

User documentation



Mobile Application IM Power

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

This document and its content are confidential. It is forbidden to reproduce the document or its parts, to show it to third parties or to use it for any other purposes than it was provided for without prior written agreement by OTE, a.s.

Access to the Intraday Electricity Market and trading on the Intraday Electricity Market via the mobile application is governed by the Business Conditions of OTE, a.s., and this user manual.

Content

1.1	Creating mobile access request	4
1.1.1	Direct activation with access to CS OTE portal	6
1.1.2	Administrator Activation (user with role RMP Administrator)	13
1.1.3	Launching Application	20
1.1.4	Limitations on the function of the profile	21
1.1.5	Profile Login	22
1.2	Transfer of Signing Certificate to the mobile device	23
1.2.1	Preparation of export of a certificate stored in Master Data	23
1.2.2	Importing certificate to Mobile Device	25
1.3	Screens headers	28
1.4	Control elements	28
1.5	Market screen	29
1.5.1	Create Order screen	30
1.6	Reports Screen	31
1.6.1	Reports control	32
1.7	Trades screen	33
1.8	Trading History screen	34
1.9	Orders screen	36
1.9.1	Modify Order screen	36
1.10	Audit log screen	38
1.11	Changes when Backup IM is active	38

Confidential

List of Pictures

Fig. 1 – Mobile access request creation scheme	5
Fig. 2 – Direct activation – Web portal CS OTE – Device management	6
Fig. 3 – Direct activation – Web portal CS OTE – Activation wizard	6
Fig. 4 – Direct activation – Web portal CS OTE	7
Fig. 5 – Acceptance of license terms	8
Fig. 6 – Direct activation – Mobile app – Login screen	8
Fig. 7 – Direct activation – Mobile app – Account information	9
Fig. 8 – Direct activation – Mobile app – Activation code	9
Fig. 9 – Administrator Activation – New profile – Typing QR code	10
Fig. 10 – Direct activation – Mobile app – Created Profile	10
Fig. 11 – Direct activation – Web portal	11
Fig. 12 – Direct activation – Web portal – Device detail	12
Fig. 13 – Administrator Activation – Menu Web portal– Devices management	14
Fig. 14 – Administrator Activation – Web portal– Devices management	14
Fig. 15 – Administrator Activation – Web portal	15
Fig. 16 – User activation with support of the Administrator - Mobile App – New profile	16
Fig. 17 – User activation with support of the Administrator - Mobile App – Profile information	16
Fig. 18 – Administrator Activation – E-mail with Activation QR code	17
Fig. 19 – Scanning QR code Screen	17
Fig. 20 – Administrator Activation – New profile – Typing QR code	18
Fig. 21 – New Profile Information (suspended yet)	18
Fig. 22 – Administrator Activation – Web portal	19
Fig. 23 – Administrator Activation – Device detail	20
Fig. 24 – Acceptance of the IM Power license agreement	20
Fig. 25 – Mobile Device detail (already Activated)	21
Fig. 26 – Available Profiles	22
Fig. 27 – Certificate Export – Web portal	23
Fig. 28 – Certificate Export – QR codes generated by computer	24
Fig. 29 – Imported Certificate information	25
Fig. 30 – Certificate Export – Mobile app – Scanning QR codes	26
Fig. 31 – Imported certificate	27
Fig. 32 – Screens headers	28
Fig. 33 – Market screen	29
Fig. 34 – Create Order screen	30
Fig. 35 – Reports screen	31
Fig. 36 – Report Orders Overview - header	32
Fig. 37 – Trades screen	33
Fig. 38 – Trading History	34
Fig. 39 – Orders screen	36
Fig. 40 – Modify Order screen	37
Fig. 41 – Screen Audit log	38
Fig. 42 – Difference between SIDC and local Backup IM	39

List of Abbreviations

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

Confidential

1.1 Creating mobile access request

- To create Mobile Access request the access to portal CS OTE (<https://portal.ote-cr.cz>) 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.

- Installing the application on a your mobile device:

a) Applications for Android:

- launch the application **Google Play** on a mobile device



- search OTE IM Power 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 IM Power or use QR code:
- download the application to your mobile device and install it



Confidential

Direct activation is possible for persons registered in the CS OTE portal. Roles with the roles listed below:

Roles related to the application IM Power application	
Passive access - Access to OTE IM Power via mobile application (Přístup k VDT elektro prostřednictvím mobilní aplikace)	(automatically when entering IMP)
- Access to the IM Power trading screen (Přístup k obchodovací obrazovce VDT)	(automatically when entering IMP)
Active access - Access to OTE IM Power via mobile application (Přístup k VDT elektro prostřednictvím mobilní aplikace)	(automatically when entering IMP)
- Access to the IM Power trading screen (Přístup k obchodovací obrazovce VDT)	(automatically when entering IMP)
- Submitting offers on IM Power via mobile application (Vkládání nabídek na VDT elektro prostřednictvím mobilní aplikace)	(role must be added by Administrator)
Přístup na reporty - Access to reports (Přístup na reporty)	(automatically when entering IMP)
- Access to OTE reports (Přístup na reporty OTE)	(automatically when entering IMP)

Note: Administrators see roles in people that they can assign / remove only.

- 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.
- Using IM Power application is not possible without transferring the certificate from CS OTE (description of certificate transfer is stated in the chapter **Transfer of Signing Certificate to the mobile device** (1.2)). If the certificate is used on a Token or other hardware repositories, the certificate cannot be exported and the private version (*.p12) of the certificate must be used for export (1.2.1).

