Polskie Sieci Elektroenergetyczne

Portal Uczestnika Rynku Mocy
User Manual

Account Establishment, Login and Bidder Role Assignment

Version: 1.0

Konstancin-Jeziorna 2026

Update history

Date	Company	Version	Update details
03.08.2026	PSE S.A.	1.0	Publication of the document

Copyright © 2026 PSE S.A.

This document is the property of PSE S.A. and may be used only for the purpose for which it was made available.

Copying or distribution of the document, in whole or in part, in any form, is prohibited without prior written consent of PSE S.A.

TABLE OF CONTENTS

1 TECHNICAL REQUIREMENTS 4
2 USER ACCOUNT ESTABLISHMENT 5
2.1 Registration using SMS code 10
2.2 Registration using OTP authentication 11
3 LOGGING INTO PURM 16
3.1 SMS code verification 17
3.2 OTP code verification 18
4 MAIN MENU 21
5 CHANGING THE AUTHENTICATION METHOD 22
5.1 Changing the authentication method to OTP code 22
5.2 Changing the authentication method to SMS code 23
5.3 Changing the default authentication method 24
5.4 Deactivating the OTP code authentication method 25
6 ASSIGNMENT OF THE RIGHTHOLDER AND BIDDER ROLE 27
6.1 Section I – General information 27
6.2 Section II – Capacity provider's identification data 28
6.3 Section III – Appendixes 29
6.4 Application signature 30
7 REVOCATION OF THE RIGHTHOLDER AND BIDDER ROLE 33
7.1 Section I – General information 33
7.2 Section II – Capacity provider's identification data 34
7.3 Section III – Appendixes 35
7.4 Application signature 36
8 BROWSING APPLICATIONS FOR THE ASSIGNMENT/REVOKEMENT OF THE RIGHTHOLDER/BIDDER ROLE 39
9 MANAGMENT OF RIGHTHOLDER/BIDDER ROLES 41
9.1 User account creation 41
9.2 Deactivation of the created user account 43
9.3 Granting rights to entity 44

1 TECHNICAL REQUIREMENTS

To use the Portal Uczestnika Rynku Mocy (PURM), you must have a computer with Internet access. Detailed technical requirements are available at https://www.pse.pl/web/pse-eng/areas-of-activity/capacity-market/purm-register.

2 USER ACCOUNT ESTABLISHMENT

PURM can be accessed at the address https://purm.pse.pl/.

User may change the language to English by clicking on the flag in the upper right corner.

NOTE: The possibility to switch to English language is only available on the homepage.

User account establishment starts by clicking "**Register**".

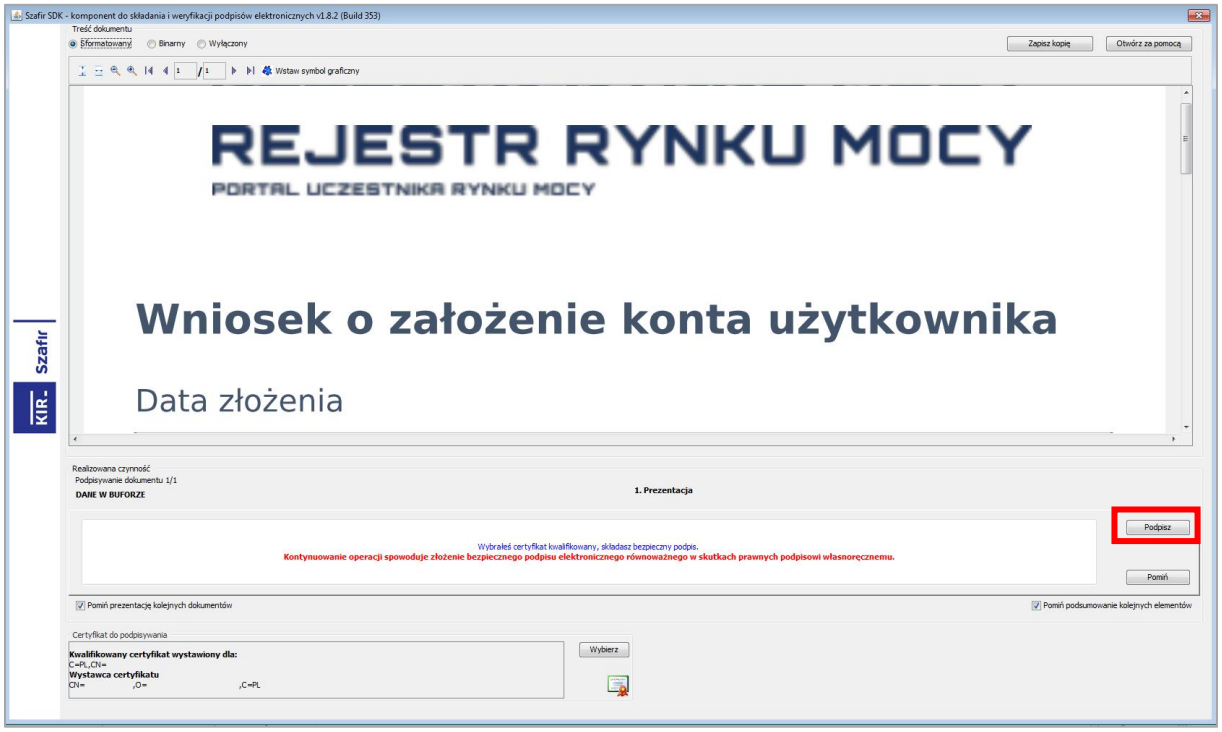
PURM requires user to fill a registration form with the following data:

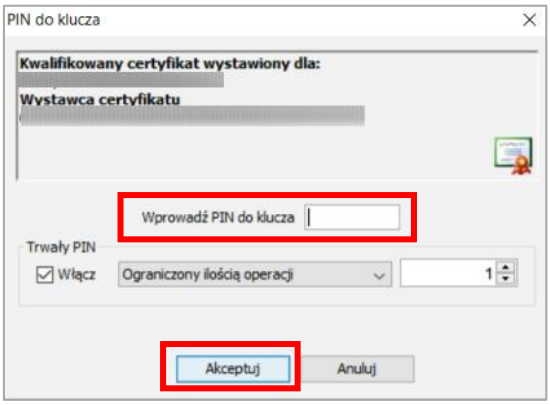
- **Name,**
- **Surname,**
- **E-mail address,**
- **Phone number.**

Mandatory fields are marked with an asterisk " * ".

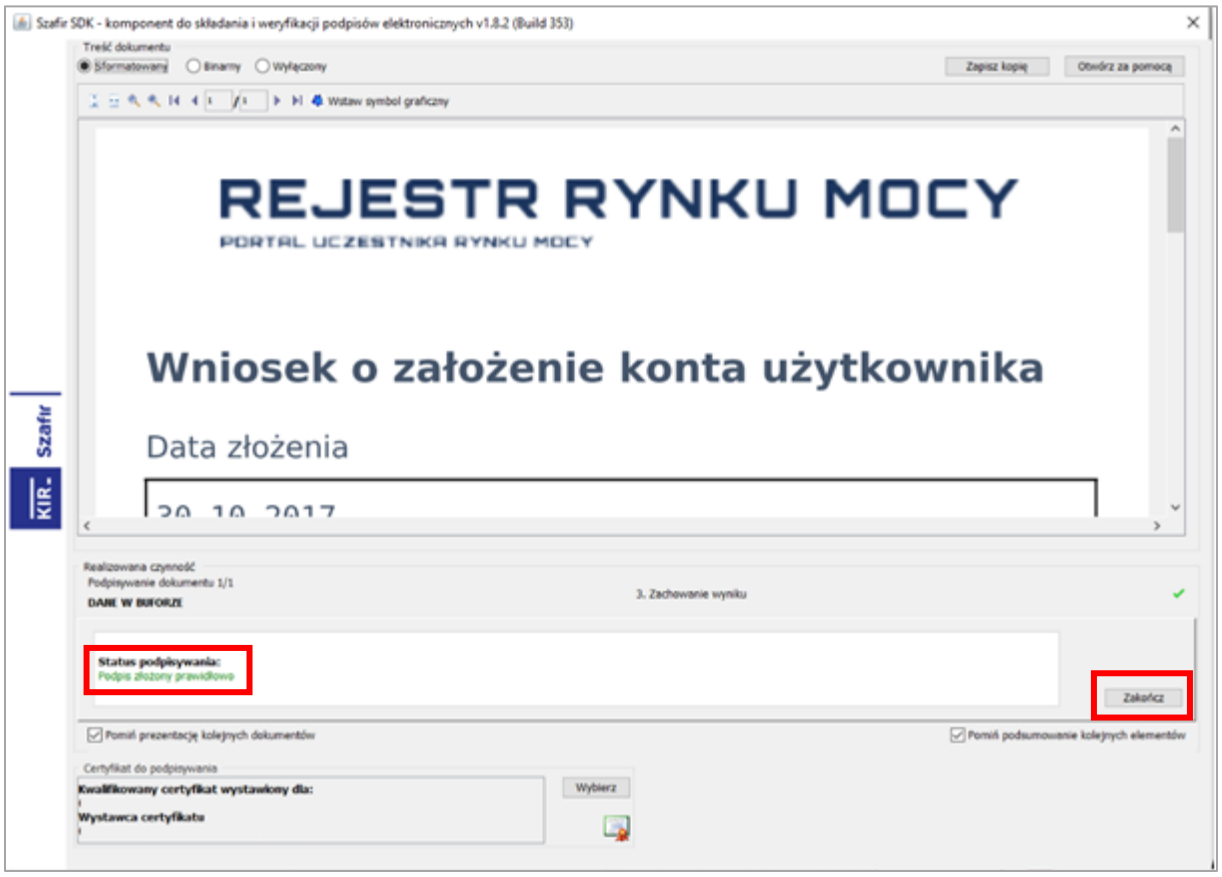
NOTE: Each user account must be assigned with a unique e-mail address. It is forbidden to set up several accounts using the same e-mail address.

After filling all mandatory fields, the process of account establishment shall be continued by clicking **"Sign with the qualified electronic signature**". PURM shall then generate an application for account establishment, which must be signed with user's qualified electronic signature. Signature shall be made by clicking "**Podpisz**" (*Sign*) and entering the PIN code assigned to the qualified electronic signature followed by clicking "**Akceptuj**" (*Confirm)*.


Szafir SDK - komponent do składania i weryfikacji podpisów elektronicznych v1.8.2 (Build 353)
Treść dokumentu
Sformatowany
Binarny
Wyłączony
Zapisz kopię
Otwórz za pomocą
Wstaw symbol graficzny
REJESTR RYNKU MOCY
PORTAL UCZESTNIKA RYNKU MOCY
Wniosek o założenie konta użytkownika
Data złożenia
Szafir
KIR
Realizowana czynność
Podpisywanie dokumentu 1/1
DANE W BUFORZE
1. Prezentacja
Podpisz
Wybrałeś certyfikat kwalifikowany, składasz bezpieczny podpis.
Kontynuowanie operacji spowoduje złożenie bezpiecznego podpisu elektronicznego równoważnego w skutkach prawnych podpisowi własnoręcznemu.
Pomiń
Pomiń prezentację kolejnych dokumentów
Pomiń podsumowanie kolejnych elementów
Certyfikat do podpisywania
Kwalifikowany certyfikat wystawiony dla:
C=PL,CN=
Wystawca certyfikatu
CN= ,O= ,C=PL
Wybierz


PIN do klucza
Kwalifikowany certyfikat wystawiony dla:
Wystawca certyfikatu
Wprowadź PIN do klucza
Trwały PIN
Włącz
Ograniczony ilością operacji
1
Akceptuj
Anuluj

After the application has been signed properly, message "**Podpis złożony prawidłowo**" (*Signature signed properly*) shall be displayed in the signature submission window.

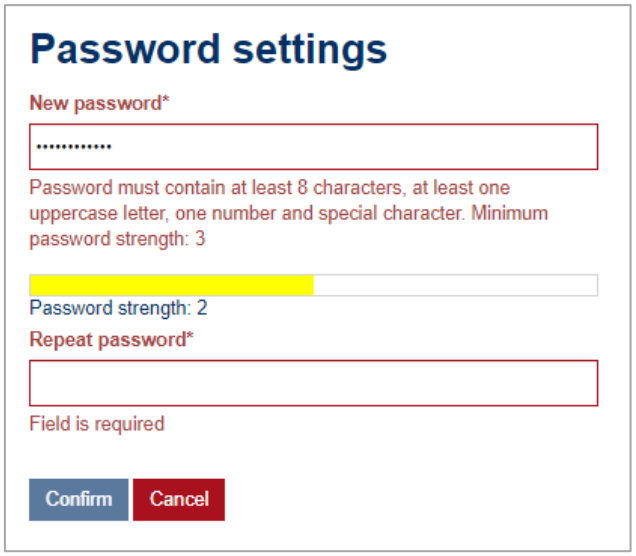


After signing the document and clicking "**Zakończ**" (*Finish*), PURM shall send an activation link to the e-mail address provided within the application. In order to proceed to the next step, user shall click on the sent link or copy it to the address bar of the internet browser in order to launch the webpage. User account activation shall be finalized by setting a password.

The password shall:

- consist of a minimum of 8 characters,
- contain at least one capital letter, one number and one special character.

An additional criterion is the strength of the password, the evaluation of which is displayed to the user under the password entry field. PURM accepts passwords with strength of 3 or more. If the entered password does not meet both conditions, an error will be displayed.

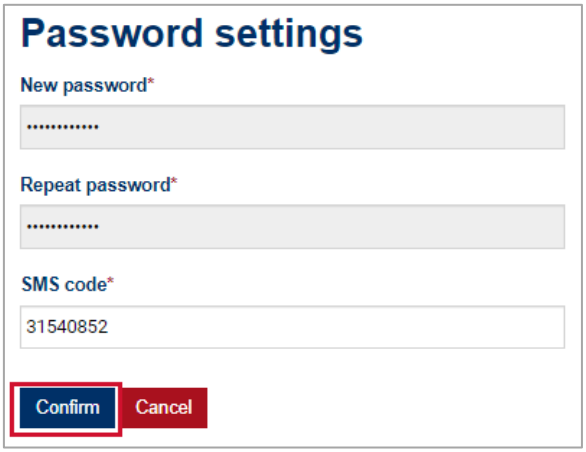


If the password meets both conditions, user shall re-enter it in the field marked as "**Repeat password**". If the passwords in both fields are identical, user is able to confirm defined password by clicking "**Confirm**".

After that, PURM shall send an SMS code to the phone number provided within the application.

