User manual
of Information system

Mobile Application IM Gas - IMG

SANDBOX

Content

List of Pictures

List of Abbreviations

Abbreviation	Meaning
CS OTE	Central system OTE
OTE	Company OTE, a.s.
PC	Personal Computer

1.1 Creating mobile access request

Install the mobile app IM Gas.

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.

Install

- Connect to SANDBOX – secure testing platform (https://portal.sand.ote-cr.cz/otemarket/).

- To create Mobile Access request the access to portal CS OTE (https://portal.sand.ote-cr.cz/otemarket/) with valid certificate is required. This is either by the user requesting access or by the **RMP master data administrator**. In addition, on-line access for mobile devices is essential (Wi-Fi, GPRS, …).

- The basic method is **Direct activation** - 1.1.1 with immediate access from the mobile application. This method is applicable to an already existing user with a valid certificate who will establish access for himself.

  Direct activation is possible for persons registered in the CS OTE portal. Roles linked with the IM gas App are listed below:

Roles related to IM gas Application	
Passive access	- EmtasGMImTsAcc - *Přístup k VDT plyn prostřednictvím mobilní aplikace/ Access to IM via IM gas app*
	- EmtasGImTsAcc - *Přístup k obchodovací obrazovce VDT / Access to IM trading screen*
Active access	- EmtasGMImTsAcc - *Přístup k VDT plyn prostřednictvím mobilní aplikace/ Access to IM gas via IM gas app*
	- EmtasGImTsAcc - *Přístup k obchodovací obrazovce VDT / Access to IM gas trading screen*
	- EmtasGMImTsMod - *Modifikace dat pro VDT plyn prostřednictvím mobilní aplikace/ Modification of IM gas data via IM gas app*
	- EmtasGImTsMod - *Modifikace dat na obchodovací obrazovce VDT/ Modifying data on the IM trading screen*
Access to reports	- Sfvotreporty - *Přístup na reporty / Access to reports*
	- SfvotreportyOTE - *Přístup na reporty OTE / Access to OTE reports*

- Another option is **Activation by the administrator** - 1.1.2 (person with *RMP Administrator* role). It is also applicable to users who do not have a valid certificate in CS OTE provided that the activating administrator has a valid certificate registered in CS OTE.

- Note: It is not possible to use the IM gas application without transferring the certificate from CS OTE (description of local storage activation is described in chapter 1.2.2 Activating Local Storage). In the case of using a certificate on a Token or other hardware storage, the export of the certificate is not possible and must be uploaded to the storage first (chapter 1.2.2 Activating Local Storage).
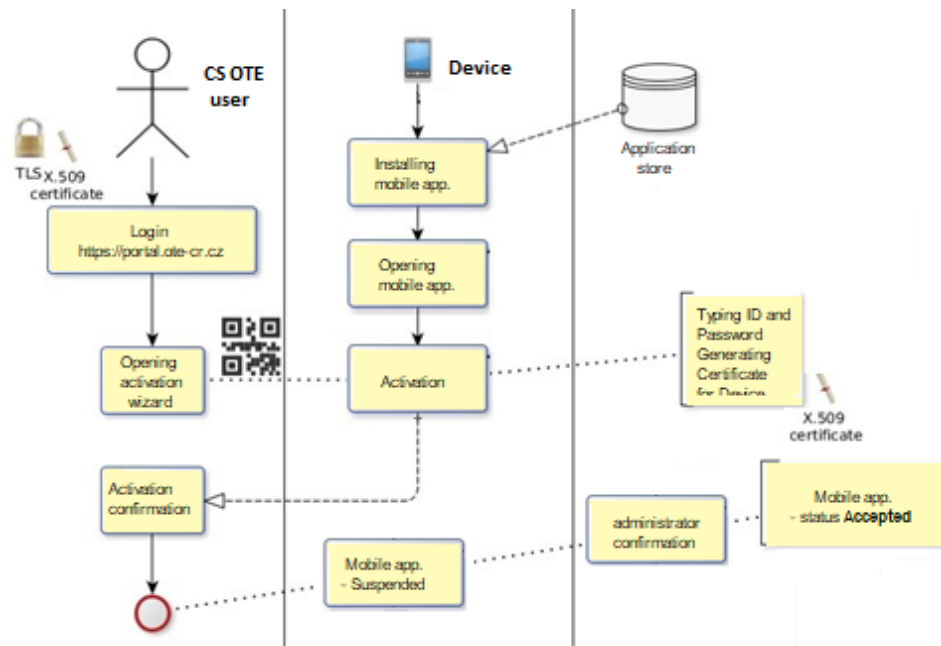
Fig. 1 – Mobile access request creation scheme

1.1.1 Direct activation with access to CS OTE portal

- To create mobile access by direct activation, first login to the CS OTE web portal (ttps://portal.sand.ote-cr.cz/otemarket/).

- Menu **Registration** choose **Mobile access – Device management**.
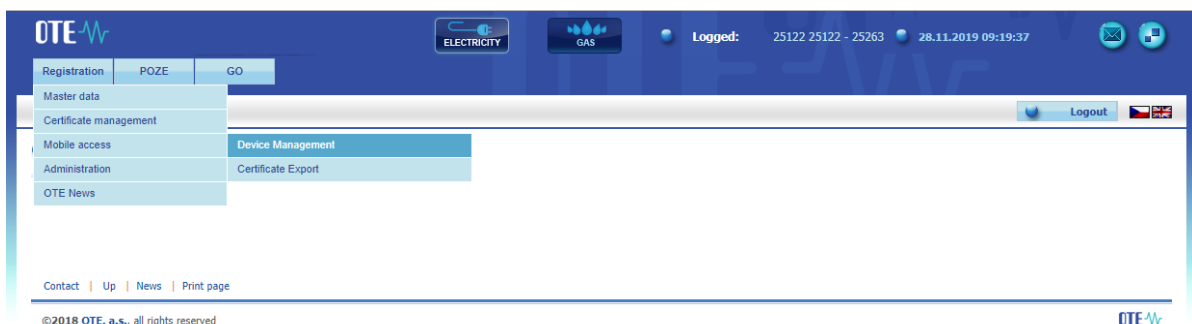
Fig. 2 – Direct activation – Web portal CS OTE – Device management

- Now press the button **New Activation.** You will see Device Detail, where your user account will be listed in the Person ID. If you have the *RMP Data Manager role*, you can click on the Person ID and select another person from your company under which an editable email will be listed.

- To start activating your mobile device, click the Activation Wizard (Fig. 3 – Direct activation – Web portal CS OTE – Activation wizard).
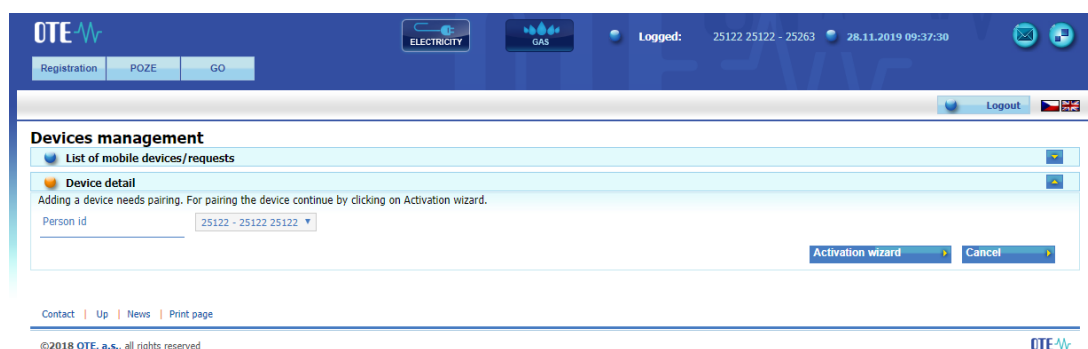
Fig. 3 – Direct activation – Web portal CS OTE – Activation wizard

