions for Remote Signing and the General Terms and Conditions for Paperless orders** respectively, then check the appropriate boxes:



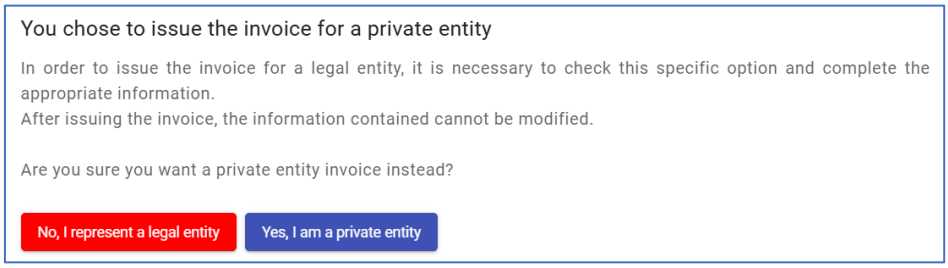
If you want the invoice to be issued in the name of a company, check the appropriate box and fill in the company details:



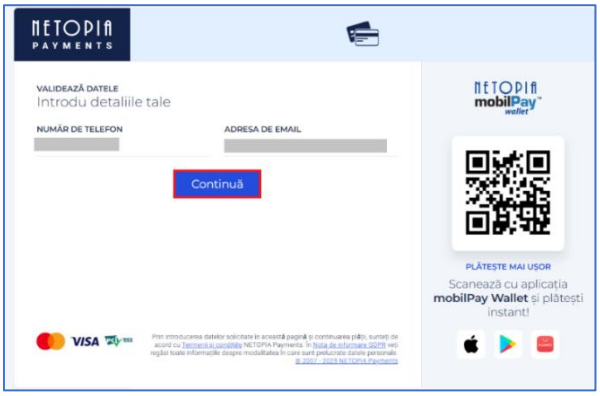
To start the payment, press the **PLACE ORDER AND PAYMENT** button:



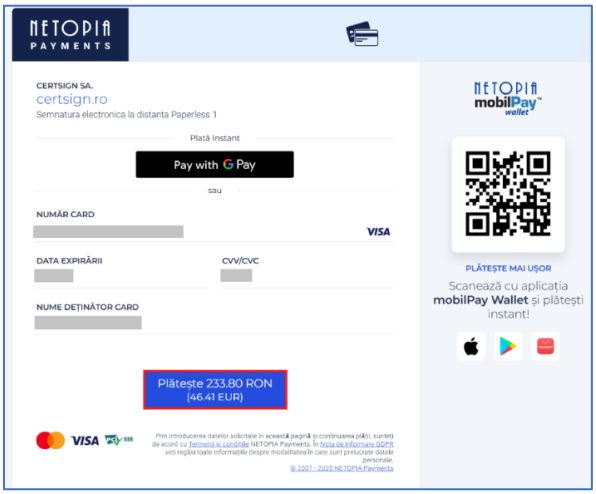
If you selected the private entity for the invoice, a pop up will appear informing you that the data on the invoice cannot be changed after issue and asking you to check if you still need the invoice for the legal entity. If you want the invoice for a legal entity, click the **No, I am private entity/Legal entity/Certified private entity/Individual enterprise.** etc. button and enter the data for the legal entity. If you want the invoice for a private entity, press the **Yes, I am a private entity** button.



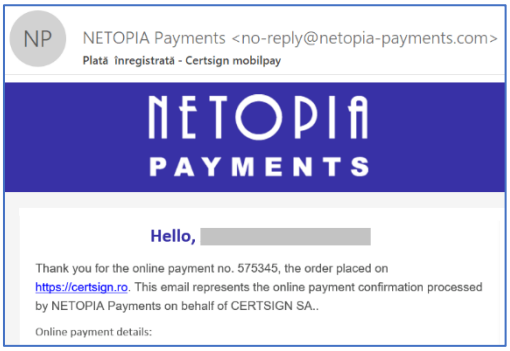
You are redirected to the payment window in the Netopia application where you need to enter your e-mail address to validate your data (phone number is already entered). To continue press the **Next/Continua** button.



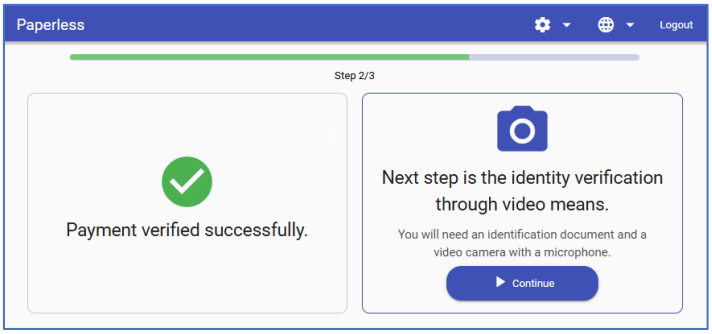
The amount for the selected package (euro + VAT) will be paid in lei at the NBR exchange rate on the day of payment. After filling in the required card details, press the **Pay** button to make the payment.



Once the payment has been made, you will receive a payment confirmation from Netopia on your registered e-mail address.

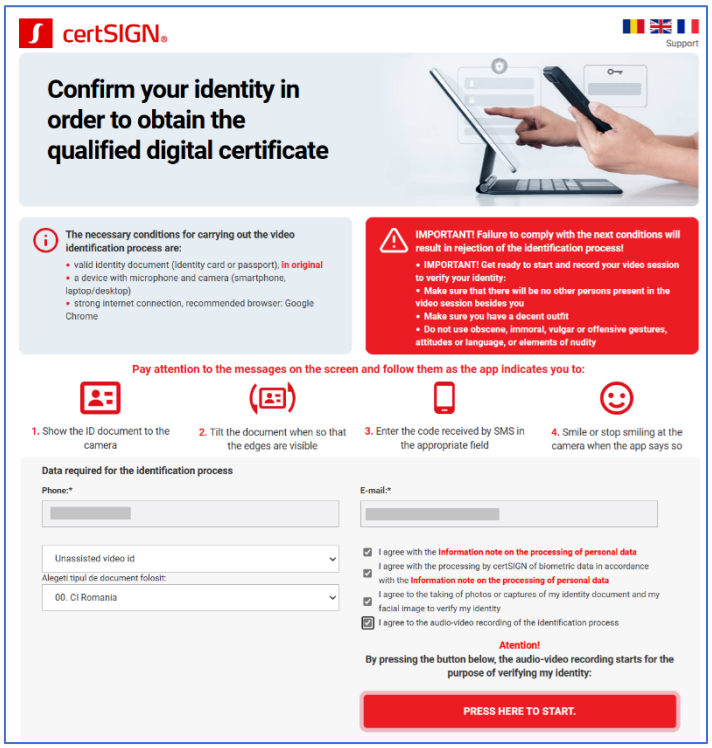


Once the payment has been confirmed in the https://websign.ro platform interface, follow the video identification step. You need your original ID, a good internet connection and access to a video camera with microphone.



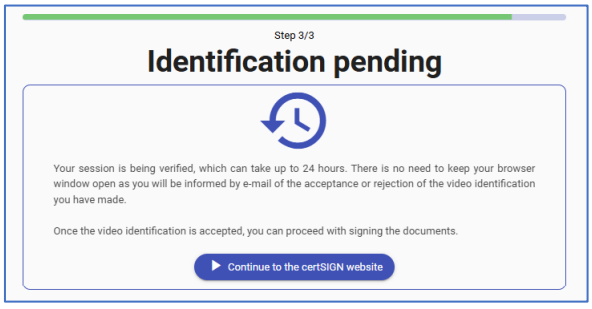
3.2. Video identification

After pressing the **Continue** button (the one in the screenshot above), you will be redirected to the video identification platform where you need to select the type of ID you identify yourself with, tick the check boxes on the right and then press the red **Click here to start** button.

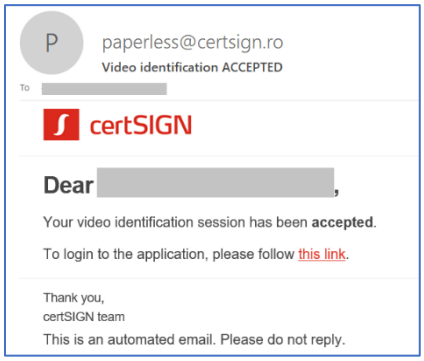


Please note! If you do not receive an SMS during the video identification process or find that the phone number is incorrect, you can change it. Subsequently, if you wish, the new phone number can be linked to your cloud account on the https://websign.ro platform.

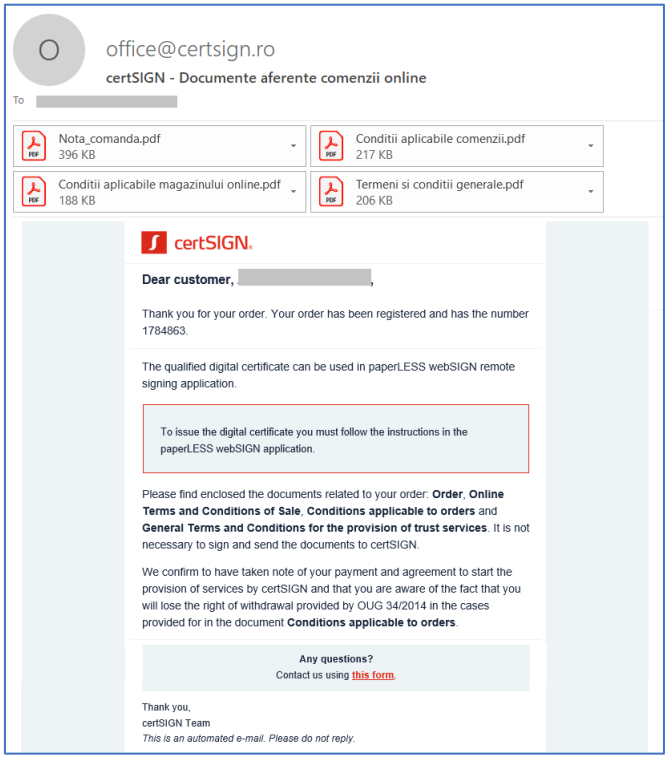
Once the video identification is completed, the platform displays information on the maximum duration of the identity verification process:



After verification of the video identification process, you will be notified by e-mail of the acceptance or rejection of the identification process and the reasons for rejection, if applicable.