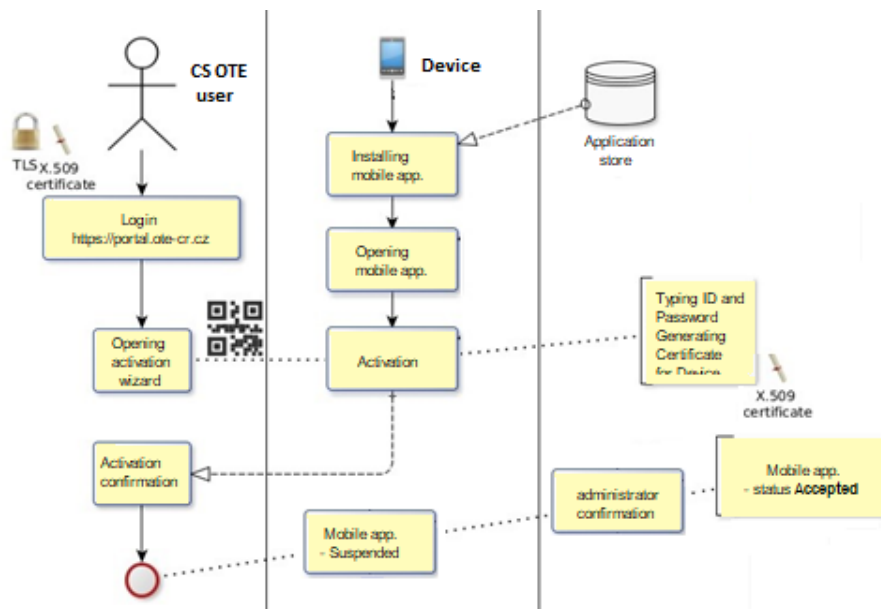


Fig. 1 – Mobile access request creation scheme

Confidential

1.1.1 Direct activation with access to CS OTE portal

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

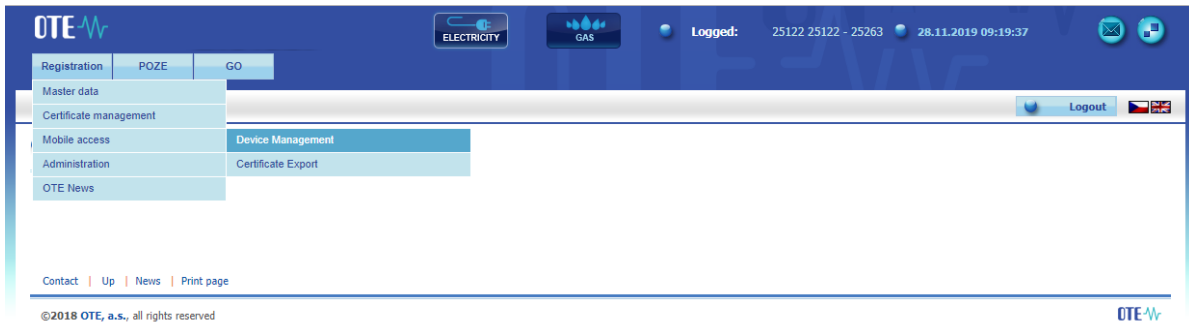


Fig. 2 – Direct activation – Web portal CS OTE – Device management

- Now press the button **New Activation**. You will see Device Detail (Fig. 3), 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).

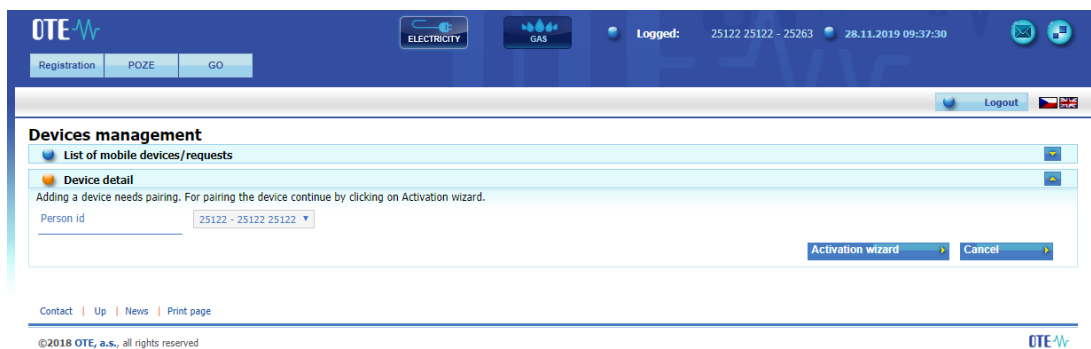


Fig. 3 – Direct activation – Web portal CS OTE – Activation wizard

Confidential

- After pressing the **Activation Wizard** button a page with generated QR code will be displayed for activating Mobile 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).

Confidential

Mobile device - Mobile Application OTE IM Power

- Launch OTE IM Power application on your mobile device.
- If you start a newly installed application, you are asked to agree to the License Terms (Fig. 5). The Licence is necessary to confirm otherwise access the application is not be allowed:

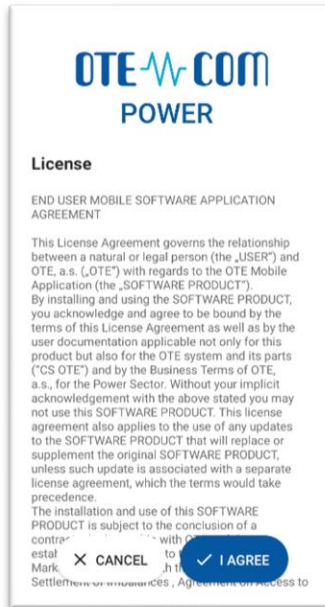


Fig. 5 – Acceptance of license terms

- The User profiles screen is then displayed (Fig. 6), where we click **New Profile**.

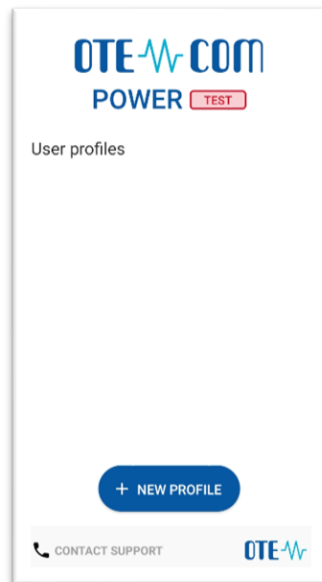


Fig. 6 – Direct activation – Mobile app – Login screen

Confidential

Fig. 7 – 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. 8). Point the camera at the QR code screen. The mobile device records the code, which is usually reflected in the device's vibration.