- After pressing the **Activation Wizard** button a page with generated QR code will be displayed for activating Moble device:
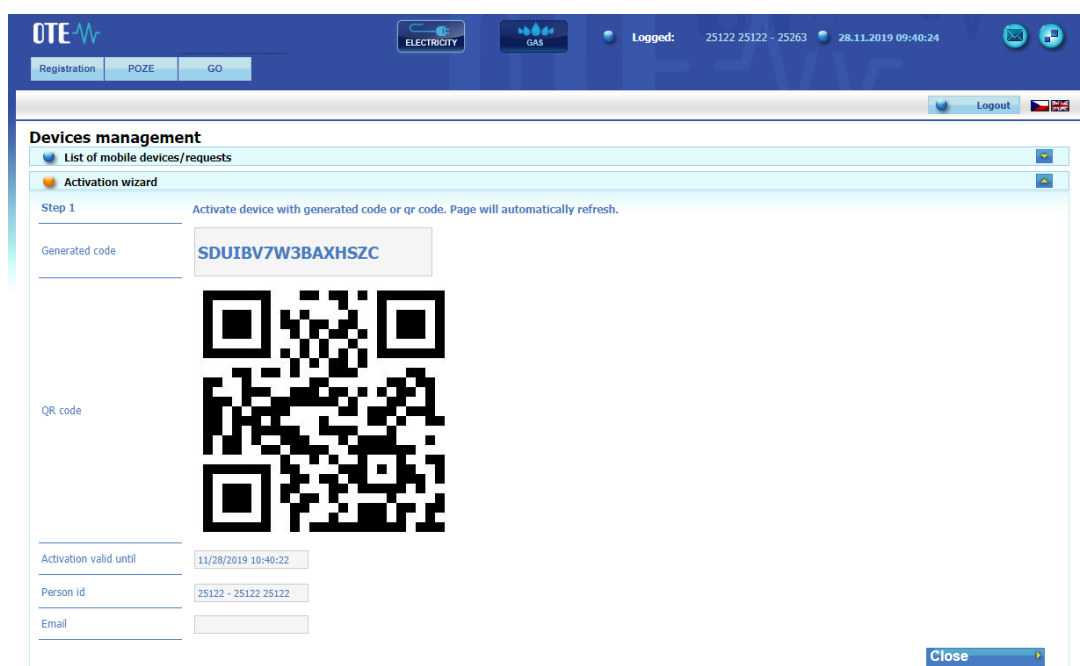
Fig. 4 – Direct activation – Web portal CS OTE

- 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. 4).

Date of revision:
3.12.2019

Document name:
Mobile application IM gas

- Open the IM gas mobile app on your mobile device.
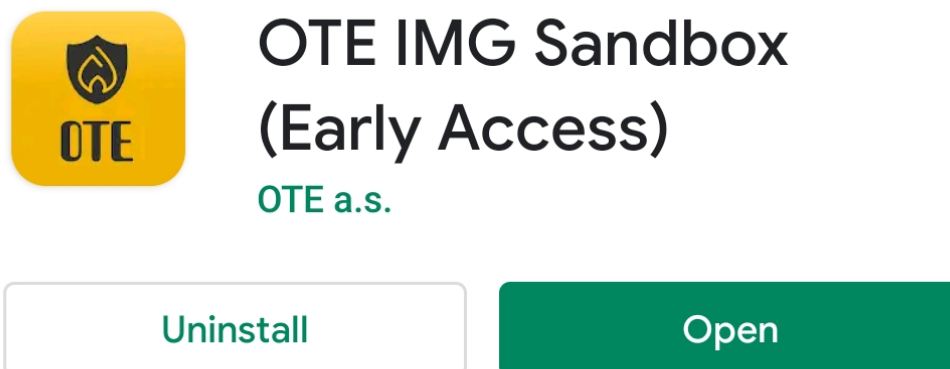
When you start a newly installed application, you are asked to agree to the License Terms (Fig. 5 – Acceptance of license terms). These terms is necessary to confirm otherwise it will not be allowed to access the application:
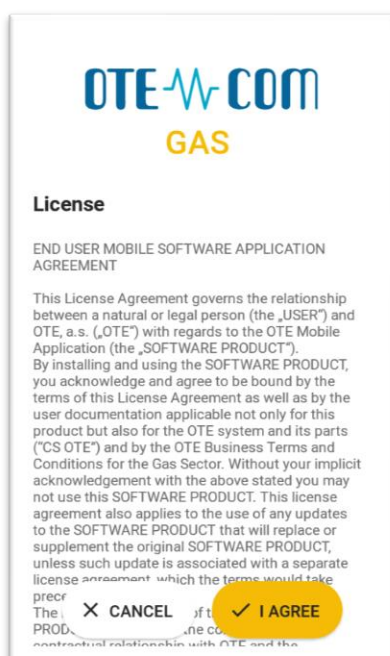
Fig. 5 – Acceptance of license terms

- The User profiles screen is then displayed (Fig. 6 – Direct activation – Mobile app –), where we click **New Profile**.
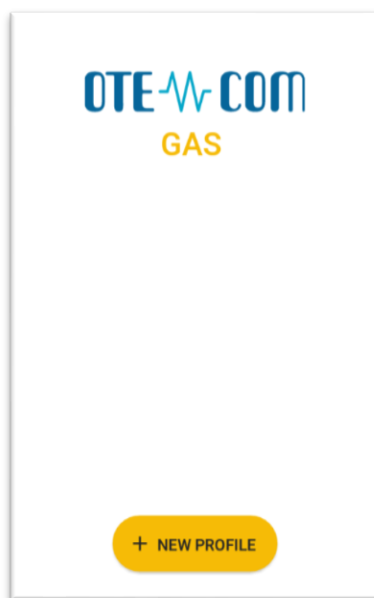
Fig. 6 – Direct activation – Mobile app – Login screen
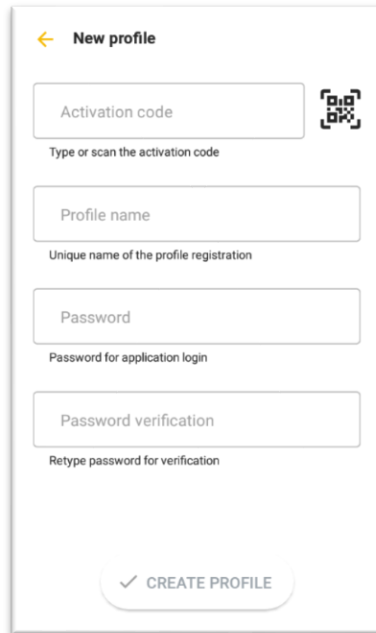
Fig. 7 – Direct activation – Mobile app – New profile

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

    This code can be detected by the camera or entered manually:
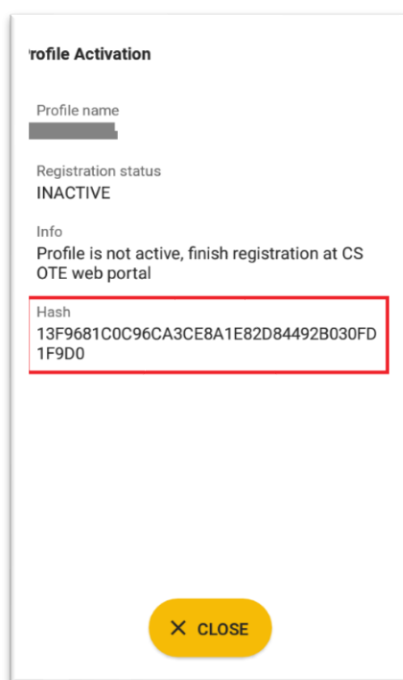
  - Press ⌞ ⌟ . Your mobile device's camera will start (Fig. 8). Point the camera at the QR code screen. The mobile device records the code, which is usually reflected in the device's vibration.

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

Fig. 8 – 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. 7) you create new, not yet approved profile in the VDP mobile app (Fig. 9 – Direct activation – Mobile app –).

2019 OTE, a.s.

Fig. 9 – Direct activation – Mobile app – Creating 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(Fig. 10 – Direct activation – Web portal – step 2)

Fig. 10 – Direct activation – Web portal – step 2

- It is **recommended to** check that the red-framed codes in Fig. 9 and Fig. 10 are the same on the mobile device and in the CS OTE web portal

  - Click **Accept** (Fig. 10) and sign with certificate .

