

Procedure for launching mobile application IM GAS on SANDBOX environment

To ensure and validate access for participants, it will be necessary to go through the steps below:

1. Run installation process of IM gas application  in your mobile device.

App Store - iOS

<https://apps.apple.com/us/app/ote-img-sandbox/id1483897722>



Google Play – OS Android

<https://play.google.com/store/apps/details?id=cz.otecr.mobile.vdp.sandbox>



OTE IMG Sandbox

OTE a.s.

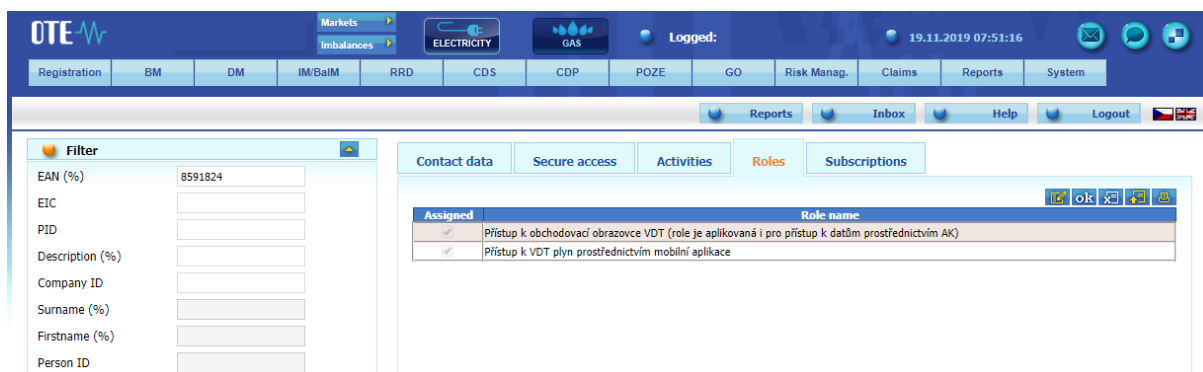
2. Login to SANDBOX test secure portal -
 - <https://portal.sand.ote-cr.cz/otemarket/>, where the user must have the current valid certificate. If the user cannot log in to the SANDBOX secure test portal, then it will be necessary

to contact his **RMP master data administrator** on Sandbox environment. In addition, on-line access for mobile devices is essential (Wi-Fi, GPRS, ...).

3. The user can check the user roles, that is, the person who will use the IM gas mobile app will have the roles listed:

- **passive approach** (read only):
 - Access to IM gas trading screen (EmtasGImTsAcc)
 - Access to IM gas via mobile application (EmtasGMImTsAcc)
- **active approach** (all functions):
 - Access to IM gas trading screen (EmtasGImTsAcc)
 - Access to IM gas via mobile application (EmtasGMImTsAcc)
 - Modification of data via mobile application (EmtasGMImTsMod)
 - Modification of data on IM trading screen (EmtasGImTsMod)

These roles can be checked in the CS OTE master data of the logged-in person – the Role tab:



Assigned	Role name
<input checked="" type="checkbox"/>	Přístup k obchodovací obrazovce VDT (role je aplikovaná i pro přístup k datům prostřednictvím AK)
<input checked="" type="checkbox"/>	Přístup k VDT plyn prostřednictvím mobilní aplikace

Fig. 1 - Roles necessary for passive access – CS OTE master data

4. **Note:** In this test environment, OTE has set up all existing OTECOM users with enrollment access for IM-gas mobile applications for testing purposes. However, OTE will set a stricter rule on the production environment, ie any person who has access to the OTECOM-gas client will ONLY have read access to the VDT mobile application. Therefore, the right to enroll in a mobile application in a production environment will need to be resolved by the user with his / her RMP master data manager.
5. Device activation procedure on SANDBOX secure portal, including creation of profile on mobile device according to attached procedure below:

There are two ways to register for the VDP mobile app:

- **direct activation** - with the possibility of user login to the CS OTE portal
- **activation by the administrator** - if we do not have access to the CS OTE portal:

Registration process: (a)direct activation

- To create mobile access by direct activation, first login to the CS OTE web portal on the SandBox environment (<https://portal.sand.ote-cr.cz/otemarket/>).
- In the **Registration** section, select **Mobile Access - Device Management**.



Fig. 2 –Web portal CS OTE – Device management

- Then click **New activation**. Mobile device detail will be displayed at the bottom of the page and your user account will be listed in the table.
- To pair the device, click **Activation Wizard**, bottom right (Fig. 3).