Fig. 8 – Direct activation – Mobile app – Activation code

Confidential

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

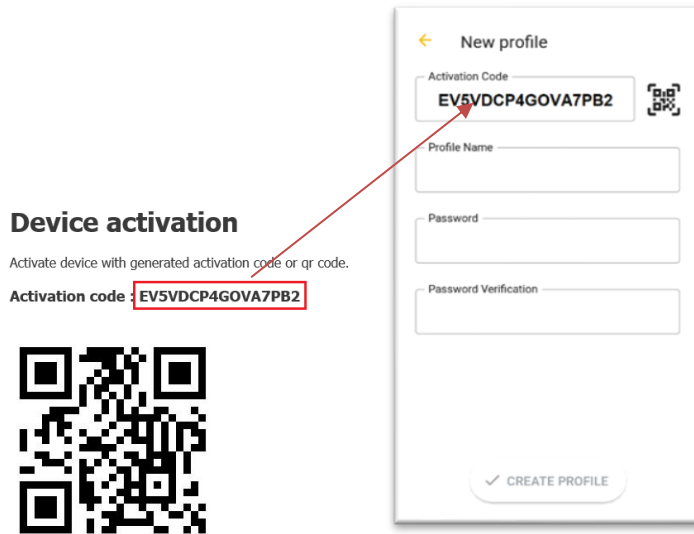


Fig. 9 – Administrator Activation – New profile – Typing QR code

- 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 new, not yet approved profile in the IM Power app. (Fig. 10).

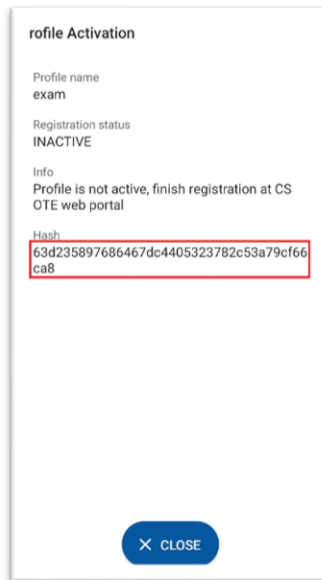


Fig. 10 – Direct activation – Mobile app – Created Profile

Confidential

- 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 item **Application** on the screen of CS OTE could be type of **IM with electricity**, **IM with Gas** or **Renewable resources** depending on the type of mobile application used to create the profile.

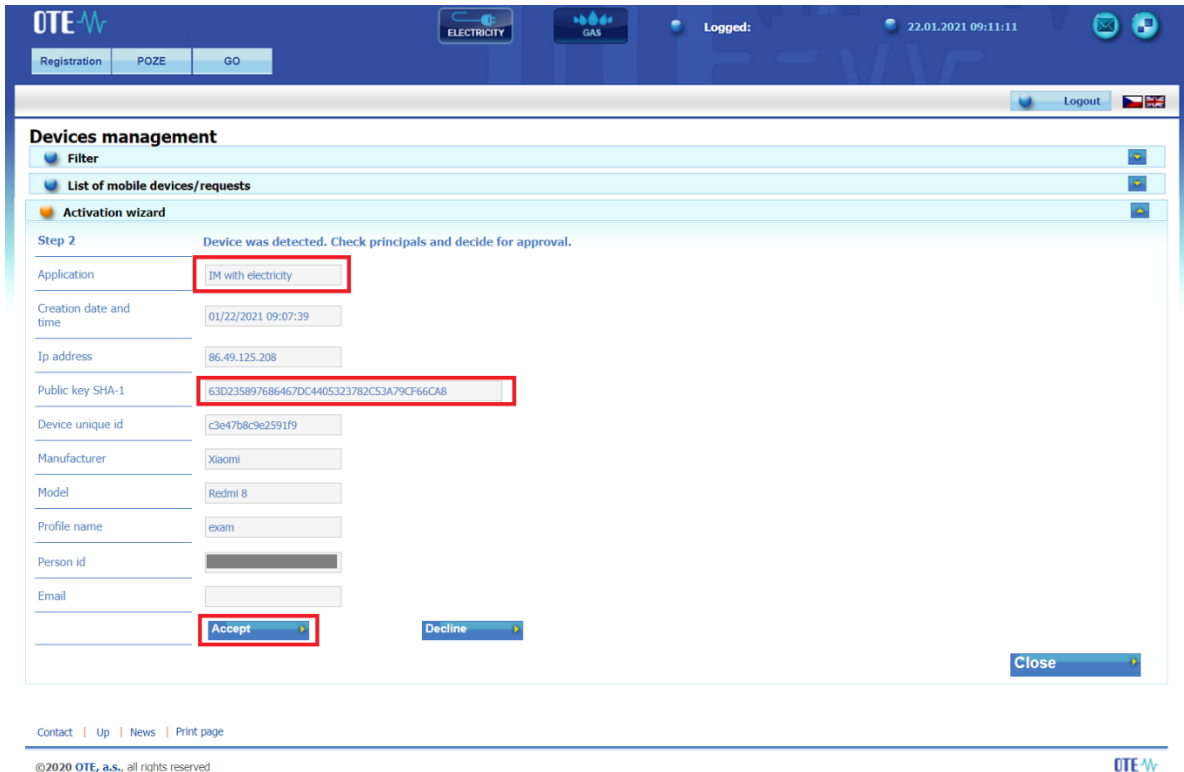


Fig. 11 – Direct activation – Web portal

- It is **recommended** to check if that the red-framed codes in (Fig. 10) and (Fig. 11) are the same on the mobile device and in the CS OTE web portal.