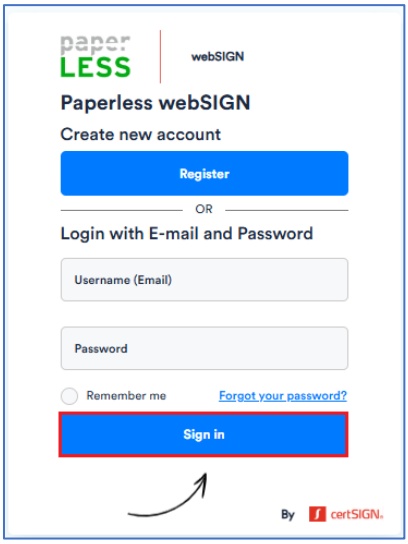


Also, by e-mail you will receive confirmation of acceptance by certSIGN of your order together with the related documents.

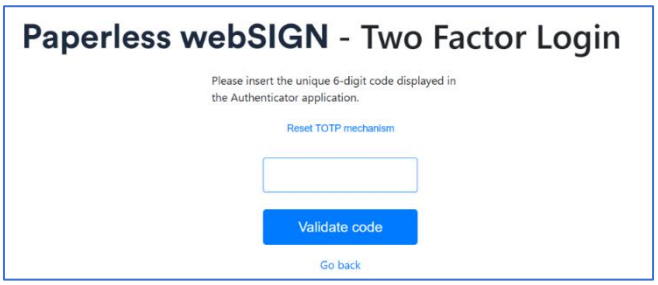


3.3. Issuing a digital certificate

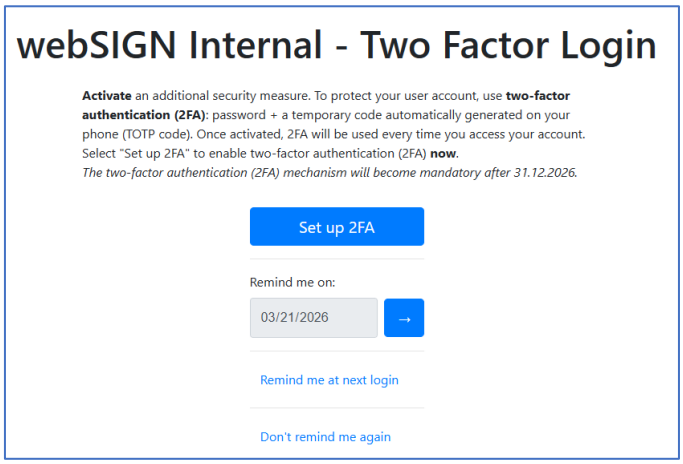
To issue the digital certificate, access the platform https://websign.ro with the email and password you use. The certificate can be issued from a Windows or macOS computer, as well as from an Android or iPhone.



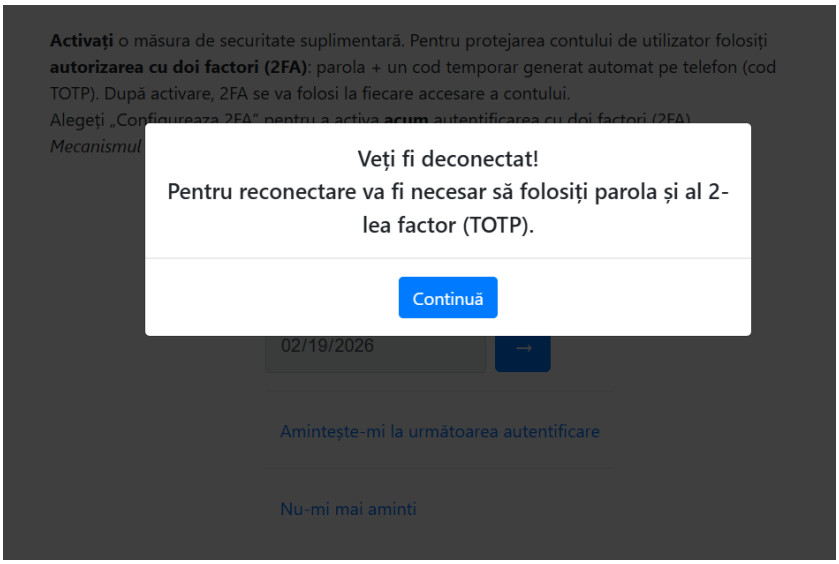
If you have set the 2FA authentication, you will be prompted to enter an authorization code from the Authenticator app on your phone.



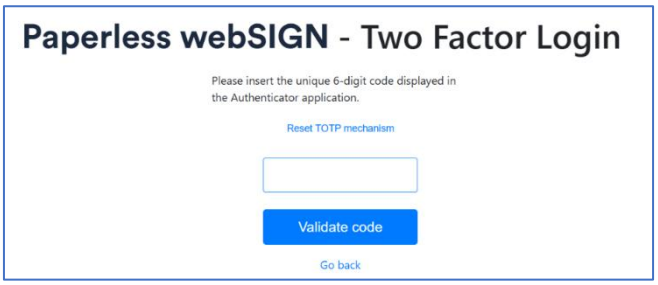
If you haven't set the 2FA authentication but want to do so now, press **Set up 2FA.** .



A pop-up will appear with a message informing you that you will be logged out and that when you log back in, after entering your username and password, you will need to enter an authorization code from the Authenticator app that you have already set up on your phone. Press the **Continua/Next** button.

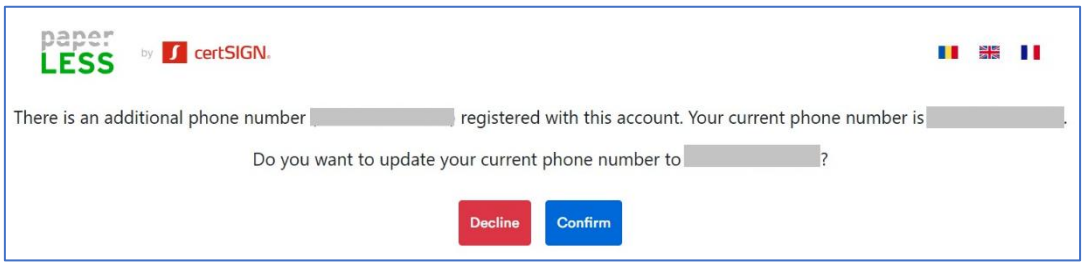


After logging in with your account password, you will be prompted to enter the authorization code displayed by the Authenticator app on your phone.

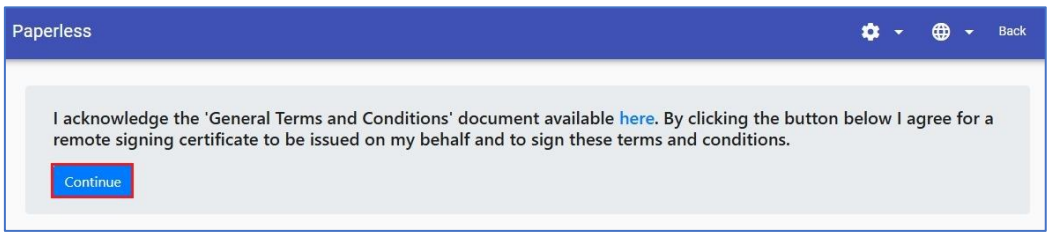


If you haven't set the 2FA and don't want to do so now, choose one of the deferral options. .

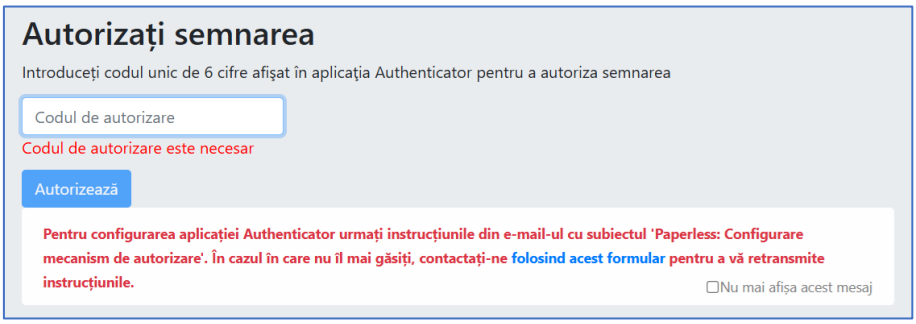
If, during the video identification stage, you chose to change your phone number for the purpose of receiving the SMS, you can associate this number with your cloud account on the https://websign.ro platform. If you want to associate this phone number with your cloud account, press the **Confirm** button. If you want to keep the number that is already associated, press the **Decline** button.