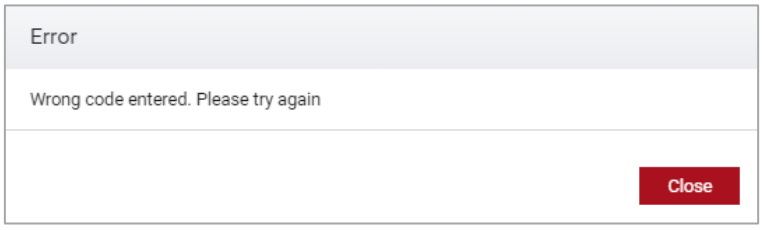
2.1 Registration using SMS code

In order to end the password setting process, received SMS code shall be entered into the "**SMS code**" field and confirmed by clicking "**Confirm**".



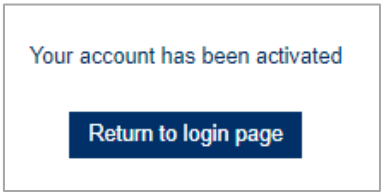
NOTE: The SMS code is active for 20 minutes. After this time, the code expires and it is necessary to go through the password setting process again.

If an SMS code is entered incorrectly, an error "**Wrong code entered. Please try again.**" will be displayed.



NOTE: After 3 unsuccessful attempts, the SMS code expires and it is necessary to go through the password setting process again.

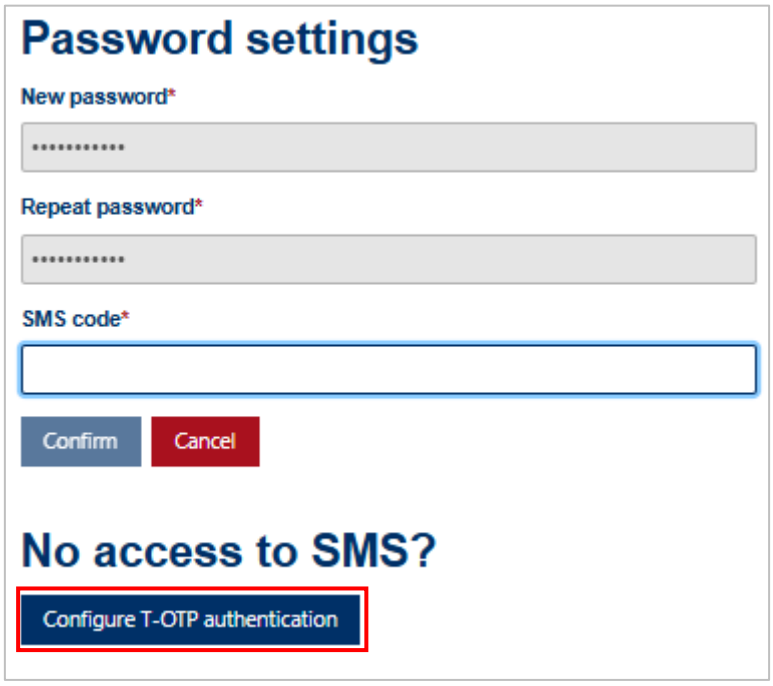
After successful verification of the SMS code, user account is activated and assigned with a defined password. Account activation is confirmed by sending an e-mail to the address provided within the application. A message confirming the account activation is also displayed.



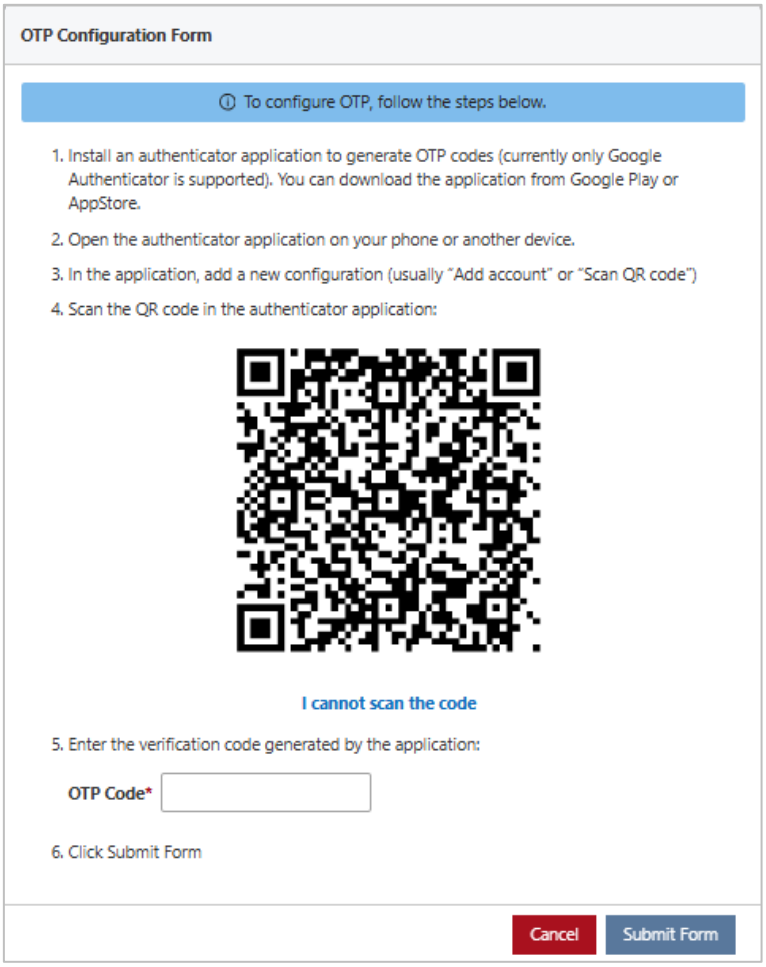
NOTE: Confirmation contains user's account number using which user is able to log into PURM with. Alternatively, e-mail address provided during account establishment can also be used.

2.2 Registration using OTP authentication

After confirming the password by clicking the "Confirm" button, the user may choose an alternative authentication method instead of the SMS code verification. To do this, click the "Configure T-OTP authentication" button.



After clicking the button, an OTP Configuration Form will open. To link the account to the authenticator app that generates one-time OTP codes, follow the instructions in the OTP configuration form.



NOTE: Currently the only supported authenticator app is Google Authenticator.

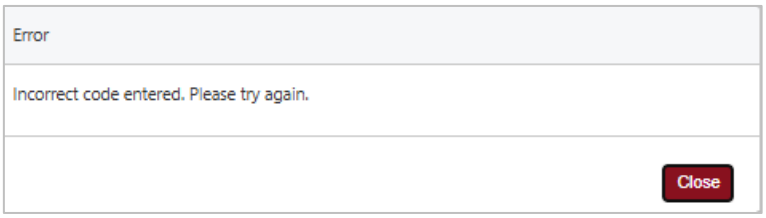
In case of issues with scanning the QR code, there is an option of manually entering the data. The user must click the “I cannot scan the code” button and follow the displayed instructions.

The authenticator app will start generating one-time verification codes after successfully linking the authenticator app with the account. The generated code should be entered into the “OTP Code” field visible in the form.

To complete the configuration, click the “Submit Form” button. After successful approval, OTP authentication will be activated and used as the method for verifying identity when logging in or performing operations within the system.

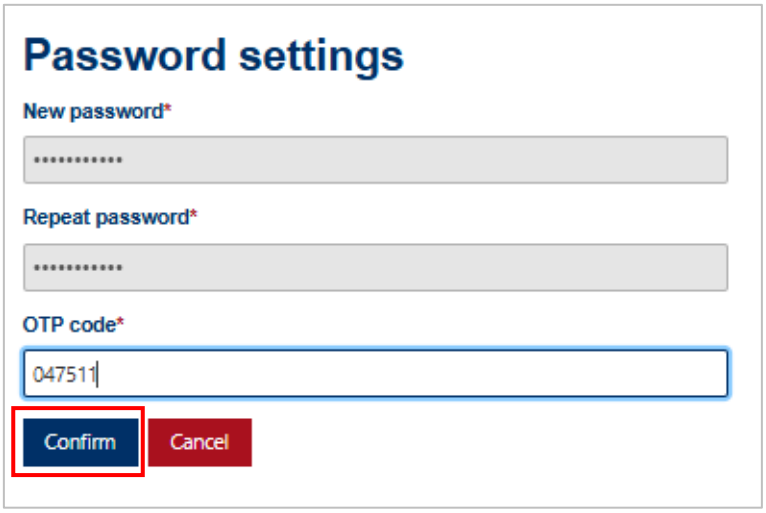
NOTE: The one-time verification code is active for 30 seconds. After that time, the application generates a new code.

If an OTP code is entered incorrectly, an error "**Incorrect code entered. Please try again.**" will be displayed.

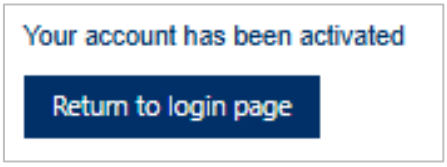


NOTE: After 3 unsuccessful entry attempts, it is necessary to remove and re-add the account in the Google Authenticator app.

To complete the account registration, it is necessary to confirm the password setup in the next step. In the "OTP Code" field the user must enter the one-time 6-digit verification code generated in the authenticator app, and then click the "Confirm" button.



After successful verification of the OTP code, user account is activated and assigned with a defined password. Account activation is confirmed by sending an e-mail to the address provided within the application. A message confirming the account activation is also displayed.

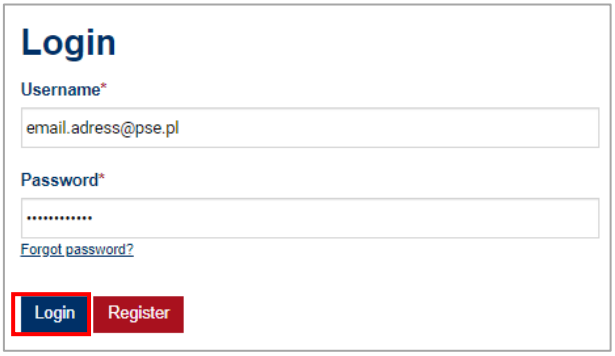


NOTE: The email confirming account activation contains the PURM user account number, which can be used to log in to PURM (alternatively, you can enter the email address provided during registration).

3 LOGGING INTO PURM

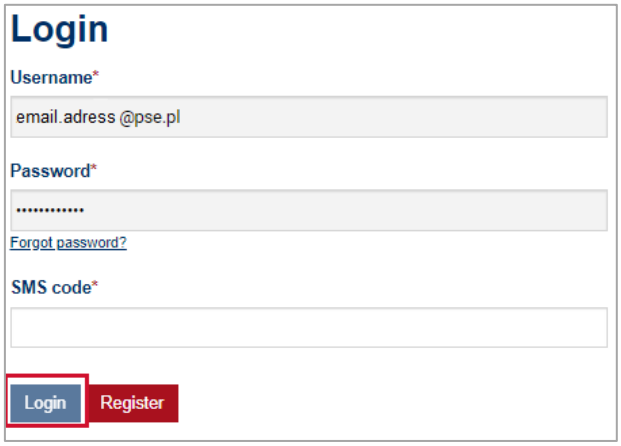
User authorization is carried out by correctly entering the username and password in the main login window.

In order to log into PURM, user shall enter the user account number or e-mail address assigned to the account and password into fields marked as "**User name**" and "**Password**". The entered data shall be confirmed by clicking "**Login**".



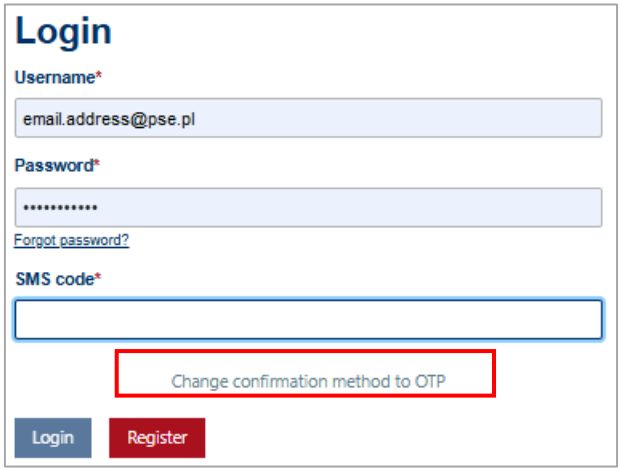
3.1 SMS code verification

If the user name and password are correct, an SMS code is sent to the phone number assigned to the account. The received code shall be entered in the "**SMS code**" field and confirmed by clicking "**Login**".



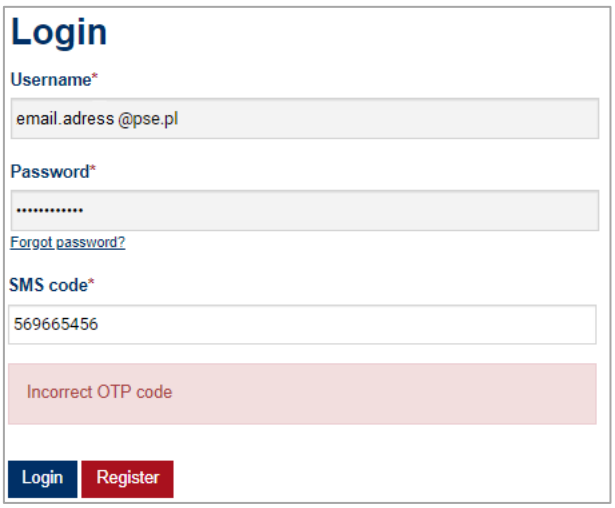
NOTE: The SMS code is active for 20 minutes. After this time, the code expires and it is necessary to log in again.

If the user has **both authentication** methods enabled, then during login it is possible to switch the confirmation method from an SMS code to OTP. The user should click the “Change confirmation method to OTP” button and follow the steps described in section 3.2.



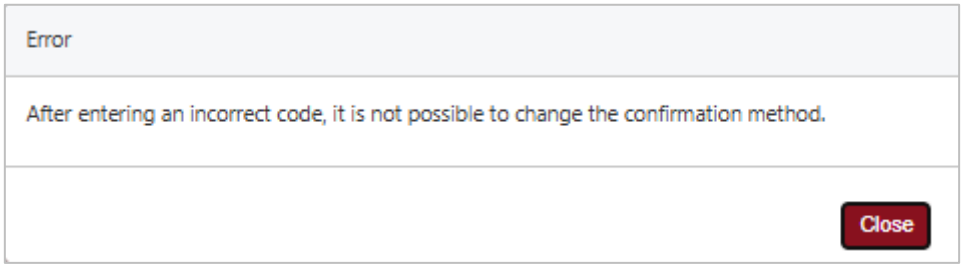
NOTE: Changing the confirmation method does not change the default authentication method.

If the SMS code is entered incorrectly, the message “Incorrect OTP code.” is displayed.



