KDPW

How to get access to KDPW Trade Repository (EMIR and SFTR) application – a Manual

Table of contents

1. Access to KDPW_TR (EMIR and SFTR) application – general information

In order to facilitate usage of various services of KDPW Group, we are introducing a modern access method – "single sign-on", abbreviated to SSO, which allows access to all KDPW services, including Trade Repository, after a single login.

At the same time the current access to KDPW_TR (EMIR) with personal certificates is being deprecated (it is necessary to migrate certificates – see details below). It will allow an easier and faster operation in KDPW_TR applications and in test environments.

Additionally, we are introducing user-friendly access management for the KDPW_TR application from the administrator's and TR services Participant's accounts. To be granted access to KDPW_TR application, it is necessary to create an access account in KDPW.

2. Creating an account in KDPW_TR (EMIR and SFTR) application

The account is created once only and can be used to access all KDPW services in testing and production enviroments.

To create a new User account in the KDPW Trade Repository in the test environment (for EMIR – TST B, for SFTR – TST), please open the page https://tst-online.kdpw.pl/en (Fig. 1). There are separate links to production and educational environments- respectively https://online.kdpw.pl/en and https://edu-online.kdpw.pl/en. Under the "Sign in" button there is a link called "Sign up now". It can be accessed by clicking the underlined text. After it is run, a registration form screen will appear (Fig. 2).

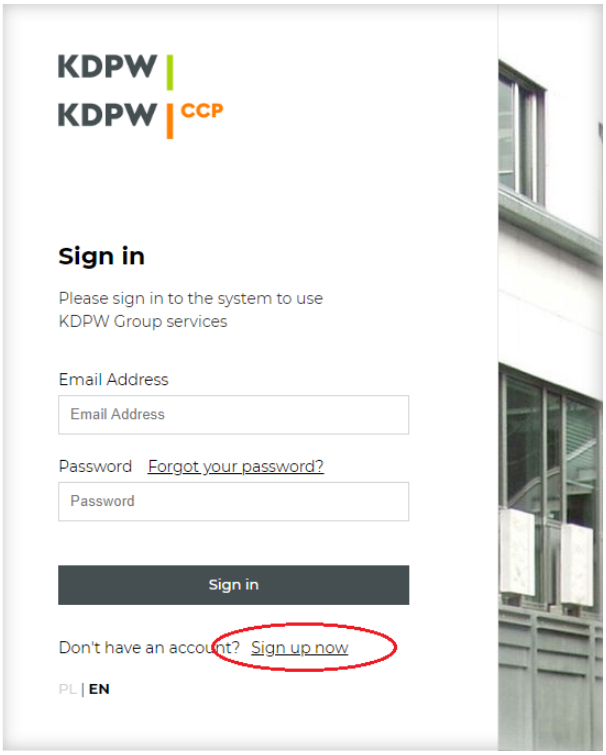

Fig. 1 – Sign in screen

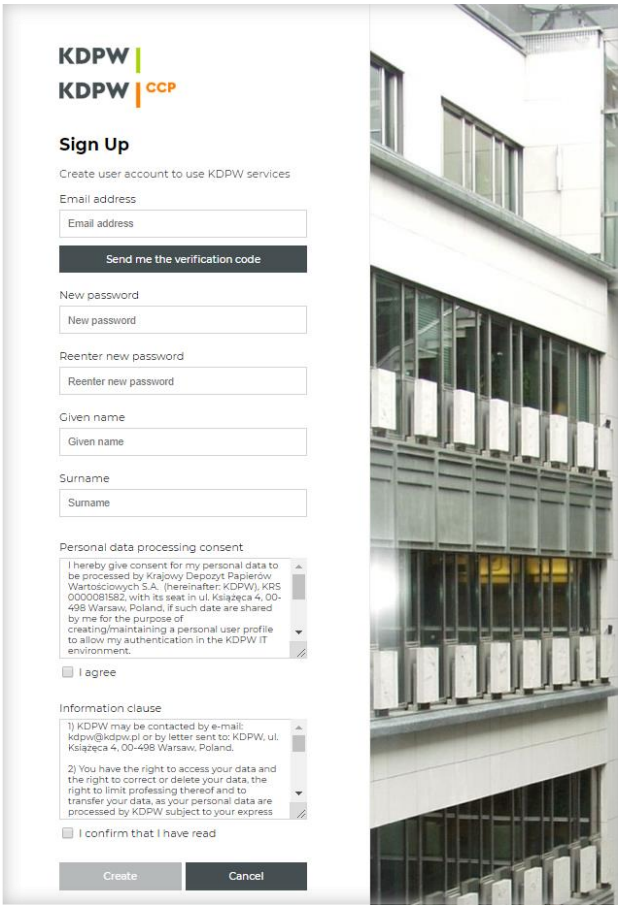

Fig. 2 – Registration form screen

The registration process starts with the verification of the applicant. Please enter an email address into the top field and then click the “Send me the verification code” button. A verification code will be sent to the email address provided.

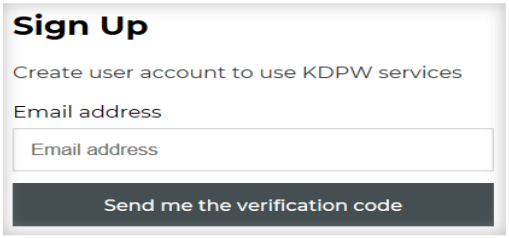

Fig 3. – Verification code screen

The applicant shall receive the following message to the email address provided:

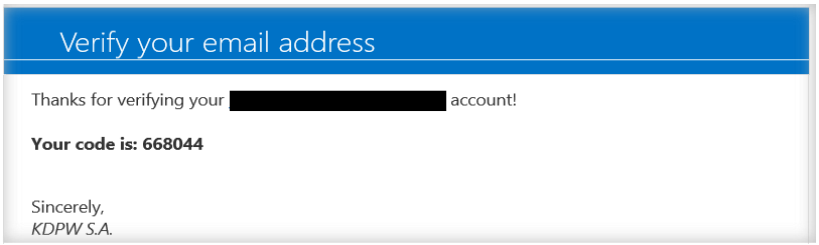

Fig. 4 – Verification code message

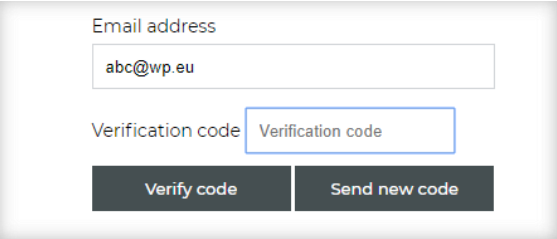

Fig. 5 – A place to enter a received verification code

Next, after the received code has been entered into the “Verification code” (blue border) field and you click the “Verify code” button (Fig. 5), a message about correct verification of the email address will appear and it will be possible to proceed with the account creation process. In case you enter an incorrect code, you will receive a message informing you about an incorrect verification code and it will be possible to get a verification code again. Please fill in the next fields (Fig. 2) as well as review the information clauses and acknowledge them by checking the boxes underneath. Then, please click the “Create” button. Your account will be created, and you will be automatically logged in for the first time; a user desktop screen will appear (Fig. 6).