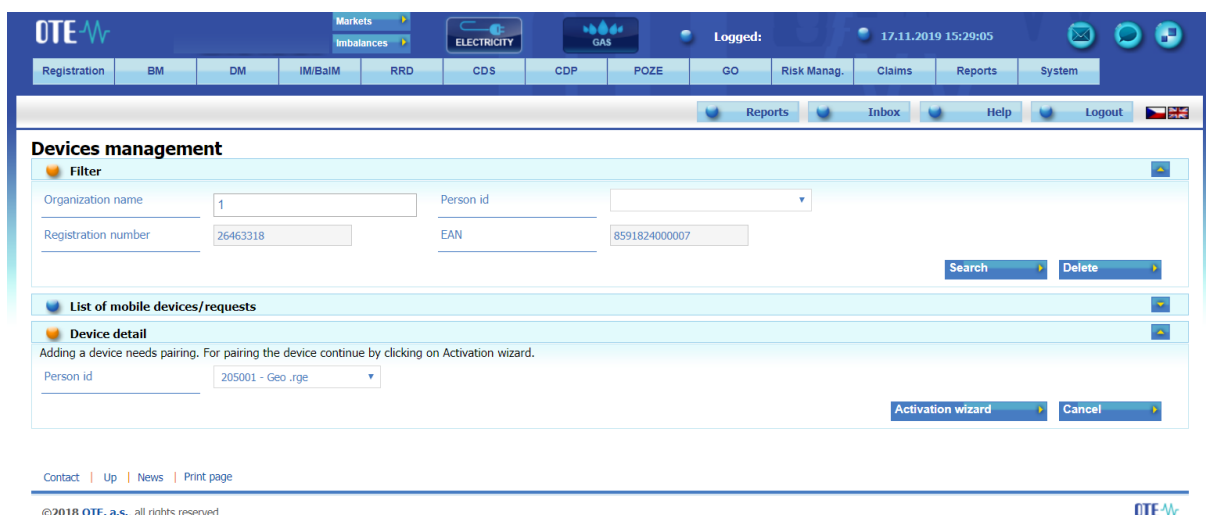


Fig. 3 – Web portal CS OTE – New Activation

2019 OTE, a.s.

Revize dne:
03.12.2019

Název dokumentu:
Postup pro zprovoznění mobilní aplikace VDP

- Pressing the Activation Wizard button will display the page with the generated QR code as shown below.



Fig. 4 – Web portal CS OTE – activation code

- This activation QR code needs to be transferred to your mobile device, and the time of its validity is shown in the field **Activation validity until** (Fig. 4).

On your mobile device, open the OTE IM gas mobile app and click **New profile**.

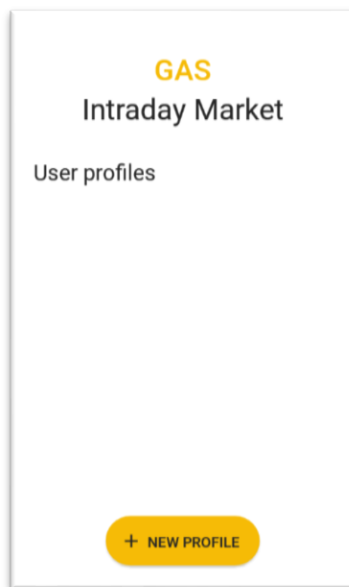


Fig. 5 – Mobile application – New profile

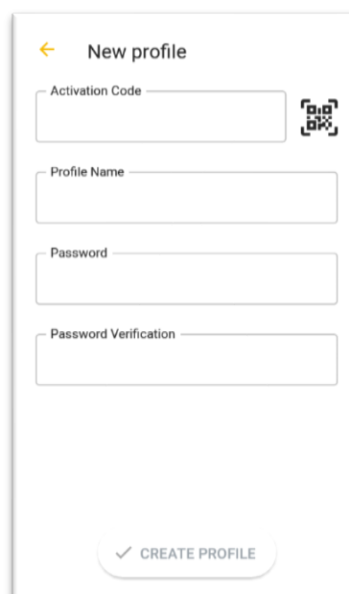

 A screenshot of a mobile application interface for creating a new profile. The title is 'New profile' with a back arrow. There are four input fields: 'Activation Code' (with a QR code icon to its right), 'Profile Name', 'Password', and 'Password Verification'. At the bottom, there is a white rounded button with a checkmark and the text 'CREATE PROFILE'.

Fig. 6 – Mobile application – Account information

- Enter the generated QR code from CS OTE portal into the Activation code field.


- Press the button  (Fig. 6 – Mobile application –). Your mobile device's camera will start (Fig. 7). 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** (from the CS OTE web portal) into the **Activation Code field**.



Fig. 7 – Mobile application – 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 Verification field. The password you enter is used to secure your profile and certificate against unauthorized use.

- Click Create profile (Fig. 6) to create a new profile in the mobile app.

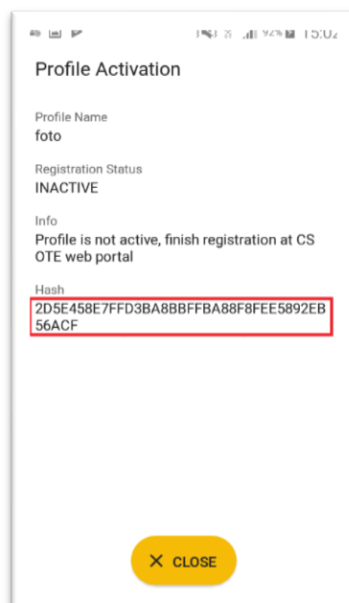


Fig. 8 – Mobile application – Creating new profile

- After you create a new profile on a mobile device, the Activation Wizard page on the web portal automatically goes to the point that requires accepting or rejecting the link for that mobile device to this account on CS OTE.
- New in this step is the Application entry, which may contain values with VDT Gas or Renewables, depending on which mobile app was used to load the Activation QR Code.