NOTE: After 3 unsuccessful attempts, the SMS code expires and it is necessary to log in again.

NOTE: If the SMS code is entered incorrectly, it is not possible to change the confirmation method to an OTP code. After clicking the "Change confirmation method to OTP" the following message is displayed.

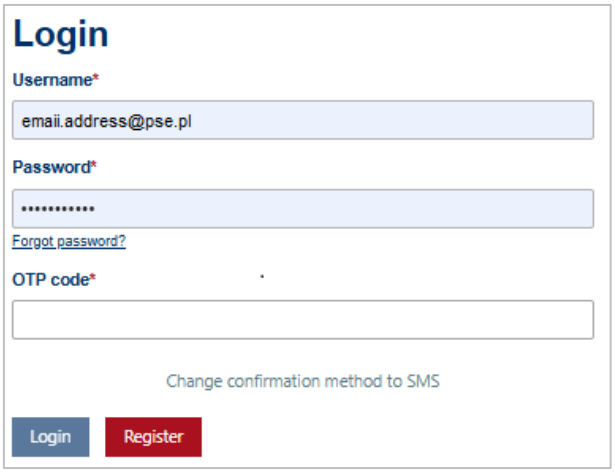


After successful verification of the SMS code, the login process is completed, and the user is redirected to the PURM home page.

3.2 OTP code verification

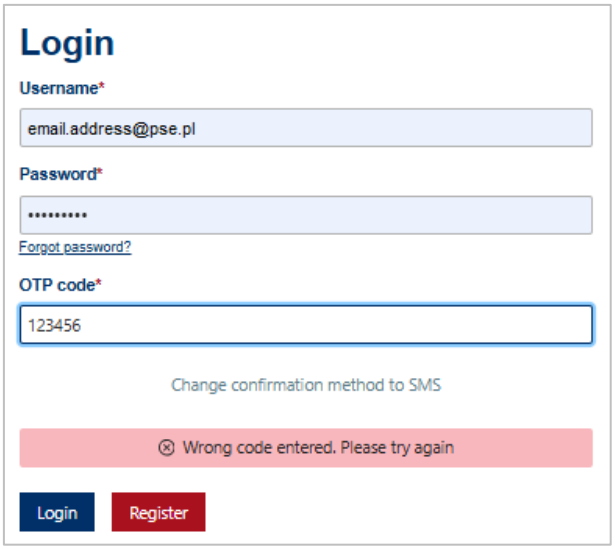
After correctly entering the username and password, the system proceeds to the verification using an OTP code. At this point, the user should open the **Google Authenticator** application and enter the one-time OTP code in the **"OTP Code"** field and confirm by clicking the **"Log in"** button.

If the user has **both authentication methods enabled** and **has not attempted to enter the OTP code**, during login it is possible to change the confirmation method from an OTP code to SMS by clicking the **"Change confirmation method to SMS"** button.



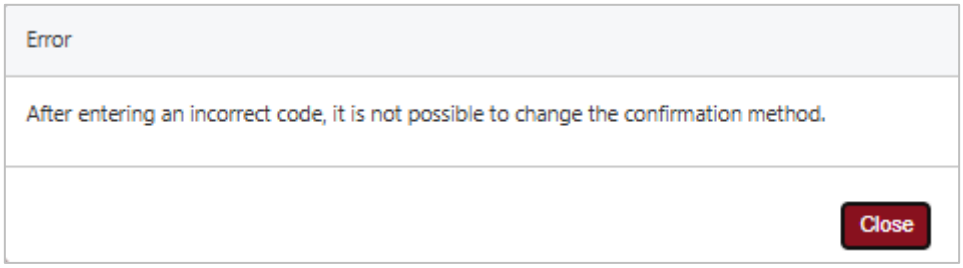
NOTE: Changing the confirmation method does not change the default authentication method.

If an incorrect OTP code is entered, the system will display an error message and allow the user to try again. After the code is entered correctly, the login process is completed, and the user is redirected to the PURM home page.



NOTE: After 3 unsuccessful entry attempts, the OTP code expires and it is necessary to go through the login process again.

NOTE: If the OTP code is entered incorrectly, it is not possible to change the confirmation method to an SMS code. After clicking the "Change confirmation method to SMS" the following message is displayed.

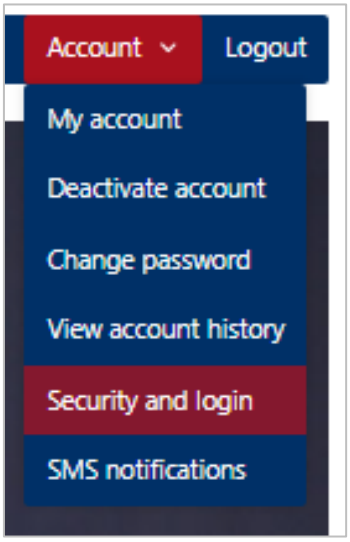

Error
After entering an incorrect code, it is not possible to change the confirmation method.
Close

4 MAIN MENU

PURM menu is available directly after logging in. In the upper right corner, user's Name and Surname is displayed.

5 CHANGING THE AUTHENTICATION METHOD

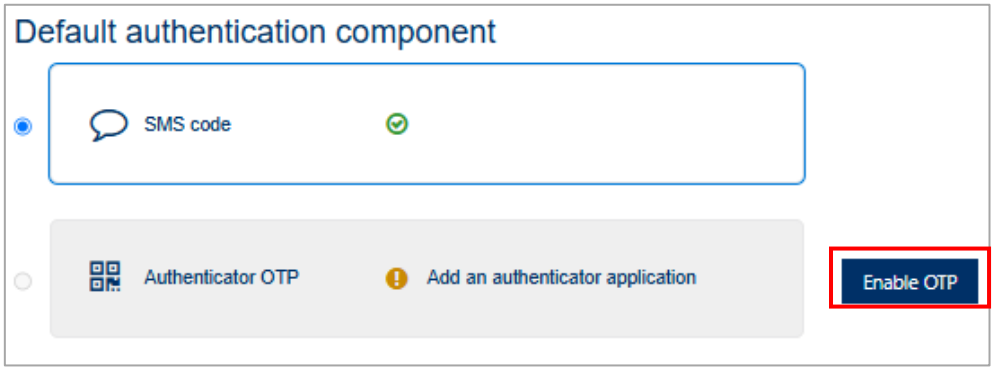
To change the authentication method, the user shall select “Account” from the main menu and then “Security and Login.”



After redirection, the authentication component that was selected by default during login is highlighted.

5.1 Changing the authentication method to OTP code

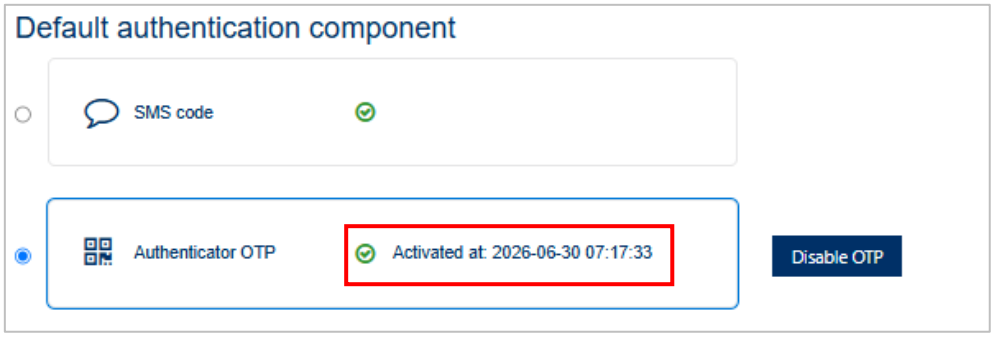
The user may change the authentication method to the OTP code application by using the “Activate OTP” button.



After clicking the „Enable OTP” button, the user shall proceed analogously to the configuration of T-OTP authentication described in section 2.2.

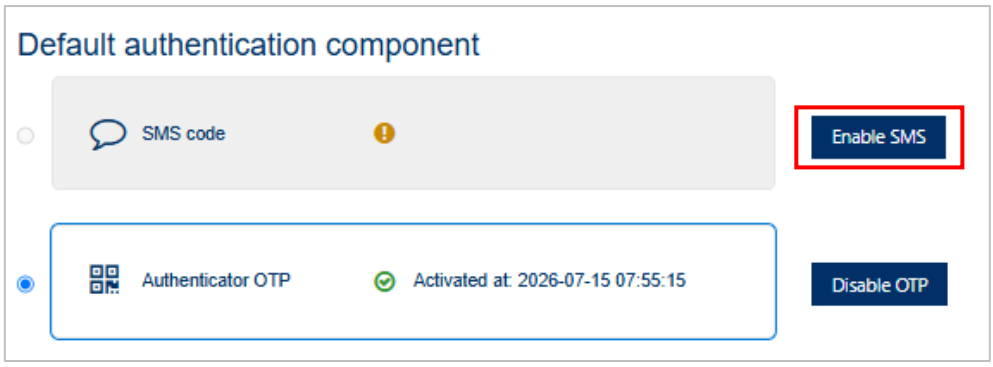
NOTE: If the user already has an account linked to PURM added in the Google Authenticator app, it is recommended to remove the account before reactivating T-OPT authentication.

After OTP code verification, the system confirms authentication together with the activation date, and the user receives an email confirming the activation of the authorization method using an OTP code.

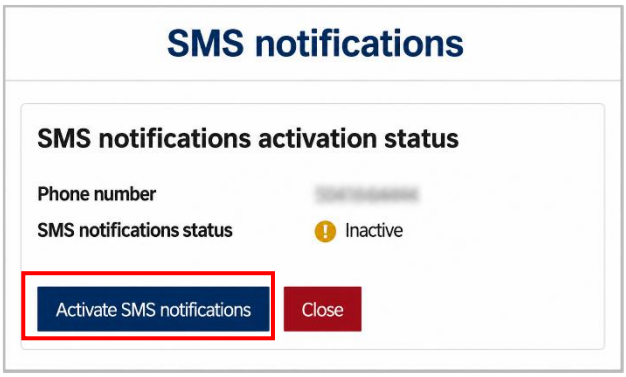


5.2 Changing the authentication method to SMS code

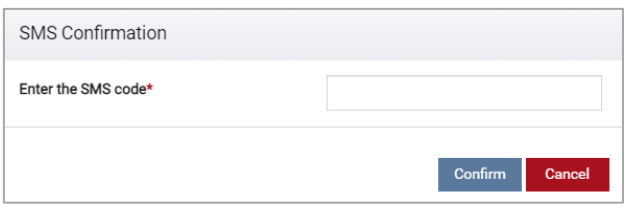
The user may change the authentication method to the SMS code application by using the “Activate SMS” button.



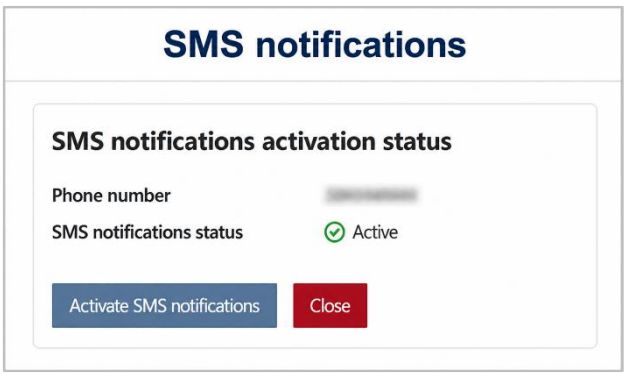
After clicking the „Enable SMS” button, the user is redirected to the “SMS Notification” tab, where the SMS notification status is “Inactive.” To activate SMS code authentication, the user shall use the “Activate SMS Notifications” button.



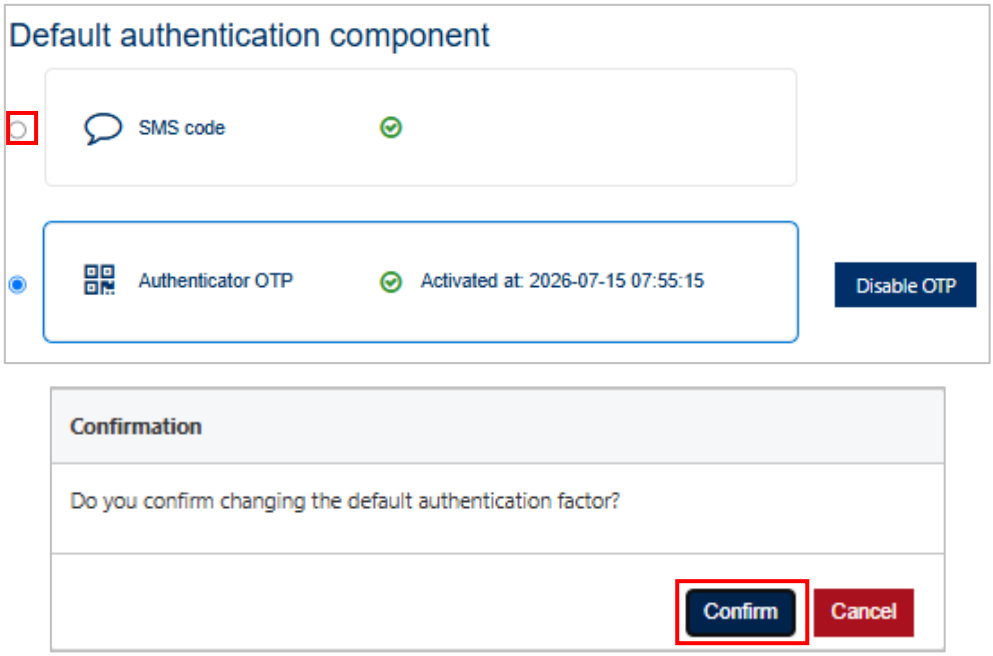
To confirm activating the verification method by SMS codes, the usher shall enter the received SMS code in the **“SMS Confirmation”** field and confirm the activation by clicking the **“Confirm”** button.



The SMS notification status will change to “Active”.