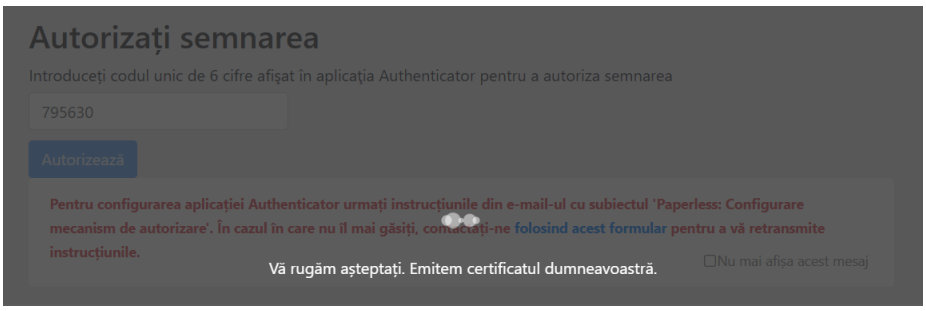
Read the terms and conditions specific to the issuance process for the new certificate and, if you agree, click **Continue** to sign the terms and the certificate will be issued.



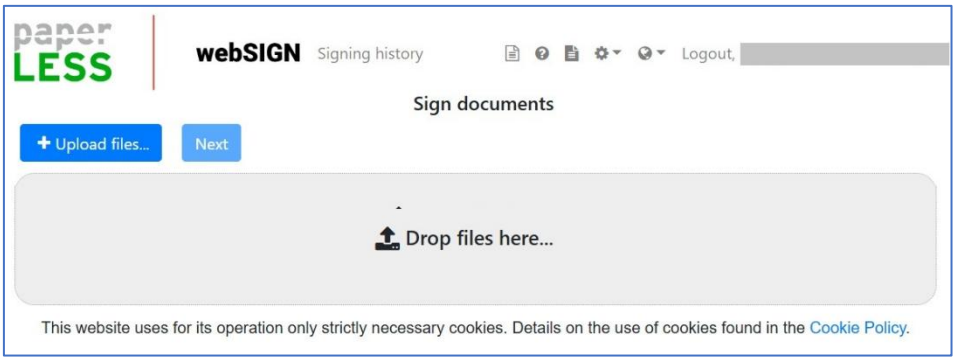
Pressing the **Continue** button will open a field asking for an authorisation code generated by the authorisation app on your phone, Microsoft Authenticator or Google Authenticator. After entering the code, the certificate will be issued.



Once the authorization code has been entered, the qualified certificate will be issued and can be used for signing during its period of validity.



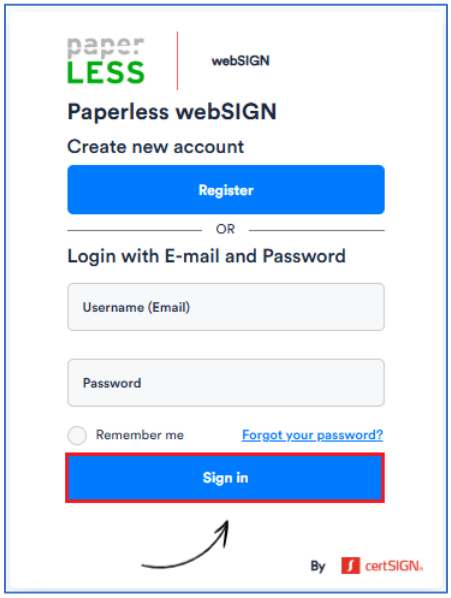
After generating the certificate, the main page of the Paperless webSIGN platform will appear, where documents can be uploaded for signing.



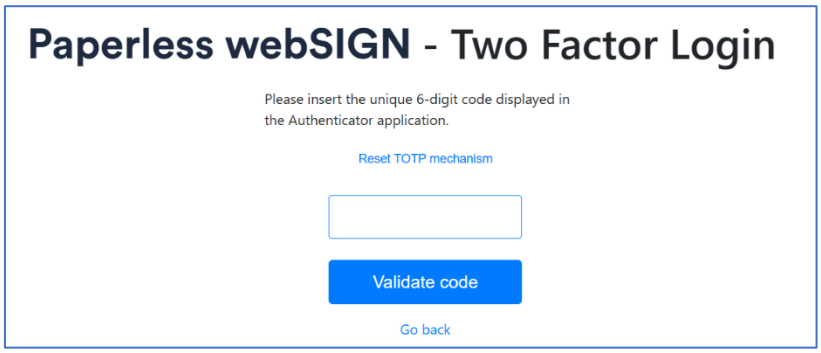
4. Change password

4.1. Change account password when login password is known

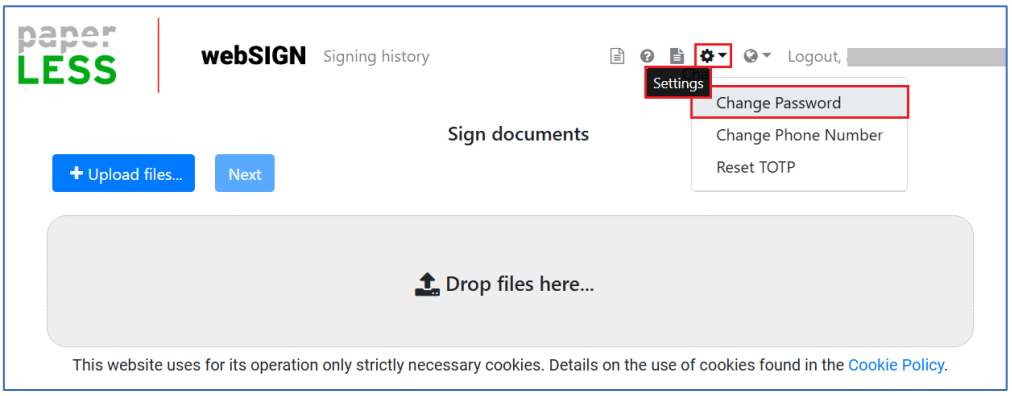
If you want to change the password of your Paperless webSIGN account, go to https://websign.ro using the email and password you signed up with.



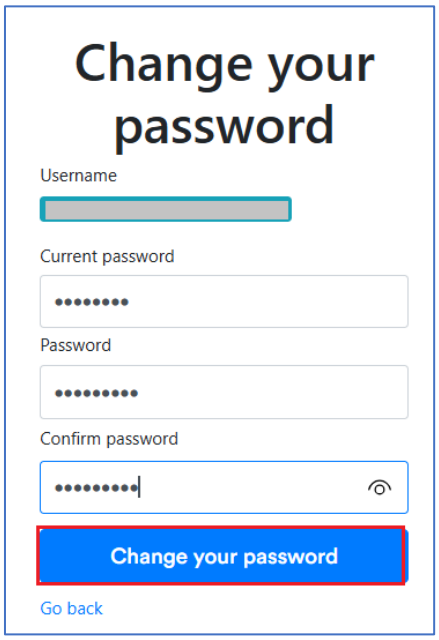
If you have set the 2FA authentication, you will be prompted to enter an authorisation code from the Authenticator app on your phone.



Go to the **Settings** and select **Change password**.

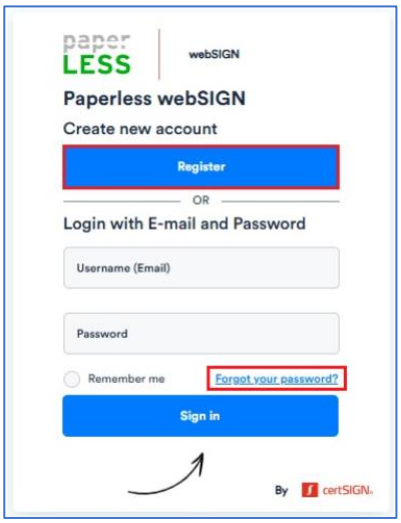


Choose your new password, then press the **Change password** button.

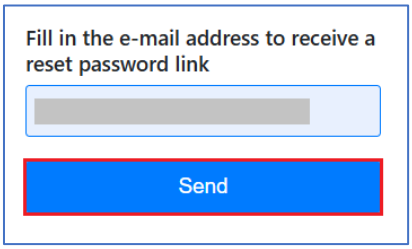


4.2. Recover account password when you don't know your login password

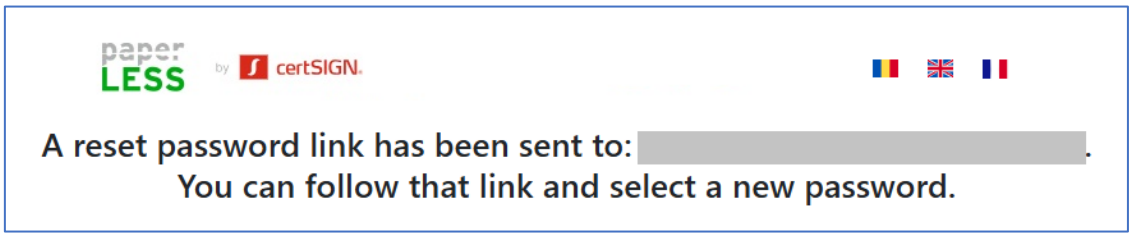
If you have forgotten the password of your Paperless webSIGN account, go to https://websign.ro and click **Forgot your password?**



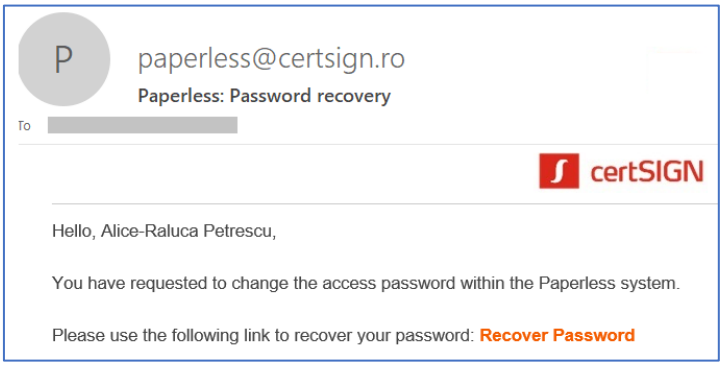
Enter the email address associated to your Paperless webSIGN platform account and press the **Send** button.