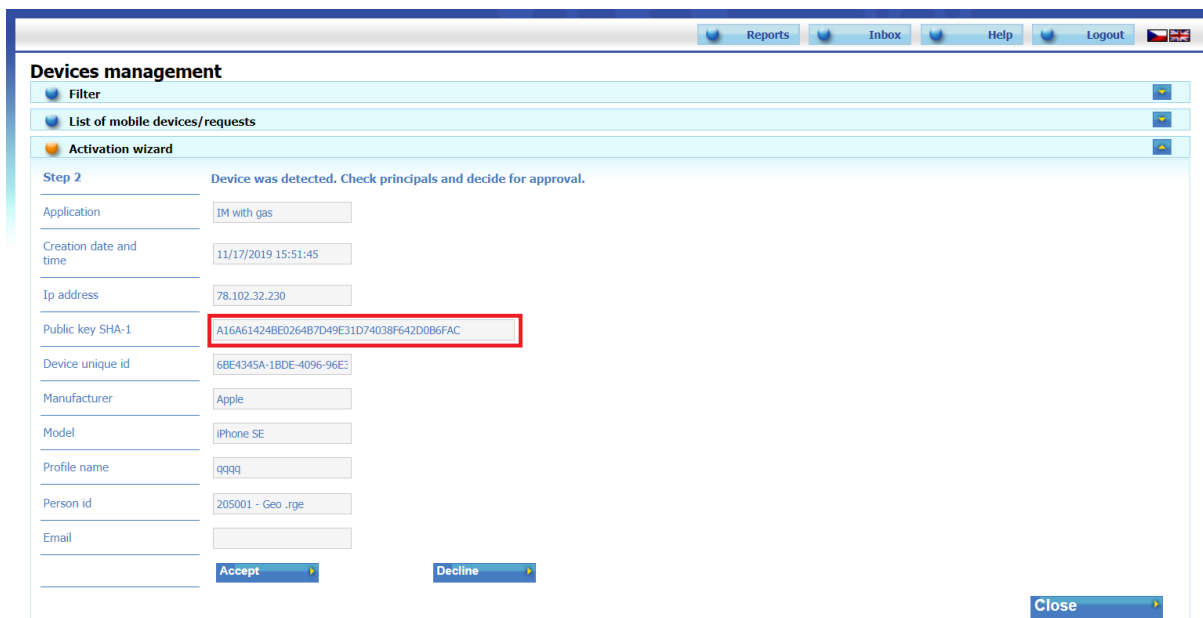


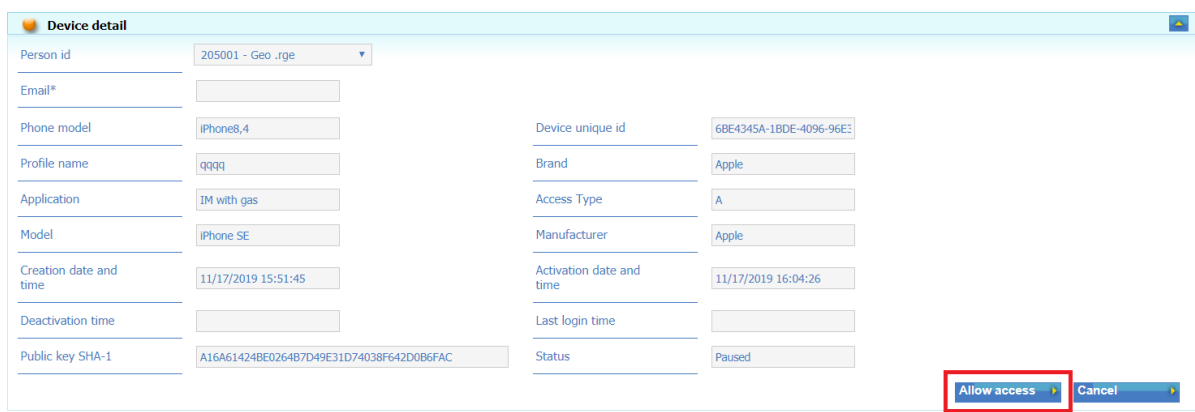
Fig. 1 –Web portal

2019 OTE, a.s.

Revize dne:
03.12.2019

Název dokumentu:
Postup pro zprovoznění mobilní aplikace VDP

- It is recommended to check that the red-framed codes [Fig. 8](#) and [Fig. 1](#) are the same on the mobile device and in the CS OTE web portal.
- Click Accept ([Fig. 1](#)) and sign with the certificate .
- After pressing the **Accept** button and **signing** the certificate, the mobile device is paired and this mobile device is clearly identifiable for CS OTE. The profile is currently in the **Suspended** state and it is not possible to log in to the mobile application yet - the permission can be granted by a person with the role of **RMP - Master Data Manager**.
- The **Mobile Device Detail** will also be displayed in Device Manager ([Fig. 10](#)). If you are a RMP **Master Data Manager** role, you will see a red boxed **Allow Access** button. Pressing this button will make it "**Approved**" and you can sign in to the mobile app under this account. If you don't see the button, contact your company's RMP Master Data Manager to activate your account.