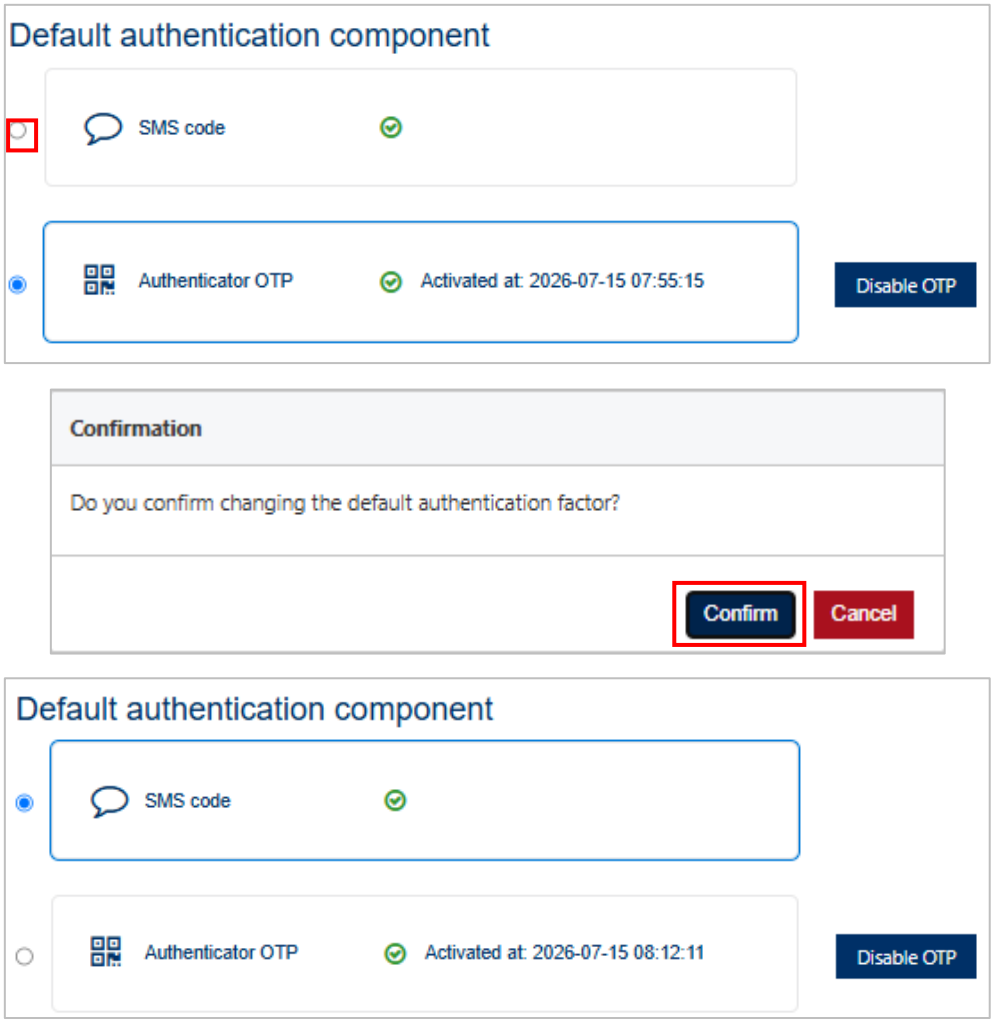


After activating the authentication method, the user may set the SMS code as the default factor in the **“Security and login”** tab. To do this, the user shall select the radio button for the authentication factor **“SMS code”** and confirm the change of the authentication method using the “Confirm” button.



5.3 Changing the default authentication method

If the user has both authentication method, it is possible to change the default authentication method by selecting the corresponding radiobutton and confirm the authentication method by clicking the “Confirm” button.

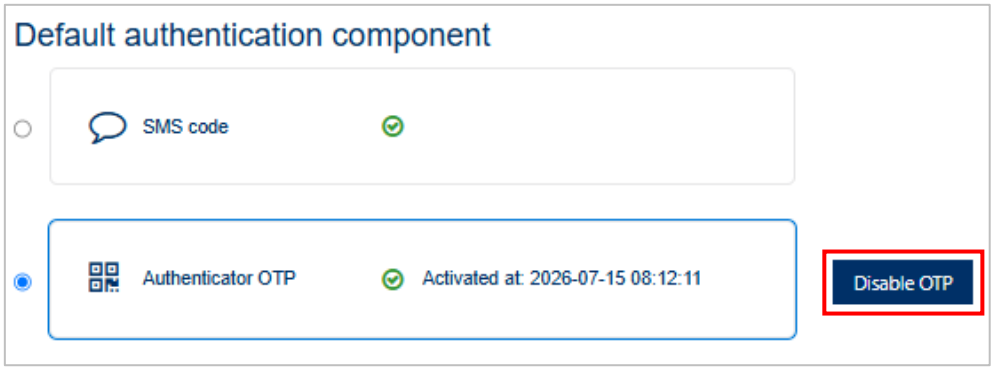


5.4 Deactivating the OTP code authentication method

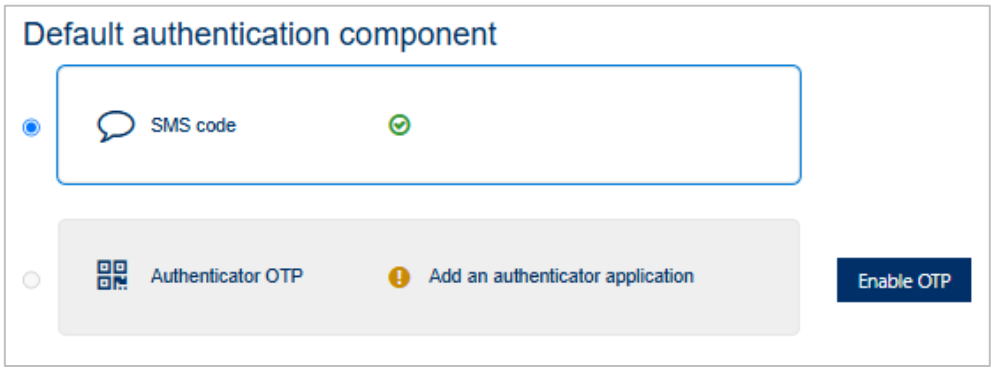
To deactivate OTP code authentication, click the **"Disable OTP"** button located on the right side of the section related to the authenticator app.

After selecting the option to disable OTP, the system will display a confirmation window in which the user shall enter a verification code sent to the phone number associated with the PURM account. The received 8-digit SMS code should be entered in the **"SMS Confirmation"** field, and then the operation should be confirmed by clicking the **"Confirm"** button.

NOTE: Deactivating the OTP authentication method is only possible if the SMS code authentication has been enabled.



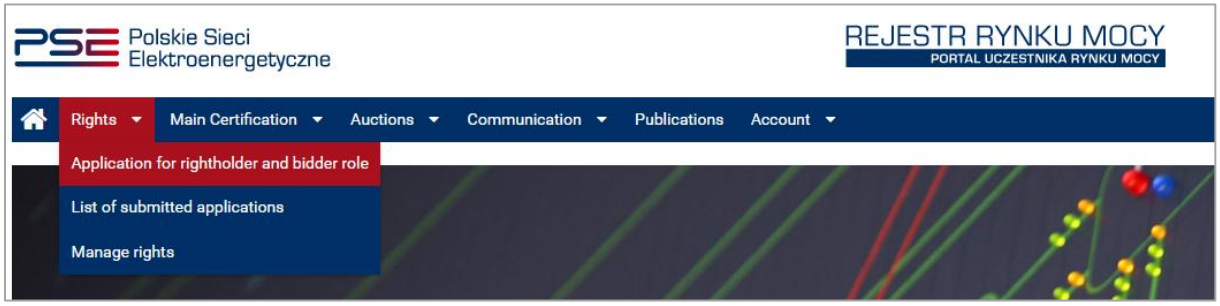
After correctly entering the code and confirming OTP authentication will be disabled, and the system will use the login method with SMS code authentication. The user will also receive an email confirming the deactivation of the OTP authorization method.



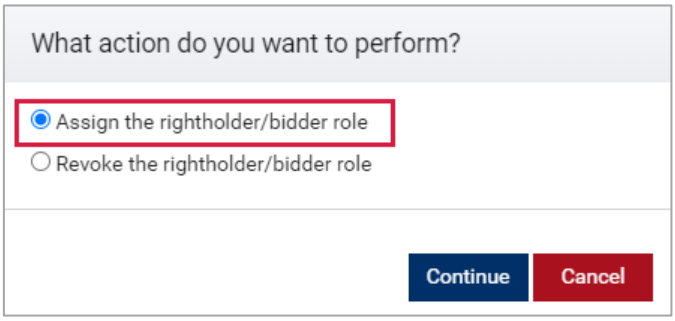
NOTE: After deactivating the OTP code authentication method, the link between the authenticator application and the PURM account is lost. To restore the connection, click the "Activate OTP" button an proceed analogously as in the configuration of T-OTP authentication described in section 2.2.

6 ASSIGNMENT OF THE RIGHTHOLDER AND BIDDER ROLE

To submit an application to be assigned with the rightholder or bidder role, user shall select "**Rights**" → "**Application for rightholder or bidder role**" from the main menu.



After choosing right option from the main menu, PURM shall ask which action user would like to perform.



To submit an application to be assigned with the bidder role, first option marked as "**Assign the rightholder / bidder role**" shall be selected. Choice shall be confirmed by clicking "**Continue**".

6.1 Section I – General information

First section of the application concerns its purpose, which may be:

- assigning the rightholder role,
- assigning the bidder role.

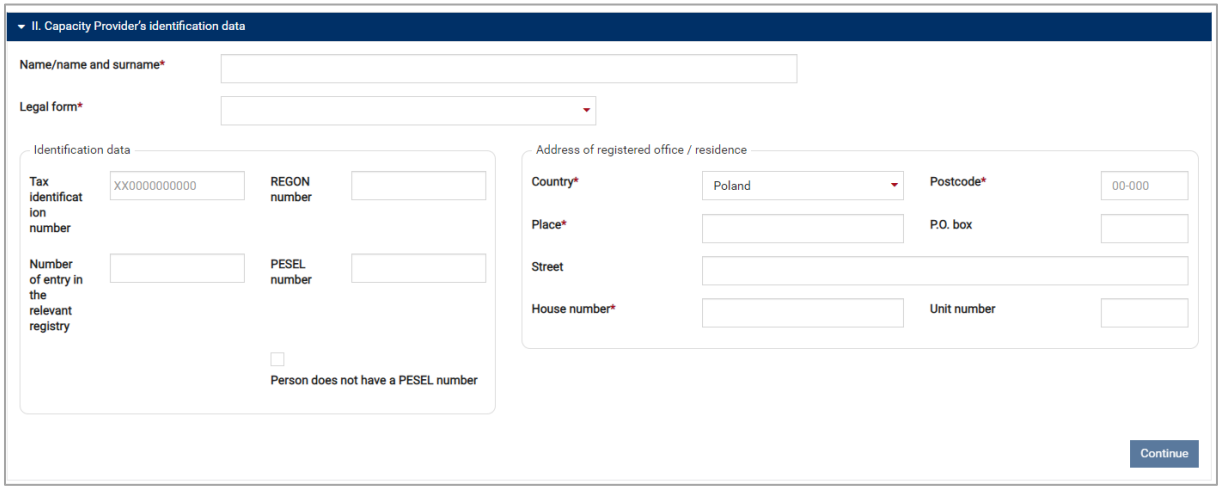
The purpose of the application is indicated by selecting one or two of the available options.

NOTE! Selecting at least one of the available options is required.

After selecting an appropriate option, the process of filling the application shall be continued by clicking "**Continue**".

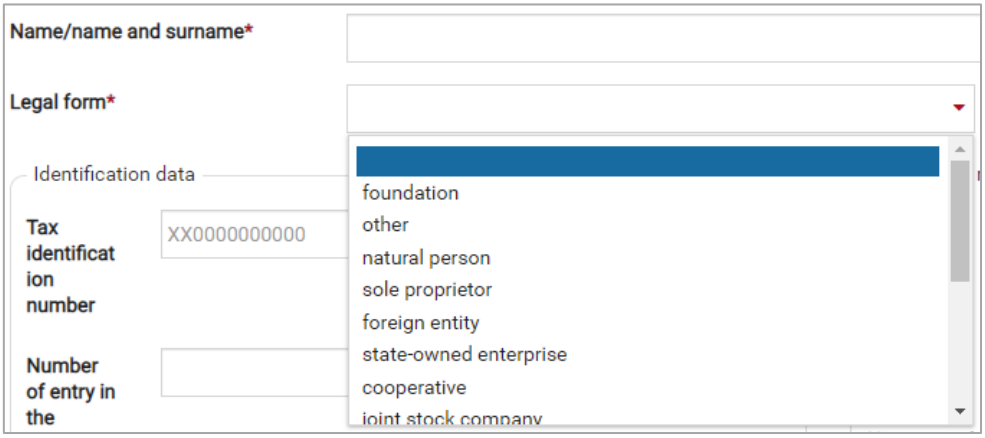
6.2 Section II – Capacity provider's identification data

Second section of the application concerns the capacity provider's identification data.



NOTE: Filling all mandatory fields, which are marked with an asterisk " * ", is required. In case of skipping any of these fields, proceeding to the next section is unavailable.

The completion of this section shall start with name or first and last name of the capacity provider and its legal form.



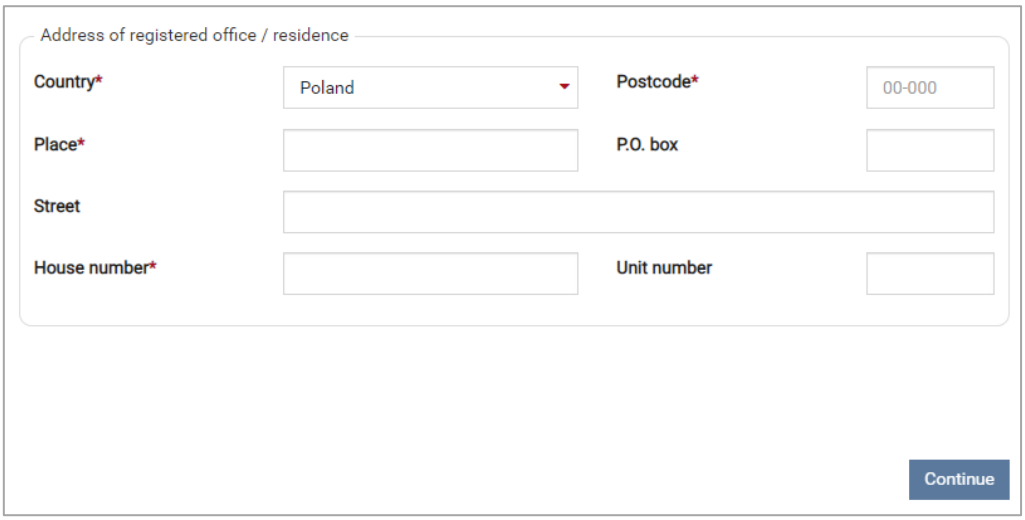
In case of entities based outside of the Republic of Poland, user shall select "**foreign entity**" from the a drop-down list marked as "**Legal form**" and then, enter the capacity provider's tax identification number.