  - After pressing the **Accept** button and confirmation 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: (Fig. 11 – Direct activation – Web portal – Device detail)

Fig. 11 – Direct activation – Web portal – Device detail

- Having the RMP Administrator role, you now see the **Allow Access** button. Press it to allow the mobile device access the VDP network. Continuation – 1.1.3 User login

2019 OTE, a.s.

Date of revision:
3.12.2019

Document name:
Mobile application IM gas

- Note: If you don't see the **Allow Access** button on the page, please contact the *RMP Administrator* for your company who can activate this account by clicking **Allow Access** on the **Mobile Detail** page**.**

--- person with role RMP Administrator ---

Log in to **CS OTE**, menu **Registration / Mobile access / Device management**
Clicking on the record will display the **Mobile Device Detail** and
at the bottom of the screen, you can see the **Allow access** button, which when pressed will give your account an "**Approved**" status and mobile device can be used normally in mobile VDP.

Pressing button **Allow access** activate possiblities for Access suspension, Account deactivation, or Certificate export - see below.

- 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.

1.1.2 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.

1st step – Administrator

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

- Menu **Registration** choose **Mobile access – Device management**.

Fig. 12 – Administrator Activation – Web portal – 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 (Fig. 13 – Administrator Activation – Web portal–).
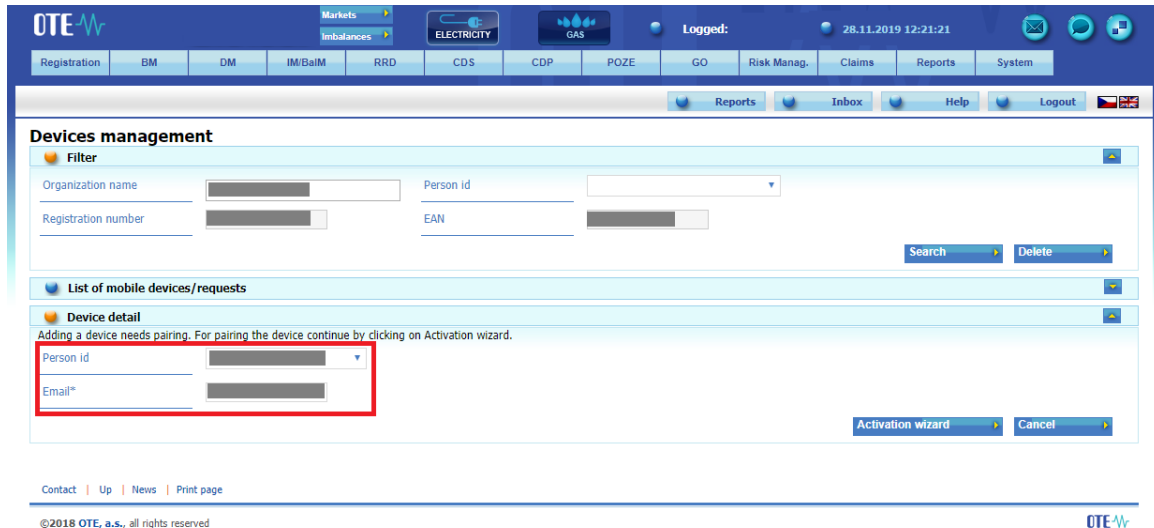
Fig. 13 – Administrator Activation – Web portal– Devices management

- After selecting the person and possibly changing the email, click on the Activation Wizard (Fig. 13).

- 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 retrieve the QR code of the selected user as the second part of the activating new profile in the mobile app (Fig. 14).
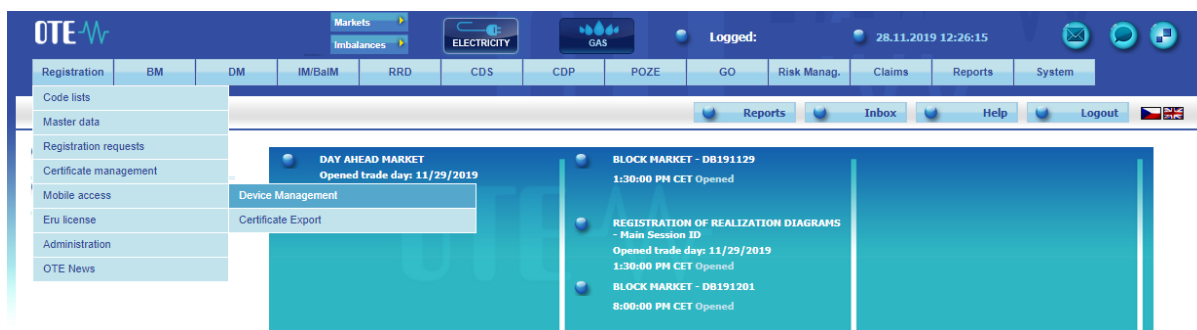

Fig. 14 – Administrator Activation – Web portal

2019 OTE, a.s.

Date of revision:
3.12.2019

Document name:
Mobile application IM gas

The person with the mobile device must transfer the QR code (2nd step - lower) from 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.
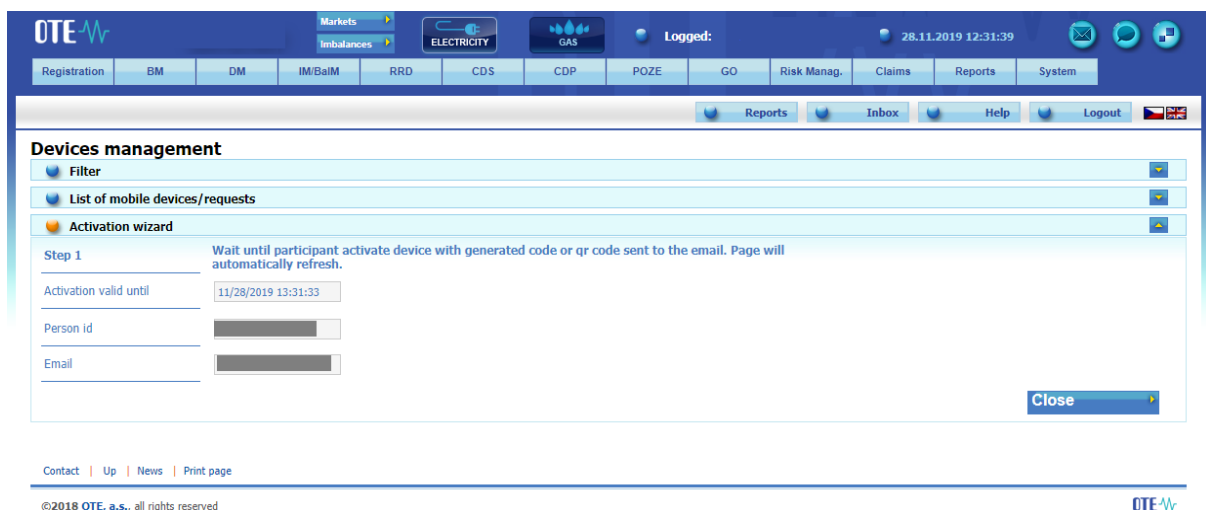
2nd step – user setting up a profile on their mobile device

- Open the IM gas mobile app.

OTE VDP Sandbox

OTE a.s.   Byznys

3 PEGI 3

ⓘ Aplikace je dosud ve vývoji a nemusí být stabilní.
ⓘ Tato aplikace je kompatibilní s vaším zařízením.

- When launching the newly installed application, the screen Acceptance of Licence terms will be displayed (See figure 5 – Acceptance of Licence Terms). The access to the app is not possible unless the acceptance of Licences terms is confirmed.
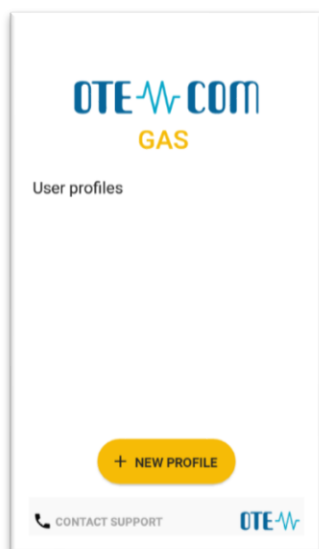
- Click **New profile**.

