Launching OTE IMP Sandbox mobile application on the OTE SandBox environment

1. Installing the application on a your mobile device:

a) Applications for Android:

- launch the application **Google Play** on a mobile device
- search OTE IMP Sandbox or use QR code:
- download the application to your mobile device and install it

b) Applications pro iOS:

- launch the application **App Store** on a mobile device.
- search OTE IMP Sandbox or use QR code:
- download the application to your mobile device and install it

2. Login to SandBox test secure portal - https://portal.sand.ote-cr.cz/otemarket/ , with an updated and valid certificate. If the user is not able to log in to the secure SandBox test portal, please contact OTE through email: Market@ote-cr.cz.

3. please check the user roles, ie the user who will use the OTE IMP SandBox mobile application will have the specified roles:

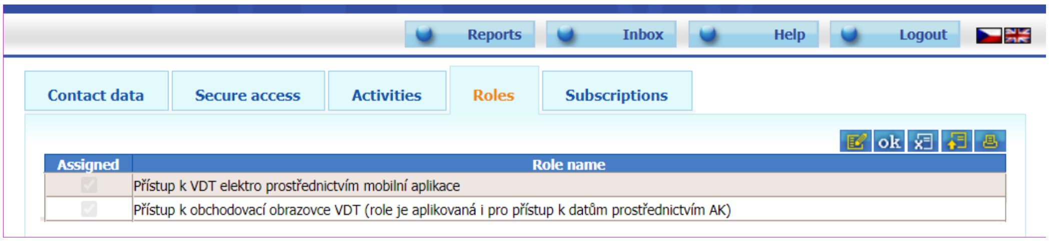
- **passive access** (reading):

  - Access to OTE IMP Sandbox via mobile application / *Přístup k VDT elektro prostřednictvím mobilní aplikace* (EmtasMImTsAcc)
  - Access to the IMP trading screen / *Přístup k obchodovací obrazovce VDT* (the role is also applied to access data via AK) (EmtasImTsAcc)

- **active access** (entering / deleting an offers):

  - Access to OTE IMP Sandbox via mobile application / *Přístup k VDT elektro prostřednictvím mobilní aplikace* (EmtasMImTsAcc)
  - Display of data and reports in a mobile application (EmtasImTsAcc)
  - Data modification for OTE IMP Sandbox via mobile application (EmtasMImIns)
  - Modification of data on the trading screen of OTE IMP Sandbox application(EmtasImIns)

We can check these roles in the master data of the CS OTE portal at the logged in person – Role tab:



Assigned	Role name
☑	Přístup k VDT elektro prostřednictvím mobilní aplikace
☑	Přístup k obchodovací obrazovce VDT (role je aplikovaná i pro přístup k datům prostřednictvím AK)

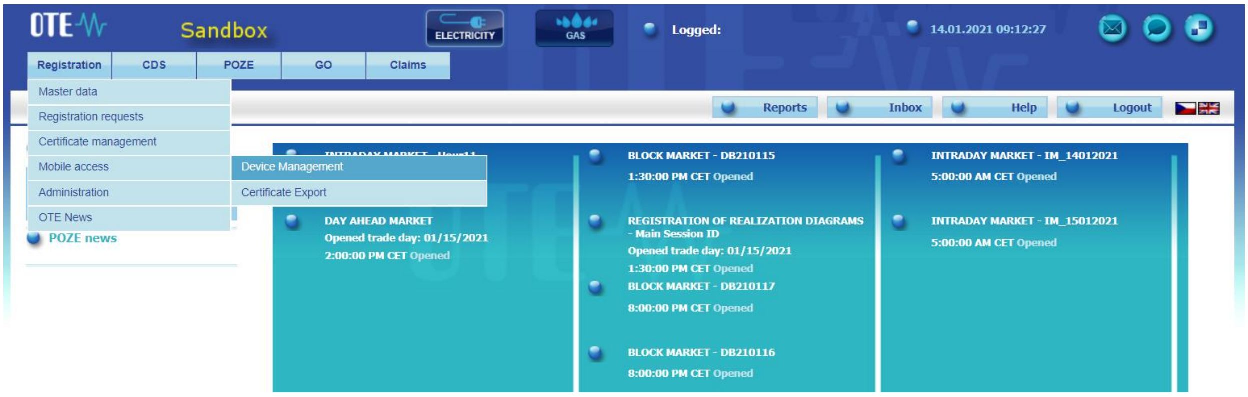
Roles necessary for passive access – master data CS OTE

4. On this test environment, OTE also set up write access for all existing OTECOM users for the OTE IMP Sandbox mobile application for testing purposes. However, OTE will set a stricter rule on the production environment, ie each person who has access to the OTECOM-ele client will ONLY have read access to the OTE IMP Sandbox mobile application. The right to write to the mobile application in the production environment will therefore have to be addressed by the user with his RUT master data administrator.

5. The procedure for activating the device on the SandBox secure portal, including creating a profile on the mobile device according to the attached procedure below:

Direct activation

- To create a mobile access by direct activation process, you must first log in to the CS OTE web portal on the SandBox environment (https://portal.sand.ote-cr.cz/otemarket/).
- Menu **Registration** choose **Mobile access – Device management**



INTRADAY MARKET - Hour11

DAY AHEAD MARKET
Opened trade day: 01/15/2021
2:00:00 PM CET Opened

BLOCK MARKET - DB210115
1:30:00 PM CET Opened

REGISTRATION OF REALIZATION DIAGRAMS - Main Session ID
Opened trade day: 01/15/2021
1:30:00 PM CET Opened

BLOCK MARKET - DB210117
8:00:00 PM CET Opened

BLOCK MARKET - DB210116
8:00:00 PM CET Opened

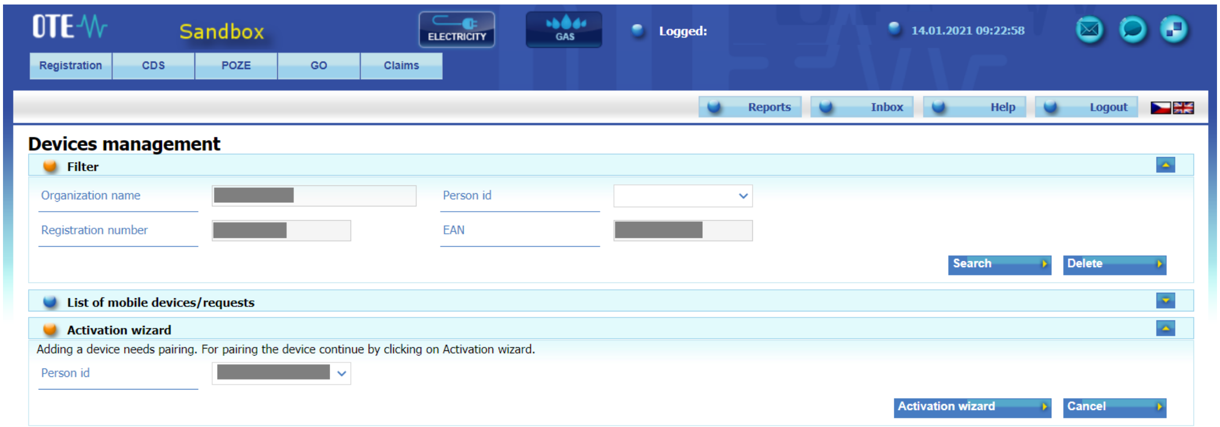
INTRADAY MARKET - IM_14012021
5:00:00 AM CET Opened

INTRADAY MARKET - IM_15012021
5:00:00 AM CET Opened

Fig. 1 – Direct activation – Web portal CS OTE – Device management

- Now press the button **New Activation.** You will see Device Detail, where your user account will be listed in the Person ID.