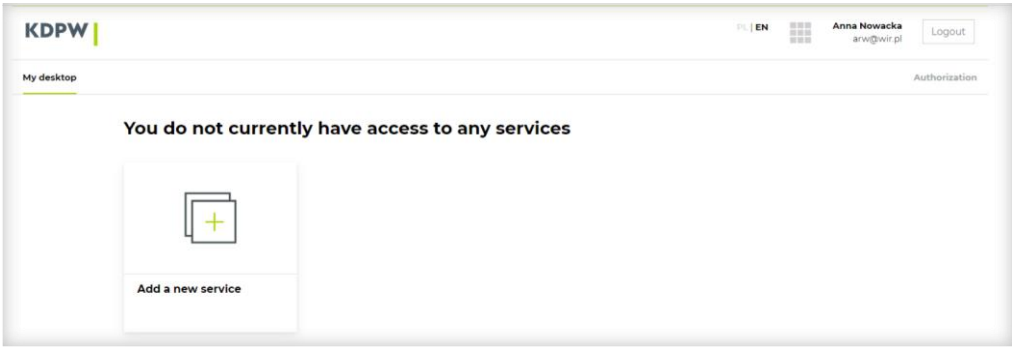

Fig. 6 User desktop screen

Please remember that the email provided is your login and it can be used to register an account once only and it is used in all enviroments – TST B, EDU and PRD.

3. Adding KDPW_TR (EMIR and SFTR) application to services covered with SSO uniform access

After clicking the “Add a new service” button (Fig. 6) the user will be redirected to the next screen (Fig. 7):

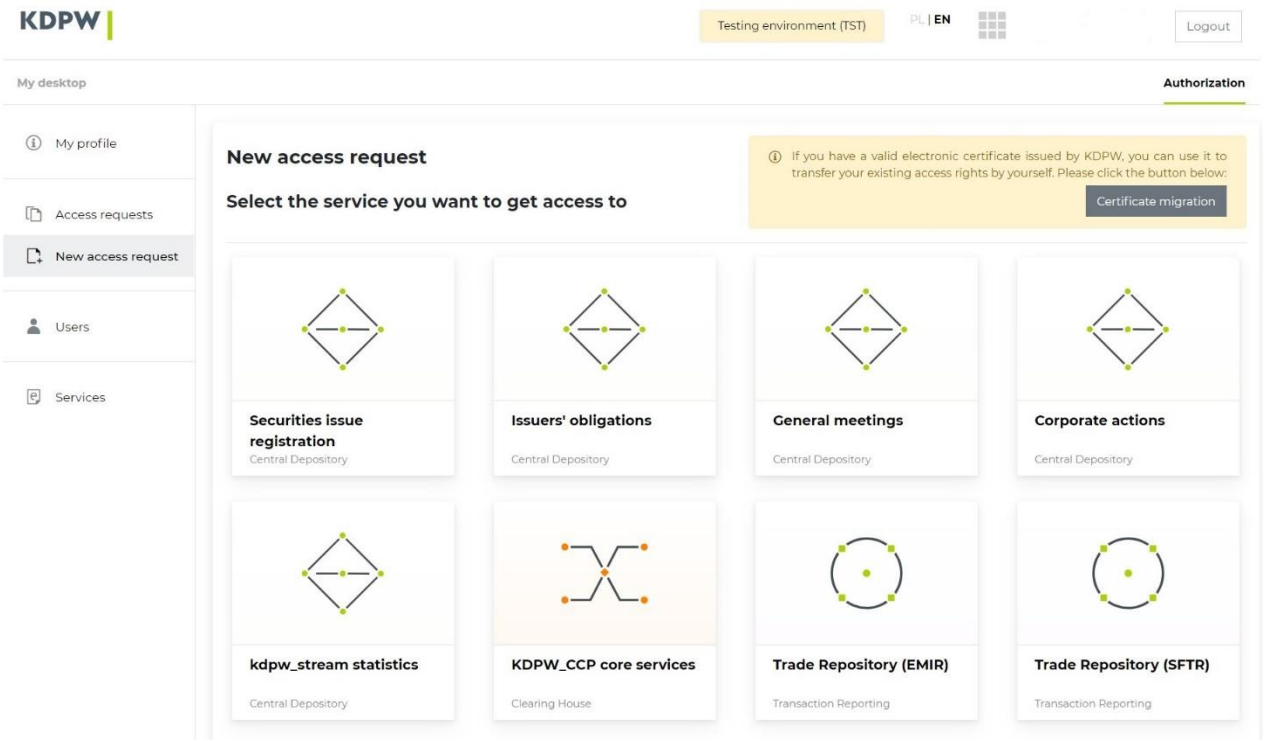

Fig. 7 A view of a profile with available services for which an access request can be submitted

Here are available all KDPW services to which you can request access.

If a user holds a personal certificate which they used to login to KDPW_TR (EMIR) application, they should use the grey button “Certificate migration” located in a yellow field in the upper-right corner of the screen. Next steps are covered by “Getting access by migrating a personal certificate”.

If a user does not hold a personal certificate, they should use the access request function.

To submit a request to access KDPW_TR a user should select the “New request” option in the left menu and then select “Trade Repository (EMIR)” or “Trade Repository (SFTR)” from the available tiles.

4. Getting Access to KDPW_TR (EMIR) by migrating a personal certificate

Participants that hold active personal certificates issued by KDPW can get access to KDPW_TR (EMIR) application by migrating the settings saved in the owned certificate. To start the procedure of permissions migration, please go from “My desktop” to the new access request view. Next, use the grey button “Certificate migration” located in a yellow field in the upper-right corner of the screen (Fig. 8).

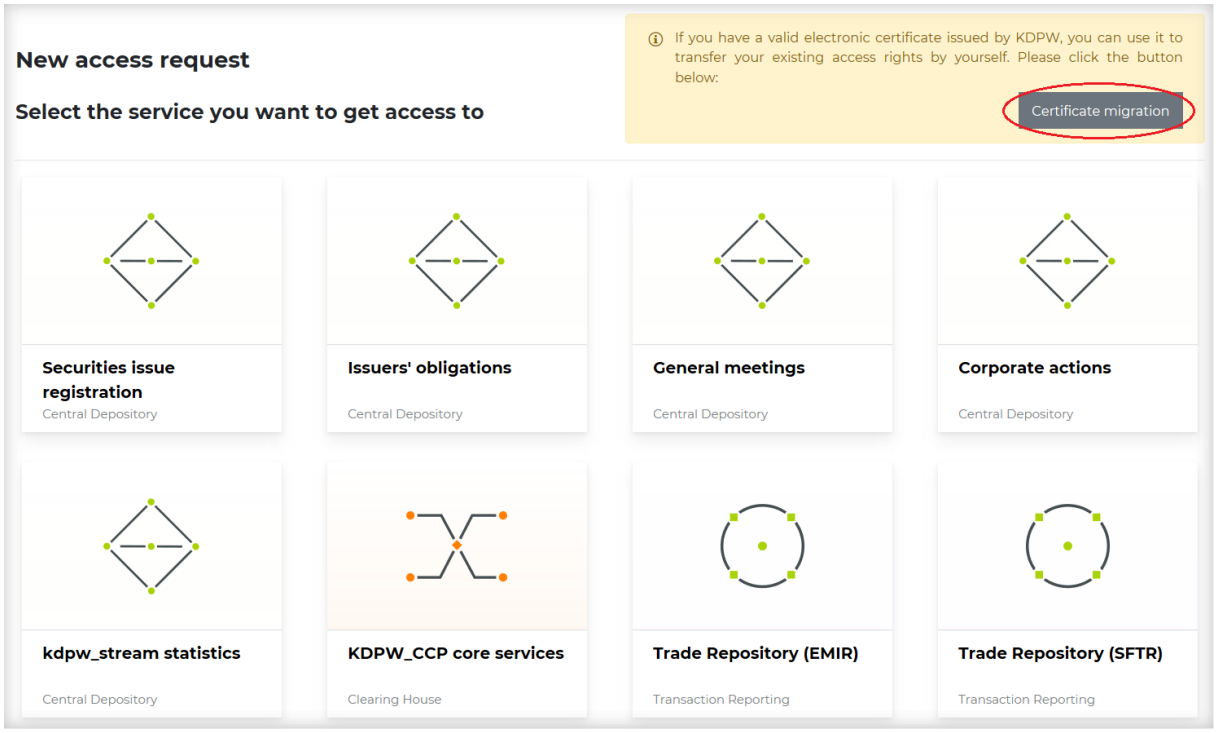

Fig. 8 Certificate migration button

In the next step please select the “Read the certificate” option by clicking a grey button located in the lower-right corner of the message and then, after a list of available certificates is shown, select a certificate from which you wish to move permissions.