Next, capacity provider's address details shall be filled, containing:

- "**Country**",
- "**Place**",
- "**Postcode**",
- "**Street**",

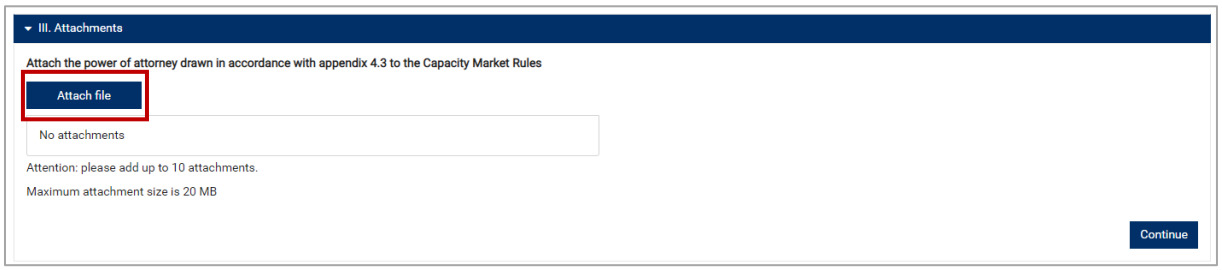
- "**House number**".

After filling all mandatory fields, user shall proceed to the next section by clicking "**Continue**".



6.3 Section III – Appendixes

Final section of the application shall contain the power of attorney authorising user to act as a bidder or rightholder on behalf of the capacity provider. The document must be drawn according to the form of Appendix 4.3 to the Capacity Market Rules.

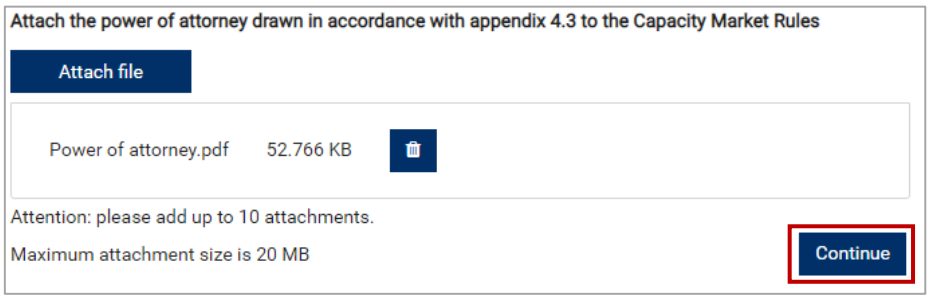


To select the appendix to be uploaded, user shall click "**Attach file**".

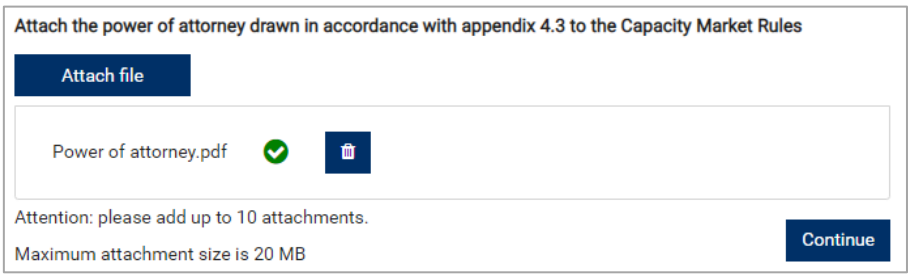
NOTE: The Appendix 4.3 in English language version is available here: https://www.pse.pl/aukcja-wstepna. Please note that this document is executed in Polish language version only.

NOTE: All appendixes submitted to PURM shall be in the .PDF format and shall be affixed with a qualified electronic signature of the person who submits the application. An exception is a power of attorney signed with a qualified electronic signatures of representatives of the entity issuing it. The size limit for a single appendix is 20 MB.

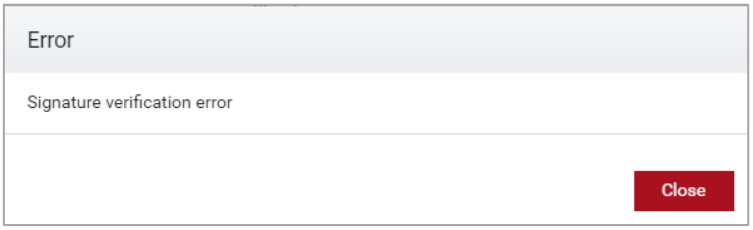
An erroneously added appendix can be deleted with the "🗑" button. When all required appendixes have been added, clicking "**Continue**" will start the process of uploading them.



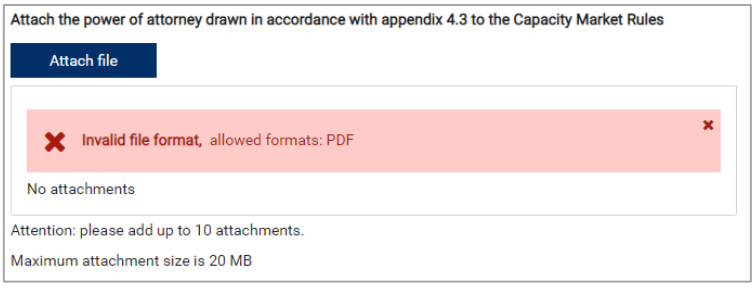
If the appendix is affixed with qualified electronic signature properly and if the process of uploading it succeeded, the appendix will be marked with "✓".



In case the appendix file is not affixed with a qualified electronic signature, an error "**Signature verification error.**" will be displayed.



It is forbidden to add appendixes in format different than .PDF. If user tries to upload a file in other format, an error "**Invalid file format, allowed formats: PDF.**" will be displayed.

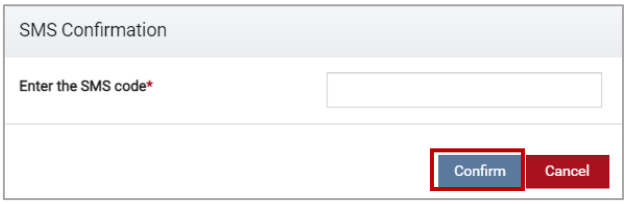


6.4 Application signature

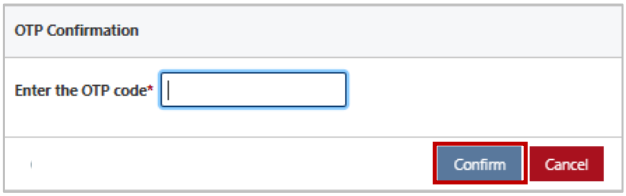
Process of signing the application shall begin with clicking "**Sign the application form**", located in the bottom right corner of the browser window.

PURM shall then generate an application to be assigned with the bidder or rightholder role, which must be signed with user's qualified electronic signature. The process of signing the application with a qualified electronic signature takes place analogously to the process of user account establishment, described in Chapter 2.

After the application has been properly signed, the user shall confirm its submission by SMS code or OTP code, depending on the default authentication method. The SMS code shall be sent to the phone number assigned to the user account, while the OTP code shall be generated in the Google Authenticator application. In order to confirm the application submission, the code shall be entered into the "**SMS Code**" field or **"OTP Code"** and confirmed by clicking "**Confirm**".



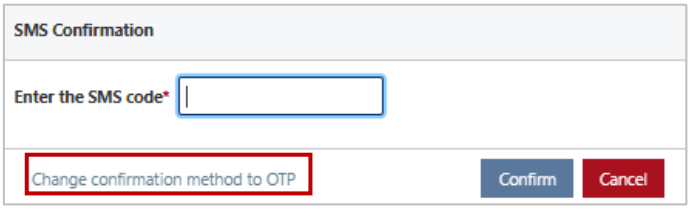
NOTE: The SMS code is active for 20 minutes. After this time SMS code expires and it is necessary to go through the application signing process again.



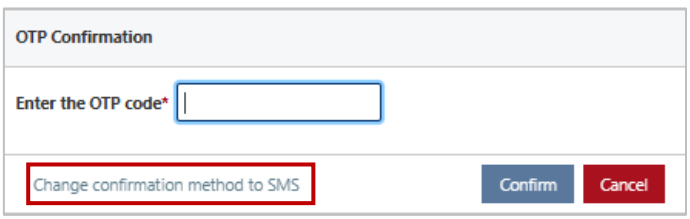
NOTE: The OTP code is active for 30 seconds. After this time the application generates a new code.

In case the user has both authentication methods enabled it is possible to change the confirmation method from OTP code to an SMS code and vice versa, depending on the default authentication method. To change the confirmation the user shall press:

- "Change the confirmation method to OTP" if the default authentication method is SMS codes,

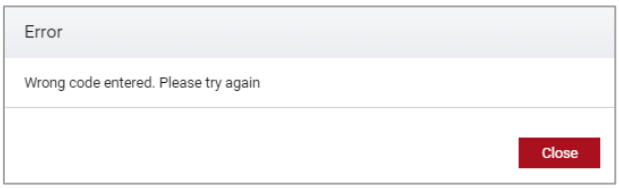


- "Change the confirmation method to SMS" if the default authentication method is OTP codes.



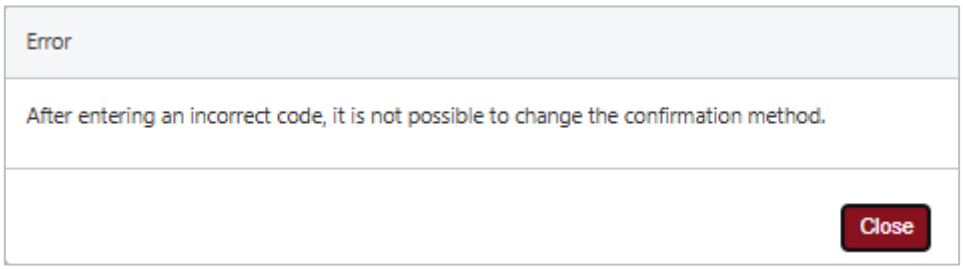
NOTE: Changing the confirmation method does not change the default authentication method.

If an SMS code is entered incorrectly, the message "**Wrong code entered. Please try again**" is displayed.



NOTE: After 3 unsuccessful input attempts, the code expires and it is necessary to go through the application signing process again.

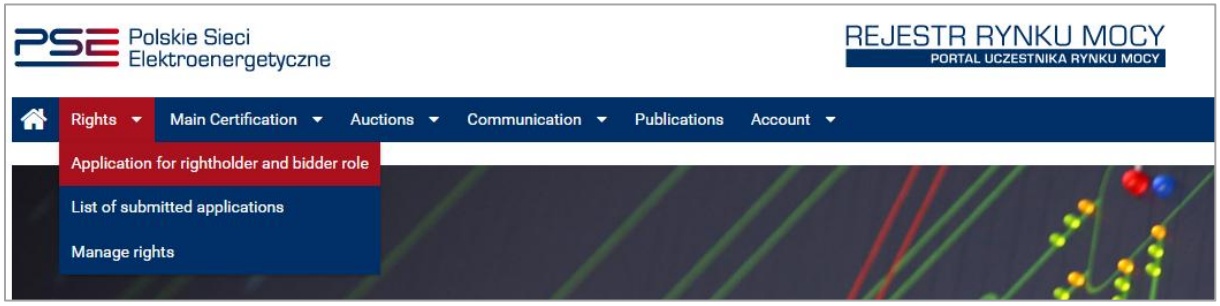
NOTE: If the SMS or OTP code is entered incorrectly, it is not possible to change the confirmation method to an OTP or SMS code. After clicking the "Change confirmation method to OTP/SMS" the following message is displayed.



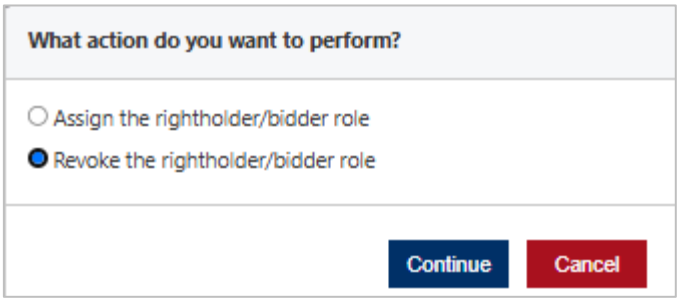
After successful verification of the SMS code or OTP code, the application is submitted and a confirmation message is sent to user's e-mail address. PURM proceeds to the application overview window.

7 REVOCATION OF THE RIGHTHOLDER AND BIDDER ROLE

To submit an application to revoke the rightholder or bidder role, user shall select "**Rights**" → "**Application for rightholder or bidder role**" from the main menu.



After choosing right option from the main menu, PURM shall ask which action user would like to perform.



Next, the "**Revoke the rightholder / bidder role**" option shall be selected. Choice shall be confirmed by clicking "**Continue**".

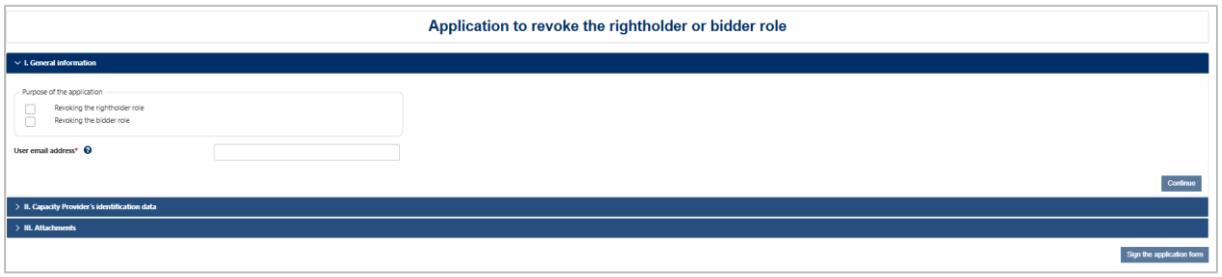
7.1 Section I – General information

First section of the application concerns its purpose. The user shall choose the purpose of the application, which may be:

- revocation of the rightholder role,
- revocation of the bidder role,
- email address of the user, whose role will be revoked

NOTE: The indicated user email address must be associated with that user's PURM account.