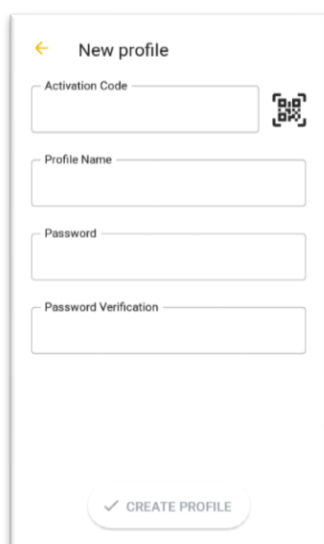Fig. 15 –User Activation with support of the Administrator - Mobile App – New profile

Fig. 16 – 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. 17):

Device activation

Activate device with generated activation code or qr code.

Activation code : EV5VDCP4GOVA7PB2

Fig. 17 – Administrator Activation – E-mail with Activation QR code

- Click ⌞⌟ on the mobile device to launch the camera of your mobile device (Fig. 16 – User Activation with support of the Administrator - Mobile App – Profile information). Point the camera at the QR code screen. The mobile device records the code, which is usually reflected in the device's vibration
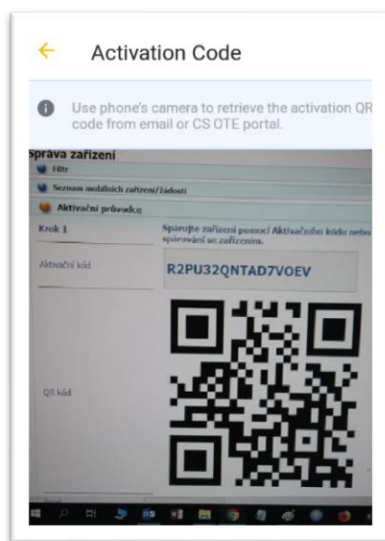

Fig. 18 – Scanning QR code Screen

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

Fig. 19 – Administrator Activation – New profile – Typing QR 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. 7) you create a new, not yet approved profile in the VDP mobile app.

Fig. 20 – New Profile Information (suspended yet)

3rd step – Administrator
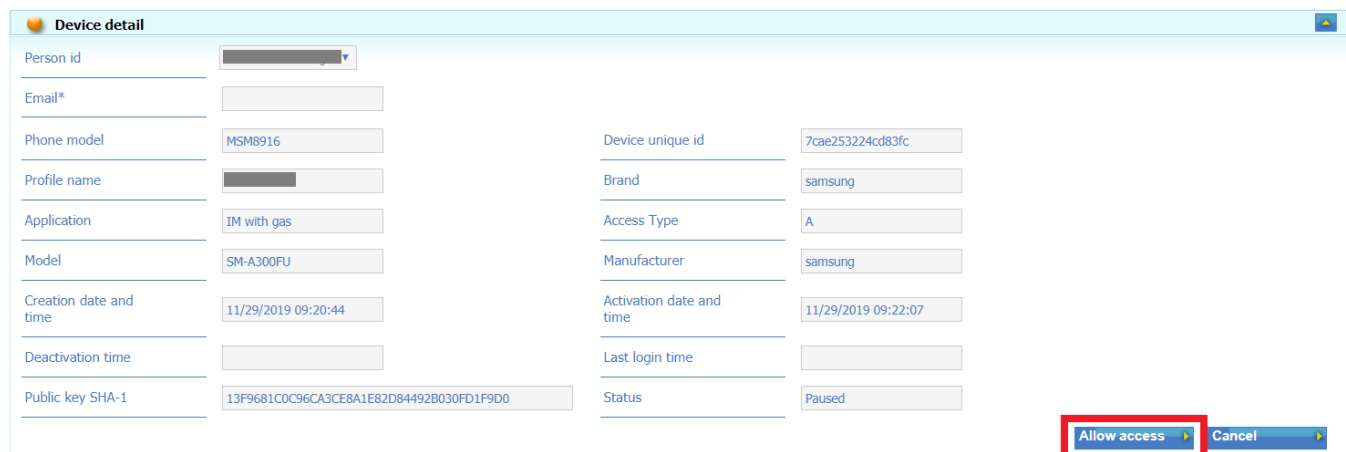
- After you create **New profile** on a mobile device, the Activation Wizard page on the RMP master data web portal automatically goes to the point where it can be checked which application was triggered and the public key fingerprint on the mobile device and CS OTE portal:

Fig. 21 – 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. 20 – New Profile Information (suspended yet) and 2 (Fig. 21 – 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. 21 – Administrator Activation – Web portal) 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 VDP network by clicking on the **Allow access** (Fig. 22 – Administrator Activation – Device detail).

Fig. 22 – Administrator Activation – Device detail

1.1.3 User login

When you start a newly installed application, you are asked to agree to the License Terms. These terms have to be confirmed otherwise it will not be allowed to access the application:

Fig. 23 – Acceptance of licence terms of IM Gas application

1.1.4 Profile Login

To sign in to the app, select your profile and enter your password on the mobile app home screen.
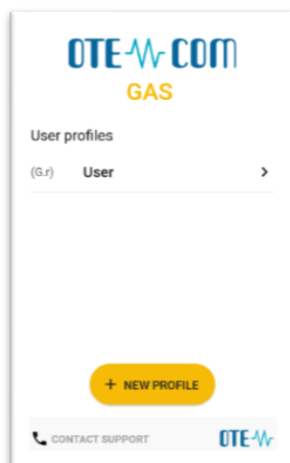

Fig. 24 – Available Profiles

- The first time you start the application, the Setup Wizard is launched automatically after login. You need to set the PIN - by entering and repeating it on the displayed numeric keypad and import the

certificate ([Transfer of the signing certificate to the mobile device](#)). If this process is not completed, it will automatically start the next time IM gas app is started until both steps are performed correctly.

1.2   Transfer of Signing Certificate to the mobile device

The process of certificate transfer from the CS OTE system requires simultaneous use of both PC and mobile device.

The following chapters describe how to upload a signing certificate to Local Storage and transfer it to a VDP mobile device.

1.2.1   Preparing to export a certificate stored in master data on a PC

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

- To transfer certificate to a mobile device, it is necessary to have the certificate uploaded to Local Storage. („how to" is described below).

- Menu **Registration** choose **Mobile Access – Certfificate Export**:

Fig. 25 – Certificate Export – Web portal

- Enter your local storage password – LS (in case the LS is not used, a message about unsetted passwords is displayed: A 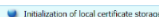password to the local storage not set / You do not have set any password right now. For work with certificates at the local storage you must have set a password.)