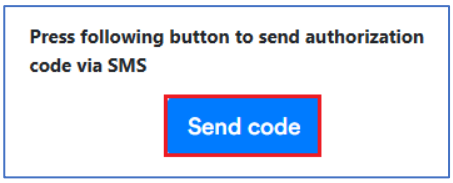
You will receive a password recovery email to the email address associated to your Paperless webSIGN account.



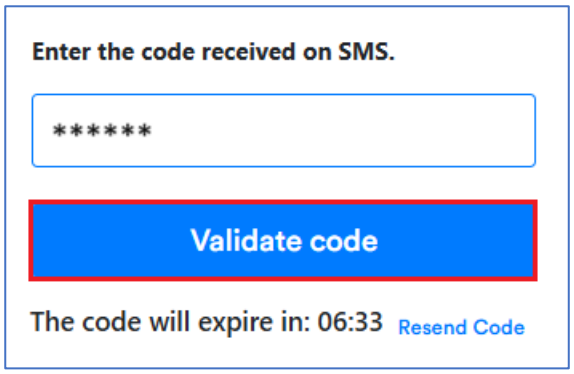
Open your email and follow the **Recover password** link.



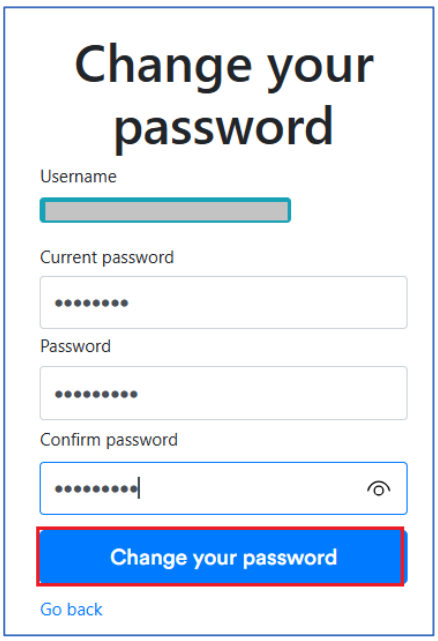
Click **Send code** to receive a code by SMS to the phone number associated to your Paperless webSIGN account.



Enter the code received on your phone and press the **Validate code** button. If you failed to enter the code within the allotted 10 minutes, near the end of the 10 minutes, the option to request another code is activated. Press the **Resend code** button to receive another code by SMS, but only after 30 minutes.

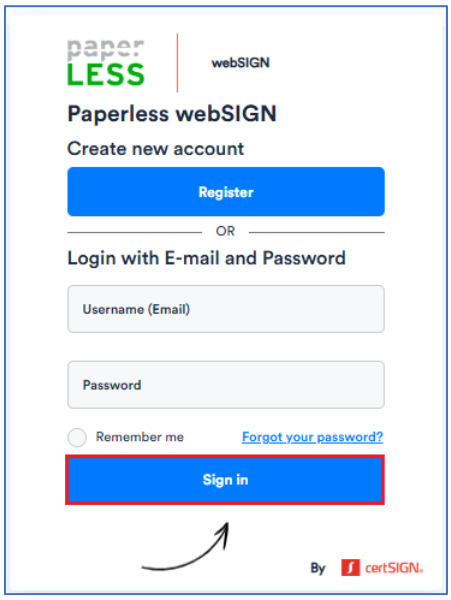


Set a new password, then click the **Change your password** button.

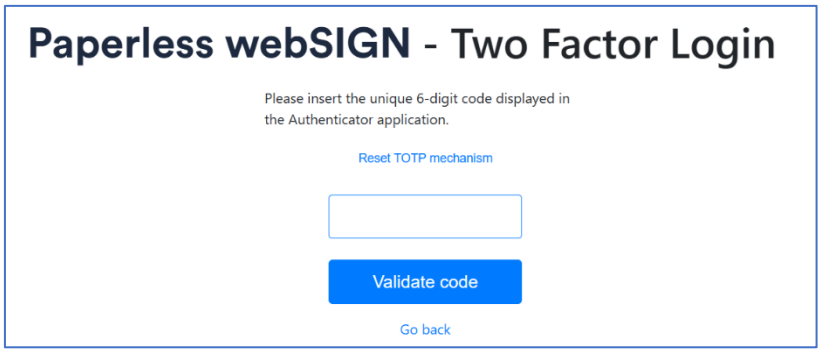


5. Change account phone number

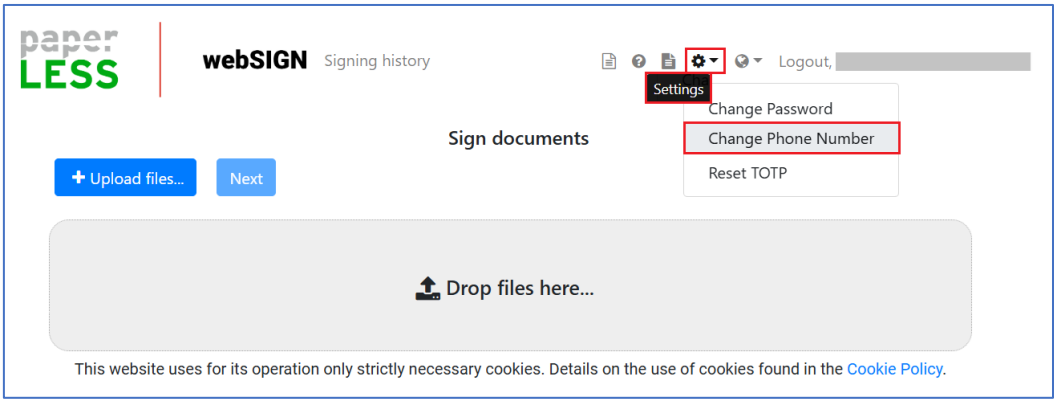
If you want to change the phone number associated to your Paperless webSIGN account, please go to https://websign.ro using the same email and password you signed up with.



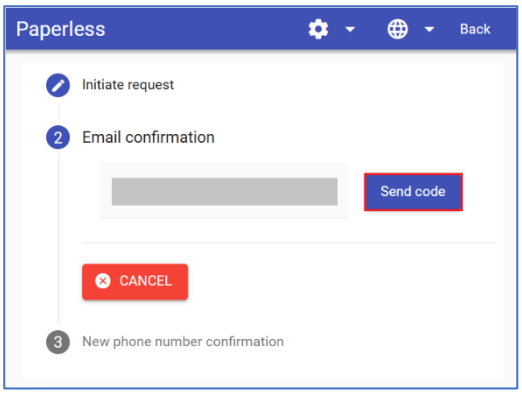
If you have set the 2FA authentication, you will be prompted to enter an authorisation code from the Authenticator app on your phone. .



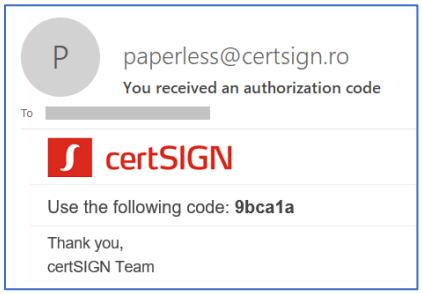
Go to **Settings** and select **Change phone number**.



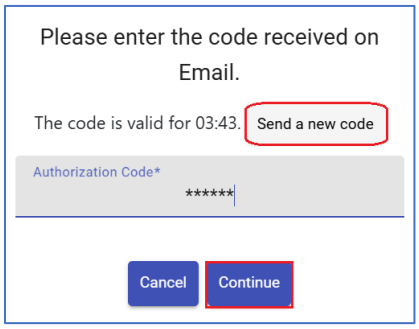
Confirm that you have access to the email address associated to the account in the Paperless webSIGN platform. Press the **Send code** button to receive the authorisation code by email.



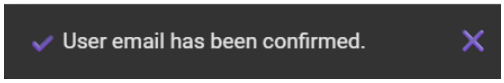
Open the email with the subject: **You have received an authorisation code** and copy that code.



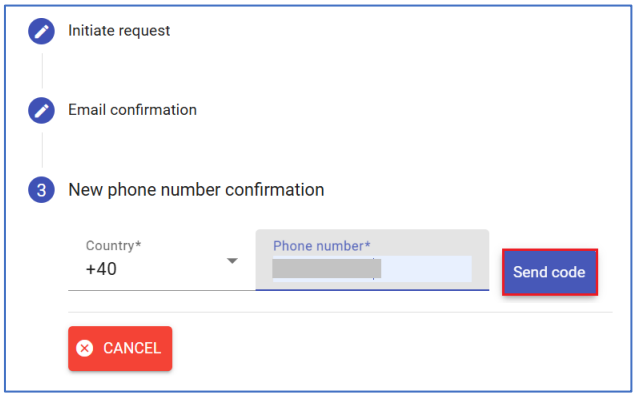
Enter the authorisation code you received in your email and click **Continue**. If you failed to enter the code within the allotted 5 minutes, click **Send a new code** to receive another one by e-mail, but only after 30 minutes.