Confidential

2024 OTE, a.s.

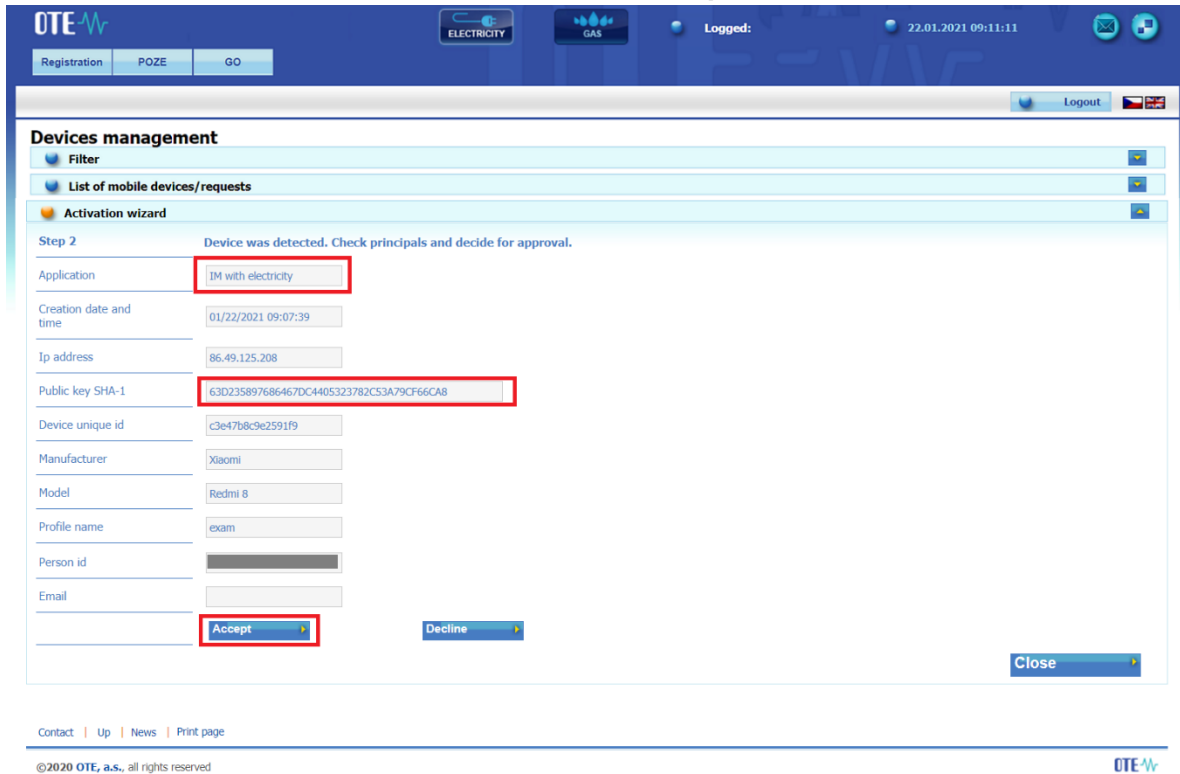
Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

- Click

Accept

(



- Fig. 11) 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. CS OTE Portal now displays **Mobile Device Detail** (Fig. 11)

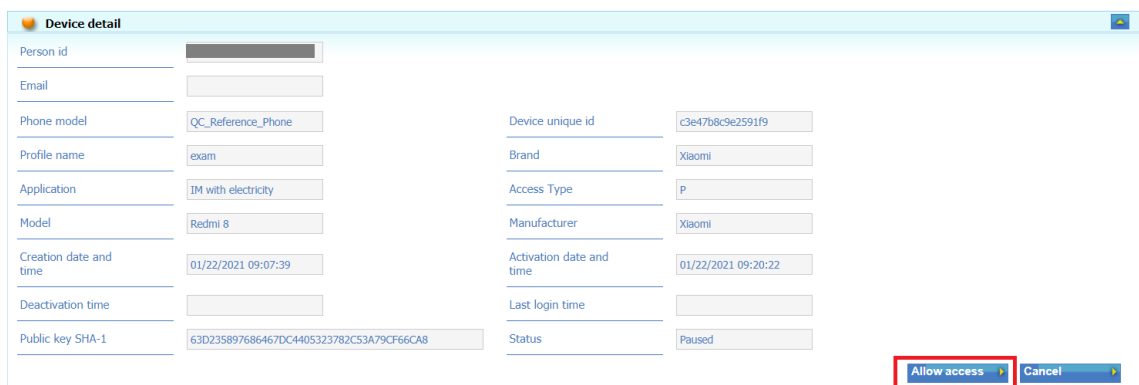


Fig. 12 – Direct activation – Web portal – Device detail

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

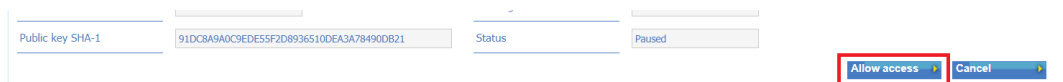
- Having the RMP Administrator role, you now see the **Allow Access** button. Press it to allow the mobile device access the IMP network. Continuation in chapter – 1.1.3
- Attention: If you do not see the **Allow access** button on the page, please contact the **Master Data Manager** for your company, who can activate this account page by clicking on **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 application.



Pressing button **Allow access** activate possibilities 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. 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**

Confidential

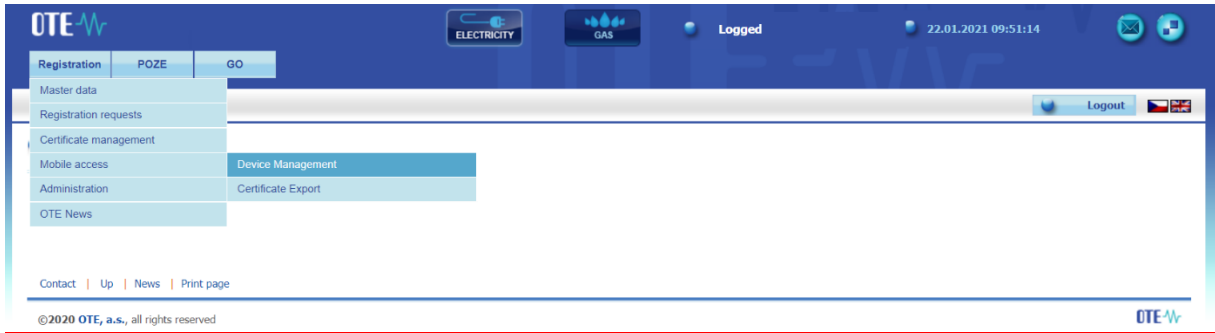


Fig. 13 – Administrator Activation – Menu Web portal– Devices management

- 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. 14 Fig. 14 –).