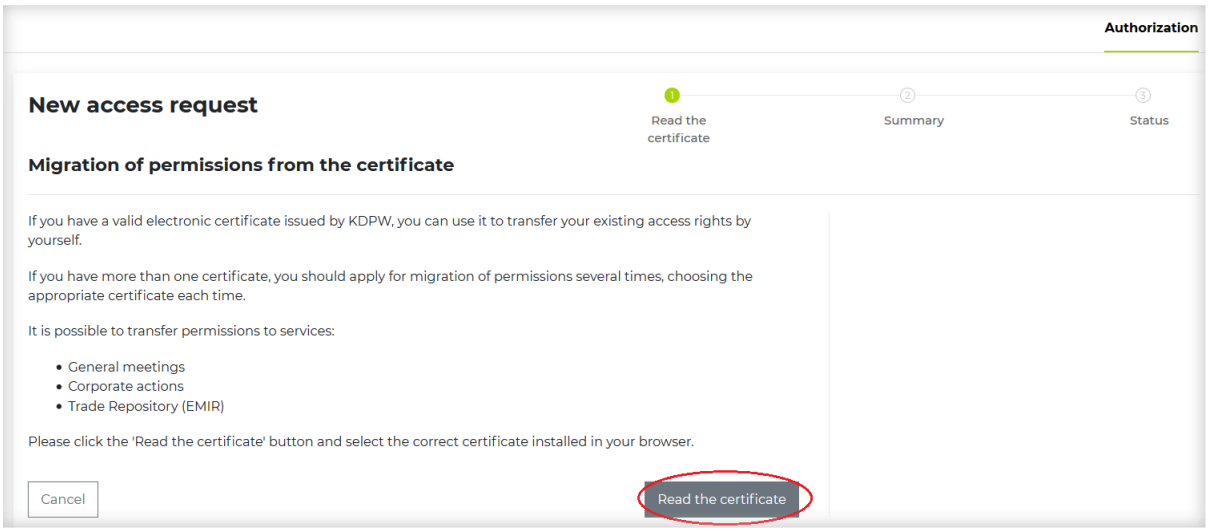

Fig. 9 Certificate migration

After having selected the certificate, in the next step (Fig. 10) please verify the data and then save the permissions by clicking the grey “Save” button located in the lower-right corner of the message. After that the user will be informed about the completion of the process (Fig. 11).

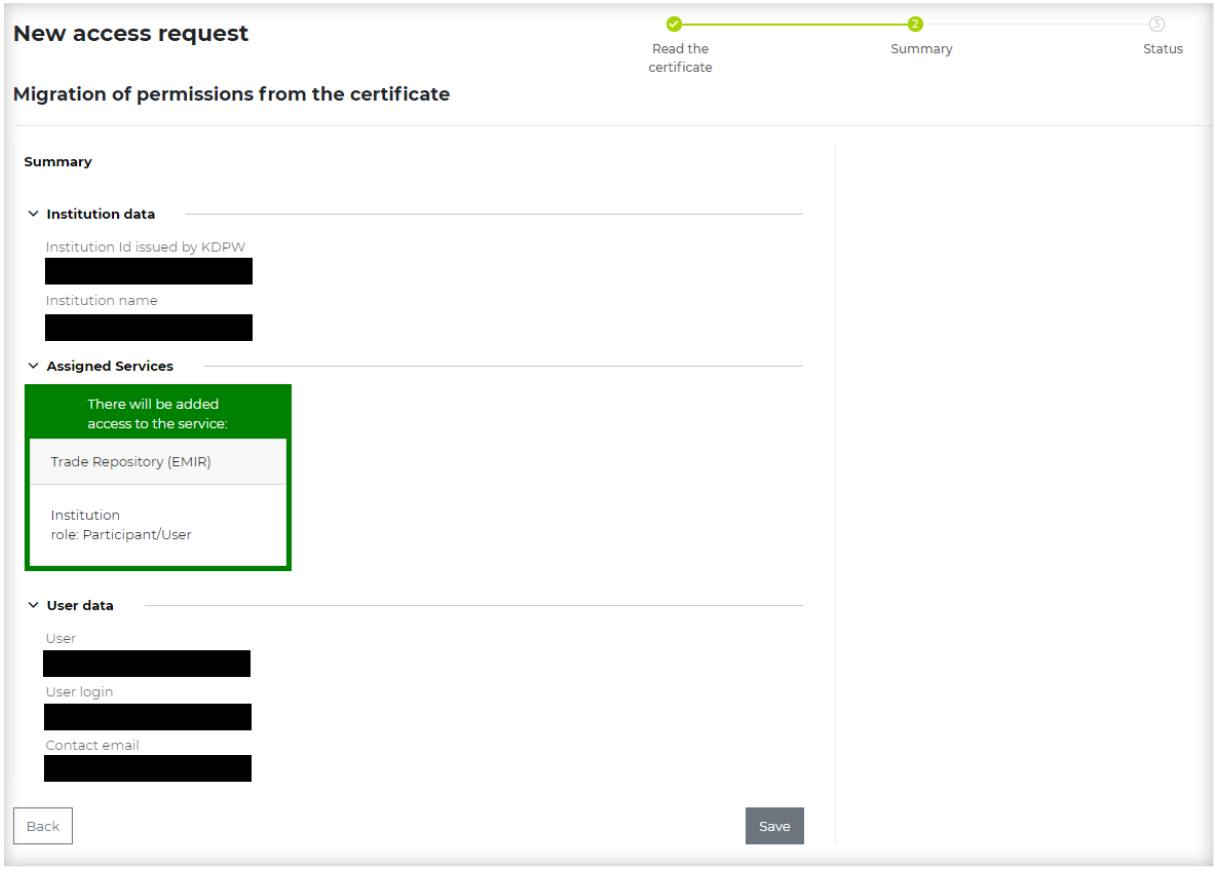

Fig. 10 Certificate migration acceptance

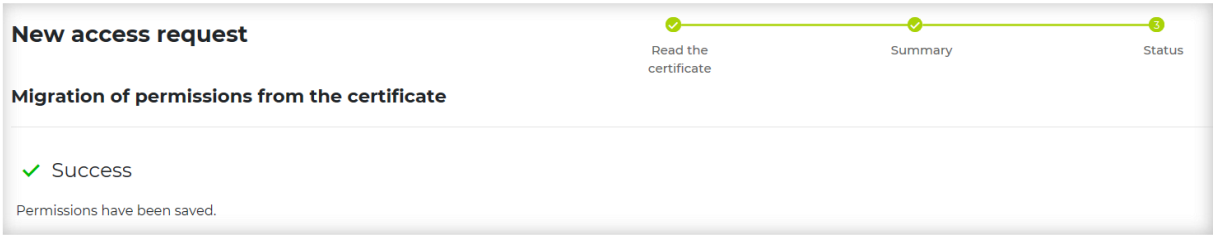

Fig. 11 Message about certificate migration

NOTE:

It is not necessary to deliver to KDPW a declaration attached to the email as part of the certificate migration process. A person who migrates the certificate will get a default “User” role. Successful completion of the steps described above allows full access to the KDPW_TR (EMIR) application in accordance with the migrated certificate.