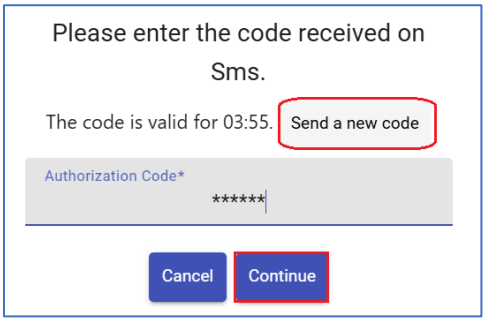
At the bottom of the page you will be informed that your e-mail address has been confirmed.



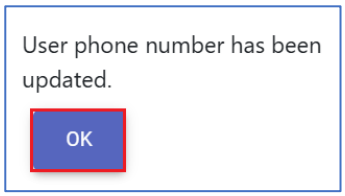
Select the country prefix and enter the phone number you want to associate with your Paperless webSIGN account and press the **Send code** button.



Enter the authorisation code received by SMS and click **Continue**. If you failed to enter the code within the allotted 5 minutes, press the **Send a new code** button to receive another SMS with an authorisation code, but only after 30 minutes.

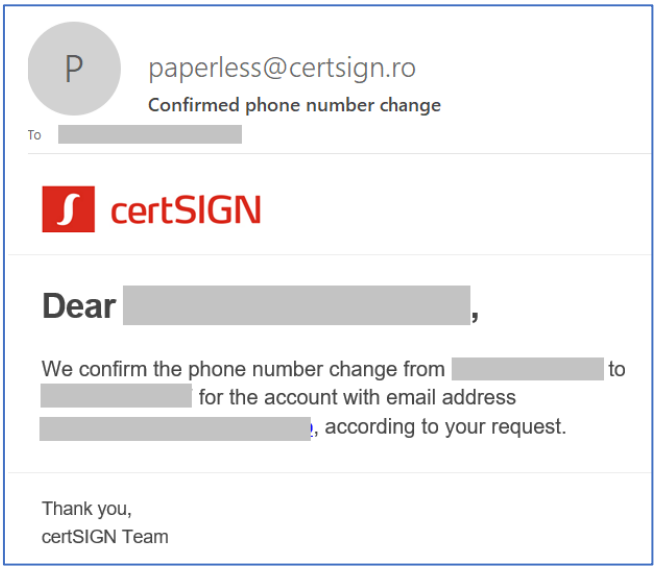


A message confirming that the phone number has been updated is displayed. Click **OK** to close it.



You will be redirected to the https://websign.ro platform, where you need to log in with the e-mail address you registered with and the corresponding password.

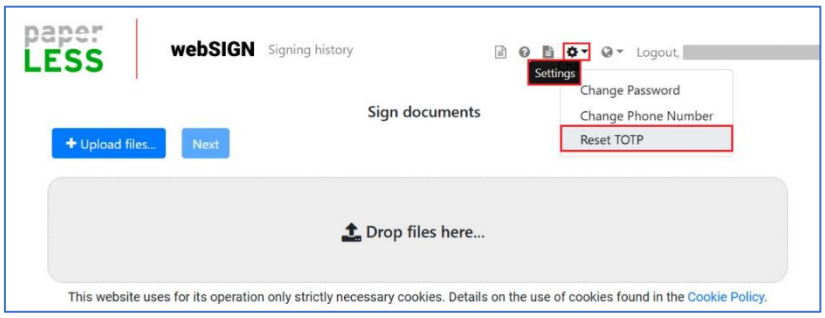
On the e-mail address associated to your Paperless webSIGN account, you will receive an e-mail confirming the phone number change.



6. Pair again the phone app with your Paperless webSIGN account

In case the authorisation code is no longer accepted (pairing has been blocked or you have changed your phone) you can pair again the app on your phone with your Paperless webSIGN account by requesting the reset from the platform itself.

1. Open Paperless webSIGN in Google Chrome. Go to Settings and select the **Reset TOTP** option.

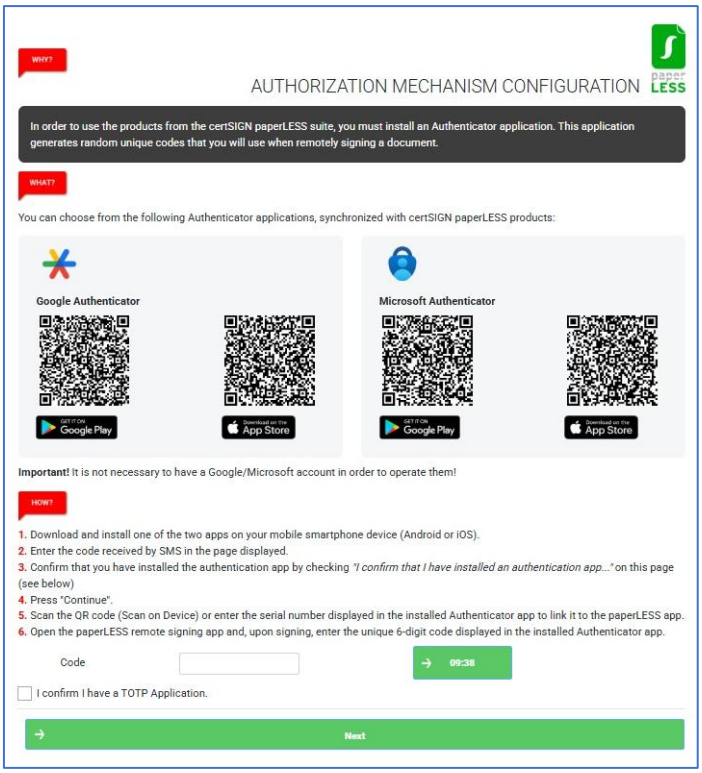


2. Press the **Reset TOTP mechanism** button to open the pairing page.

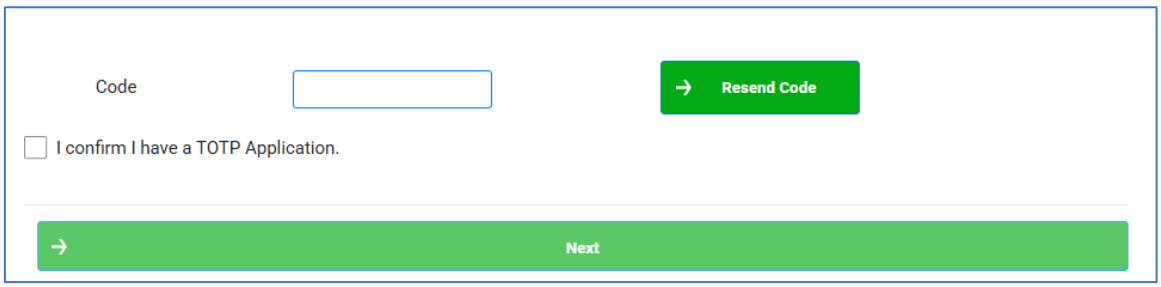
3. Scroll down to the bottom of the page, enter the code you received by SMS when prompted to reset the TOTP mechanism, tick that you have the authorisation app installed and press **Next**.

If you don't have any of the authorisation apps installed on your phone, then install one.

If you already have one installed, delete your previous certSIGN Paperless account.

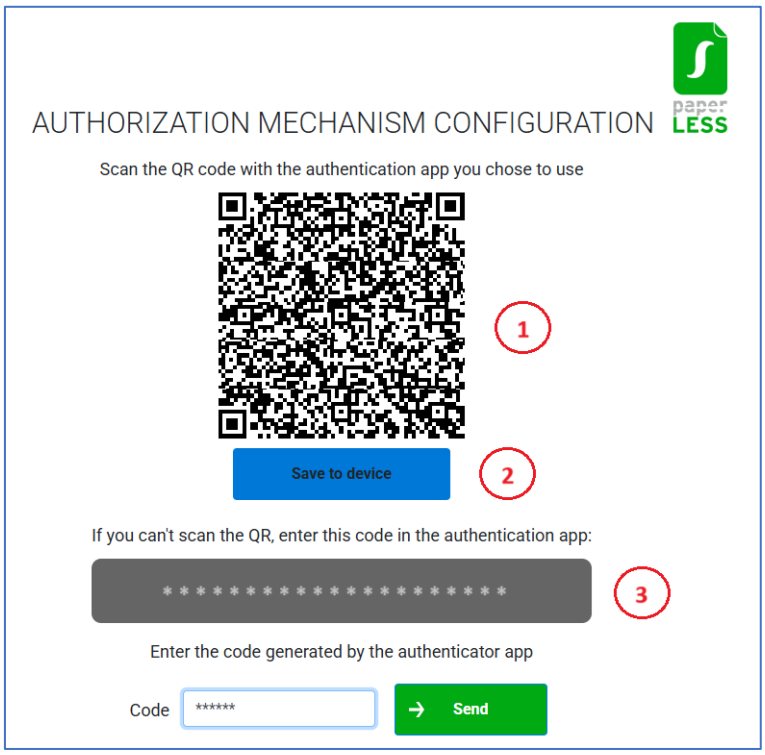


4. If you failed to enter the code within the allotted 10 minutes, at the end of the 10 minutes, the timer next to the **Authorisation Code** field stops. Press the **Resend code** button to receive another code by SMS, but not before 30 minutes.



5. Scan the QR code with the authorisation app on your phone, then enter one of the authorisation codes displayed on your phone in the field below the QR code and press **Send code**.