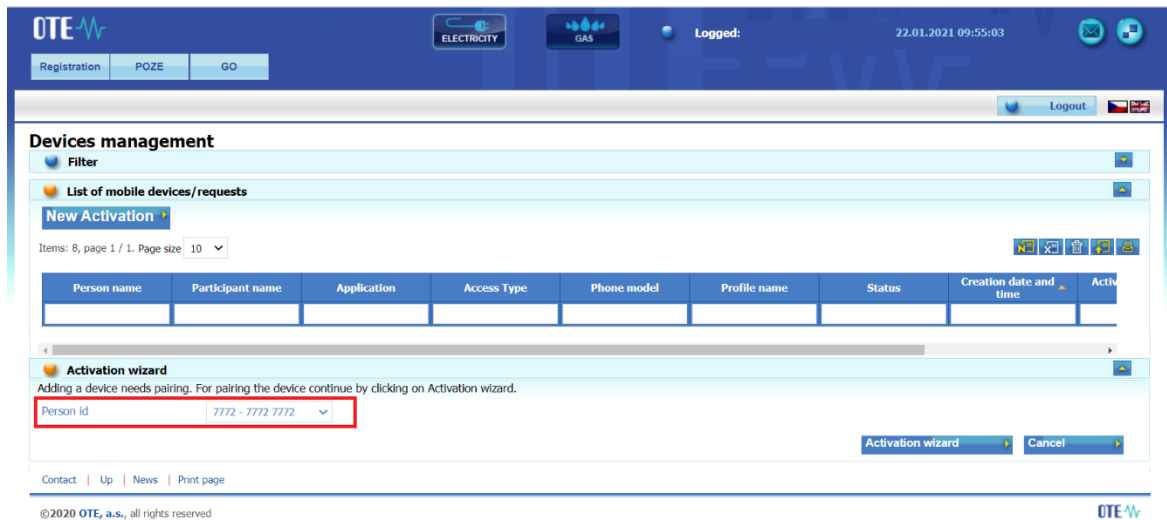


Fig. 14 – Administrator Activation – Web portal– Devices management

- After selecting the person and possibly changing the email, click on the **Activation Wizard** button (Fig. 14).
- 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 process activating new profile in the mobile app (Fig. 15).
- It is necessary to read the QR code by the mobile device (Fig. 8) within one hour, otherwise the activation will expire.
- 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

Confidential

paired with CS OTE within one hour, otherwise the activation will expire and the activation process must be repeated.

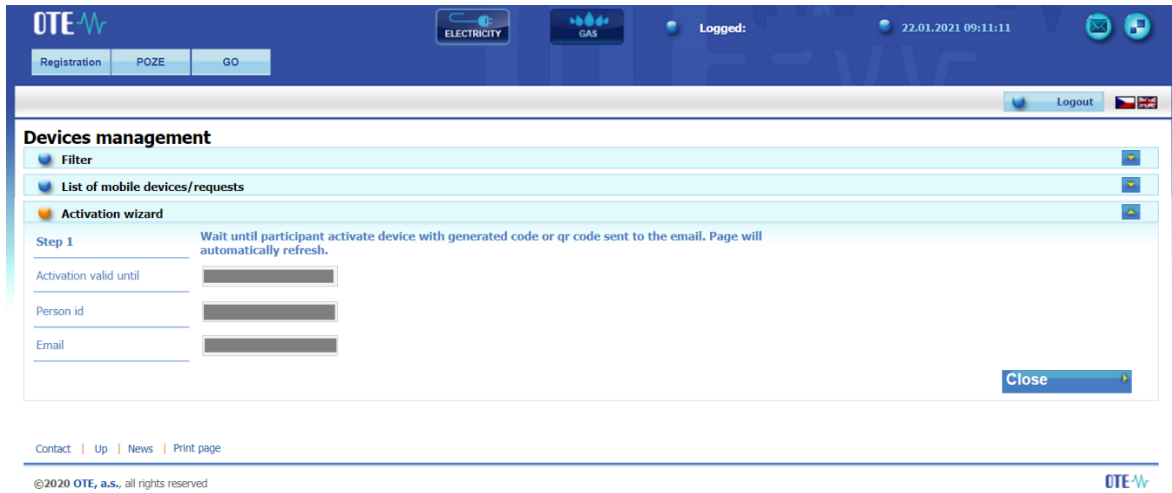


Fig. 15 – Administrator Activation – Web portal

2nd step – User setting up a Profile on his Mobile Device

- Launch mobile application OTE IM Power on your Mobile Device.
- If you start a newly installed application, you are asked to agree to the License Terms (Fig. 5). The Licence is necessary to confirm otherwise it will not be allowed to access the application.
- Click **New profile**

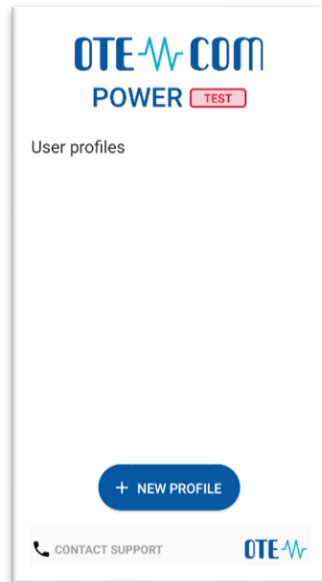


Fig. 16 – User activation with support of the Administrator - Mobile App – New profile

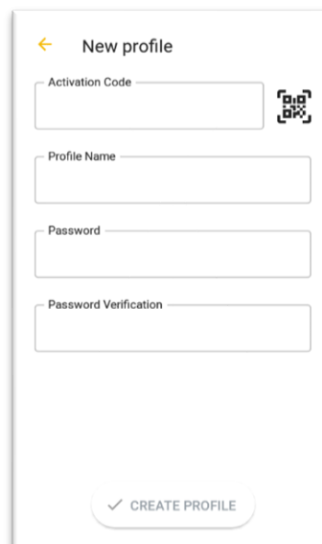


Fig. 17 – User activation with support of the Administrator - Mobile App – Profile information

Confidential

- In the Activation Code field, enter the QR code from the email sent by your administrator (Fig. 18):


Device activation

Activate device with generated activation code or qr code.

Activation code : EV5VDCP4GOVA7PB2



Fig. 18 – Administrator Activation – E-mail with Activation QR code

- Click  on the mobile device to launch the camera of your mobile device (Fig. 17). Point the camera at the QR code on the screen. The mobile device records the code, which is usually reflected in the device's vibration.