- To start activating your mobile device, click the Activation Wizard (Fig. 2).



Devices management

Filter

Organization name [redacted]

Person id

Registration number [redacted]

EAN [redacted]

List of mobile devices/requests

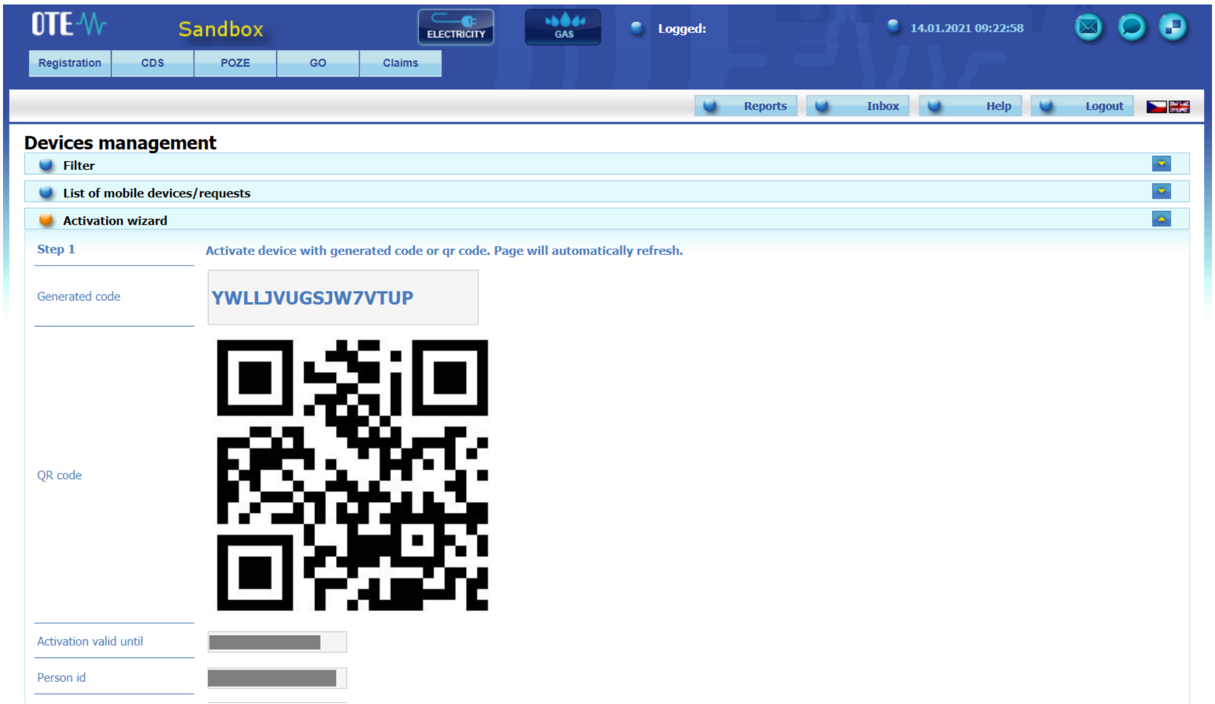
Activation wizard

Adding a device needs pairing. For pairing the device continue by clicking on Activation wizard.

Person id [redacted]

Fig. 2 – Direct activation – Web portal CS OTE – Activation wizard

- After pressing the **Activation Wizard** button a page with generated QR code will be displayed for activating Moble device:



Devices management

Filter

List of mobile devices/requests

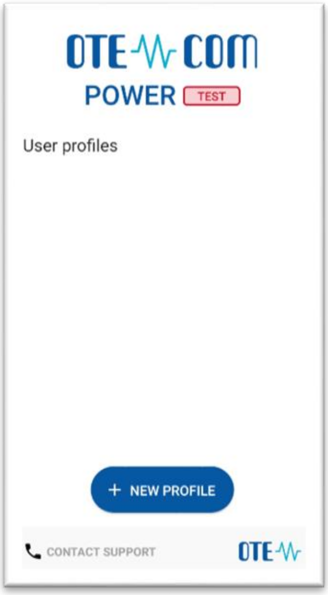
Activation wizard

Step 1	Activate device with generated code or qr code. Page will automatically refresh.
Generated code	YWLLJVUGSJW7VTUP
QR code	
Activation valid until	[redacted]
Person id	[redacted]

Fig. 3 – Direct activation – Web portal Sandbox

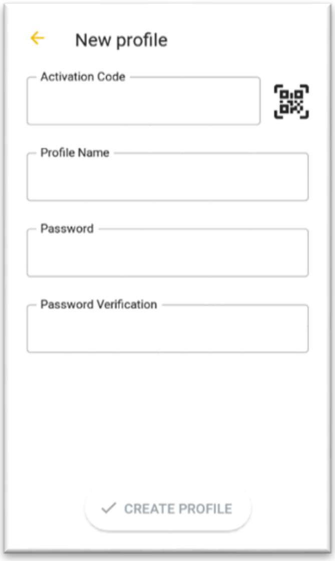
- Now you need to transfer your activation QR code to your mobile device until certain time, which is listed in the field **Activation valid until** (Fig. 3).

- Launch OTE IMP Sandbox application on your mobile device.
  When you start a newly installed application, you are asked to agree to the License Terms. These terms is necessary to confirm otherwise it will not be allowed to access the application.
  Then click **New profile**.



User profiles

Fig. 4 – Direct activation – Mobile app – New profile



New profile

Activation Code

Profile Name

Password

Password Verification

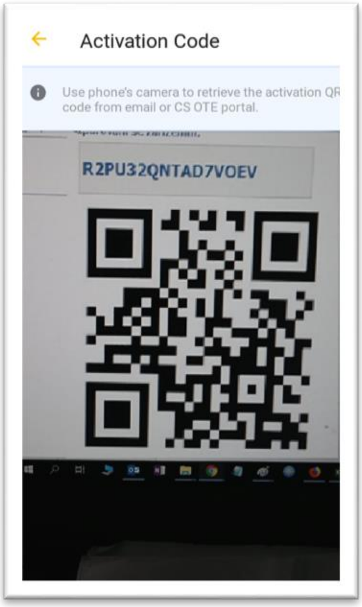
Fig. 5 – Direct activation – Mobile app – Account information

- Enter the generated QR code in the **Activation code** field.