Having successfully completed the steps described in this point, the user gets access to the KDPW_TR (EMIR and/or SFTR) application, which is confirmed in the “Access to services” view in the user profile (Fig. 12).

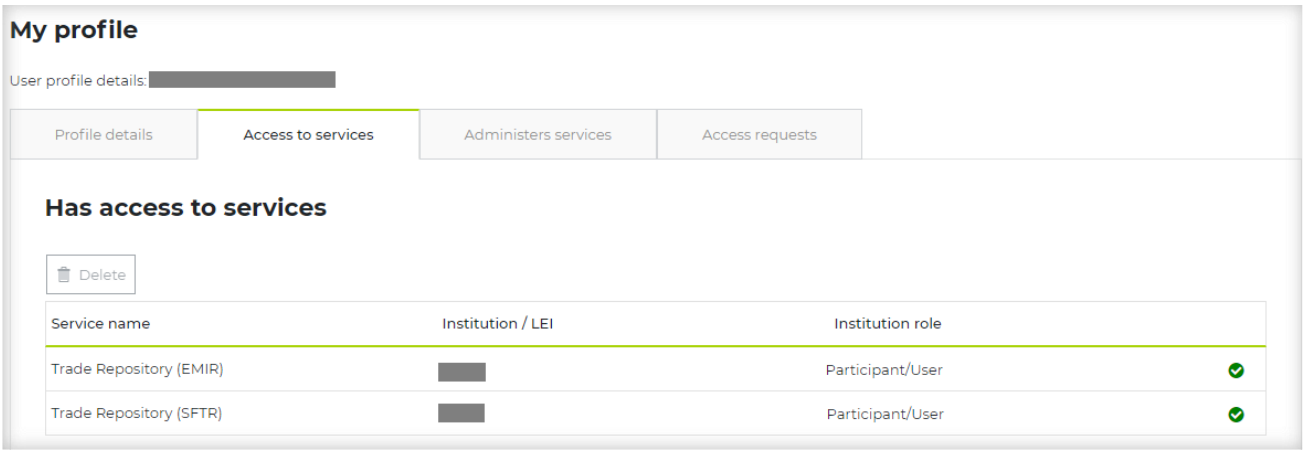

Fig. 12 Access to services screen

5. Getting access to KDPW_TR (EMIR and SFTR) by requesting access.

All KDPW_TR (SFTR) Participants as well as KDPW_TR (EMIR) Participants who do not hold active personal certificates issued by KDPW can get access to the application by submitting a request. A request for EMIR and SFTR need to be submitted separately.

To do that, please select “My desktop” from the upper-left corner of the screen and click the “Authorization” link located in the upper-right corner.

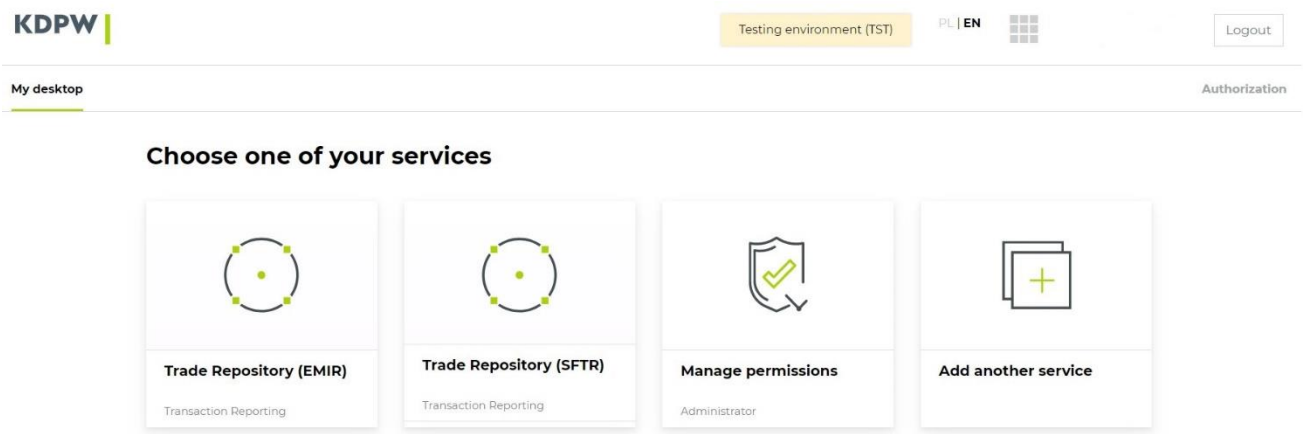

Fig. 13 User’s desktop

After you are redirected to a user's profile screen (Fig. 14), please select "New access request" from the left menu.

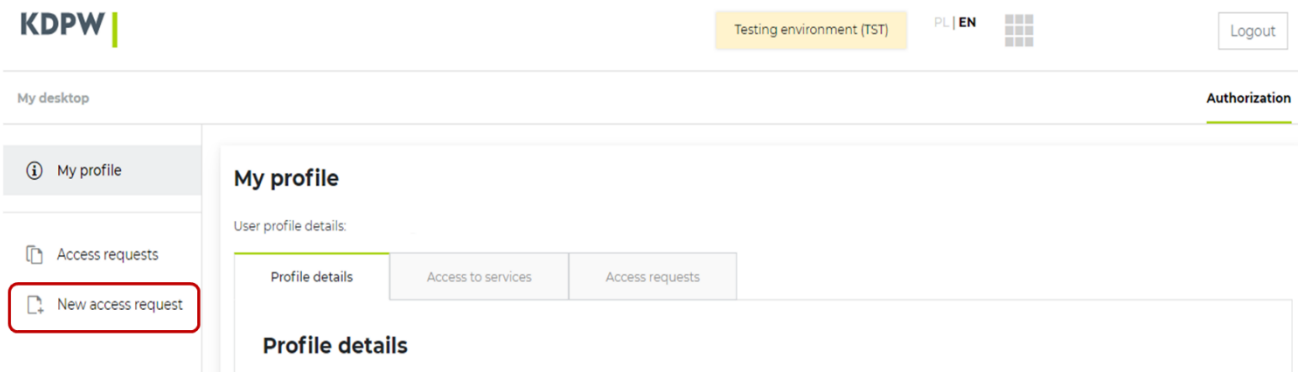

Fig. 14 User's profile screen

By using "Back" or "Continue" buttons located in the lower part of the page, it is possible to go back to the previous screens to fix incorrectly entered data. Each step of request submission is visualized as a green graphic located in the upper-right corner of the screen.