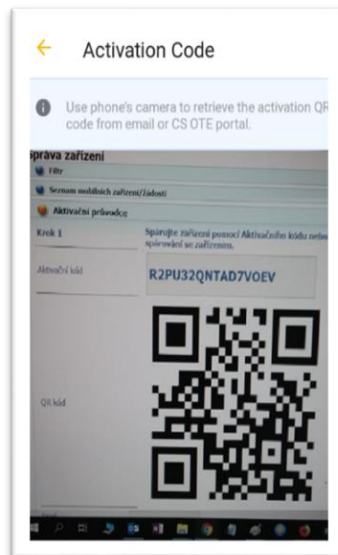


Fig. 19 – Scanning QR code Screen

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

- 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**



Fig. 20 – 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. 20) you create a new, not yet approved profile in IM Power mobile app.

Fig. 21 – New Profile Information (suspended yet)

Confidential

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:

Activation wizard	
Step 2 Device was detected. Check principals and decide for approval.	
Application	IM with electricity
Creation date and time	02/28/2021 10:12:14
Ip address	78.102.206.126
Public key SHA-1	E52FD808A5FD2F51DC54CAE4F0115FCEC8546D7B
Device unique id	561794F1-7D76-4FB8-892A
Manufacturer	Apple
Model	iPhone SE
Profile name	ppppp
Person id	
Email	
<input type="button" value="Accept"/> <input type="button" value="Decline"/> <input type="button" value="Close"/>	

Fig. 22 – Administrator Activation – Web portal

- We recommend checking**
 - whether column **Application** contains the desired application for which the activation is to be performed;
 - If the red-framed codes (Fig. 21 – New Profile Information (suspended yet)) and (Fig. 22 – Administrator Activation – Web portal Fig. 22 –), displaying the public key fingerprint are identical on the mobile device and in the CS OTE web portal.
- By clicking on **Accept** (Fig. 22) 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 IM Power network by clicking on the **Allow access** (Fig. 23).

Confidential

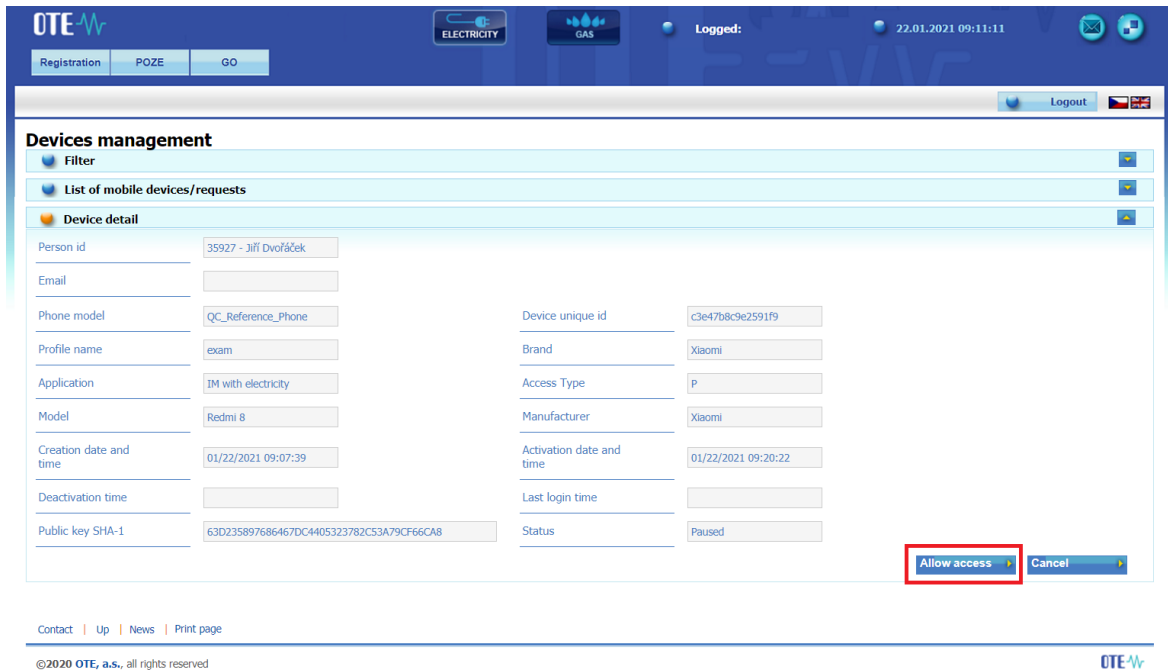


Fig. 23 – Administrator Activation – Device detail

1.1.3 Launching Application

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 OTE IM Power application.

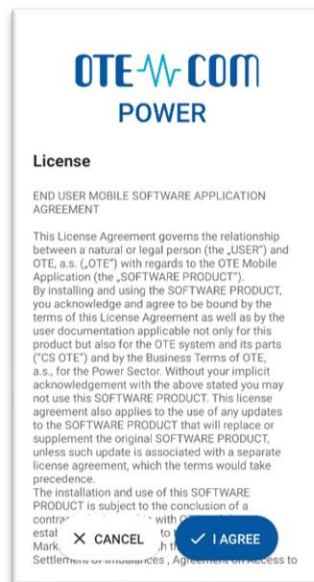


Fig. 24 – Acceptance of the IM Power license agreement

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

1.1.4 Limitations on the function of the profile

- a) To temporarily suspend the profile function go to **Mobile Access / Device Management**, select the profile and press the button **Pause access**(Fig. 24). Ten minutes after entering this request, it will not be possible to use the selected profile. Subsequently, the profile can be activated again by clicking on **Allow access**.
- b) To permanently deactivate the account, select the **Deactivate** option, thus permanently deleting this profile. Ten minutes after entering this request, it will not be possible to use the selected profile.