  This code can be detected by the camera or entered manually:

  - Press ⛶ . Your mobile device's camera will start (Fig. 6). Point the camera at the QR code screen. The mobile device records the code, which is usually reflected in the device's vibration.

  - The second option is to type the **Activation Code** itself (located on CS OTE web portal) to the field **Activation code**.



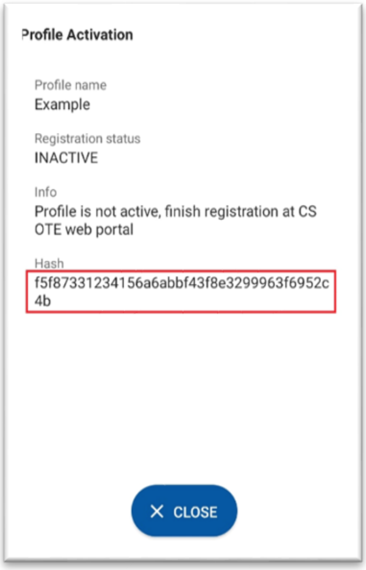
Activation Code

Use phone's camera to retrieve the activation QR code from email or CS OTE portal.

R2PU32QNTAD7VOEV

Fig. 6 – Direct activation – Mobile app – Activation code

- Enter a name for the new profile in the **Profile Name** field.
- Create a Password that contains at least 4 characters and repeat it in the Password field again. The password you enter is used to secure your profile and certificate against unauthorized use.
- Clicking **Create profile** (Fig. 5) you create new, not yet approved profile in the IMP Sandbox mobile ap.



Profile Activation

Profile name
Example

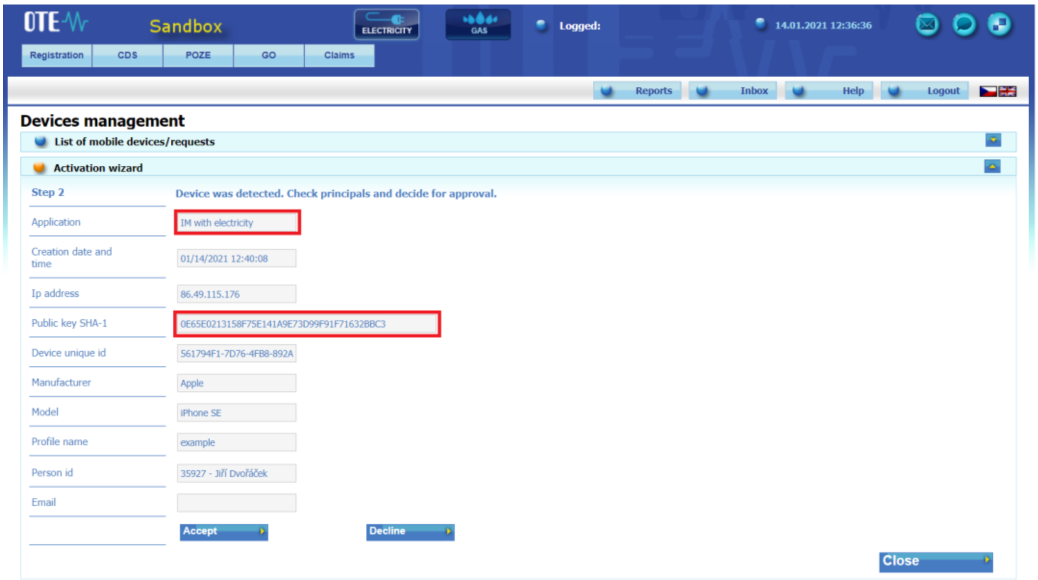
Registration status
INACTIVE

Info
Profile is not active, finish registration at CS OTE web portal

Hash
f5f87331234156a6abbf43f8e3299963f6952c4b

Fig. 7 – Direct activation – Mobile app – Created profile

- After you create a new profile on a mobile device, the Activation Wizard page on the web portal automatically goes to a point that requires accepting or rejecting the link for that mobile Device to this account on CS OTE.
  The **Application** on the screen of CS OTE could be type of ***IM with Gas*** , ***Renewable resources,*** or **IMD with electricity** depending on the type of mobile apllication used to create the profile.



Devices management

List of mobile devices/requests

Activation wizard

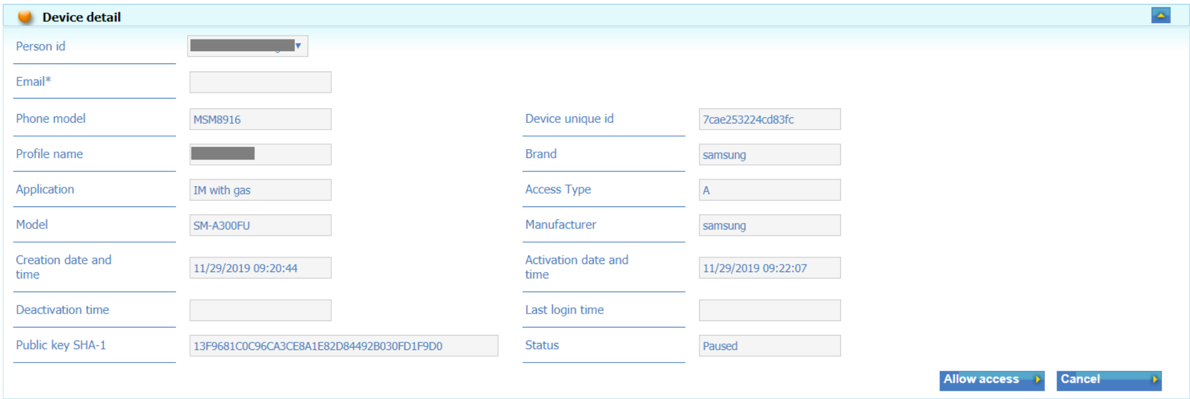
Step 2	Device was detected. Check principals and decide for approval.
Application	IM with electricity
Creation date and time	01/14/2021 12:40:08
Ip address	86.49.115.176
Public key SHA-1	0E65E0213158F75E141A9E73D99F91F71632BBC3
Device unique id	561794F1-7D76-4FB8-892A
Manufacturer	Apple
Model	iPhone SE
Profile name	example
Person id	35927 - Jiří Dvořáček
Email	

Fig. 8 – Direct activation – Web portal

- It is **recommended to** check that the red-framed codes in Fig. 7 and Fig. 8 are the same on the mobile device and in the CS OTE web portal.
- Click **Accept** (Fig. 8) and sign with certificate.