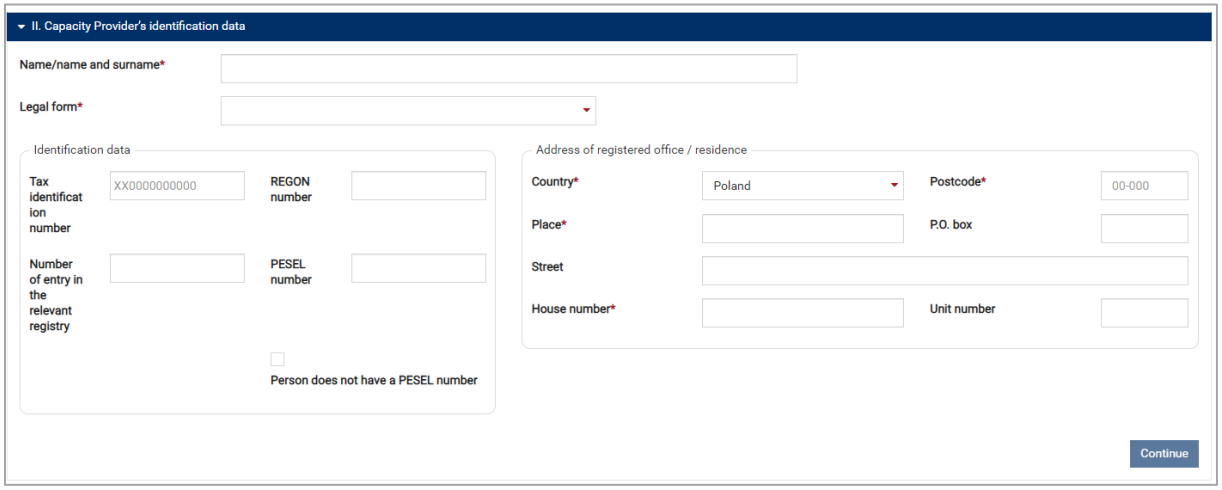
The purpose of the application shall be indicated by selecting one or two of the available options, and the user's email address shall be provided by entering it in the required field.



NOTE: It is necessary to choose at least one of the available options.

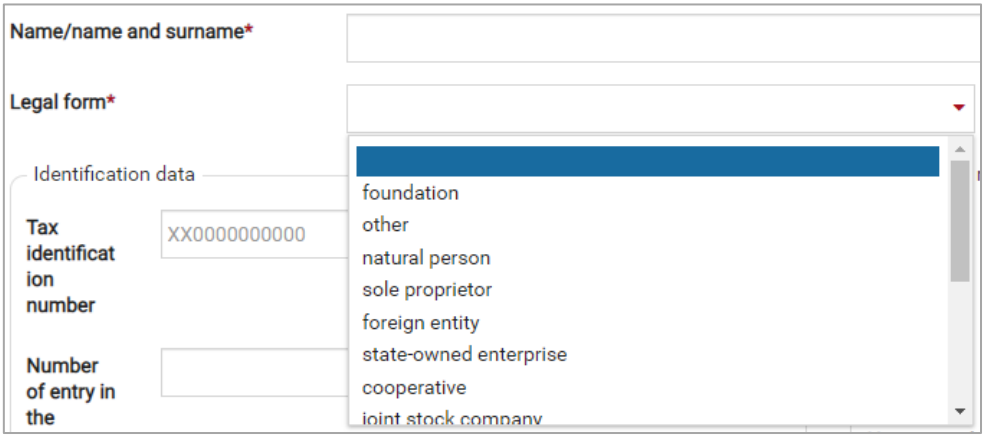
7.2 Section II – Capacity provider's identification data

Second section of the application concerns the capacity provider's identification data.



NOTE: Filling all mandatory fields, which are marked with an asterisk " * ", is required. In case of skipping any of these fields, proceeding to the next section is unavailable.

The completion of this section shall start with name or first and last name of the capacity provider and its legal form.



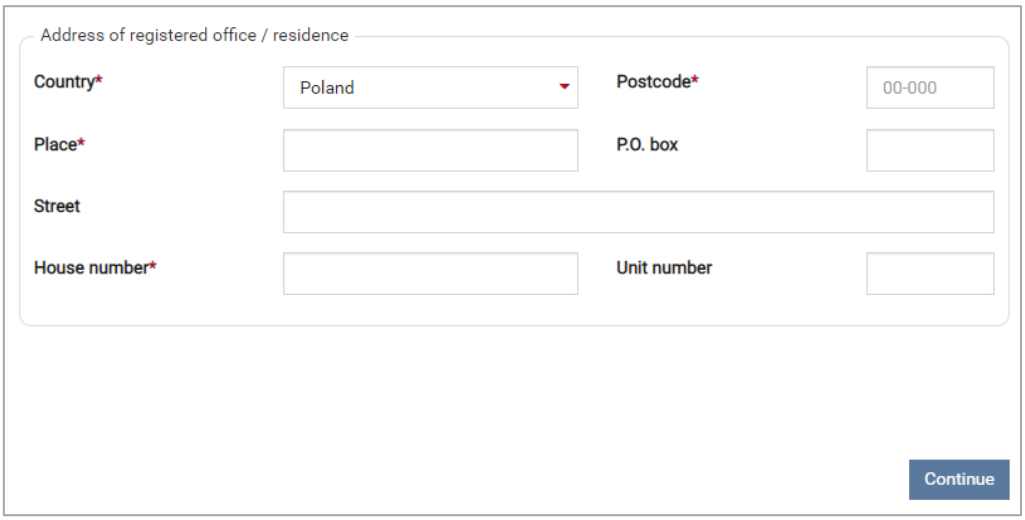
In case of entities based outside of the Republic of Poland, user shall select "**foreign entity**" from the drop-down list marked as "**Legal form**" and then, enter the capacity provider's tax identification number.

Next, capacity provider's address details shall be filled, containing:

- "**Country**",
- "**Place**",
- "**Postcode**",
- "**Street**",

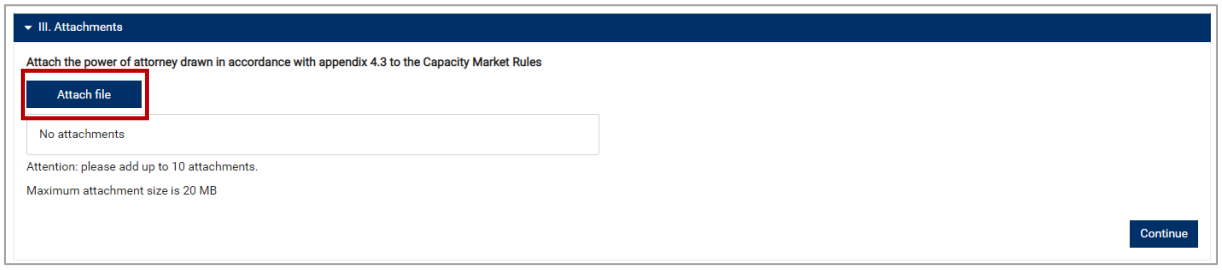
- "**House number**".

After filling all mandatory fields, user shall proceed to the next section by clicking "**Continue**".



7.3 Section III – Appendixes

Final section of the application shall contain the power of attorney authorising user to act as a bidder or rightholder on behalf of the capacity provider. The document must be drawn accorting to the form of Appendix 4.3 to the Capacity Market Rules.

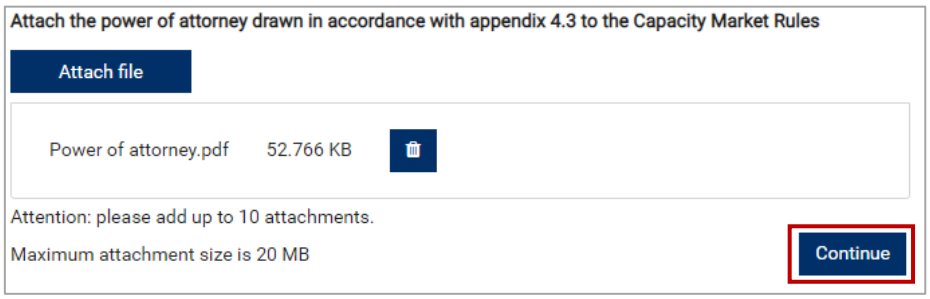


To select the appendix to be uploaded, user shall click "**Attach file**".

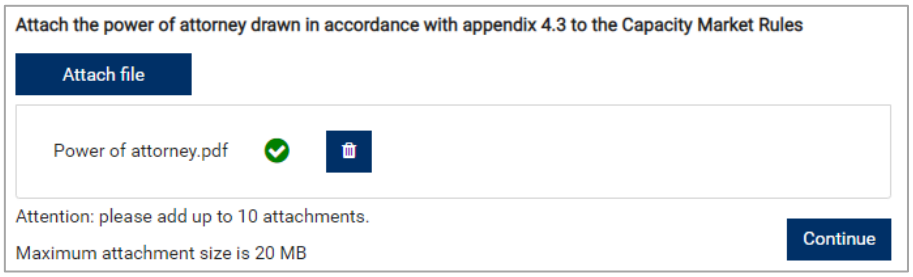
NOTE: The Appendix 4.3 in English language version is available here: https://www.pse.pl/aukcja-wstepna. Please note that this document is executed in Polish language version only.

NOTE: All appendixes submitted to PURM shall be in the .PDF format and shall be affixed with a qualified electronic signature of the person who submits the application. An exception is a power of attorney signed with a qualified electronic signatures of representatives of the entity issuing it. The size limit for a single appendix is 20 MB.

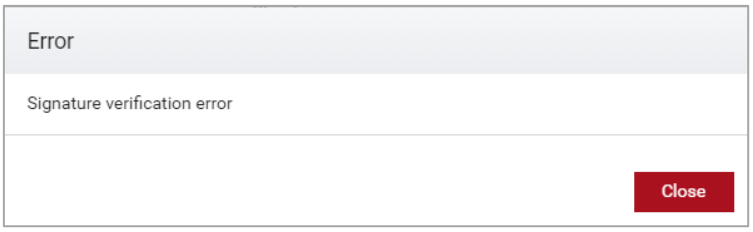
An erroneously added appendix can be deleted with the " " button. When all required appendixes have been added, clicking "**Continue**" will start the process of uploading them.



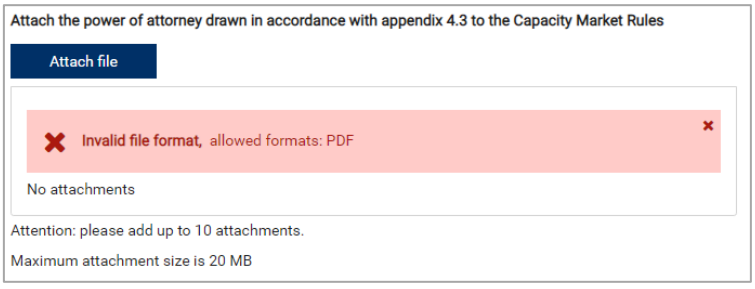
If the appendix is affixed with qualified electronic signature properly and if the process of uploading it succeeded, the appendix will be marked with " ".



In case the appendix file is not affixed with a qualified electronic signature, an error "**Signature verification error.**" will be displayed.



It is forbidden to add appendixes in format different than .PDF. If user tries to upload a file in other format, an error "**Invalid file format, allowed formats: PDF.**" will be displayed.

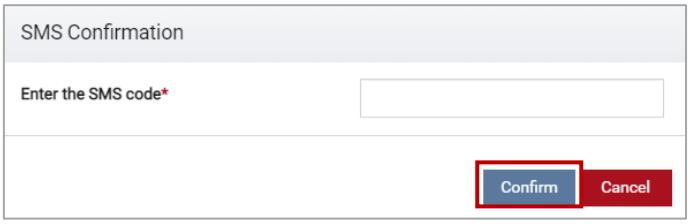


7.4 Application signature

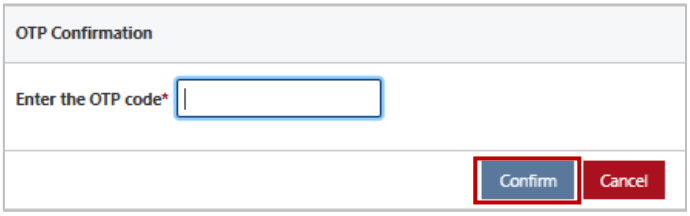
Process of signing the application shall begin with clicking "**Sign the application form**", located in the bottom right corner of the browser window.

PURM shall then generate an application to be assigned with the bidder role, which must be signed with user's qualified electronic signature. The process of signing the application with a qualified electronic signature takes place analogously to the process of user account establishment, described in Chapter 2.

After the application has been properly signed, the user shall confirm its submission by SMS code or OTP code, depending on the default authentication method. The SMS code shall be sent to the phone number assigned to the user account, while the OTP code shall be generated in the Google Authenticator application. In order to confirm the application submission, the code shall be entered into the "**SMS Code**" field or **"OTP Code"** and confirmed by clicking "**Confirm**".



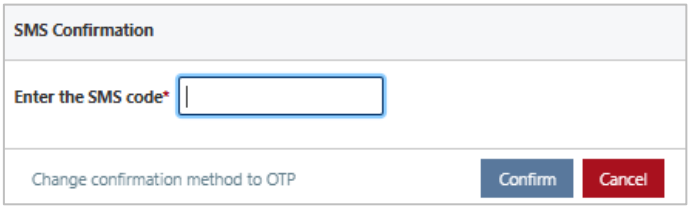
NOTE: The SMS code is active for 20 minutes. After this time SMS code expires and it is necessary to go through the application signing process again.



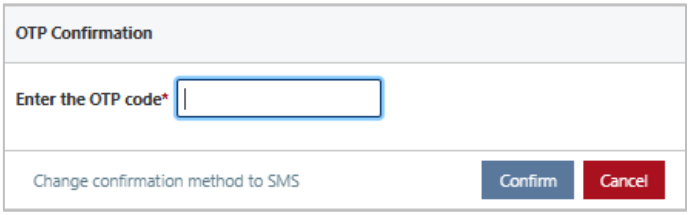
NOTE: The OTP code is active for 30 seconds. After this time the application generates a new code.

If the user has both authentication methods enabled, the confirmation window will allow switching the confirmation method from an OTP code to SMS and vice versa, depending on which authentication method is set as the default.

- "Change the confirmation method to OTP" if the default authentication method is SMS codes.

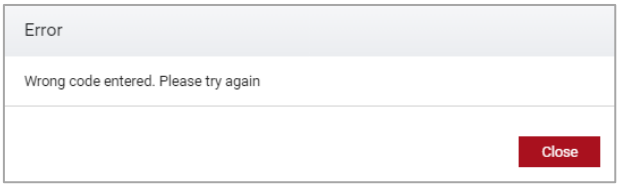


- Change the confirmation method to SMS" if the default authentication method is OTP codes.



NOTE: Changing the confirmation method does not change the default authentication method.

If an SMS code is entered incorrectly, the message "**Wrong code entered. Please try again**" is displayed.