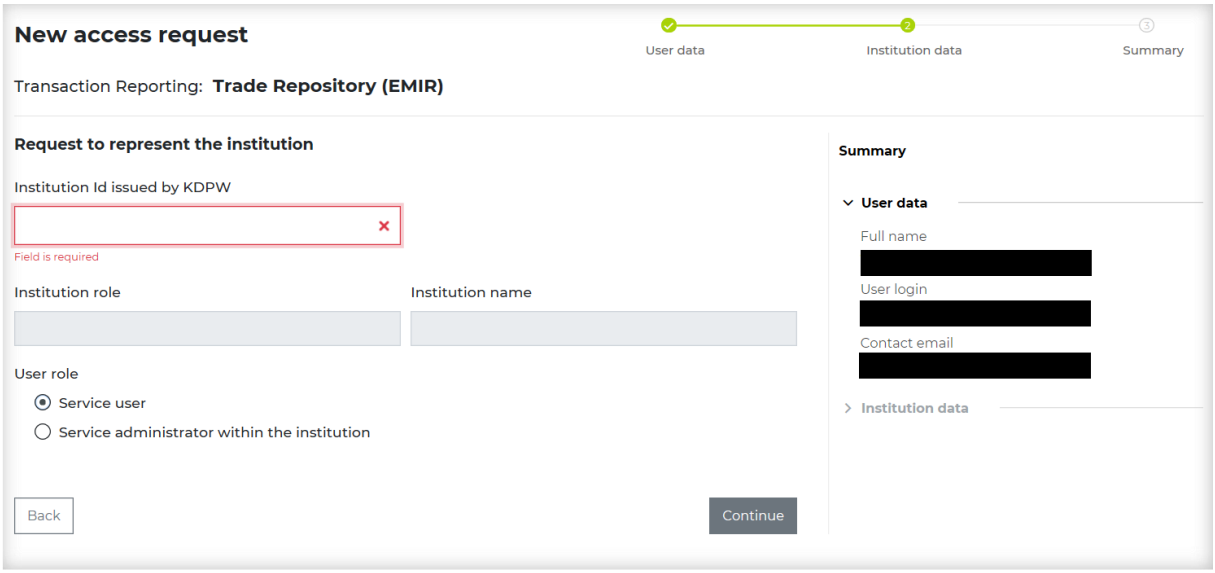

Fig. 15 New Access request – screen 2 (the same screen will show up for the Trade Repository SFTR)

After you accept, a summary screen will appear. Next, the user should review the content of the information clause and acknowledge it by checking the box underneath. If the data is correct, please click the grey "Submit request" button located in the lower-right corner of the summary (Fig. 16).

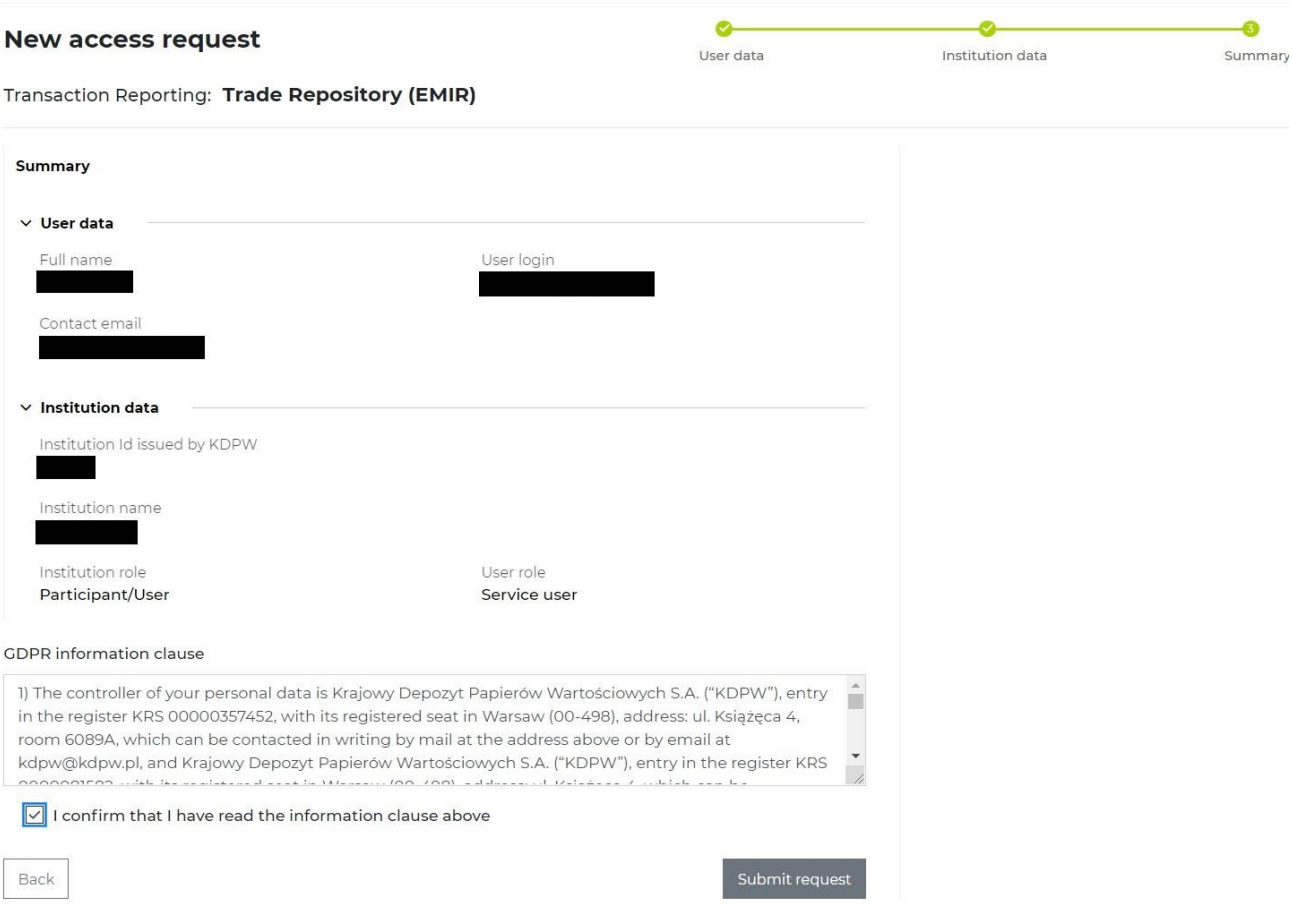

Fig. 16 New Access request – screen 3 (the same screen will show up for the Trade Repository SFTR)

After the request is submitted, a message confirming its correct submission will appear and a new entry awaiting approval will be created in the "Access requests" tab (Fig. 17). The user will receive a request submission confirmation at the provided contact email address.

In case an administrator role is selected with an institution, you should fill in a declaration that will be attached to the confirmation email. The declaration should be filled in according to the instruction attached to the message and sent back to the KDPW office.

In case a User role is selected, a request should be approved by the administrator.