- After pressing the **Accept** button and confirming by **signature** the mobile device is paired and from now is clearly identifiable for CS OTE. Now your account is in the "**Suspended**" status and your mobile device can't sign in to the mobile app yet. The **Mobile Device Detail** appears on the portal– permission can be performed by a person with the **Master Data Administrator role**.

- Having the RMP Administrator role, you now see the **Allow Access** button. Press it to allow the mobile device access the IMP network. Continuation – 2.Login to SandBox test secure portal -



Device detail

Person id	[redacted]		
Email*			
Phone model	MSM8916	Device unique id	7cae253224cd83fc
Profile name	[redacted]	Brand	samsung
Application	IM with gas	Access Type	A
Model	SM-A300FU	Manufacturer	samsung
Creation date and time	11/29/2019 09:20:44	Activation date and time	11/29/2019 09:22:07
Deactivation time		Last login time	
Public key SHA-1	13F9681C0C96CA3CE8A1E82D84492B030FD1F9D0	Status	Paused

Fig. 9 - Direct activation – Web portal – Device detail

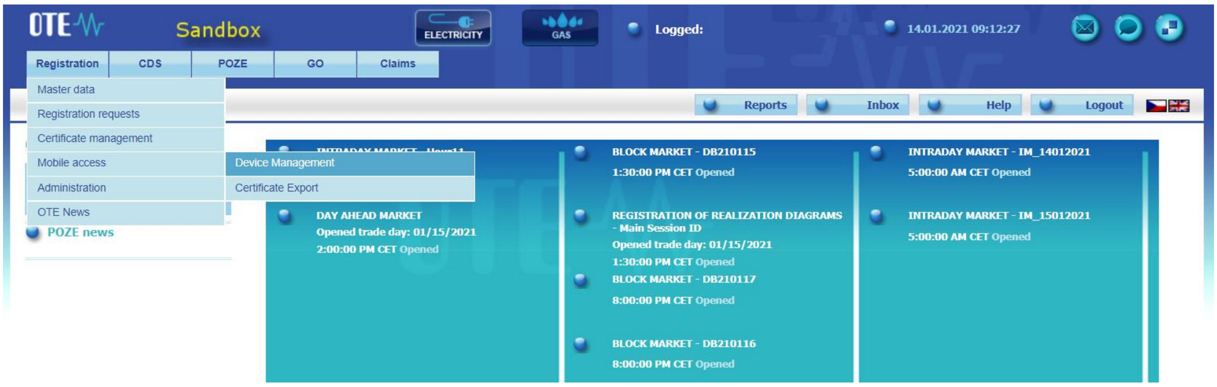
- Now the account is in the Approved status and the direct activation is completed successfully. The mobile application can be logged in and after the import of a valid qualified certificate registered in CS OTE, the mobile application can be fully used.

Administrator Activation (user with role RMP Administrator)

- Administrator activation for another user registered in master data is applicable to a user who may or may not have a certificate to access CS OTE. Activation is performed in three steps. The process is done in the three steps.

1st step – Administrator

- Log in to the portal CS OTE (https://portal.sand.ote-cr.cz/otemarket/).
- Menu **Registration** choose **Mobile access – Device management**.



DAY AHEAD MARKET
Opened trade day: 01/15/2021
2:00:00 PM CET Opened

BLOCK MARKET - DB210115
1:30:00 PM CET Opened

REGISTRATION OF REALIZATION DIAGRAMS - Main Session ID
Opened trade day: 01/15/2021
1:30:00 PM CET Opened

BLOCK MARKET - DB210117
8:00:00 PM CET Opened

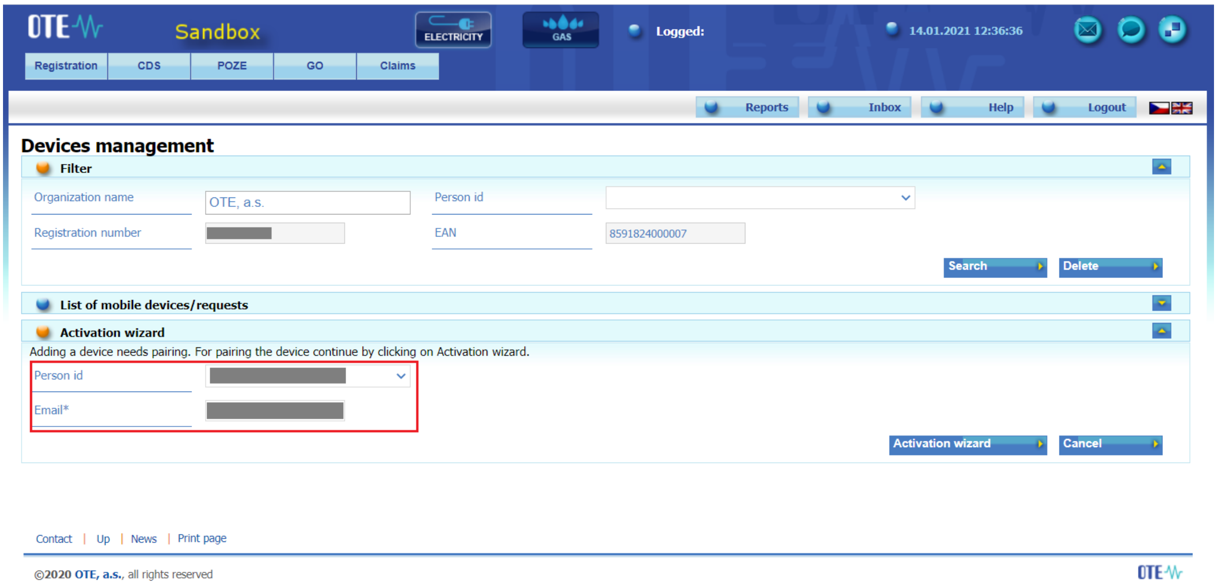
BLOCK MARKET - DB210116
8:00:00 PM CET Opened

INTRADAY MARKET - IM_14012021
5:00:00 AM CET Opened

INTRADAY MARKET - IM_15012021
5:00:00 AM CET Opened

Fig. 10 – Administrator Activation – Web portal CS OTE – Device management

- After selecting **New activation**, the **Device detail** is displayed on the page.
- Select a person from the list: **Person ID** - the ID of the person for whom you are creating mobile access. When you select the desired user, an **email** field appears that can be left or changed:



Devices management

Filter

Organization name	OTE, a.s.	Person id	
Registration number	[redacted]	EAN	8591824000007