Device detail	
Person id	205001 - Geo .rge
Email*	
Phone model	iPhone8,4
Profile name	qqqq
Application	IM with gas
Model	iPhone SE
Creation date and time	11/17/2019 15:51:45
Deactivation time	
Public key SHA-1	A16A61424BE0264B7D49E31D74038F642D0B6FAC
Device unique id	6BE4345A-1BDE-4096-96E3
Brand	Apple
Access Type	A
Manufacturer	Apple
Activation date and time	11/17/2019 16:04:26
Last login time	
Status	Paused
Allow access Cancel	

Contact | Up | News | Print page

©2018 OTE, a.s., all rights reserved

Fig. 10 – Web portal – Device detail (Master data Manager RMP)

- Direct activation is successfully completed and you can now sign in to the mobile app. - see chapter Registration process.

Administrator activation (with RMP master data management role)

- 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.

2019 OTE, a.s.

Revize dne:
03.12.2019

Název dokumentu:
Postup pro zprovoznění mobilní aplikace VDP

1st step – Administrator

- Log in to CS OTE portal (<https://portal.sand.ote-cr.cz/otemarket/>).
- In the Registration section, select Mobile Access - Device Management.



Fig. 21 – Web portal – Device management

- After selecting New activation, the Mobile device detail will be displayed at the bottom of the page.
- Select a person from the list: Person ID - the name of the person for whom you are creating mobile access. After selecting the desired user, an e-mail field is displayed that can be left or edited.

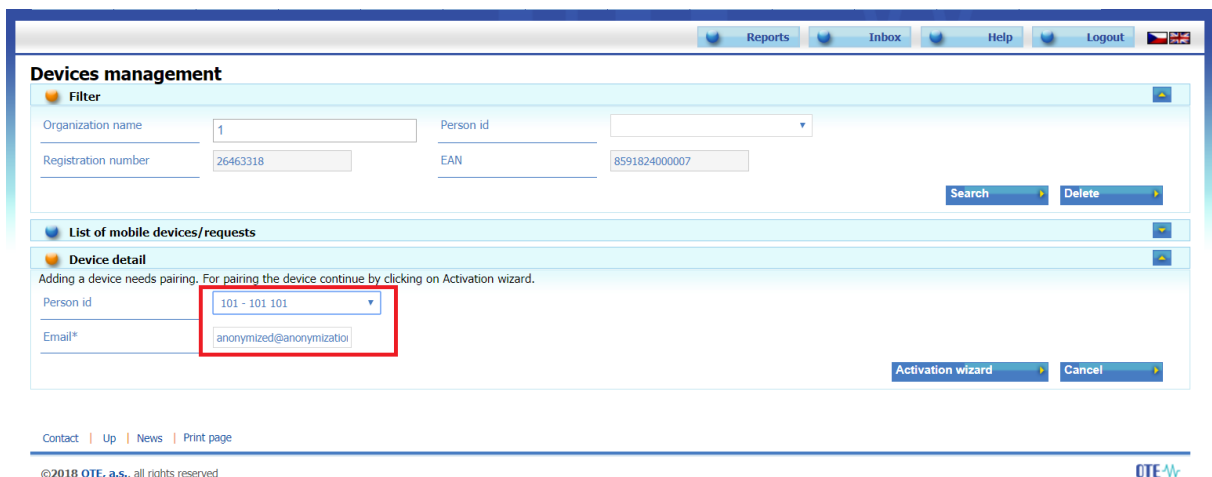


Fig. 3 – Web portal – Device management

- After selecting the person and possibly changing the email, click on the Activation Wizard (Fig. 3).

2019 OTE, a.s.

Revize dne:
03.12.2019

Název dokumentu:
Postup pro zprovoznění mobilní aplikace VDP

- A message containing a QR code designed to activate your mobile device has been sent to the email.
- The system now waits for one hour to read the QR code of the selected user as part of the activation of the new profile in the mobile application ([Fig.13](#)).
- Therefore, a person with a mobile device must transfer the QR code of the activation email to the activation process of the mobile application (see above). The code must be loaded and paired with CS OTE within one hour, otherwise the activation will expire and the activation process must be repeated.