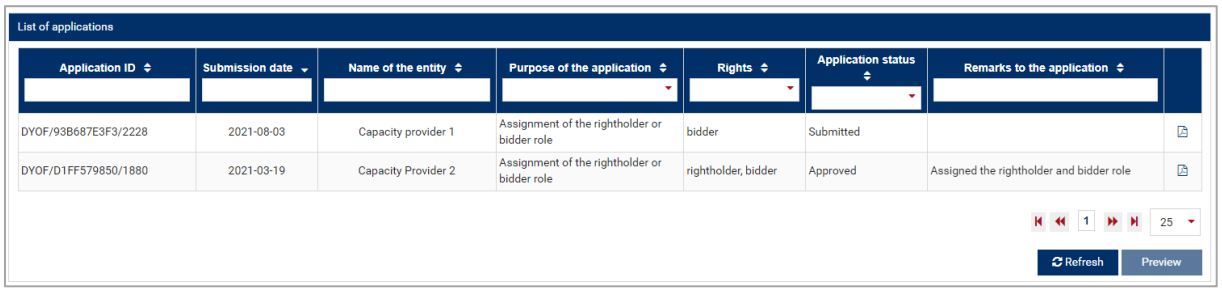
NOTE: After 3 unsuccessful input attempts, the code expires and it is necessary to go through the application signing process again.

After successful verification of the SMS code or OTP code, the application is submitted and a confirmation message is sent to user's e-mail address. PURM proceeds to the application overview window.

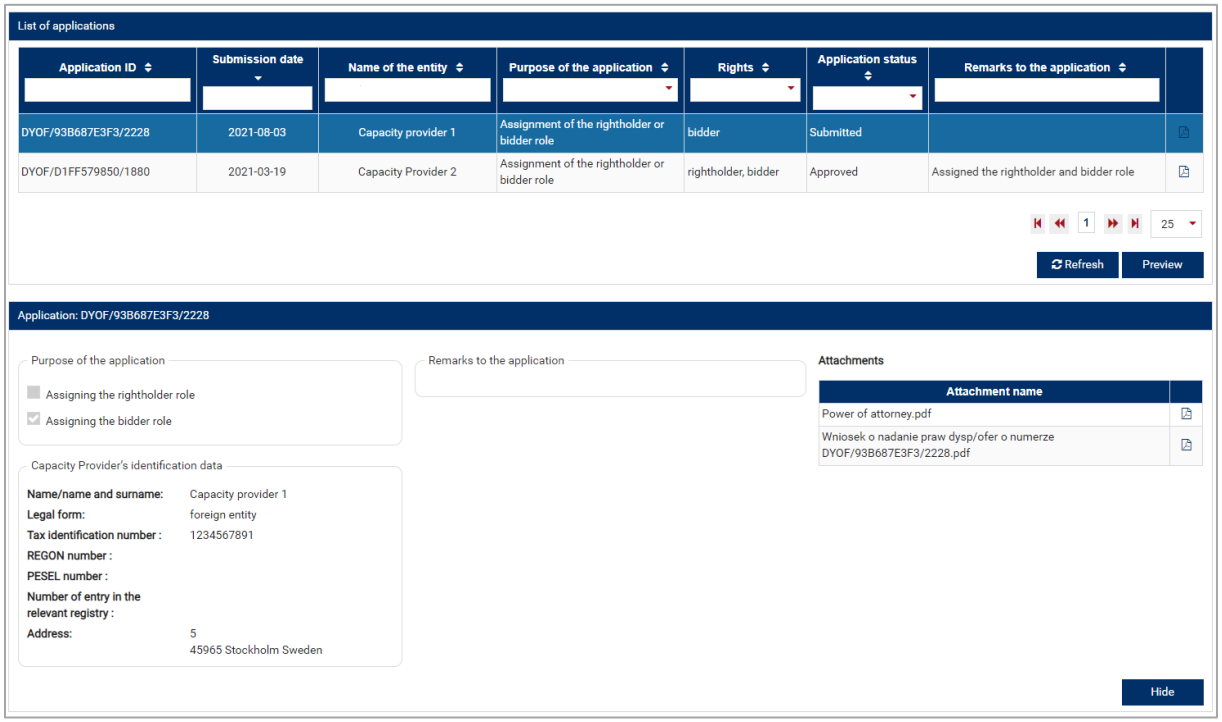
8 BROWSING APPLICATIONS FOR THE ASSIGNMENT/REVOKEMENT OF THE RIGHTHOLDER/BIDDER ROLE

In order to view the submitted applications to be assigned with the rightholder or bidder role, user shall select "**Rights**" → "**List of submitted applications**" from the main menu.

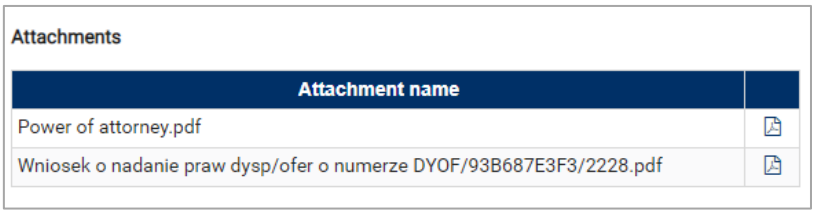
PURM proceeds to the list of applications submitted by user. The list may be refreshed by clicking "**Refresh**".



User may sort the applications by each column and search for a given application by entering the searched phrase in the field under the column name. Selecting the application is possible by clicking on a given row of the table. After selecting the application, user is able to go through its details by clicking "**Preview**".



In the application details, on the right side, a table with submitted appendixes is displayed. User is able to download them by clicking on the document icon on the right side of the table.



NOTE: Each appendix is scanned for viruses and malware. Due to the scanning process, the preview of the submitted application and appendixes may be available with a delay.

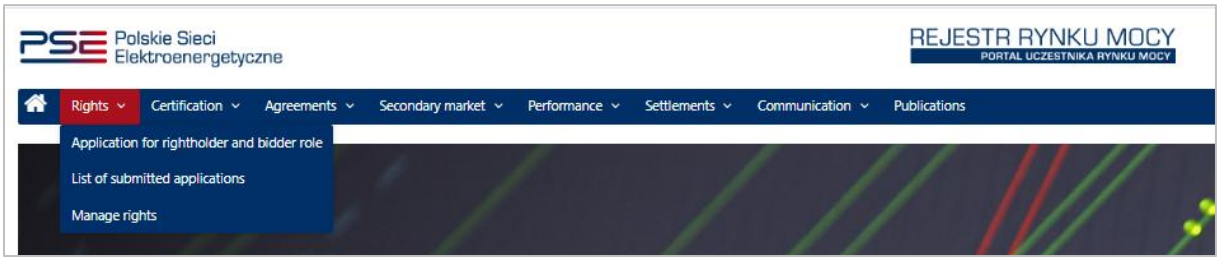
The yellow icon on the right side of the document indicates that the scanning process is in progress and that document shall be available for download after it is completed.

9 MANAGMENT OF RIGHTHOLDER/BIDDER ROLES

User may view the assigned roles.

NOTE! If the user has been appointed the rightholder role, it is possible to establish new PURM user accounts and assign them rightholder and bidder roles.

To access the rights management panel, the user shall log in to the PURM account. Then, from the main menu, the user shall select: „Rights → „Manage Rights".



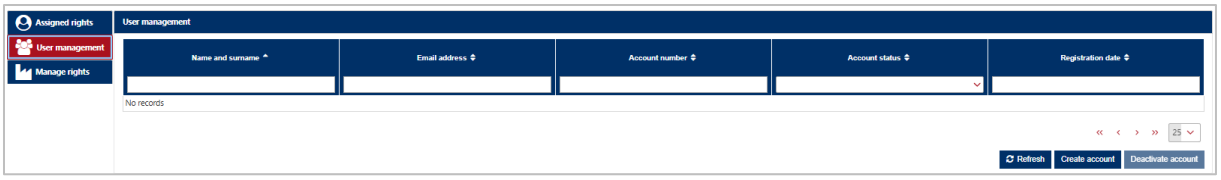
The user is then taken to the "Assigned rights" user rights management panel. The table allows the user to view the rights assigned to the user for individual entities.

PURM proceeds to the list of rights assigned to the user.

9.1 User account creation

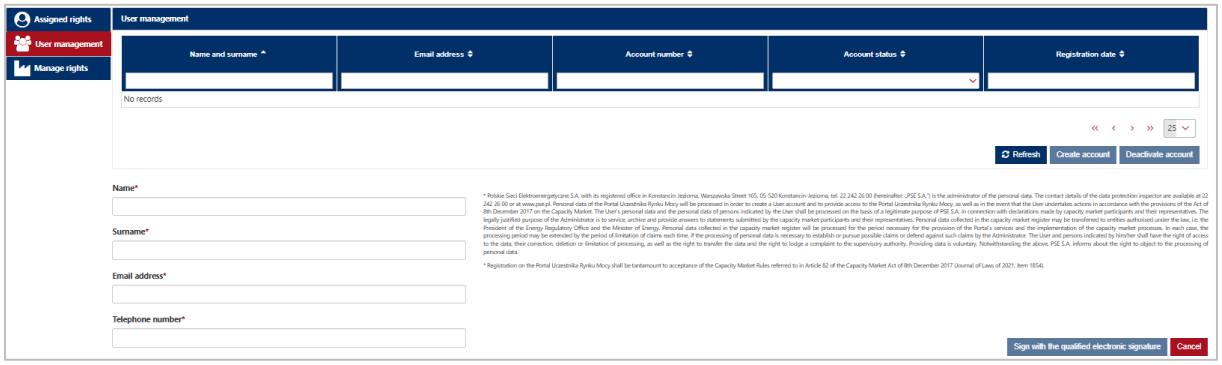
Creating a user account within management of roles is analogous to the account registration process described in section 2.1.

To navigate to the user account creation screen, user shall select the "User Management" option in the side panel. After selecting it, a list of accounts created by the administrator is displayed. To create a new account, user shall select the "Create Account" button



After starting the user account creation process, a registration form is displayed in which the following data shall be entered:

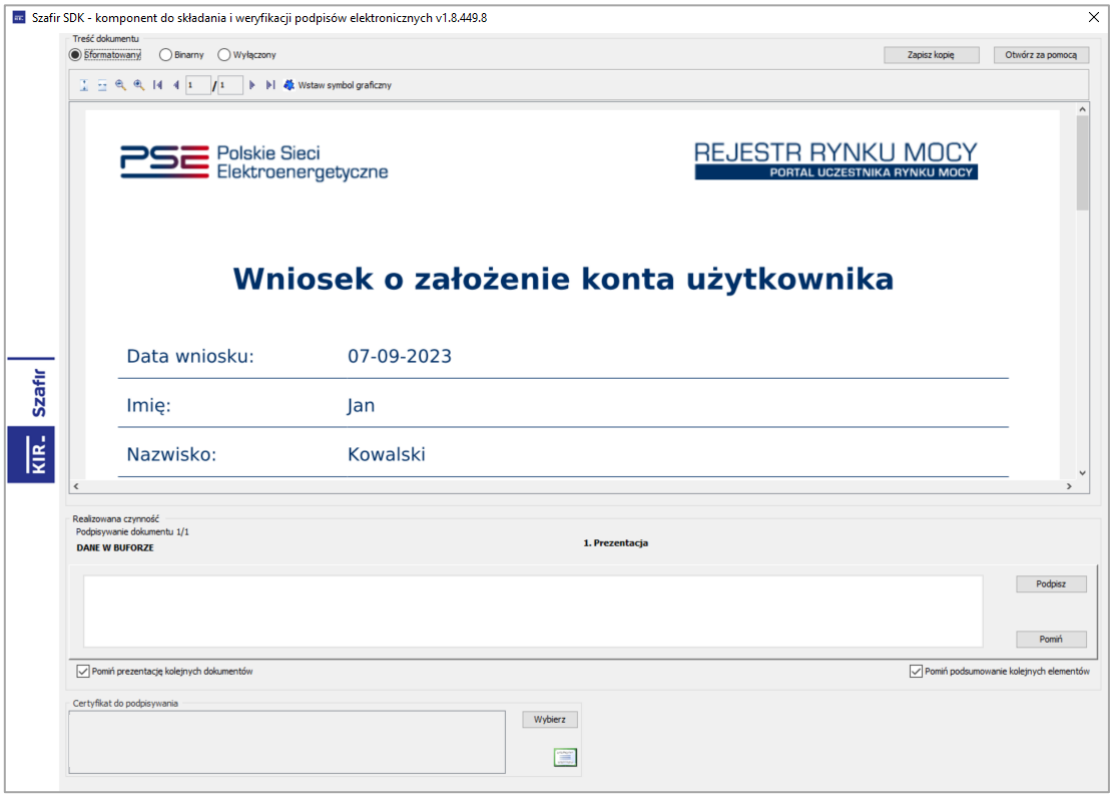
- name and surname
- email address
- phone number



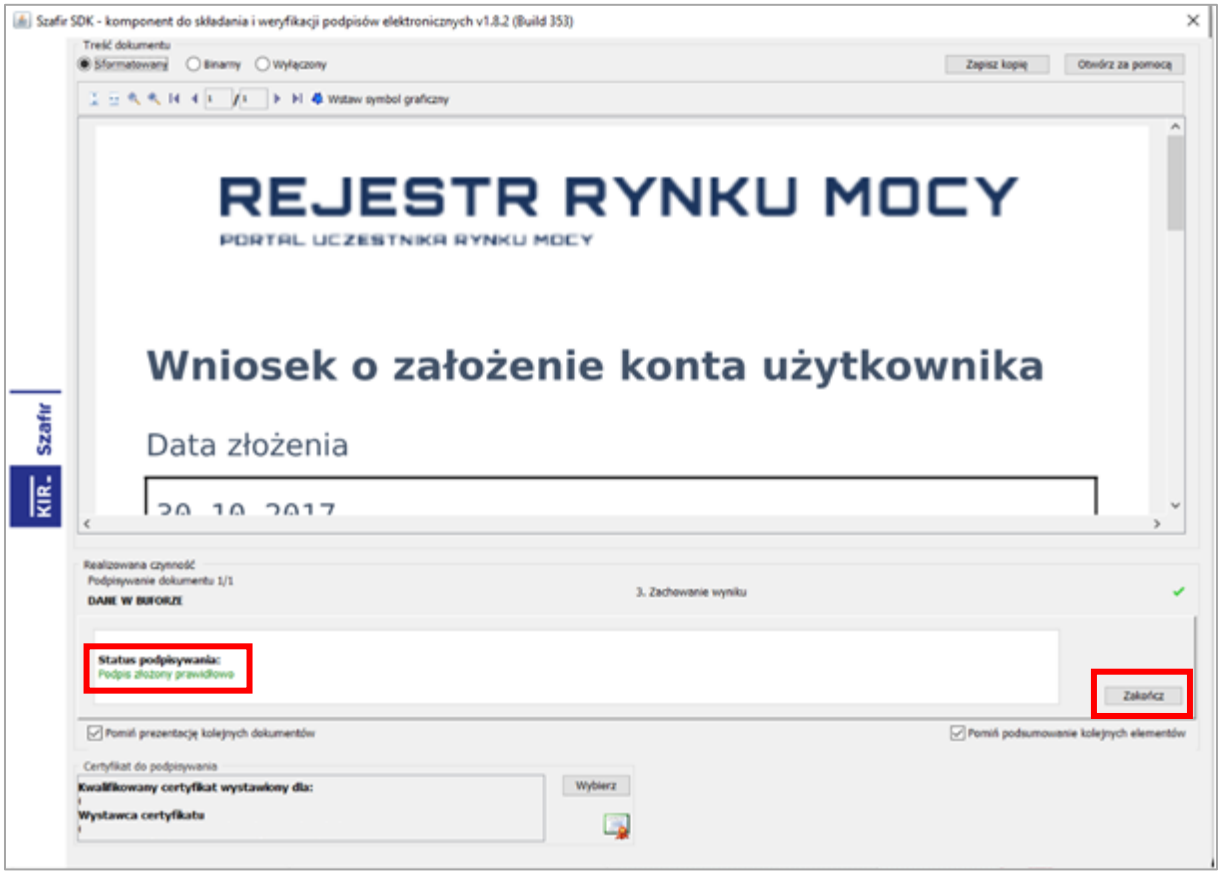
NOTE: Each account mut be assigned a unique email address. It is not possible to create multiple PURM accounts using the same email address.