List of mobile devices/requests

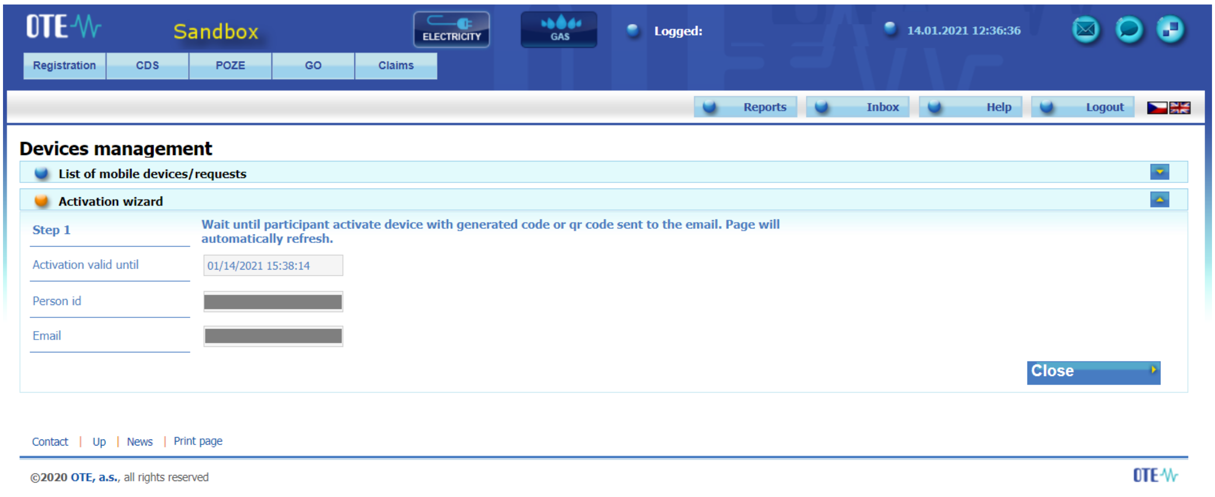
Activation wizard

Adding a device needs pairing. For pairing the device continue by clicking on Activation wizard.

Person id	[redacted]
Email*	[redacted]

Fig. 11 – Administrator Activation – Web portal– Devices management

- After selecting the person and possibly changing the email, click on the **Activation Wizard** button (Fig. 11).
- A message containing the QR code designed to activate your mobile device has been sent to the email. The system now waits for one hour to retrieve the QR code of the selected user as the second part of the activating new profile in the mobile app (Fig. 12). It is necessary to read the QR code by the mobile device within one hour, otherwise the activation will expire (see above).



Devices management

Step 1 — Wait until participant activate device with generated code or qr code sent to the email. Page will automatically refresh.

Activation valid until: 01/14/2021 15:38:14

Person id: [redacted]

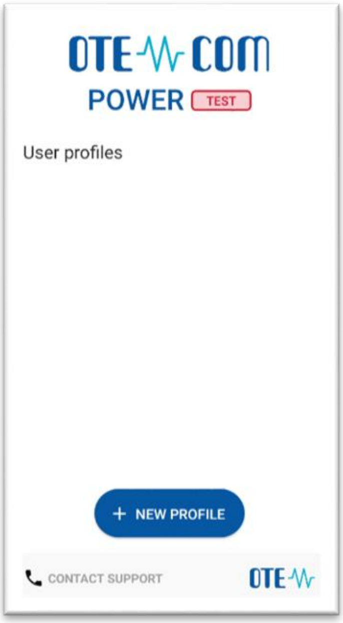
Email: [redacted]

©2020 OTE, a.s., all rights reserved

Fig. 12 – Administrator Activation – Web portal

2nd step – user setting up a profile on their mobile device

- Launch mobile application **OTE IMP Sandbox.**
- Click the button **New profile**



User profiles

Fig. 13 – User Activation with support of the Administrator - Mobile App – New profile

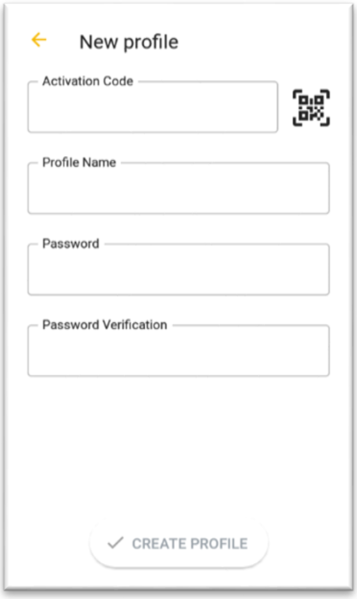
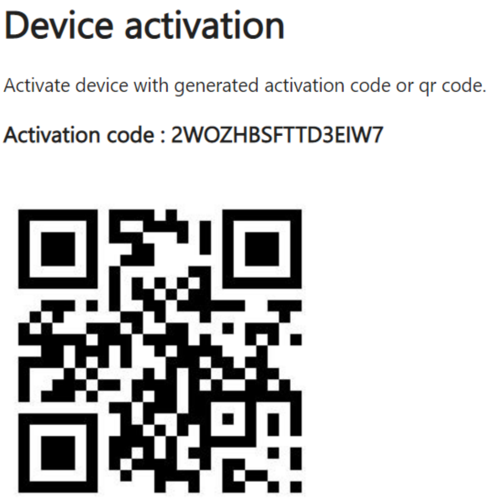


Fig. 14 - User Activation with support of the Administrator - Mobile App – Profile information

- In the Activation Code field, enter the QR code from the email sent by your administrator (Fig. 15) this way:



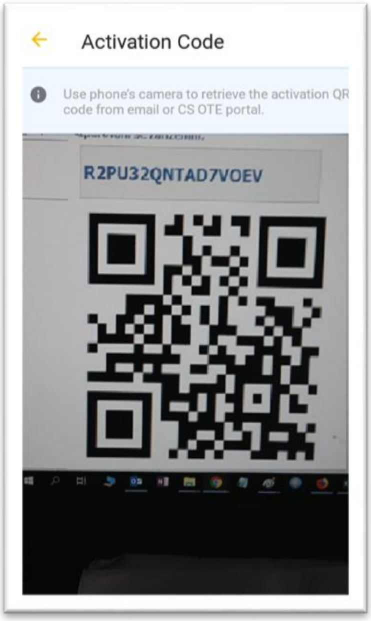
Device activation

Activate device with generated activation code or qr code.

Activation code : 2WOZHBSFTTD3EIW7

Fig. 15 – Administrator Activation – E-mail with Activation QR code

- Click ⛶ on the mobile device to launch the camera of your mobile device (Fig. 16).
  - Point the camera at the QR code screen. The mobile device records the code, which is usually reflected in the device's vibration.