- To **transfer the certificate** to the mobile device, **the LS must be activated** - see the following chapter.
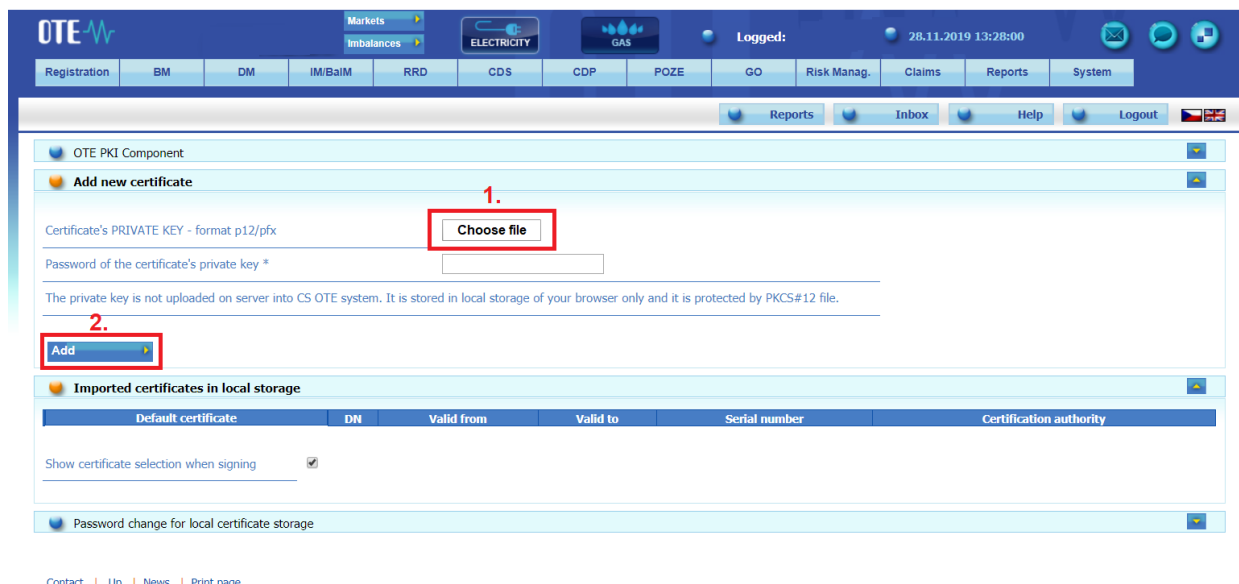
(In case of logging into LS and displaying the statement of certificates please skip 1.2.2 Local Storage activation.)

1.2.2 Activating Local Storage

Menu **Registration** choose **Certificate management** – **Settings of certificates**

- At the bottom of the page, click the Initialize local storage bar : ![Initialization of local certificate storage]

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

Now it is necessary to upload a qualified certificate that is registered in CS OTE and is to be transferred to the mobile device by clicking on **1.Select file**. After selecting the file *xxxxx.p12* and entering the password for this certificate, click **2.Add.**
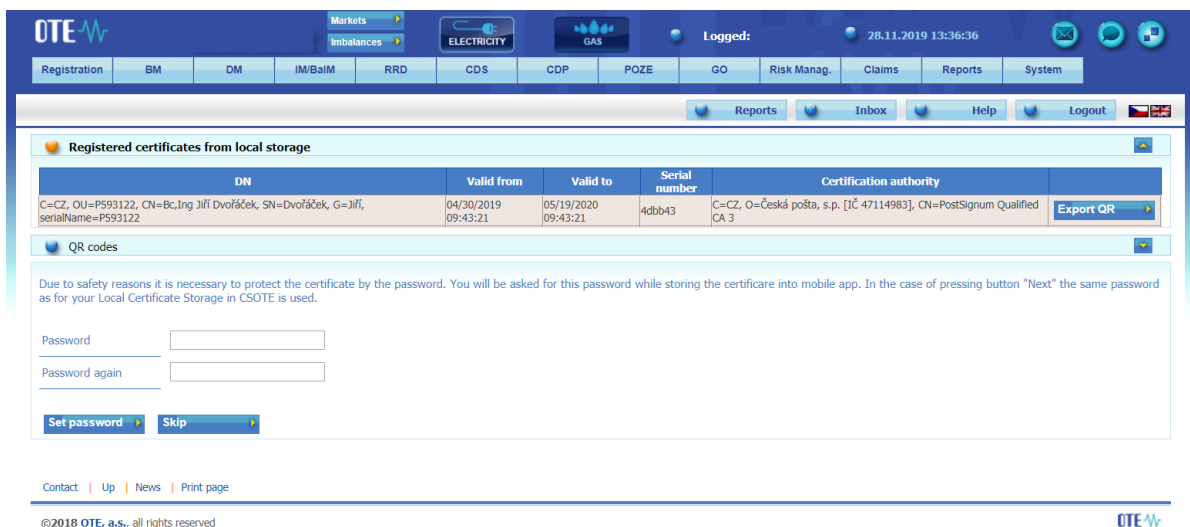
Fig. 26 – Importing qualified certificate into Local Storage

- The following screen lists the certificates that can be transferred from the Local Certificate Store to your mobile device (Fig. 27 – Certificate Export - Entering the password for certificate transmission).

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

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

Fig. 27 – Certificate Export - Entering the password for certificate transmission

- If Skip is selected, the same password will be used for the given certificate as set in the Local certificate store on the PC.

Date of revision:
3.12.2019

Document name:
Mobile application IM gas

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

By clicking menu **4** - above the first displayed QR code we can increase the number of generated codes and thus ensure the possibility of reading the codes even to older mobile devices that are not able to read this code.
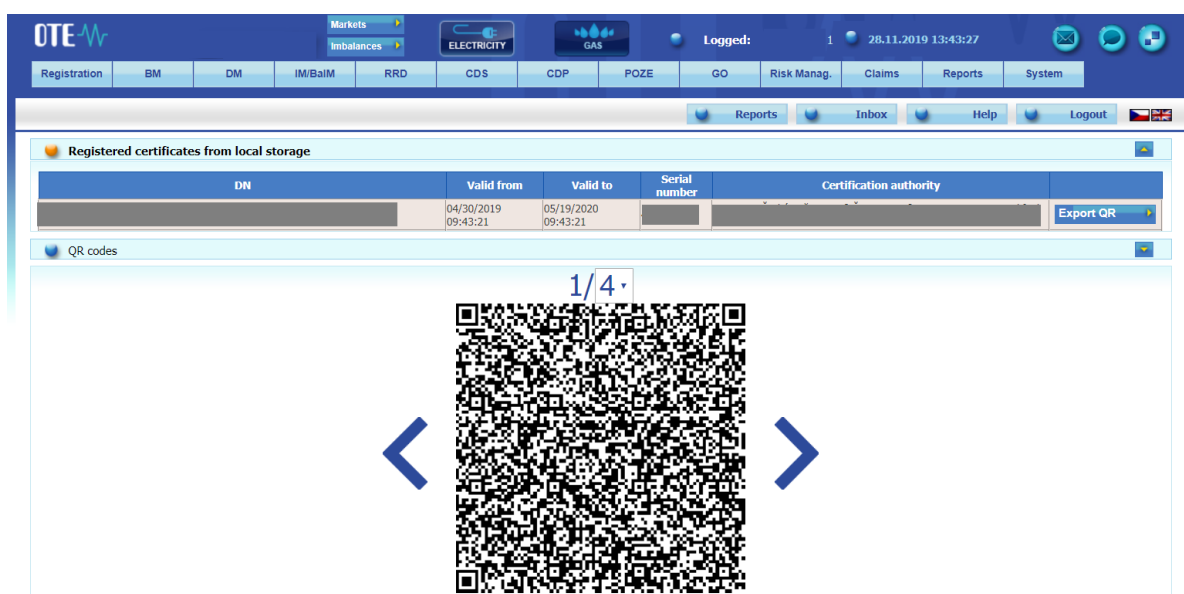

Fig. 28 – Certificate Export – QR codes generated by computer

1.2.3 Importing certificate to the mobile device

Mobile application requires signing certfificate for the work, If you first open the app, as the second step of the **Setup Wizard** is import Certificate. By clicking the **Import** button the certificate could be imported do Mobile Device

- If you want to replace an already uploaded certificate with another certificate registered in CS OTE (eg. when renewing the certificate) we can do this by selecting **Certificate** from the menu application VDP.

- Information about the saved certificate is displayed, if one has already been imported (Fig. 29 – Imported Certificate information)

- The buttons for **Import** new certificate and **Test** validity of saved certificate are also displayed (Fig. 29 – Imported Certificate information)
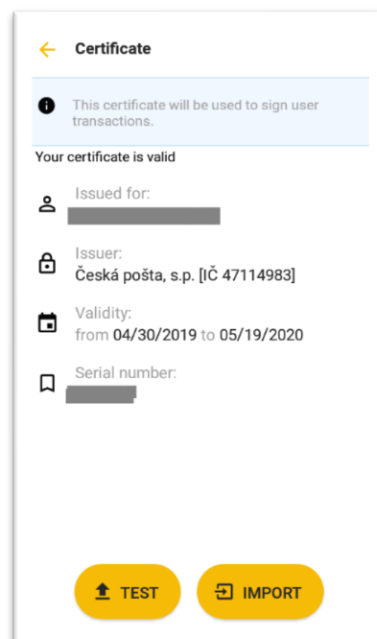
Fig. 29 – Imported Certificate information

- To upload another certificate, choose **IMPORT.**

Fig. 30 – Certificate Export – Mobile app – Scaning QR codes

- To move between QR codes, 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 the reading can be performed even in different order .