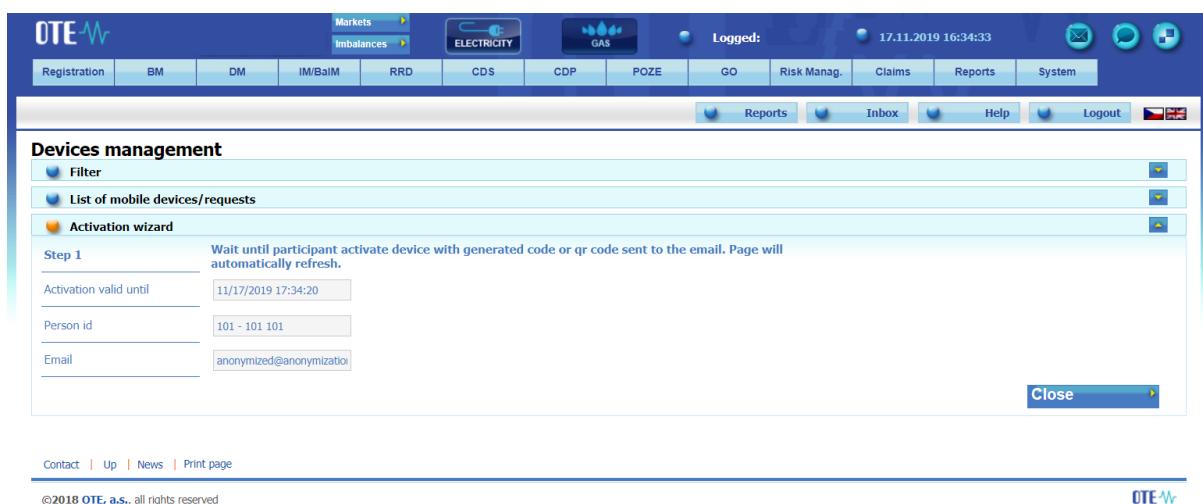
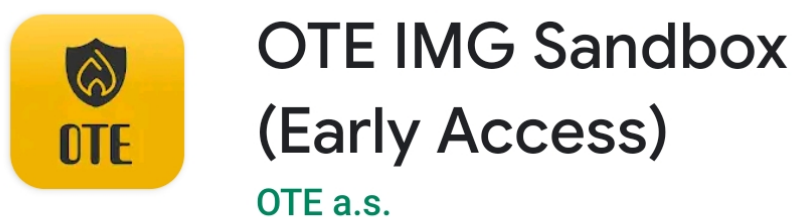


Fig. 4 – Web portal – information about Activation QR code

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

- Open the mobile app Im gas.



Uninstall

Open

- Click **New Profile**.

2019 OTE, a.s.

Revize dne:
03.12.2019

Název dokumentu:
Postup pro zprovoznění mobilní aplikace VDP

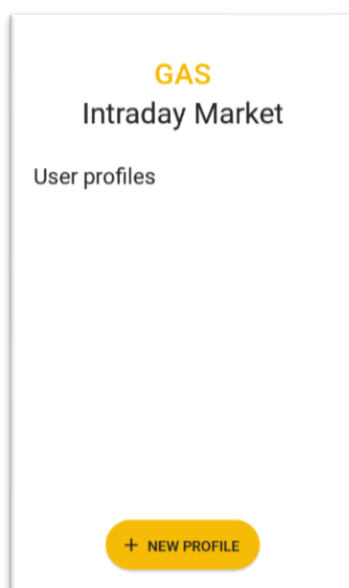


Fig. 54 – Mobile app – New profile


 A screenshot of a mobile application interface for creating a new profile. The title is 'New profile' with a back arrow on the left. There are four input fields: 'Activation Code' (with a QR code icon to its right), 'Profile Name', 'Password', and 'Password Verification'. At the bottom, there is a button with a checkmark and the text 'CREATE PROFILE'.

Fig 15 – Mobile app – Account information

- In the Activation Code field, enter the QR code from the e-mail sent by the administrator (Fig. 6) as follows:


Device activation

Activate device with generated activation code or qr code.

Activation code : ZAKTPGMSMILUHM30



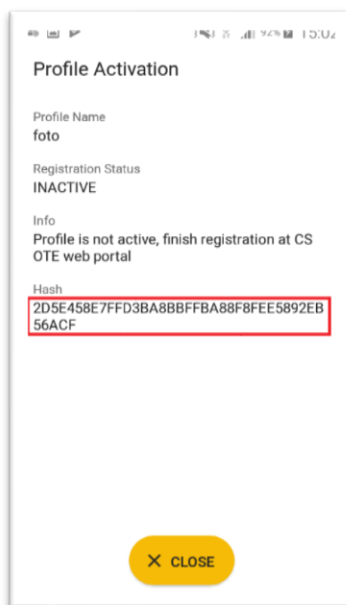
Fig. 16 – E-mail with activation code

- Press the icon  (Fig 15 – **Mobile app** –). Your mobile device's camera will start (Obr. 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 copy the text **Activation Code itself** (from the CS OTE web portal) in the **Activation Code** field.



Obr. 6 - Mobile app – Scanning QR code

- In the box **Profile name** (Fig 15 – **Mobile app** –) enter a new profile name.
- Create a **Password** that contains at least 4 characters and repeat it in the **Password Verification** field again. The password you enter is used to secure your profile and certificate against unauthorized use.
- Pressing **Create Profile** (Fig 15 – **Mobile app** – create a new profile in the mobile app.