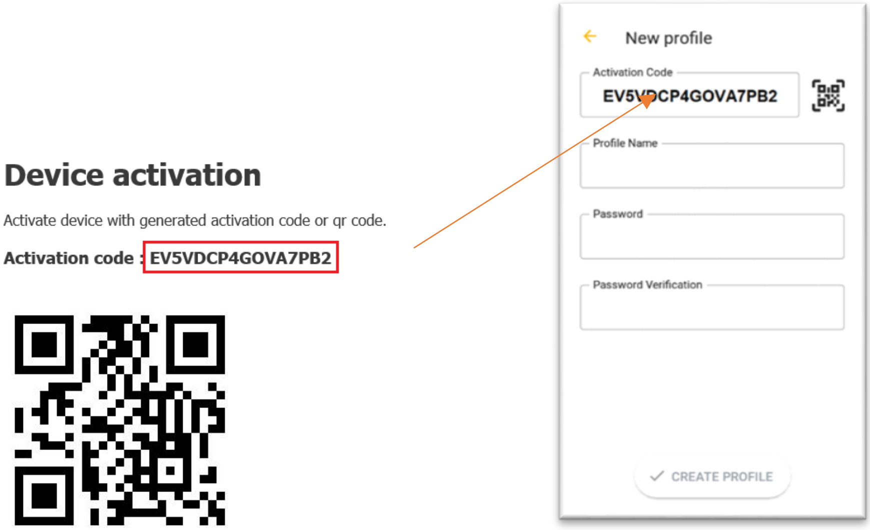
Activation Code

Use phone's camera to retrieve the activation QR code from email or CS OTE portal.

R2PU32QNTAD7VOEV

Fig. 16 - User Activation with support of the Administrator - Mobile App – New profile

- The second option is to copy the **Activation Code** itself (from the CS OTE web portal) to the field **Activation code**.



Device activation

Activate device with generated activation code or qr code.

Activation code : EV5VDCP4GOVA7PB2

New profile

Activation Code: EV5VDCP4GOVA7PB2

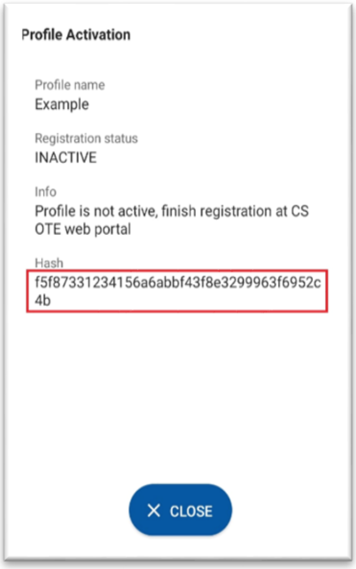
Profile Name

Password

Password Verification

- Enter the name for the new profile in the **Profile Name** field.
- Create a **Password** that contains at least 4 characters and repeat it in the **Password** field **again**. The password you enter is used to secure your profile and certificate against unauthorized use.

- Clicking **Create profile** you create a new, not yet approved profile in OTE IMP Sandbox mobile app.



Profile Activation

Profile name
Example

Registration status
INACTIVE

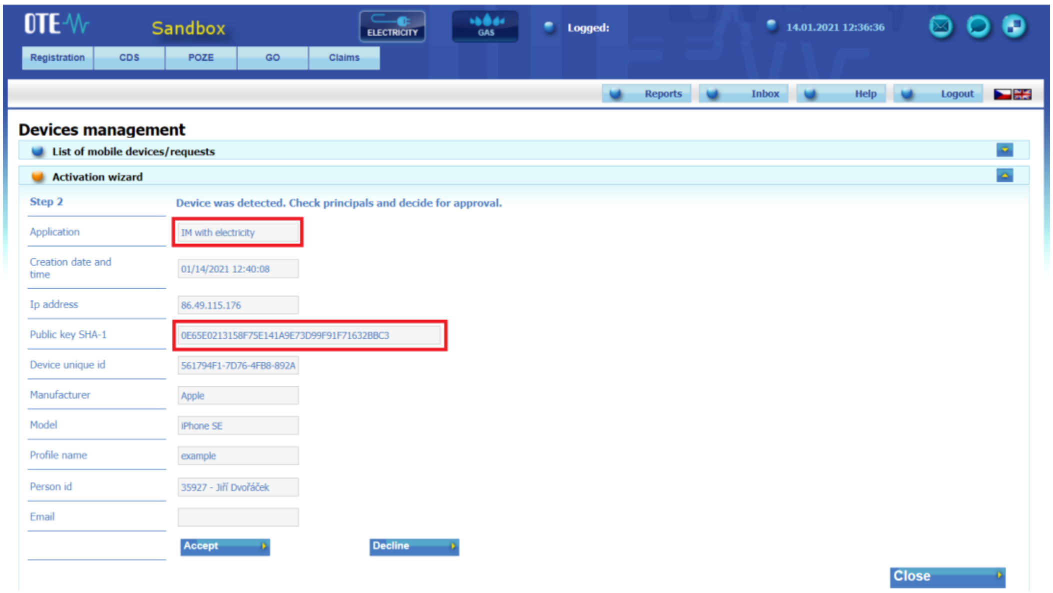
Info
Profile is not active, finish registration at CS OTE web portal

Hash
f5f87331234156a6abbf43f8e3299963f6952c4b

Fig. 17 – New Profile Information (suspended yet)

- After you create **New profile** on a mobile device, the Activation Wizard page on the RMP master data web portal automatically goes to the point where it can be checked which application was triggered and the public key fingerprint on the mobile device and CS OTE portal.
- Contact your Administrator now to finish activating process**.**

<u>3rd step – Administrator</u>



Devices management

List of mobile devices/requests

Activation wizard

Step 2	Device was detected. Check principals and decide for approval.
Application	IM with electricity
Creation date and time	01/14/2021 12:40:08
Ip address	86.49.115.176
Public key SHA-1	0E65E0213158F75E141A9E73D99F91F71632BBC3
Device unique id	561794F1-7D76-4FB8-892A
Manufacturer	Apple
Model	iPhone SE
Profile name	example
Person id	35927 - Jiří Dvořáček
Email	

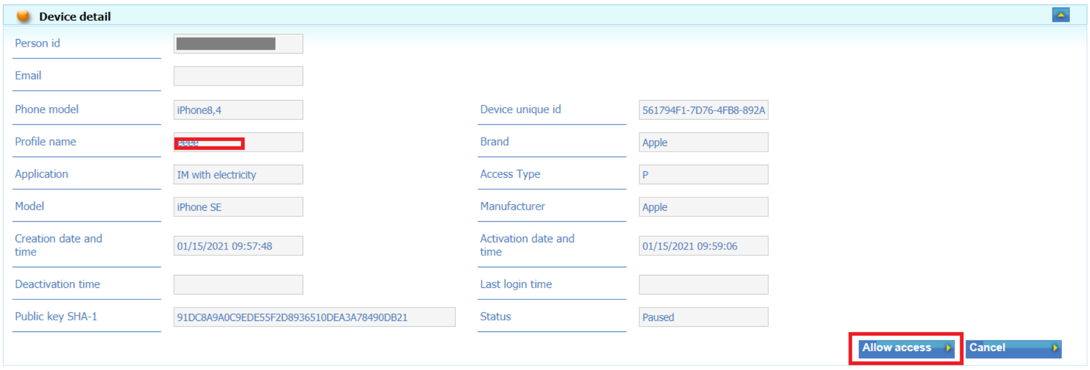
Fig. 18 – Administrator Activation – Web portal

- **We recommend checking**

  - 1. **Application** –whether it contains the desired application for which the activation is to be performed
  - 2. If the **red-framed codes** - Fig. 17 (New Profile Information (suspended yet)) and Fig. 18 (Administrator Activation – Web portal) displaying the public key fingerprint are identical on the mobile device and in the CS OTE web portal.