- After the import process is complete, you are prompted for the password that was used to transfer the certificate.

Information about new imported certificate now will be displayed (Fig. 31 –):
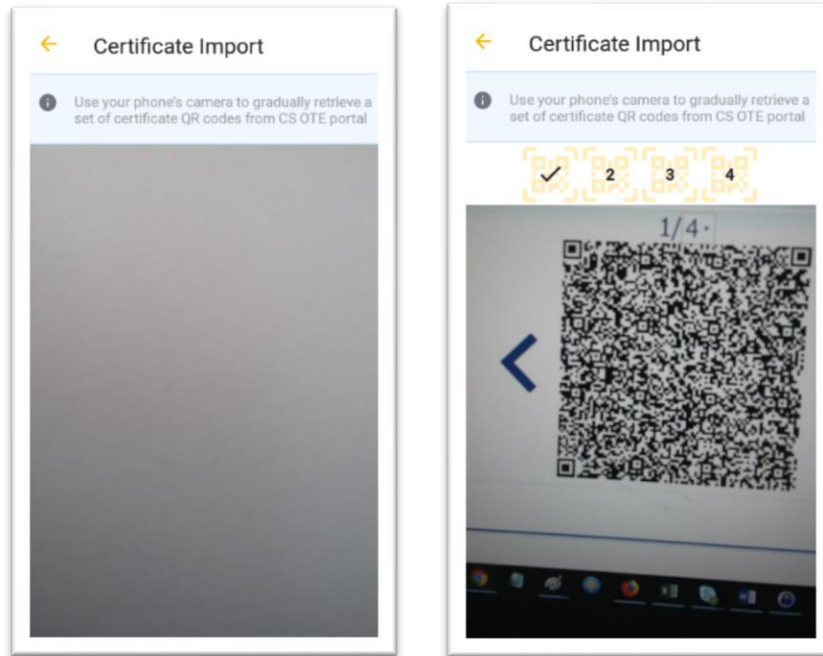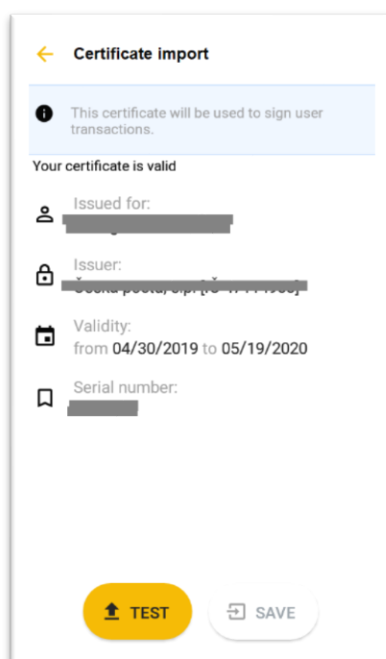

Fig. 31 – Imported certificate

- After pressing **TEST** and successfully validating the certificate the **Save** button will be enabled.

Clicking **Save Certificate**, you store this certificate in the device and it could be used to sign reports and the **VDP application is ready** to use.

1.3 Screens headers

The header of each primary screen of the application contains following icons: System menu, Market name, Connection status and identification of the logged user, News, Content refresh.
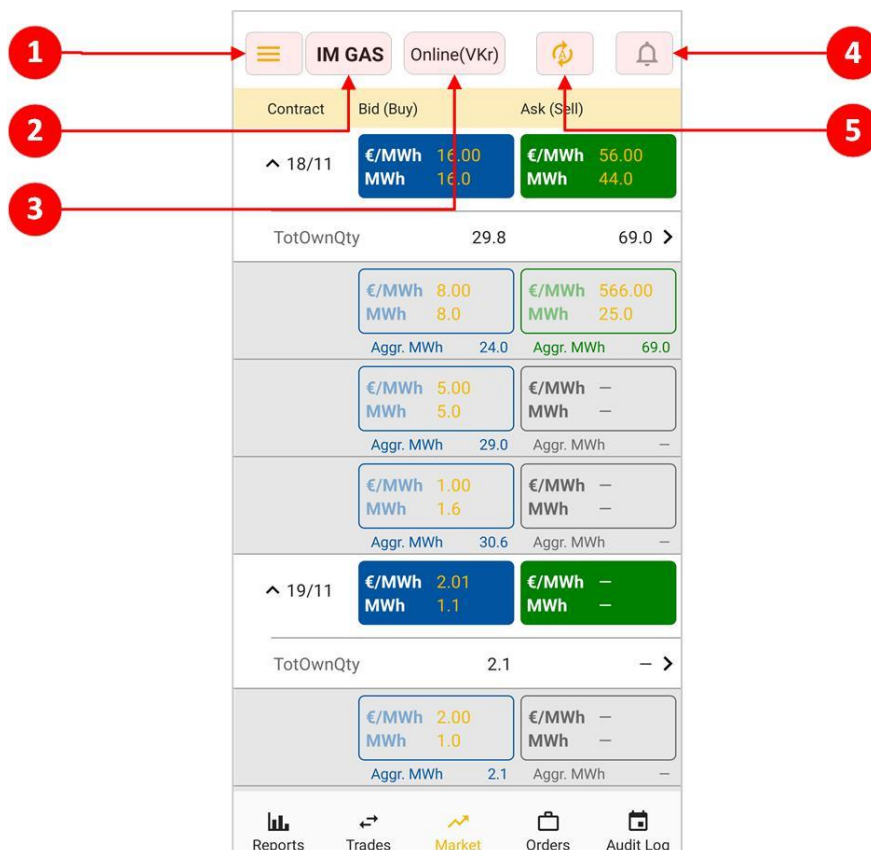

Fig. 32 – Screens headers

1   System menu – guide to information and settings screens Profile Details, Certificate, Settings, About Application, Contact Support, Logout
2   Market name – currently active market to which the displayed information and operations are related
3   Connection status and identification of the logged user – connection status of the mobile application (Online/Offline), shortcut of logged user is written in the brackets
4   News – contains information messages, also signals new VIP news (colored icon indicates unread messages)
5   Content refresh – button for manual refresh of screen content (A – indicates auto refresh enabled)

1.4 Control elements

- Back button ← – button is active only outside the primary screen, allows you to return to the previous screen