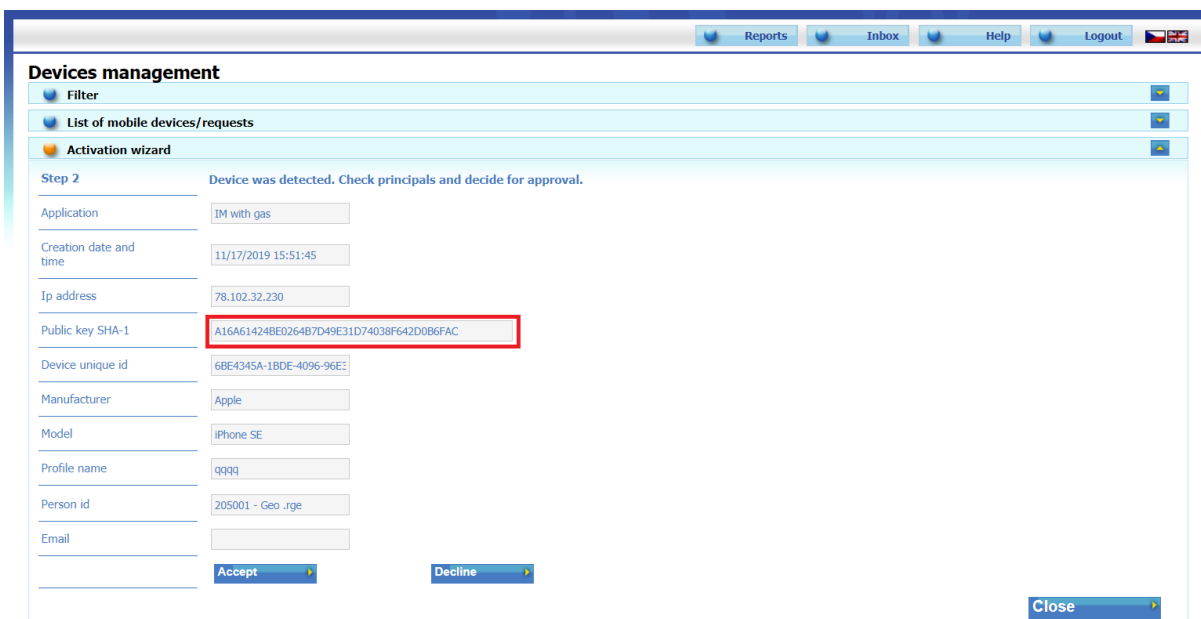


Obr. 7 – Last step of activation process in mobile app.

- **Contact the RMP master of the company to complete the activation of your profile.**

3rd step – administrator

- After you create a **new profile** on a mobile device, the Activation Wizard page on the CS OTE portal will automatically go to the point that **requires accepting or rejecting** the link for that mobile device to this account on CS OTE.



Devices management

Filter

List of mobile devices/requests

Activation wizard

Step 2 Device was detected. Check principals and decide for approval.

Application IM with gas

Creation date and time 11/17/2019 15:51:45

Ip address 78.102.32.230

Public key SHA-1 A16A61424BE0264B7D49E31D74038F642D0B6FAC

Device unique id 6BE4345A-1BDE-4096-96E3

Manufacturer Apple

Model iPhone SE

Profile name qqqq

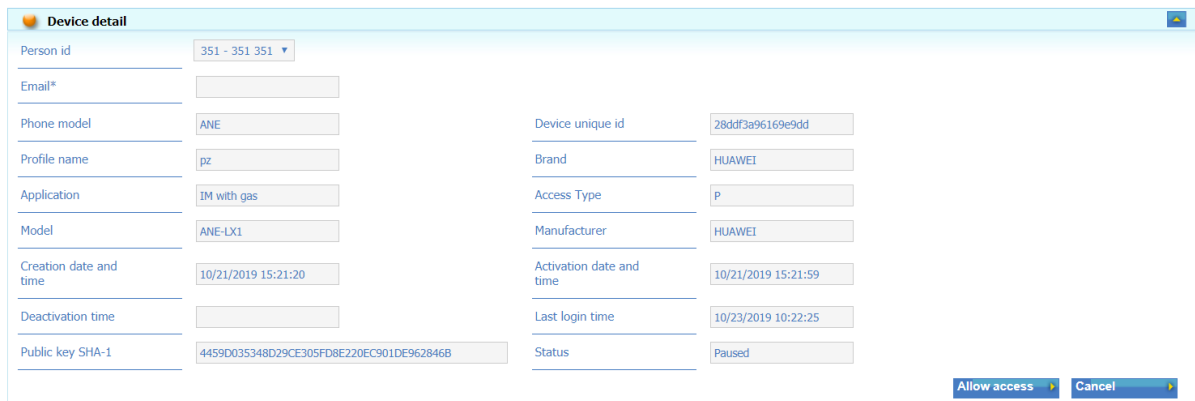
Person id 205001 - Geo .rge

Email

Accept Decline Close

Obr. 8 – Web portal – New profile information

- **We recommend checking:**
 - box **Application** – contains the type of application (VDP, POZE) for which the activation is intended
 - The **red-framed codes** (Obr. 7) and (Obr. 8) displaying the public key fingerprint are identical on the mobile device and in the CS OTE web portal.
- To create a new account for the application click on **Accept** (Obr. 8) and sign with the certificate, or click on Reject and registration will be canceled
- Pressing Accept and signing will pair and the mobile device of the user for whom you enable mobile access. The mobile device is now clearly identifiable for CS OTE. After importing a valid qualified certificate (see below), the user can then use it fully to sign the submitted reports.
- The Mobile Device Detail will also be displayed in Device Manager (Fig. 10). On this page, you'll see **Allow access** button. Pressing it will put the suspended account in the Approved status and sign in to the mobile app under that account.