- By clicking on **Accept** (Fig. 18) and signing with certificate, the mobile device of the user for whom you approve mobile access is clearly identifiable for CS OTE. However, this profile is currently suspended and cannot be signed in.

- At the same time, CS OTE also displays the **Mobile Device Detail** in Device Manager, where after checking the linked application it is possible to allow access of the mobile device to the VDE Sandbox network by clicking on the **Allow access** (Fig. 19 – Administrator Activation - Web portal – Fig. **9**). As RUT - Master Data Manager on the page, you will see a **Allow Access** button. Pressing it will change to the **Approved** state and it is possible to log in to the mobile application under this account. If you do not see the button, contact RUT Data Administrator for your company, who can activate the account.



Device detail

Person id	[redacted]		
Email			
Phone model	iPhone8,4	Device unique id	561794F1-7D76-4FB8-892A
Profile name	eeee	Brand	Apple
Application	IM with electricity	Access Type	P
Model	iPhone SE	Manufacturer	Apple
Creation date and time	01/15/2021 09:57:48	Activation date and time	01/15/2021 09:59:06
Deactivation time		Last login time	
Public key SHA-1	91DC8A9A0C9EDE55F2D8936510DEA3A78490DB21	Status	Paused

Fig. 19 – Administrator Activation - Web portal – Device detail

Login Process

- Launch OTE IMP Sandbox mobile application
- When you start a newly installed application, you are asked to agree to the License Terms. These terms is necessary to confirm otherwise it will not be allowed to access the application.
- Select the created profile

- Enter a password or fingerprint

- If the login is unsuccessful after 5 incorrectly read fingerprints, then it is indicated by a lock symbol next to the fingerprint on the login screen. Entering the password is still possible.

- If the login is successful, the **Setup Wizard** will appear

- PIN must be set and repeated (enter the same 4-digit PIN twice in succession on the displayed numeric keypad)

- Fingerprint configuration – if our mobile device allows BIOmetric authentication, we can choose whether we want to use the fingerprint for Login or/and for entering the PIN.

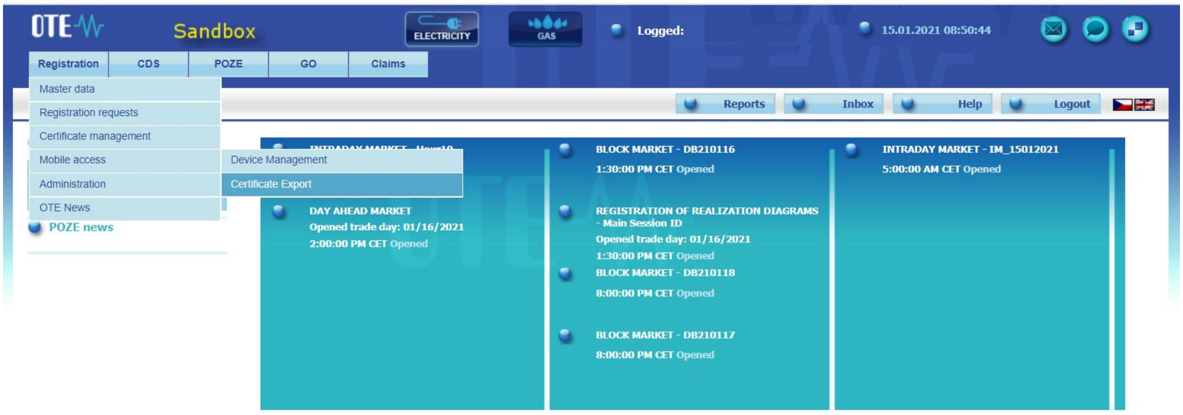
- In the next step, it is necessary to import a qualified certificate stored in CS OTE:

The process of transferring a certificate from the CS OTE system requires the simultaneous use of a PC with activated local storage for the CS OTE or PKi component and a mobile device.

Transfer a certificate to a mobile device

1) Log in to the Sandbox CS OTE web portal (https://portal.sand.ote-cr.cz/otemarket/)

- In menu **Registration**, select **Mobile Access - Certificate Export**.(Fig. 20)



INTRADAY MARKET - Hour10

DAY AHEAD MARKET
Opened trade day: 01/16/2021
2:00:00 PM CET Opened

BLOCK MARKET - DB210116
1:30:00 PM CET Opened

REGISTRATION OF REALIZATION DIAGRAMS - Main Session ID
Opened trade day: 01/16/2021
1:30:00 PM CET Opened

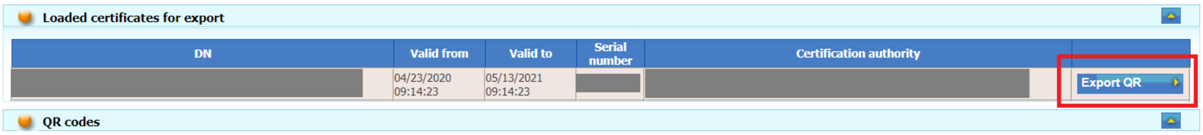
BLOCK MARKET - DB210118
8:00:00 PM CET Opened

BLOCK MARKET - DB210117
8:00:00 PM CET Opened

INTRADAY MARKET - IM_15012021
5:00:00 AM CET Opened

Fig. 20 – Certificate Export – Web portal

a) In the case of an active Local Store, certificates are displayed directly, which can be exported to a mobile device by clicking on **Export QR** (see below):