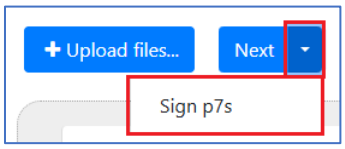
The mechanism will be paired again and you will be redirected to the signing platform to upload your documents.



7. Sign with the qualified digital certificate for remote signing

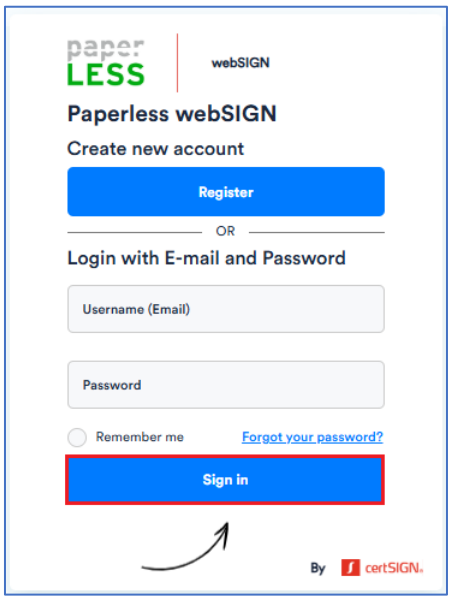
7.1. Sign using Paperless webSIGN

The Paperless webSIGN platform supports the online signing of non-editable, unlocked and password-free .pdf and non-.pdf documents on Windows and macOS. .pdf documents will have an internal signature and can be verified and viewed using the free Adobe Acrobat Reader DC application. Non-.pdf documents will be signed as .p7s and can be verified and viewed using the clickSIGN application, which is also provided by certSIGN. To sign with the .p7s extension and .pdf files, click the arrow at the right of the **Next** button.

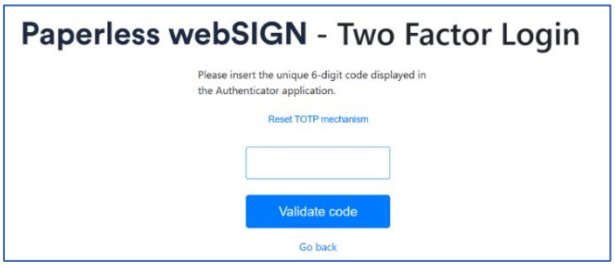


Please note! Smart .pdf documents (such as ANAF forms and declarations) CANNOT be signed in the Paperless webSIGN platform. They can only be signed locally, on Windows or macOS, using the Adobe Acrobat Reader DC application, after locally importing the certificate through the virtual token application, Paperless vToken.

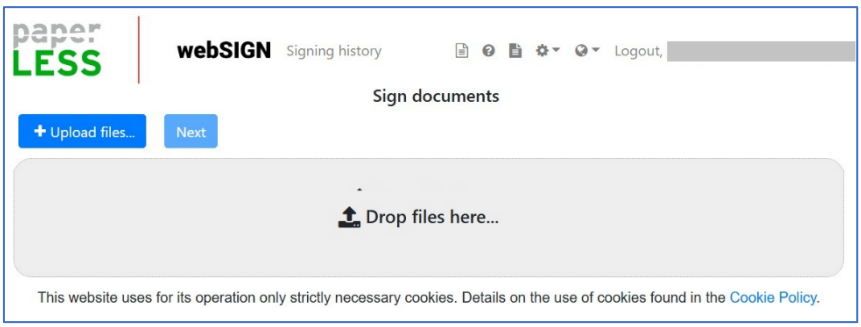
.**1.** In order to sign using Paperless webSIGN you must be logged in, with the user name and password previously created, on the Paperless webSIGN webpage from the address provided at the time of purchase:



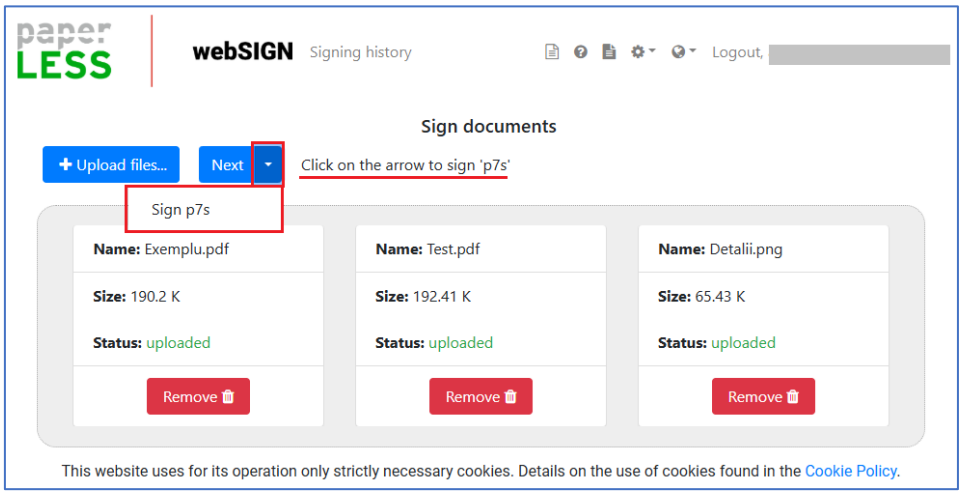
If you have set the 2FA authentication, you will be prompted to enter an authorisation code from the Authenticator app on your phone.



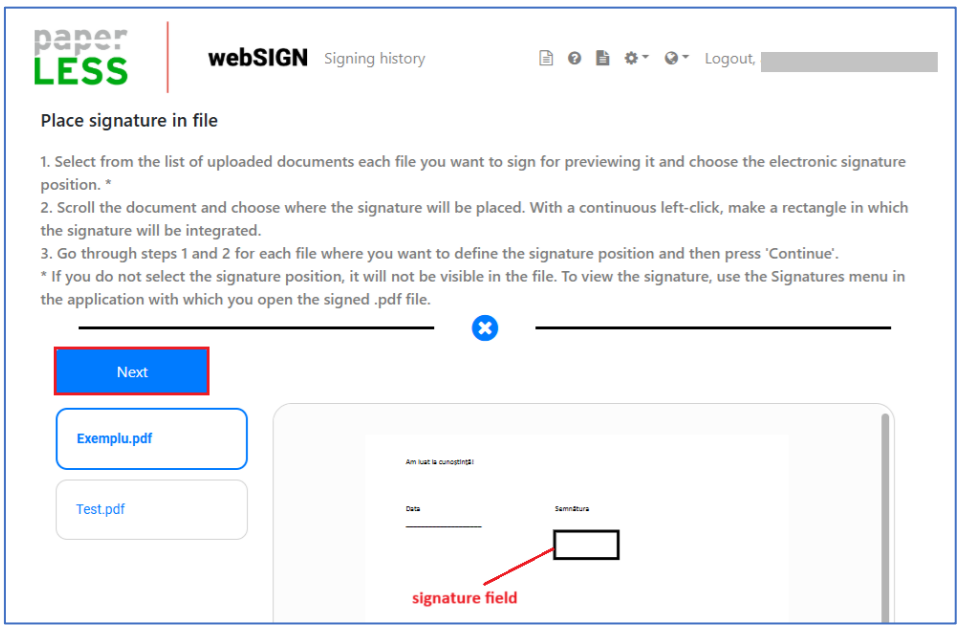
2. Upload the files to sign either by clicking the **Upload files** button or by using the **drag &drop** option.



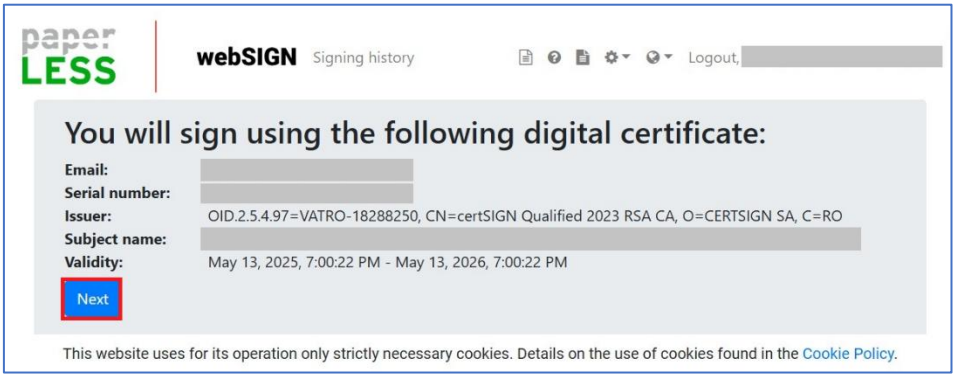
3. Once uploaded, the documents page will be displayed. If you have uploaded a document that you do not want to sign, press the **Remove** button. To proceed to the signing stage, press the **Next** button (to keep the .pdf documents in the same .pdf format) or click  to sign all the documents as.p7s.



4. To create a visible signature on .pdf documents, select each individual document, draw the signature placeholder, and press the **Next** button. If you want an invisible signature, click **Next** without setting the signature placeholder.