Obr. 9 –Web portal – Device detail

Login process

- Launch VDP mobile application Choose profile and type Password
- If the login is successful, the Setup Wizard appears
 - Set and repeat PIN (enter the same 4-digit PIN on the numeric keypad displayed twice)
 - Fingerprint configuration – if our mobile device allows BIometric verification, we can choose whether we want to use fingerprint for Login or PIN input
- the next step is to import the certificate:
 - The process of certificate transfer from the CS OTE system requires simultaneous use of a PC with activated local storage for CS OTE and mobile devices.


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

- In the menu **Registration**, choose **Mobile Access - Certificate Export**.



Obr. 10 –Web portal – export certificate

- Enter the password to the Local Storage - LS (in case the LS is not used, a message about unset password is displayed:

 **A password to the local storage not set**
You do not have set any password right now. For work with certificates at the local storage you must have set a password.

To **transfer the certificate** to the mobile device, the **LS must be activated** – see next chapter.

2019 OTE, a.s.


Revize dne:
03.12.2019

Název dokumentu:
Postup pro zprovoznění mobilní aplikace VDP

(In case of login to LS and displaying certificates, please skip chapter Activating Local Storage.)

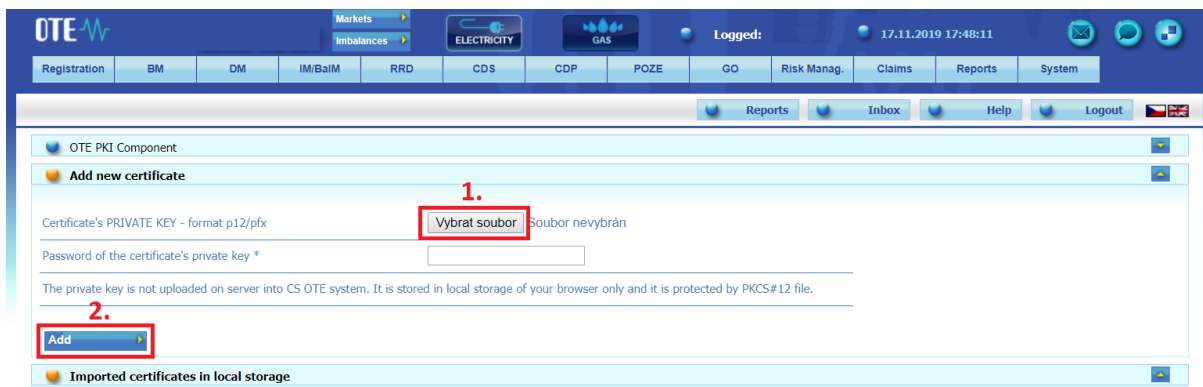
Activating Local Storage

- In the menu **Registration**, select **Certificate management – Settings of Certificates**
- At the bottom of the page, click the Initialization of local storage bar:

 Initialization of local certificate storage

After entering, repeating the Password and saving, the local storage page is displayed.

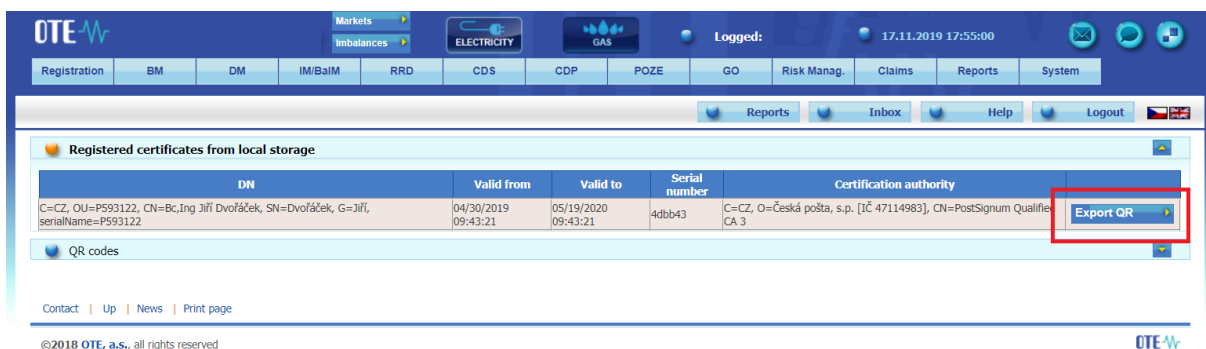
Now you need to upload a qualified certificate that is registered in CS OTE and is to be transferred to the mobile device. Click **Vybrat soubor** (Choose file). After choosing file xxxxx.p12 with certificate and typing **Password** click **2. Add** (Přidat).