- Return to the top of the list

1.5 Market screen

After logging to the application the Market screen is displayed. This screen provides the user with up-to-date information about the status of active orders and about the market depth (the next 3 orders with the lowest price for sale and three orders with the highest price for purchase; the price and quantity values for own orders are color-coded), which can be "collapsed" by the user. The orders are shown as aggregated, sorted by price, and the quantity is also shown in the cumulative quantity (Aggr. MWh.).
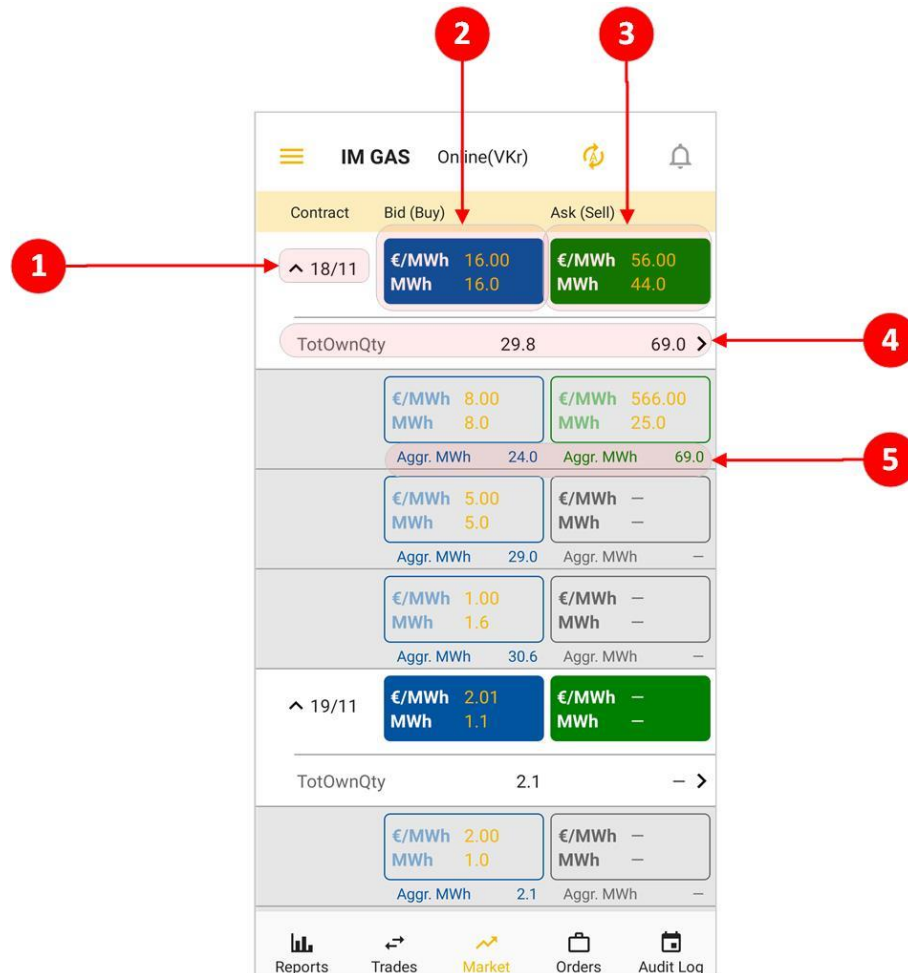

Fig. 33 – Market screen

1   The name of the contract with the possibility of collapsing market depth (after clicking)
2   Best order to buy – after clicking user is forwarded to the *Create Order screen* – create order Sell / Quick Accept
3   Best order to sell - after clicking user is forwarded to the *Create Order screen* – create order Buy / Quick Accept
4   Total Own Quantity – after clicking user is forwarded to *Orders by contract* screen
5   Aggregated quantity (MWh)

1.5.1 Create Order screen

The *Create Order* screen allows users to enter their own orders or take advantage of the quick acceptance option. **Quick Accept** serves for a buy / sell operation through predefined values that correspond to the opposite operation (sell / buy) entered by another user. If the contract does not contain any active order, the *Create Order* form opens with blank price and quantity parameters.

Fig. 34 – Create Order screen

6   Date and name of the contract – possibility of contract selection
7   Order to – switch button to select the buy/ sell operation
8   Type – display of order type and its restriction (LMT/ICB, (NON)/(FOK)/(IOC))
9   State – switch button for setting the active / inactive order
10   Quantity / price setting field using the keypad
11   Quantity / price setting buttons
12   Update content manually
13   View of a maximum five best orders to buy and sell

1.6 Reports Screen
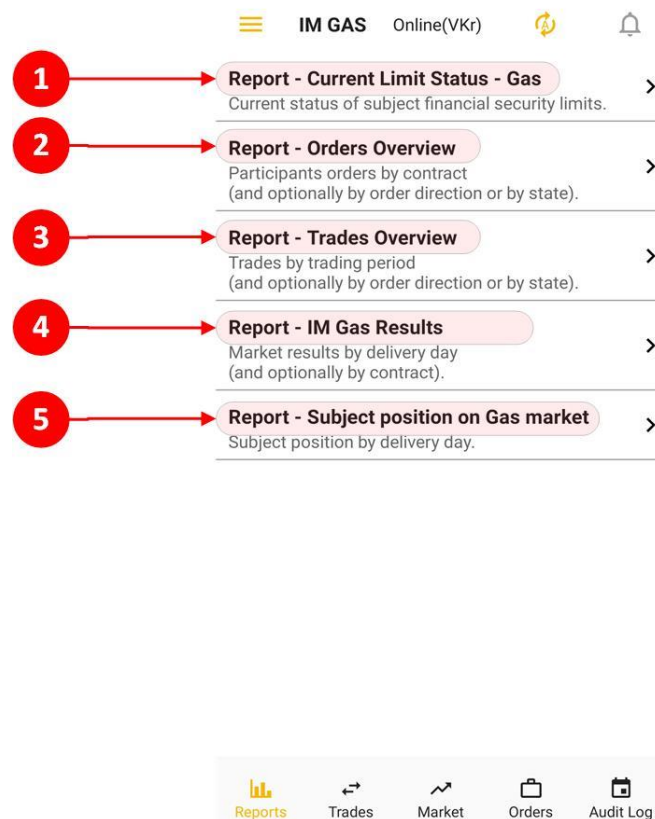
Provides list of all reports in the mobile app.

Fig. 35 – Reports screen

14 Report – Current Limit Status – Gas – displays an overview of the current BRP limits
15 Report – Orders Overview – displays the order data related to the selected contract
16 Report – Trades Overview – displays trades data
17 Report – IM Gas Results – displays the summary results of the intraday gas market
18 Report – Subject position on Gas market – displays the current position of BRP

1.6.1 Reports control

Click the report to view its content with default values. Each report has its own selection parameters. These include: Date selection, Contract selection, Order Direction, Order Status. Some parameters are used only in certain reports.

Fig. 36 – Report Orders Overview - header

1.7 Trades screen

It is used for monitoring the progress of trading and current trading results. Only contracts opened for trading are displayed on the screen.

Fig. 37 – Trades screen

19 TotalQty – quantity of all trades created during the session in MWh
20 TotOwnQty – Total own quantity
  • The total quantity sold, calculated as the sum of all trades for a given contract where the participant acts on the **sales** side in MWh.
  • The total quantity purchased, calculated as the sum of the quantity of all trades for a given contract where the participant acts on the **purchase** side in MWh.

21 Click the contract for displaying the *Trading History* screen

1.8 Trading History screen

Displays trading data related to the contract selected on the Trades screen.