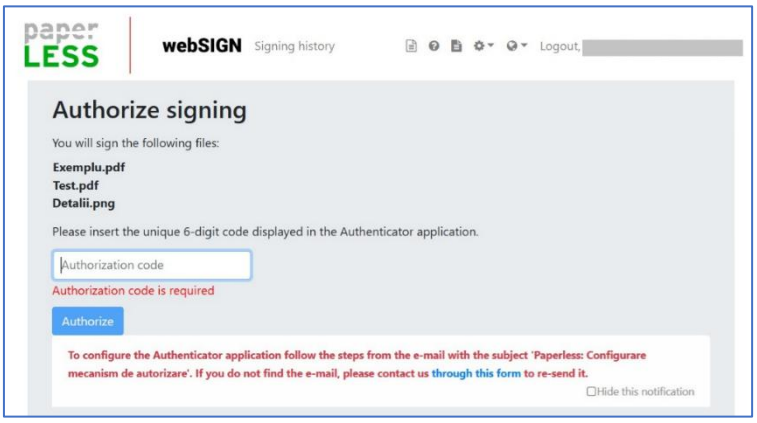


5. After uploading the documents, the details of the digital certificate to be used for signing will be displayed. Press the **Next** button to continue signing with the presented certificate.

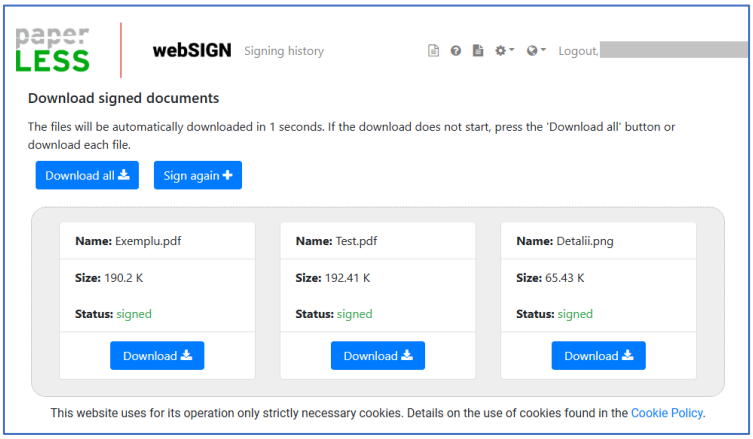


6. To authorise the signing of documents you need to enter the code displayed by the authorisation extension in your browser. A code is valid 30 seconds after it appears. Once entered, press the **Authorise** button.

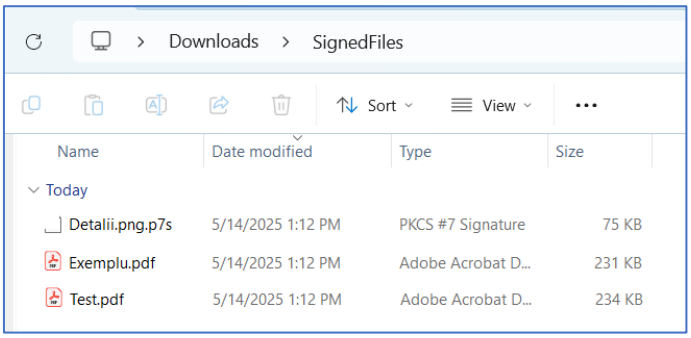
Note: *If you have not configured the authorisation application, please refer to the information in Chapter 1 of this document. If you have these settings, you can tick the* ***Hide this notification*** *check box so that the next time you sign, this message will no longer be displayed*.



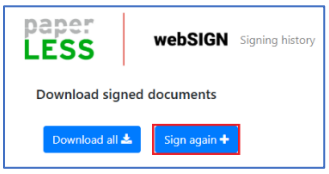
7. After signing, the download page is displayed and the files are automatically downloaded in a zip archive, as **SignedFiles.zip** in the Downloads folder. You can also download the files individually by clicking the **Download** button below each document.



8. After signing, .pdf documents keep their .pdf extension and are signed inside, while those with a different extension (non-.pdf) are signed with a .p7s signature.



9. If you want to continue signing other documents, go to **Sign again**.



7.2. Sign documents on a local station

After issuing the digital certificate in the Paperless webSIGN platform, you can sign various types of documents locally: .pdf (using Adobe Reader), respectively .doc, .docx, .xls, .xlsx (using clickSIGN), on both Windows and macOS, using this digital certificate and the virtual token application, **Paperless vToken**. The application is compatible with Windows operating systems from 10 upwards and macOS from Catalina upwards.

To install the Paperless vToken app, follow the steps below:

1. Download the Paperless vToken app from one of the following links, depending on your operating system:

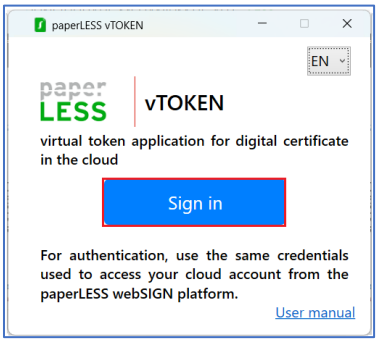
https://www.certsign.ro/vToken/vToken-Launcher.exe – for Windows

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

For Windows, after downloading, you need to install the application.

For macOS, the application is downloaded and updated only through the App Store.

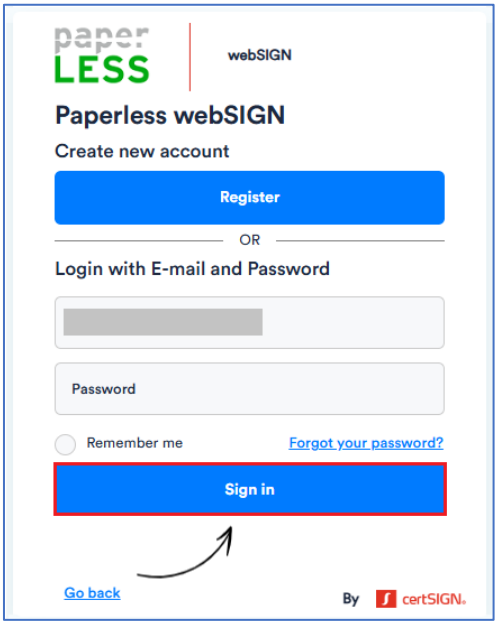
2. Open the Paperless vToken app from the shortcut created on the Desktop during installation and click **Sign in**.



3. On the browser page that opens, enter the email associated with your Paperless webSIGN account and press the **Sign in** button.

4. Enter the password to access your Paperless webSIGN account and press the **Sign in** button.

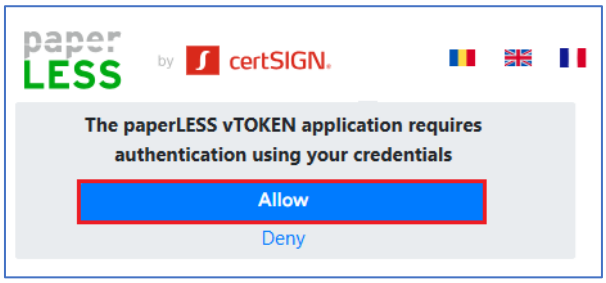
If the e-mail address you entered is not the correct one, press the **Go back** button and repeat the step to enter the correct e-mail address.



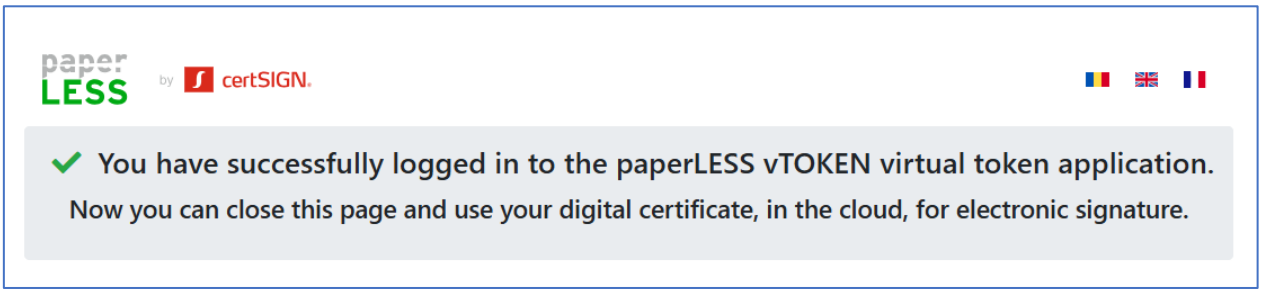
If you have set the 2FA authentication, you will be prompted to enter an authorisation code from the Authenticator app on your phone.

.

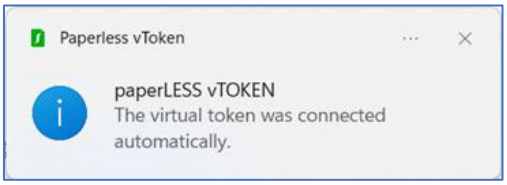
5. The app will prompt you to give permission to authenticate with the credentials you entered earlier. Press the **Allow** button to continue access.



6 You will receive a notification indicating successful authentication in the Paperless vToken application.



7. The app will also open in the System Tray section. Upon opening, the qualified digital certificate for remote signing will be automatically imported into the operating system's certificate store and can be used to sign .pdf, .doc, .docx, .xls, .xlsx documents.



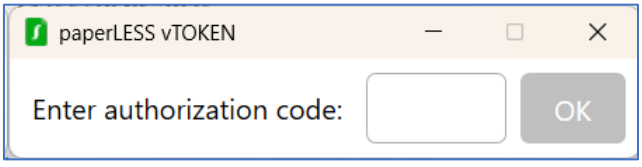
8. For signing .pdf, .doc, .docx, .xls, .xlsx documents, use the signing tools integrated in the applications designed for these types of files, namely:

– Adobe Reader for .pdf fles;

– Word for .doc, .docx files;

– Excel for .xls, .xlsx files.

To authorize signing you need to enter the authorisation code from the previously installed auth application.