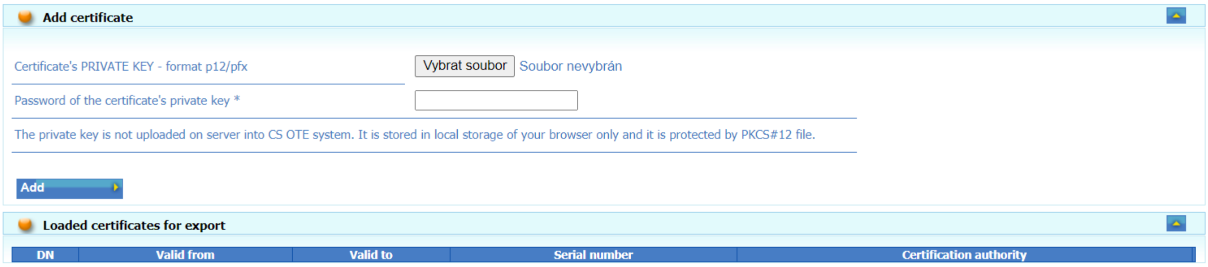


Loaded certificates for export

DN	Valid from	Valid to	Serial number	Certification authority	
[redacted]	04/23/2020 09:14:23	05/13/2021 09:14:23	[redacted]	[redacted]	Export QR

QR codes

b) In the case of an active PKi component, a form will be displayed allowing to load the given certificate from a * .p12 file with all the necessary security elements:



Add certificate

Certificate's PRIVATE KEY - format p12/pfx	Vybrat soubor Soubor nevybrán
Password of the certificate's private key *	

The private key is not uploaded on server into CS OTE system. It is stored in local storage of your browser only and it is protected by PKCS#12 file.

Add

Loaded certificates for export

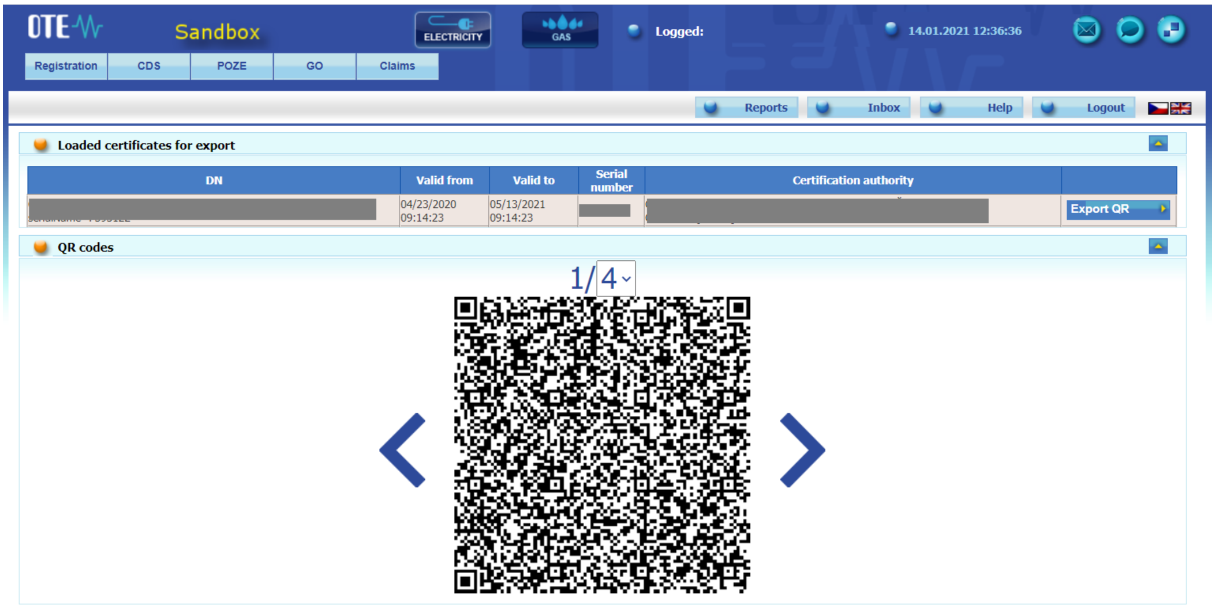
DN	Valid from	Valid to	Serial number	Certification authority

After loading, the certificate will be displayed in the form as after a) and it is possible to transfer it with the **Export** button.

- Clicking on **Export QR**, which is located in the last column of the table next to the given certificate, will start the transfer process using QR codes.

- You will then be prompted to enter the password and repeat it for the certificate transfer. The password will be required when saving the certificate to the mobile device and is used to secure the certificate against unauthorized use.

- The following screens will contain a specified number of QR codes containing information about the certificate that needs to be transferred to the mobile device.

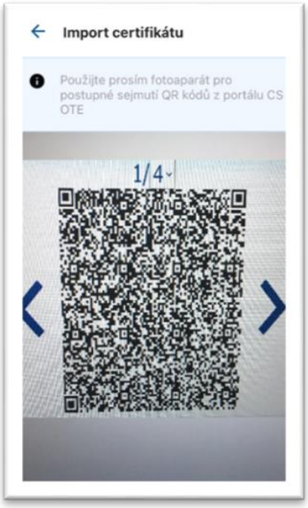


DN	Valid from	Valid to	Serial number	Certification authority	
[redacted]	04/23/2020 09:14:23	05/13/2021 09:14:23	[redacted]	[redacted]	Export QR

Fig. 21 – Certificate Export – QR codes generated by computer

2) Click the **Import** button on your mobile device to begin the certificate transfer process. This certificate is transferred by gradual scanning of all QR codes generated on the CS OTE portal (https://portal.sand.ote-cr.cz/otemarket/).

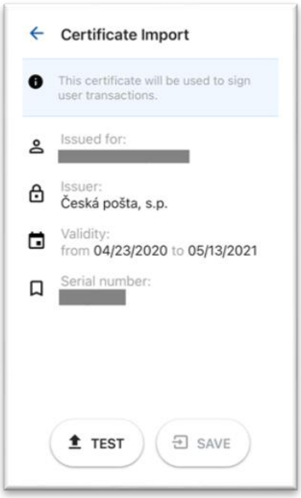
- You can increase the number of QR codes on the 1st screen on the portal – by clicking on the menu at 4 above the QR code - for better transfer if you have a mobile device with an older camera.


Import certifikátu

Použijte prosím fotoaparát pro postupné sejmutí QR kódů z portálu CS OTE

Fig. 22 – Certificate Export – Mobile app – Scaning QR codes

- To move between QR codes on the PC, use the "<" ">" icons next to the QR code in the CS OTE portal.
- The mobile device automatically recognizes which QR code it is, and therefore the reading can be performed in a different order.
- After reading the last code, the dialog for the password is displayed - after entering the password for certificate transfer, the information about the certificate is displayed:



Certificate Import

This certificate will be used to sign user transactions.

Issued for:
[redacted]

Issuer:
Česká pošta, s.p.

Validity:
from 04/23/2020 to 05/13/2021

Serial number:
[redacted]

Fig. 23 – Imported certificate

Press the **Test** button to verify that the downloaded certificate can be used in the OTE IMP Sandbox application and the **Save** button will be displayed. Press it to save the certificate to the device.

- The installed OTE IMP Sandbox application is now ready for use on the OTE SandBox environment.