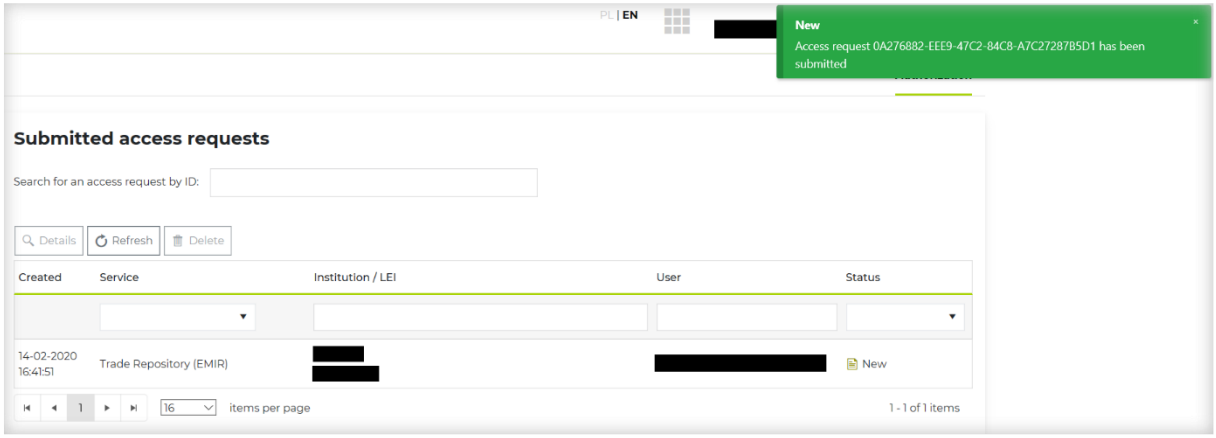

Fig. 17 Submitted access requests view

6. Service administrator – a role description

An account with an Administrator role can manage access permissions to the application on behalf of the Participant/entity who is a recipient of the service. The Administrator is allowed to grant access to the application to other persons as well as to revoke access from persons who have access as a User. The Administrator does not hold permissions to grant access to or revoke access from other persons acting with administrator role. This role is created for each application made available within the KDPW access system separately. Information which services a user manages are visible in the "Administers services" tab, which is available in "My profile" view as shown in the Fig. 18.

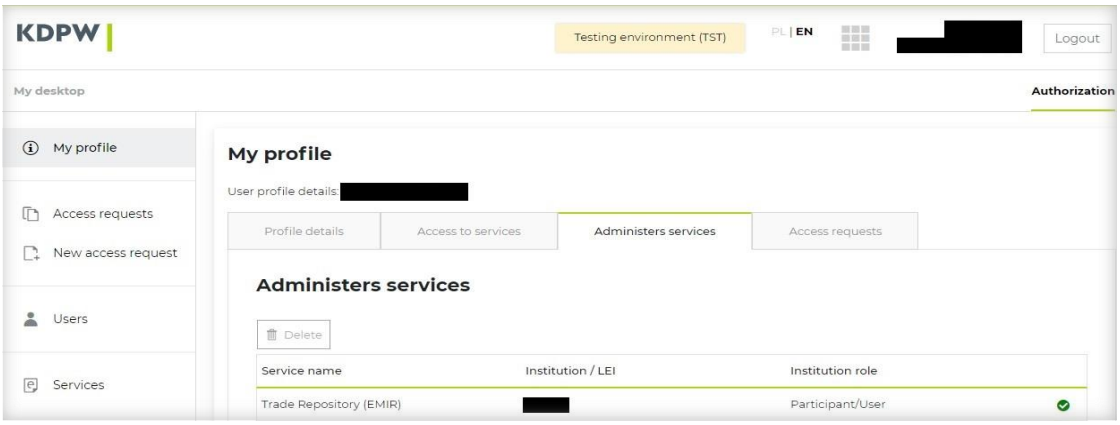

Fig. 18 Administrated services

Access requests for a service which the user administers are available in the "Access requests" view. The system user can filter requests by service type, institution name/LEI, email account and request status, as shown in Fig. 19.

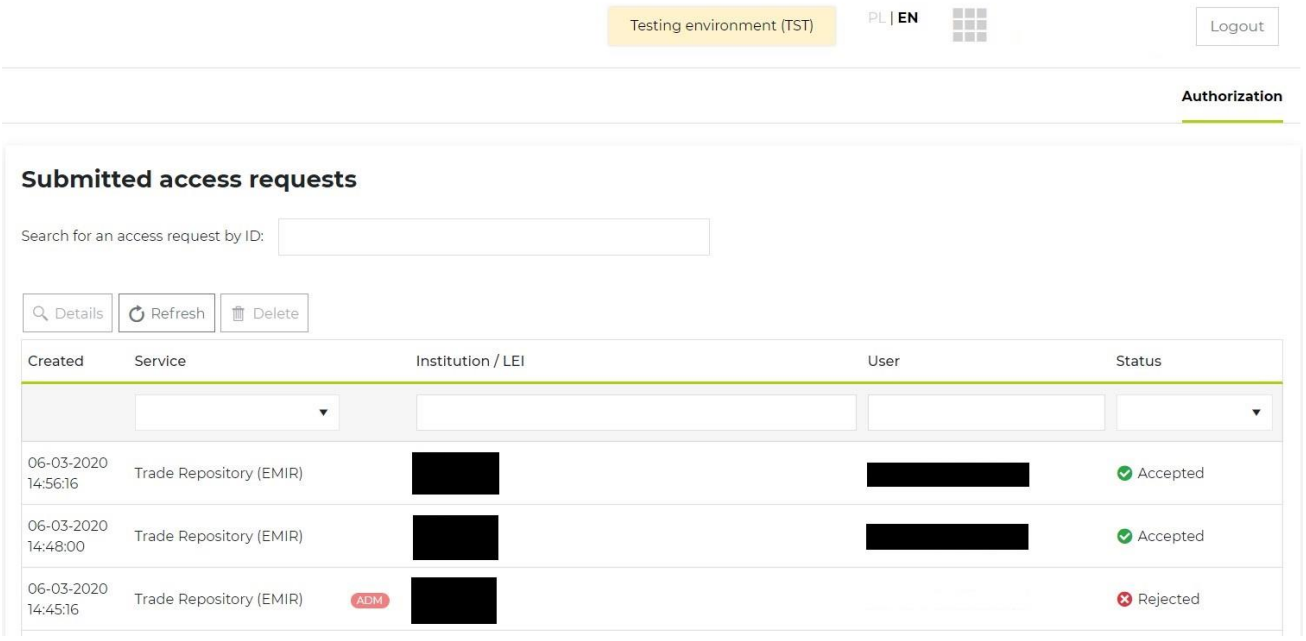

Fig. 19 Submitted requests

To approve or reject a request with a “New” status, select it with a left click and then click the “Details” button located above the request list.