8. Use a qualified digital certificate for remote signing to sign in on online platforms

After issuing the digital certificate in the Paperless webSIGN platform, you can access various web platforms that require digital certificate authentication on both Windows and macOS using this digital certificate and the virtual token application, Paperless vToken. The application is compatible with Windows operating systems from 10 upwards and macOS from Catalina upwards.

To install the Paperless vToken app, follow the steps below:

1. Download the Paperless vToken app from one of the following links, depending on your operating system:

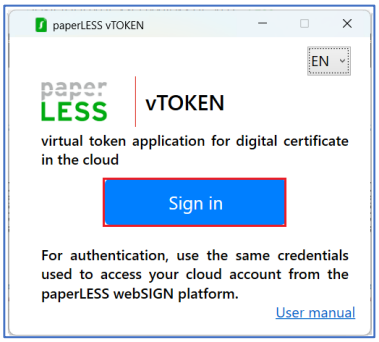
https://www.certsign.ro/vToken/vToken-Launcher.exe – for Windows

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

For Windows, after downloading, you need to install the application.

For macOS, the application is downloaded and updated only through the App Store.

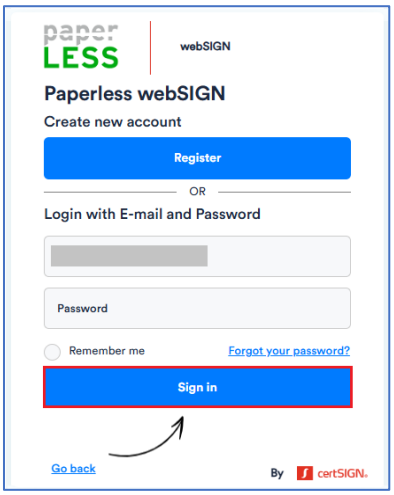
2. Open the Paperless vToken app from the shortcut created on the Desktop during installation, then press the **Sign in** button.



3. On the browser page that opens, enter the email associated with your Paperless webSIGN account and press the **Sign in** button.

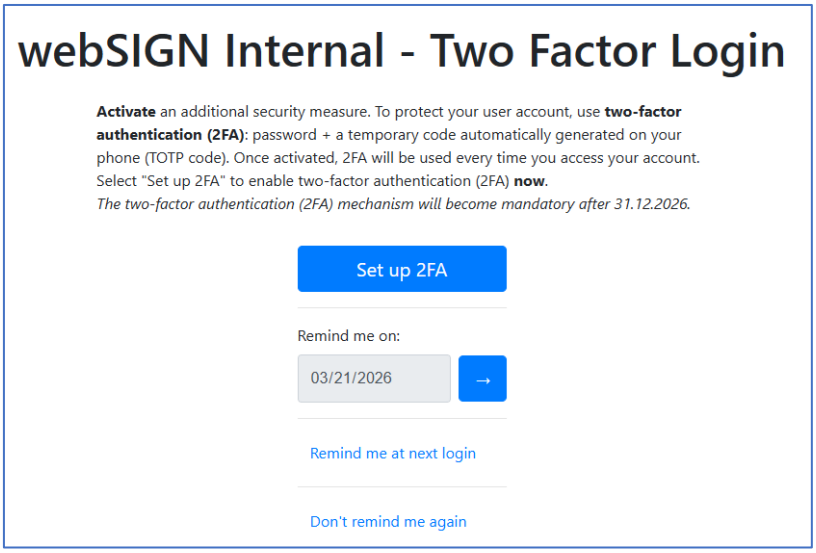
4. Enter the password to access your Paperless webSIGN account and press the **Sign in** button.

If the e-mail address you entered is not the correct one, press the Go back button and repeat the step to enter the correct e-mail address.

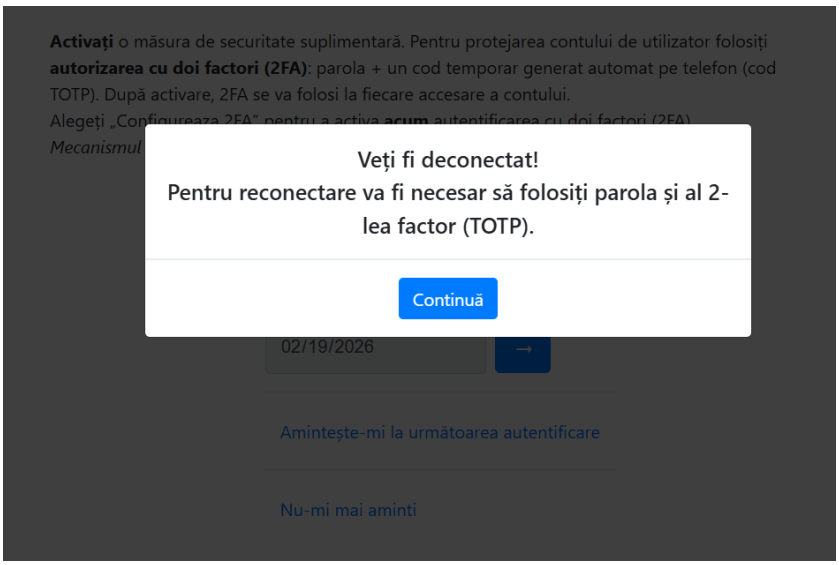


If you have set the 2FA authentication, you will be prompted to enter an authorisation code from the Authenticator app on your phone. .

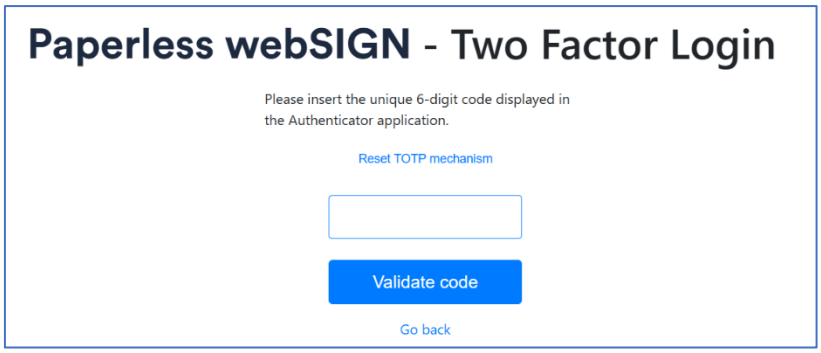
If you haven't set the 2FA authentication but want to do so now, press **Set up 2FA.** .



A pop-up message will appear to inform you that you will be logged out. When you log back in, you will need to enter an authorisation code from the Authenticator app that you have already set up on your phone, after entering your username and password. Press the Continua/Next button.

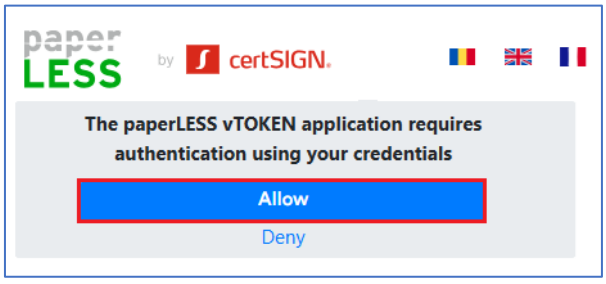


After logging in with your account password, you will be prompted to enter the authorization code displayed by the Authenticator app on your phone. .

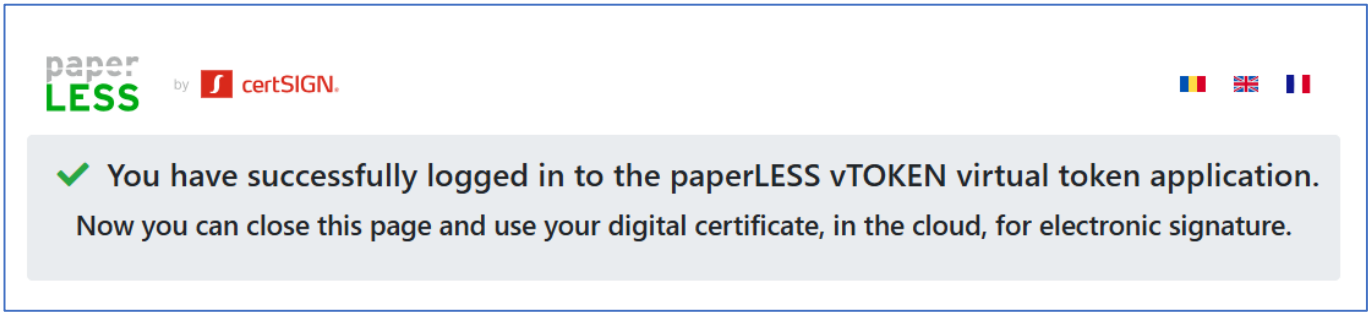


If you haven't set the 2FA and don't want to do so now, choose one of the deferral options. .

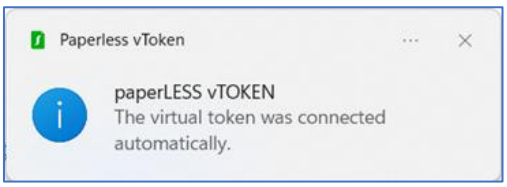
5. The app will prompt you to give permission to authenticate with the credentials you entered earlier. Press the **Allow** button to continue access.



6. You will receive a notification indicating successful authentication in the Paperless vToken application.



7. The app will also open in the System Tray section. Upon opening, the qualified digital certificate for remote signing will be automatically imported into the operating system's certificate store and can be used for authentication on various web platforms that require a qualified digital certificate.



8. To authenticate, open the web platform of your choice, select the qualified digital certificate displayed, then enter the authorisation code (from the authorisation app installed on your phone) to authorise authentication.