After completing the required fields, the account creation process shall continue by clicking the ”Sign form” button, which generates an application for creating an account in the register. The application must then be signed with a qualified electronic signature.

After filling all mandatory fields, the process of account creation shall be continued by clicking **“Sign with the qualified electronic signature**”. PURM shall then generate an application for account establishment, which must be signed with user’s qualified electronic signature. Signature shall be made by clicking "**Podpisz**" (*Sign*) and entering the PIN code assigned to the qualified electronic signature followed by clicking “**Akceptuj**” (*Confirm)*.



After the application has been signed properly, message "**Podpis złożony prawidłowo**" (*Signature signed properly*) shall be displayed in the signature submission window.



After signing the document and clicking "**Zakończ**" (*Finish*), PURM shall send an activation link to the e-mail address provided within the application. In order to proceed to the next step, user shall click on the sent link or copy it to the address bar of the internet browser in order to launch the webpage. User account activation shall be finalized by setting a password

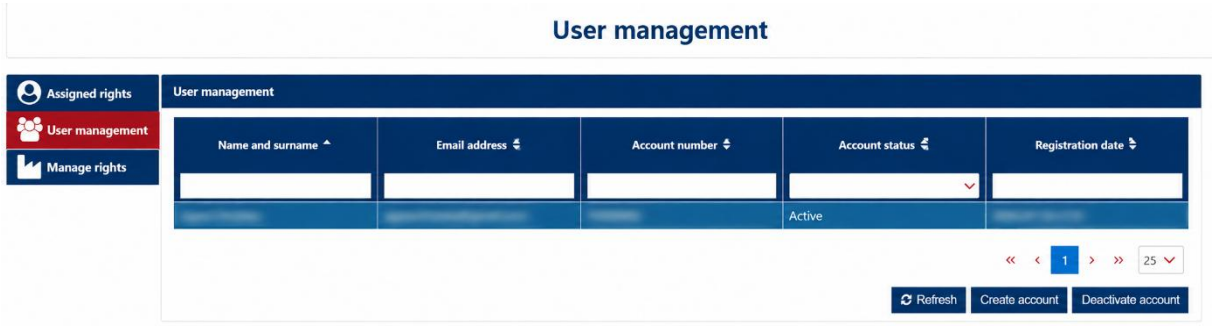
NOTE: Account activation is finalized by the new PURM user, analogously to Chapter 2.

9.2 Deactivation of the created user account

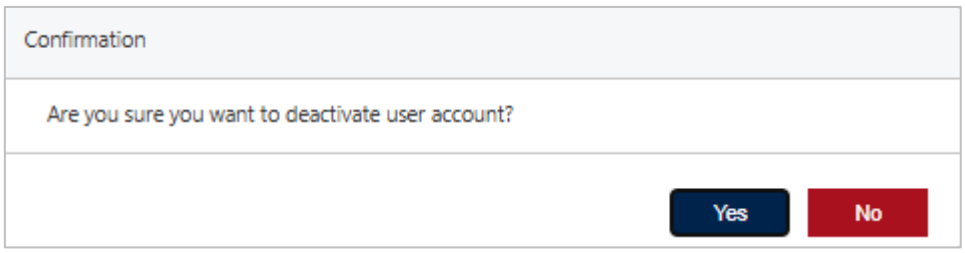
The user may deactivate the created PURM user account in the “User menagement” panel.

NOTE: Deactivation of the PURM user account is irreversible.

To deactivate the created PURM user account, user shall chose the account from the list and press the “Deactivate account" button.



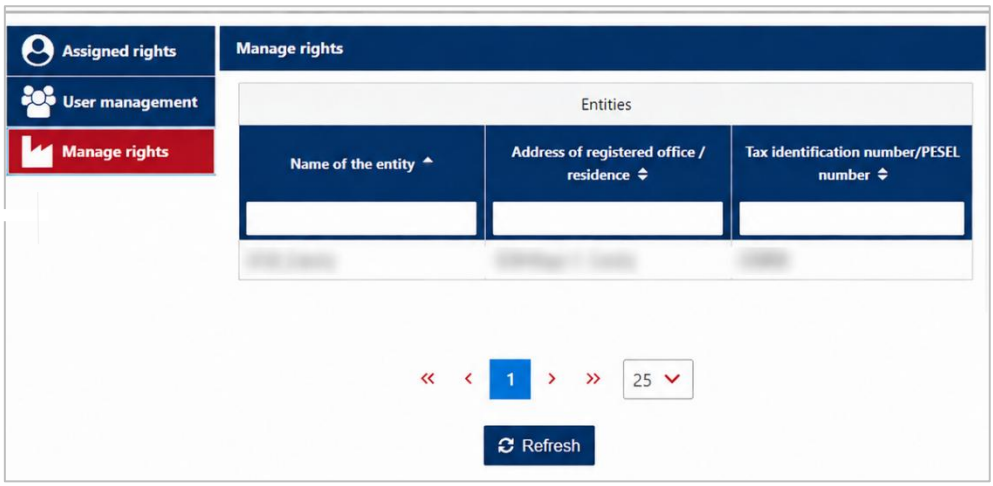
Next, the user shall confirm the account deactivation by pressing “Yes” in the displayed window.



The user account shall be deactivated. User will not be able to log into the account.

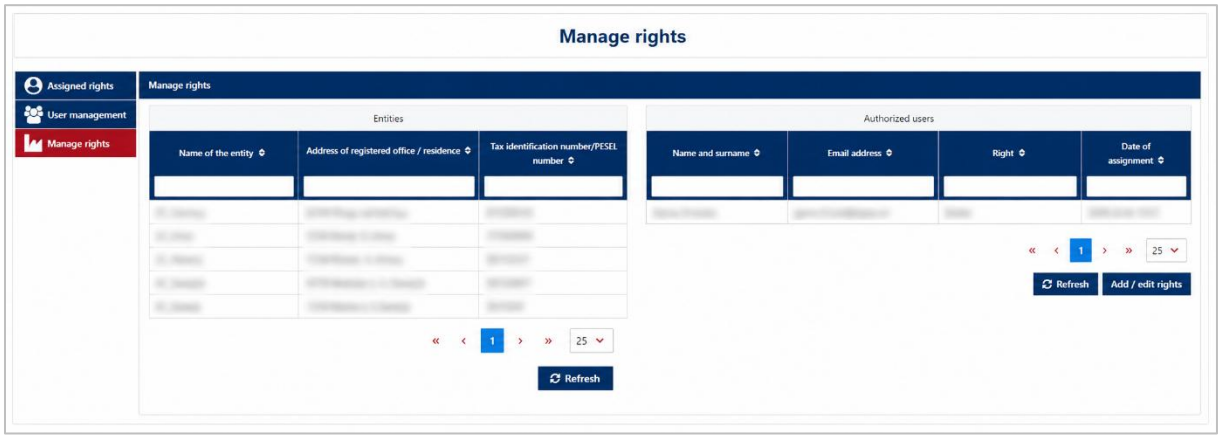
9.3 Granting rights to entity

To grant rights to a selected user, user shall proceed to the “Manage rights” panel, which is located in the side panel.

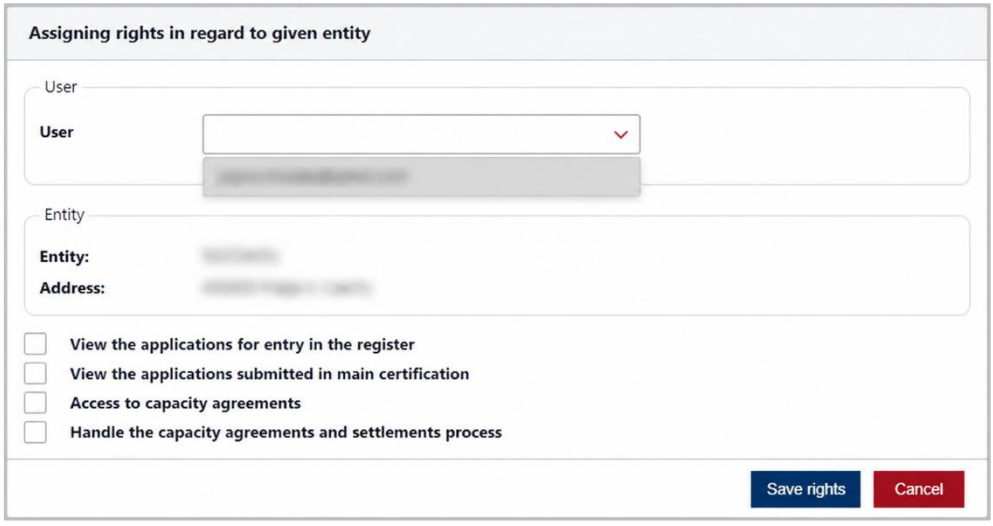


The list contains entities for which the user acts as the authorized rightsholder.

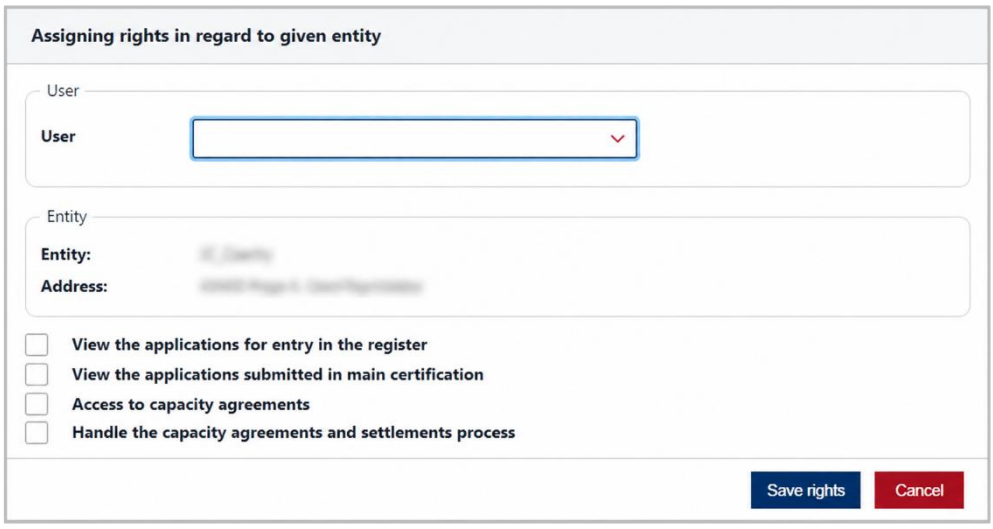
After selecting the appropriate entity, a list of users who have been granted rights is displayed on the right-hand side. To grant or edit rights, the user shall select the “Add/Edit Rights” button.



After selecting the button, a window for granting rights to the indicated entity will be displayed. The rightholder may grant rights both to created user accounts and to other PURM users. Users created by the rightholder shall be selected from the list of created accounts (the list contains the email addresses of all accounts created by the user).

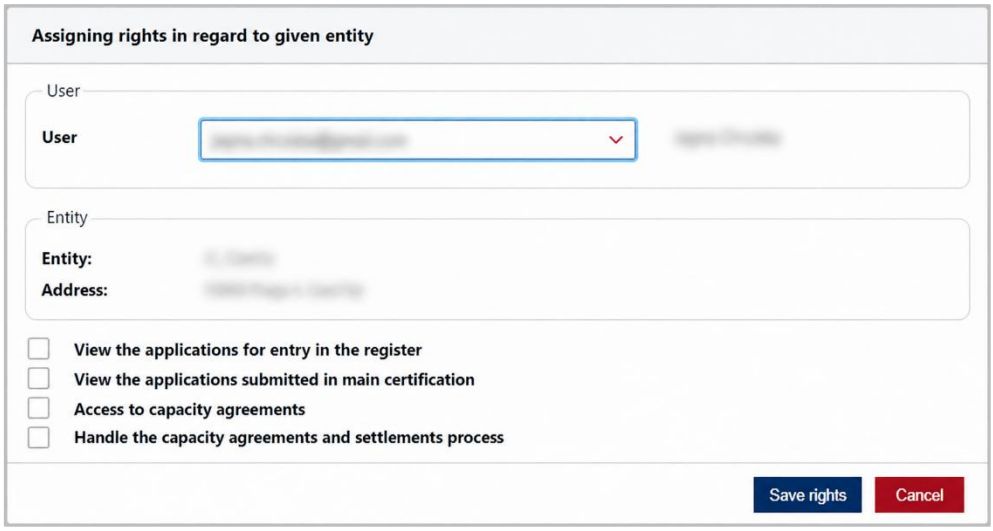


NOTE: By selecting the empty field from the list, after clicking it user may can enter the email address of any PURM user who should be granted rights.



NOTE: Rights can only be granted with to an active user account.

After selecting the appropriate email address, the user's details shall be displayed.



If the user and the entity have been specified, the user shall proceed to the rights selection window to choose which rights are to be granted by clicking the **"Rights"** button.

In the displayed window the user may select any of the 4 types of rights:

- View the applications for entry in the register
- View the applications submitted in main certification
- Access to capacity agreements
- Handle the capacity agreements and settlements process

To grant rights, the usher shall select the appropriate checkboxes in the rights assignment window. After selecting the rights, the user shall confirm the selection by clicking the **"Save rights**" button or close the window by clicking the **"Cancel"** button.

To revoke granted rights, the usher shall select the user and the entity from the list again, then, in the displayed window, clear the appropriate rights and save the changes by clicking the **"Save rights"** button.