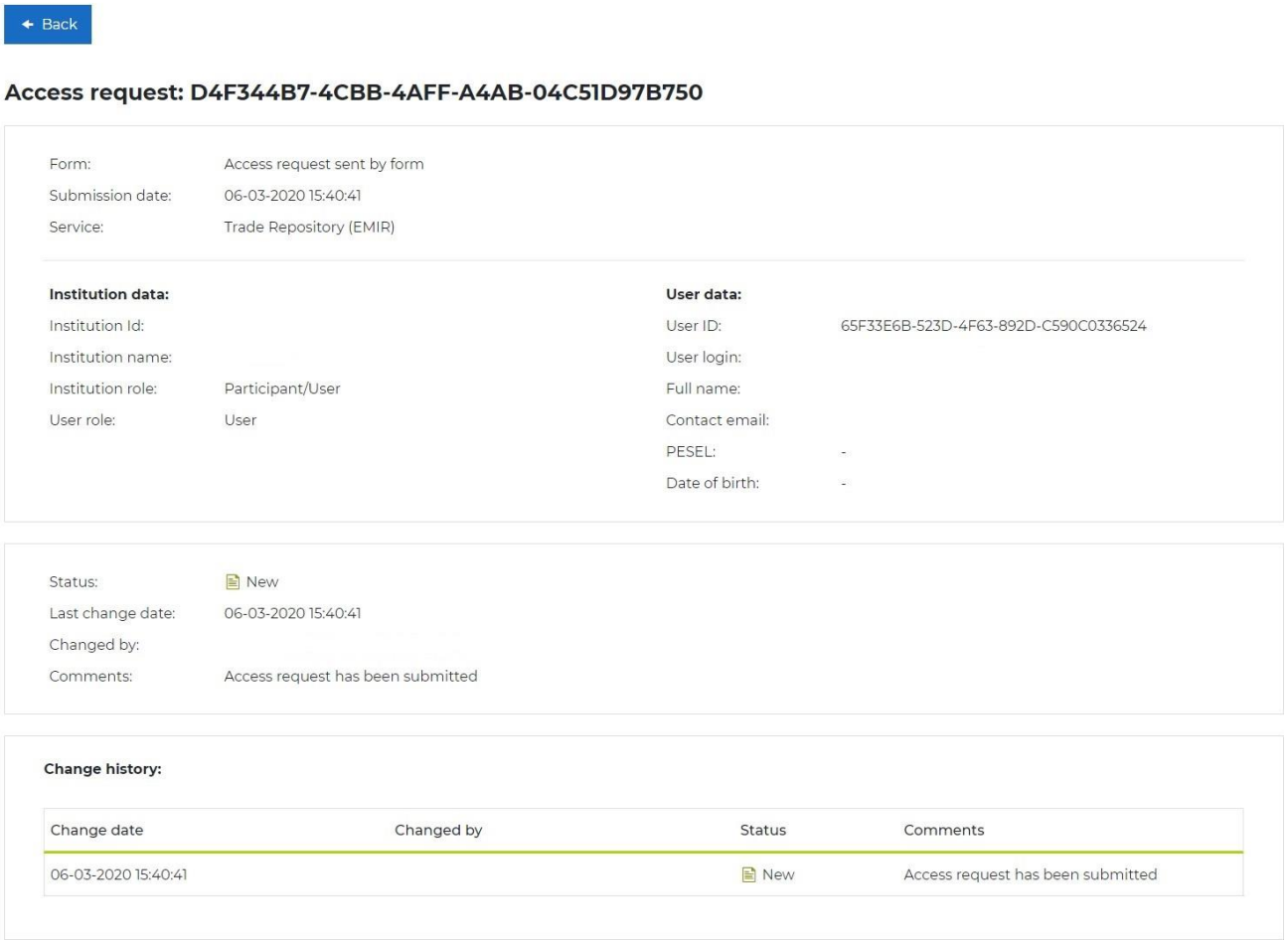

Fig. 20 Request approval

You will be redirected to the screen with the User data on behalf of whom the request has been submitted as well as the user data and a current state of request processing, as shown in Fig. 20.

From this view the service Administrator can approve or reject the request and add comments to their decision. After clicking “Approve access”, the user who submitted the request will be automatically granted application access permissions. Selecting “Reject” will refuse access. In both cases the User requesting an access will be informed about the Administrator’s decision by email.

NOTE: By approving an access request for a user, the administrator grants the user authorization to communicate with KDPW in the service.

The administrator can also revoke access to particular services from users. To do it, from the “Services” view left click on the appropriate service and select the “Details” button located above the list (Fig. 21).

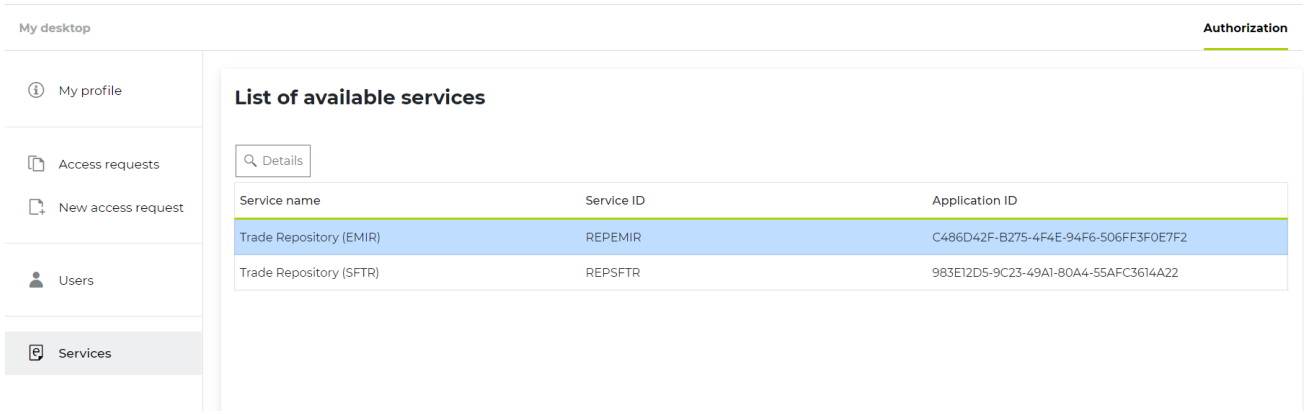

Fig. 21 Revoking access

The steps described above will redirect you to the “Services” details view, from which you need to go to “Authorised users”. From this tab the administrator can revoke access to the service by left clicking an appropriate user and selecting the “Delete” button located above the user table (Fig. 22). Using the “Delete” button will revoke access to the application from the selected person acting as a User.

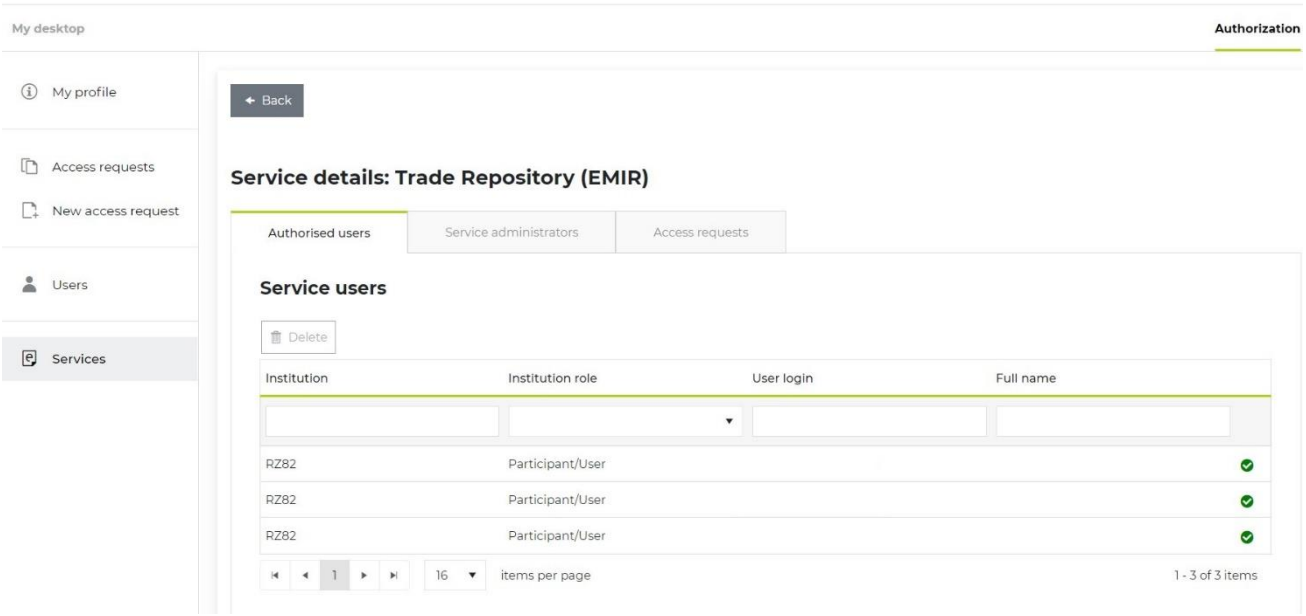

Fig. 22 Revoking access to the service

You can also remove user from the “Users” view by left clicking on an appropriate user and selecting the “Details” button (Fig. 23).