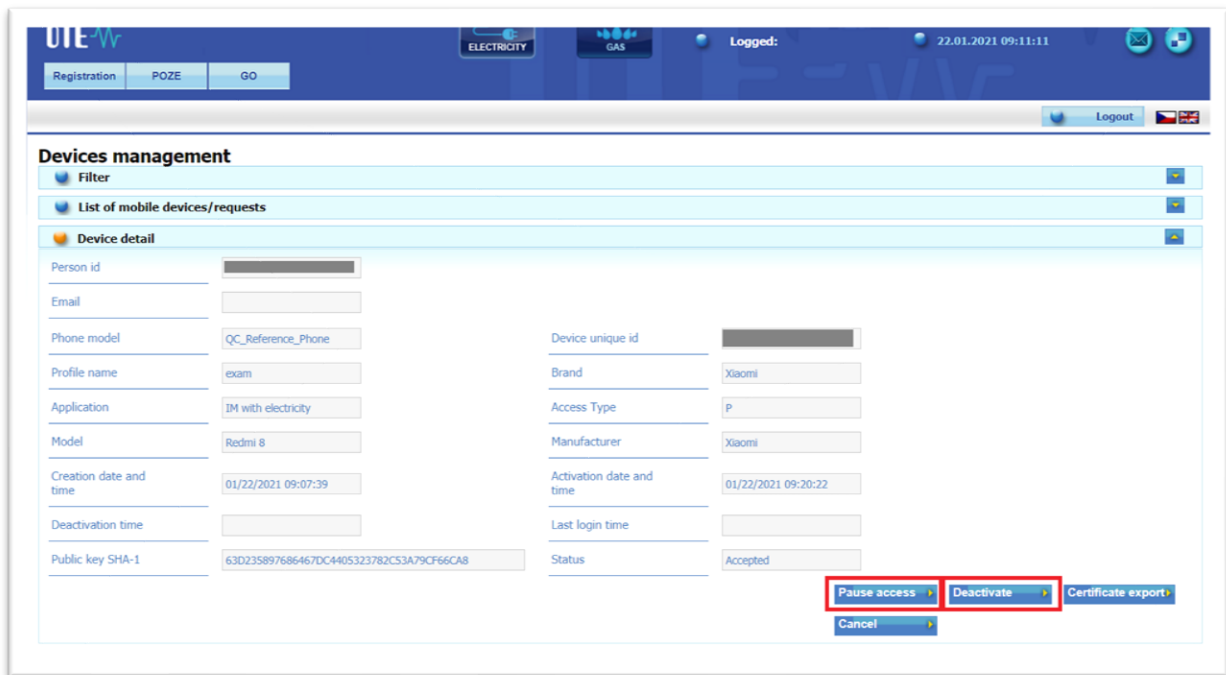


Fig. 25 – Mobile Device detail (already Activated)

-
- 1) Removing the role for trading on VDT from the mobile phone (EmtasIMIns) has a delay of up to 5 minutes, the trading of the user from OTECOM will not be limited.
 - 2) Removing the role for any business on VDT (EmtasIMIns) is effective immediately, ie from the mobile up to 5 minutes. bids will be sent, but will return with an error immediately after the role is removed.

Confidential

1.1.5 Profile Login

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

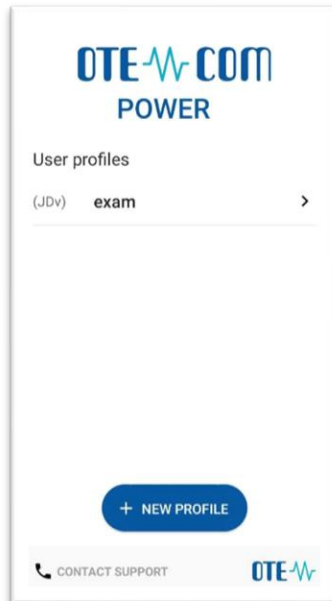


Fig. 26 – Available Profiles

- 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 Power is started until both steps are performed correctly.

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

1.2 Transfer of Signing Certificate to the mobile device

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.

1.2.1 Preparation of export of a certificate stored in Master Data

- Log in to the web portal CS OTE (<https://portal.ote-cr.cz/otemarket/>).
- To transfer your 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 – Certificate Export**:

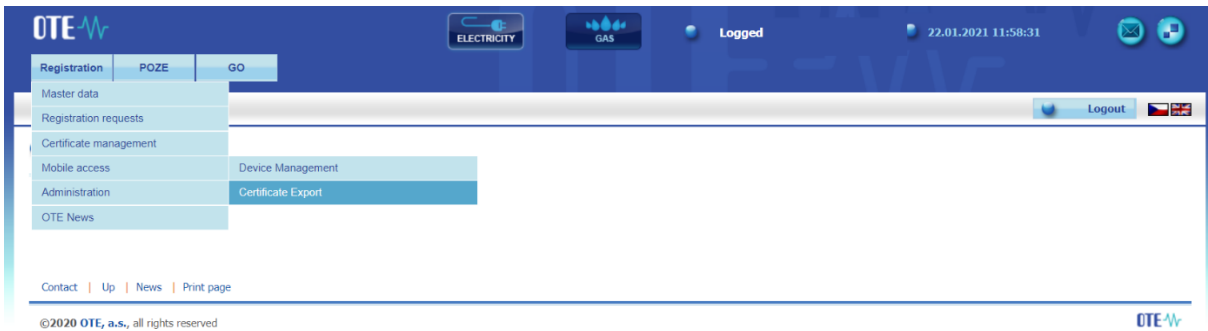


Fig. 27 – Certificate Export – Web portal

- a) In the case of an **active Local Storage**, 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	Export QR
	04/23/2020 09:14:23	05/13/2021 09:14:23			Export QR

QR codes

Confidential

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

Now it is necessary to upload a certificate for transmission that is **qualified**, must **contain a private part** and is **registered in CS OTE** by clicking on **Select file**. After selecting the file **xxxxx.p12** and entering the password for this certificate, click **Add**. *(The private part is not sent to the server - it is stored locally in the browser directory with PKCS # 12 security. After the certificate is transferred to the mobile device, the private part of the certificate can be deleted from the browser.)*

- 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.