Obr. 30 – Upload the certificate to Local Storage

Continue of exporting certificate to mobile device

- Certificates from the LS can be transferred from the portal to the mobile device by clicking on **Export QR** displayed in the stored qualified certificates:



Obr. 11 – Local Storage – exporting certificate

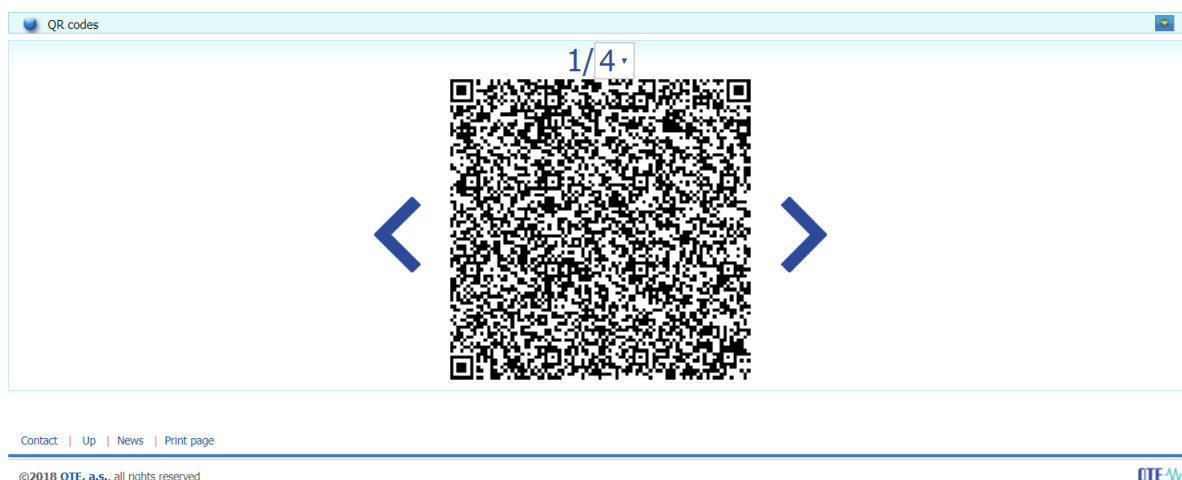
- You will then be prompted to enter the **password** and repeat it.
- The password is required when saving the certificate to a mobile device and is used to secure the certificate against unauthorized use:



Obr.12 – setting password for certificate transfer

If **Skip** is selected, the same password will be used for the given certificate as set in Local certificate store:

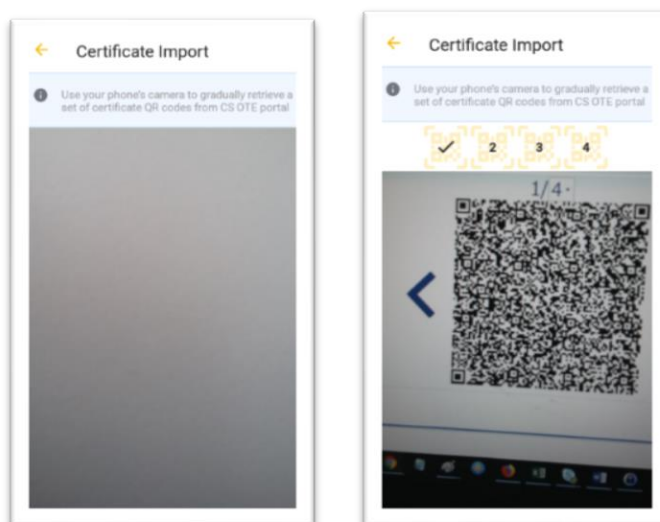
- The following web portal screens will contain QR codes containing information about the certificate that must be transferred to the mobile device.



Obr. 13 – Portal CS OTE – QR code of certificate

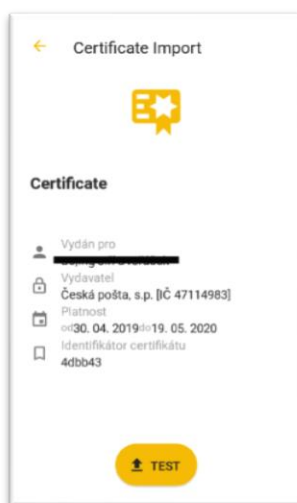
2a) Mobile device – (continued in the mobile Setup Wizard) click on the Import button to transfer the certificate by sequentially reading all QR codes generated on the CS OTE portal (<https://portal.sand.ote-cr.cz/otemarket/>):

- You can increase the number of QR codes on the 1st screen – click menu at 4 above the QR code - for better portability if you own a mobile device with an older camera.



Obr. 14 – Certificate import – reading 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 detects which QR code it is, and therefore loading can be performed in different order.
- After retrieving the last code, a dialog for the certificate password is displayed - after entering the password for certificate transmission, information about the certificate is displayed:



Obr. 15 –Certificate import

Press the **Test** button to verify that the retrieved certificate can be used in the VDP application and then the **Save** button is displayed. Pressing it will save the certificate to the device.

- The installed **IM gas application** is now ready to use.