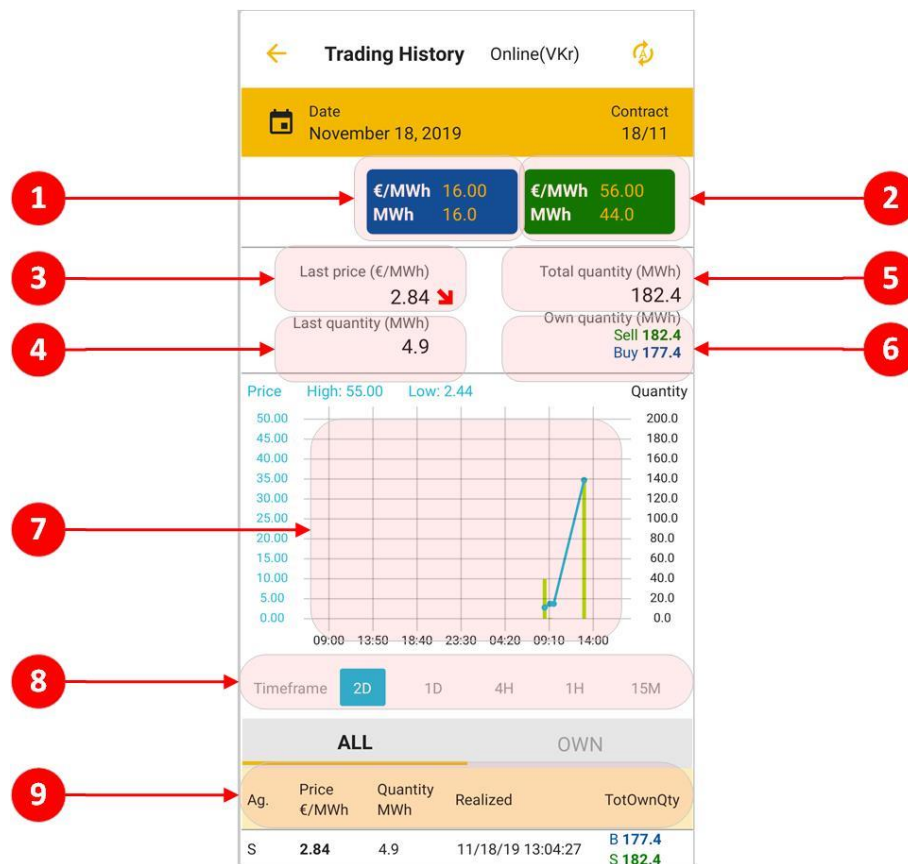
Fig. 38 – Trading History

22   Best order to buy - after clicking user is forwarded to the *Create Order* screen – create order Sell / Quick Accept
23   Best order to sell - after clicking user is forwarded to the *Create Order* screen – create order Buy / Quick Accept
24   Last price (€/MWh) – price of the last trade in EUR / MWh with trend indication
25   Last quantity (MWh) - quantity of the most recent trade in MWh
26   Total quantity (MWh) - quantity of all trades created during the session in MWh
27   Own quantity (MWh) – displays:
- Total quantity sold, calculated as the sum of all trades for a given contract where the participant acts on the sales side in MWh.
- The total quantity purchased, calculated as the sum of the quantity of all trades for the given contract, where the participant acts on the purchase side in MWh.

28   Graph – used for displaying progress of the prices and traded quantities of the selected contract in time
- Points curve – price progression
- Columns – quantity progression

29   Timeframe – time span of graph, *2D* (2 gas days), *1D* (1 gas day), *4H* (4 hours), *1H* (1 hour), *15M* (15 minutes)

30   Information about trades of a chosen contract (select all or own)

- Ag. - Aggressor – accepting party of the trade (buyer / seller), if the value is not filled, it means that the trade was created in the auction
- Price (€/MWh) – Price of the created trade in Eur / MWh
- Quantity (MWh) - The quantity of the created trade in MWh
- Realized – Time stamp of trade creation
- TotOwnQty – The cumulative **own** quantity at a time point in MWh – calculated as the sum of the quantity of all trades for a given contract and the direction of a given trade where the participant acts on the **sale / purchase** side in MWh.

1.9   Orders screen

It provides an overview of all orders created by a logged market participant and related to currently open contracts. Allows you to go to the *Modify Order* screen.

Fig. 39 – Orders screen

31   Filters orders according to whether they are active / inactive or both
32   Selection of order/orders for their activation/deactivation/delete -> after selection, the confirmation buttons for these operations are displayed
33   After click the order form *Modify Order* is opened

1.9.1   Modify Order screen

This screen allows the logged user to adjust the orders.

Limit order modification allows the user for changing only following attributes:

- order state (Active/Inactive),
- order quantity,
- order price.

Iceberg order modification allows the user for changing only following attributes:

- Order state (Active/Inactive).

An order cannot be modified if:

- it is deleted or withdrawn from trading (has expired);

- ID order is invalid;

- Max. version of the bid in the system does not match with the required bid version for modification.

Fig. 40 – Modify Order screen

34   The identification number, version, date and time of the created order that the user wants to modify
35   Operation – information about the order direction (Buy / Sell)
36   Valid to – time period of order validity for trading (time restriction)
37   Activity – switch button for setting the active / inactive order
38   Type – type of order and its restriction (LMT/ICB, (NON)/(FOK)/(IOC))
39   Quantity / price setting field using the keypad
40   Quantity / price setting buttons
41   Update content of the best orders table (Automatic or Manual)
42   View of a maximum five best orders to buy and sell
43   Buttons for delete order or its modification

1.10 Audit log screen

Informs user of the following events:

- Order reception
- Order modification
- Order activation/deactivation
- Order deletion
- System order deletion
- Trade creation
- Contract generation
- Change state of contract
- Change the deactivation flag of contract
- Modification of market settings
- Acceptance/cancelation of VIP news (see chapter 1.3)

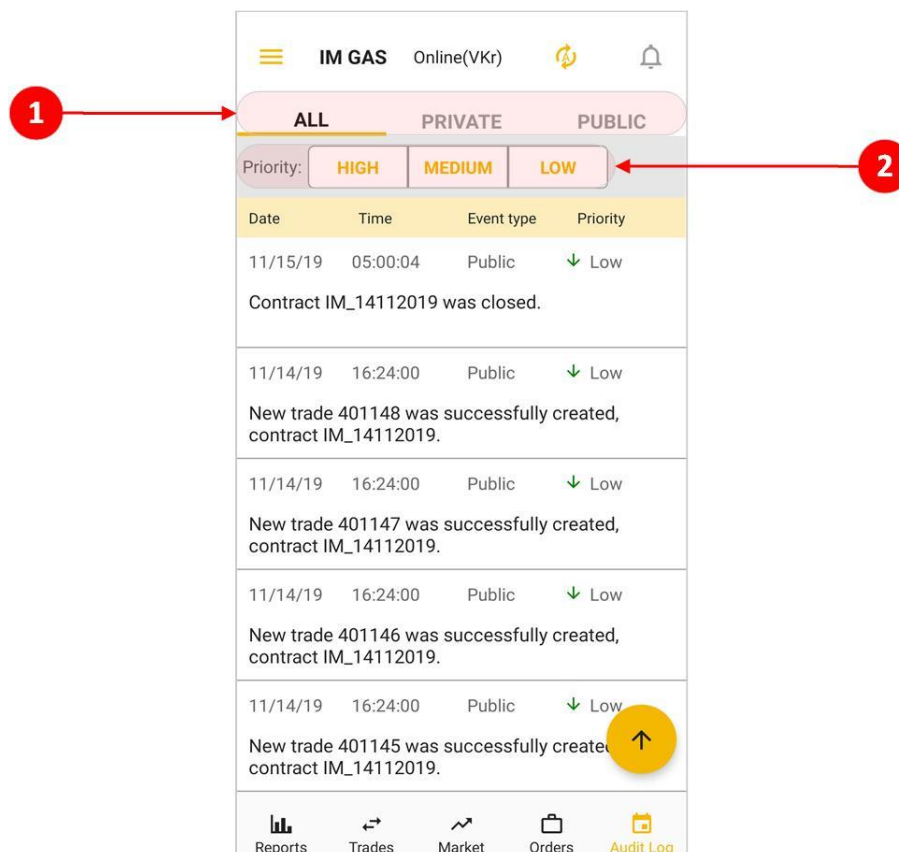Fig. 41 – Screen Audit log

44   Filter by message type – ALL/PRIVATE/PUBLIC
45   Filter by message priority – HIGH, MEDIUM, LOW

1.11 User logout

- To log out of the profile, select **Logout** from the application menu and then confirm **Logout.**
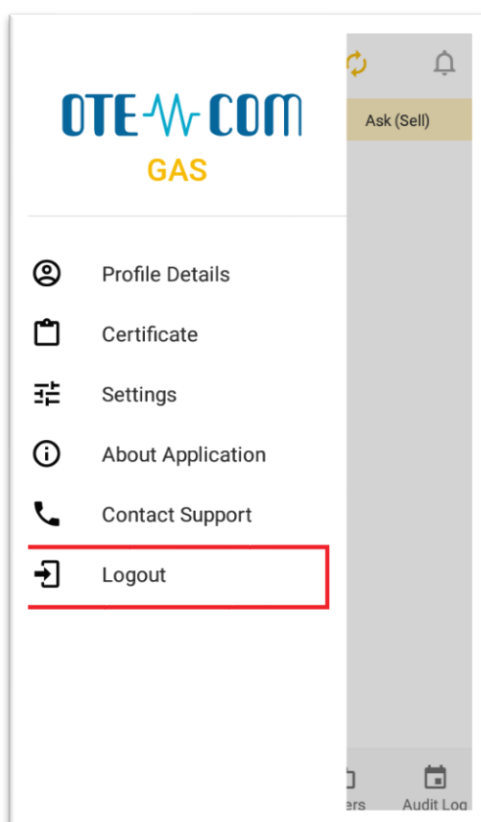

Fig. 42 – User Log out