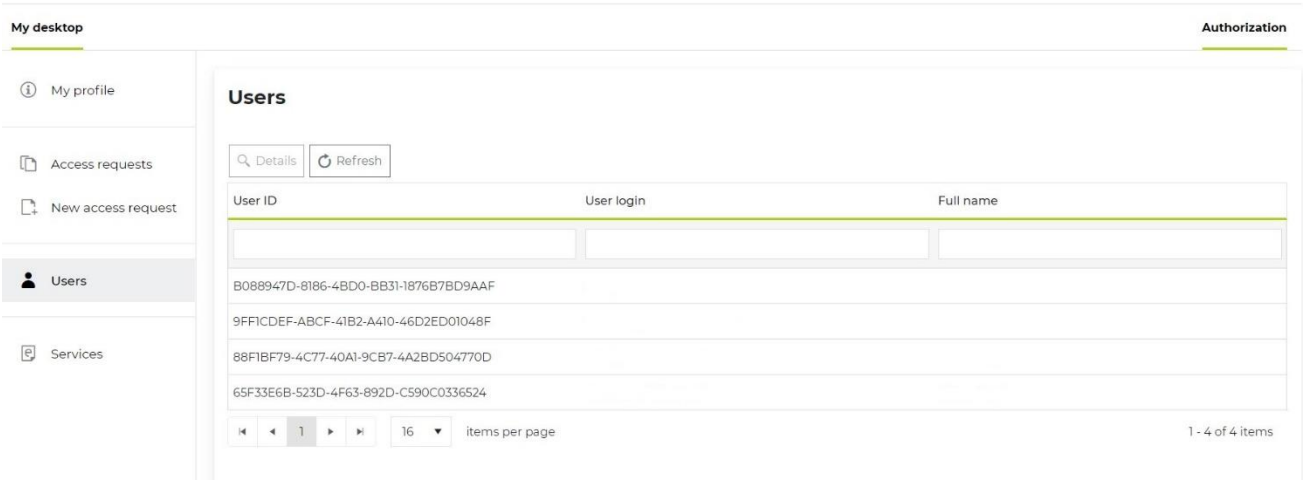

Fig. 23 Service Users

The steps described above will redirect you to the view from which you can go to the User information and services they have access to as a User or an Administrator. It is also possible to show requests submitted from the account. In the "Access to services" tab you can see services to which the user has access. From this tab you can revoke their access (Fig. 24).

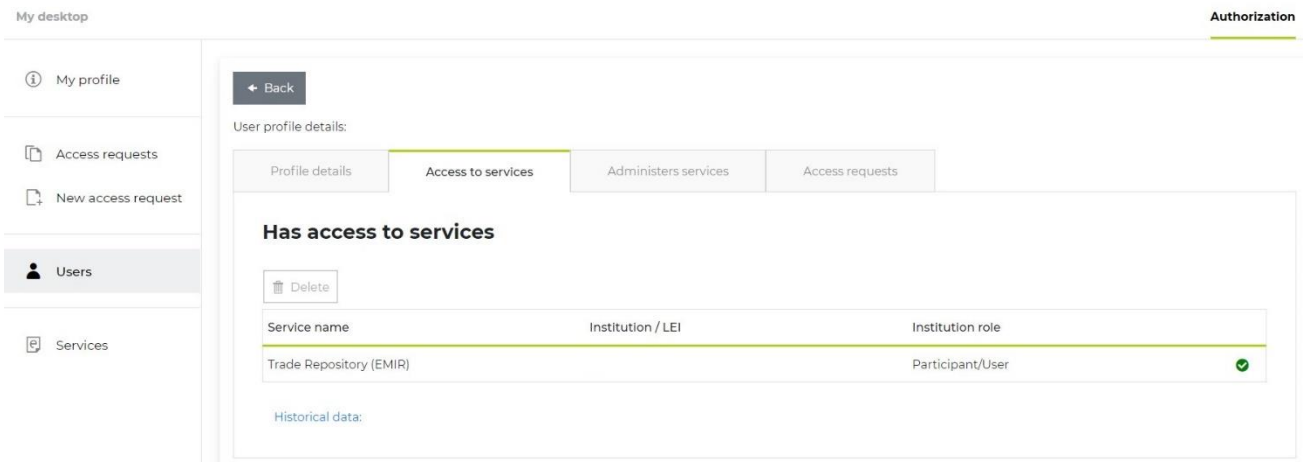

Fig. 25 Revoking access to the service

The Administrator can review the details of a service for which they act as an Administrator. To do this, in the "Services" view left click the appropriate service and select the "Details" button located above the list (Fig. 21). There are thematic tabs on the service screen (Fig. 25) which provide the following information:

- Permitted users – a list of persons with access to the service as users
- Service administrators – a list of persons with access to the services as administrators
- Submitted requests – a list of access requests submitted by users and administrators within a particular service and the status of these requests

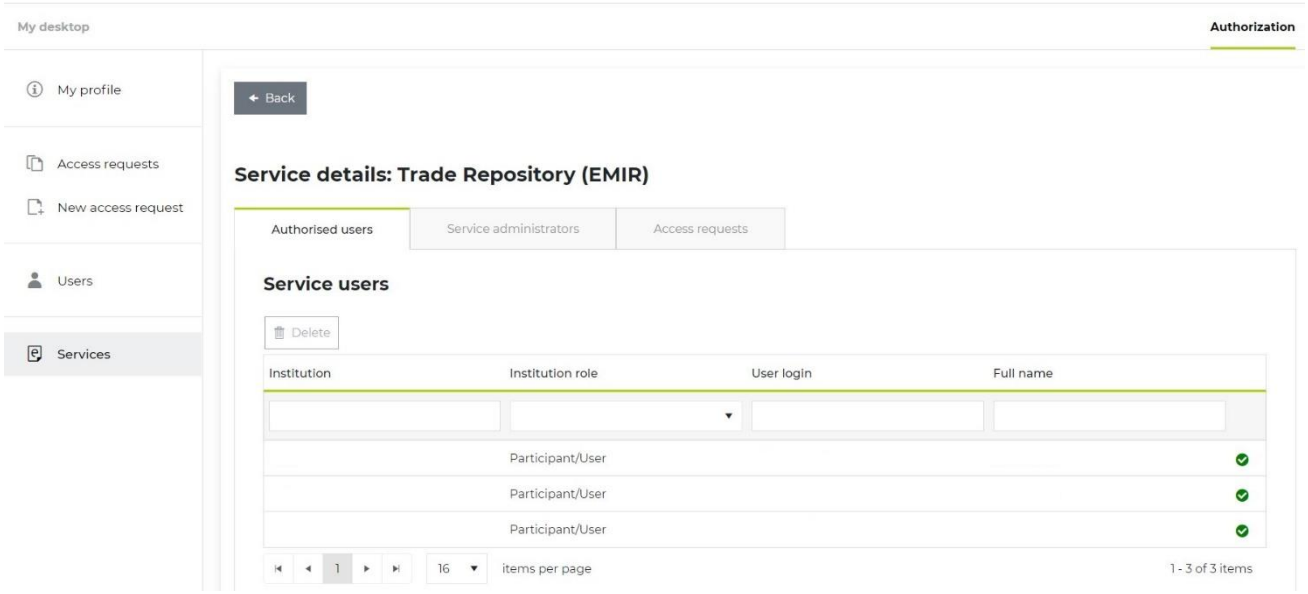

Fig. 25 Information about the service (the same screen will show up for Trade Repository SFTR)