You can increase the number of QR codes on the 1st screen on the portal (**Fig. 28 Fig. 28 –**) – by clicking on the menu at 4 above the QR code - for better transfer if you have a mobile device with an older camera:



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

Confidential

1.2.2 Importing certificate to Mobile Device

- Mobile application requires signing by certificate for the work, If you first open the app, as the second necessary step of the **Setup Wizard** is import Certificate. By clicking the **Import** button in the Mobile App. the certificate could be imported to Mobile Device (continue **IMPORT** below).
- 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 IM Power application:
 - Information about the saved certificate is displayed, if one has already been imported (Fig. 29)
 - The buttons for **Import** new certificate and **Test** validity of saved certificate are displayed (Fig. 29)

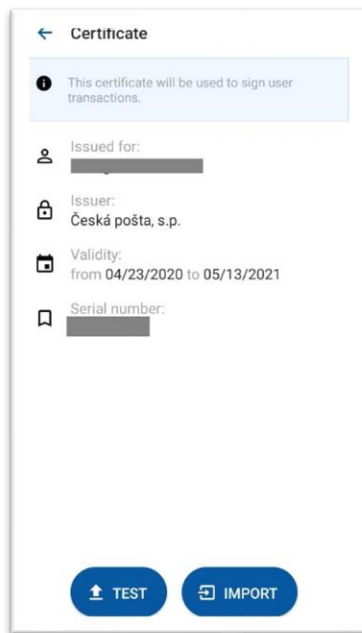


Fig. 29 – Imported Certificate information

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

- To upload new certificate, choose **IMPORT** and use your mobile device camera to scan the codes:

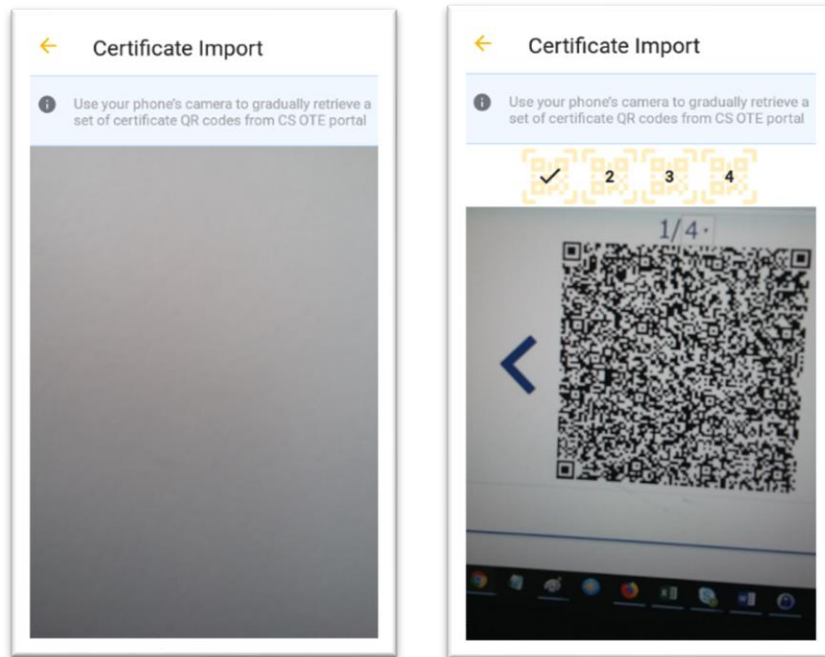


Fig. 30 – Certificate Export – Mobile app – Scanning QR codes

- 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.
- Then the information about the retrieved certificate is displayed (Fig. 31). Press the **Test** button to verify that the downloaded certificate can be used in the OTE IM Power application and if sign is OK, the **Save** button will be displayed.

Confidential

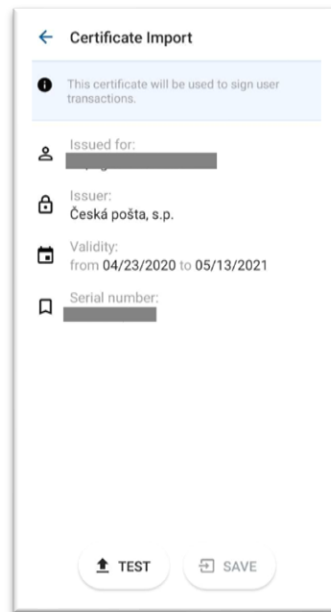


Fig. 31 – Imported certificate

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

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

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, Content refresh, News.

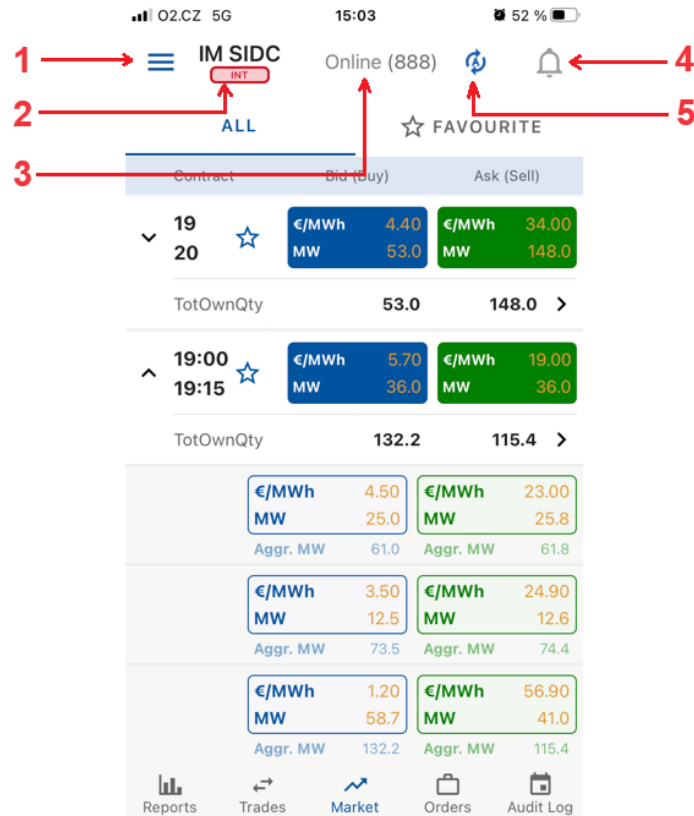




Fig. 32 – Screens headers

- 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 Content refresh – button for manual refresh of screen content (A – indicates auto refresh enabled)
- 5 News – contains information messages, also signals new VIP news (colored icon indicates unread messages)

1.4 Control elements

- Back button  is active only outside the primary screen, allows you to return to the previous screen
- Return to the top of the list 

Confidential

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 shown/ hidden by the user. The orders are shown as aggregated, sorted by price, and the quantity is also shown in the cumulative quantity (Aggr. MW).

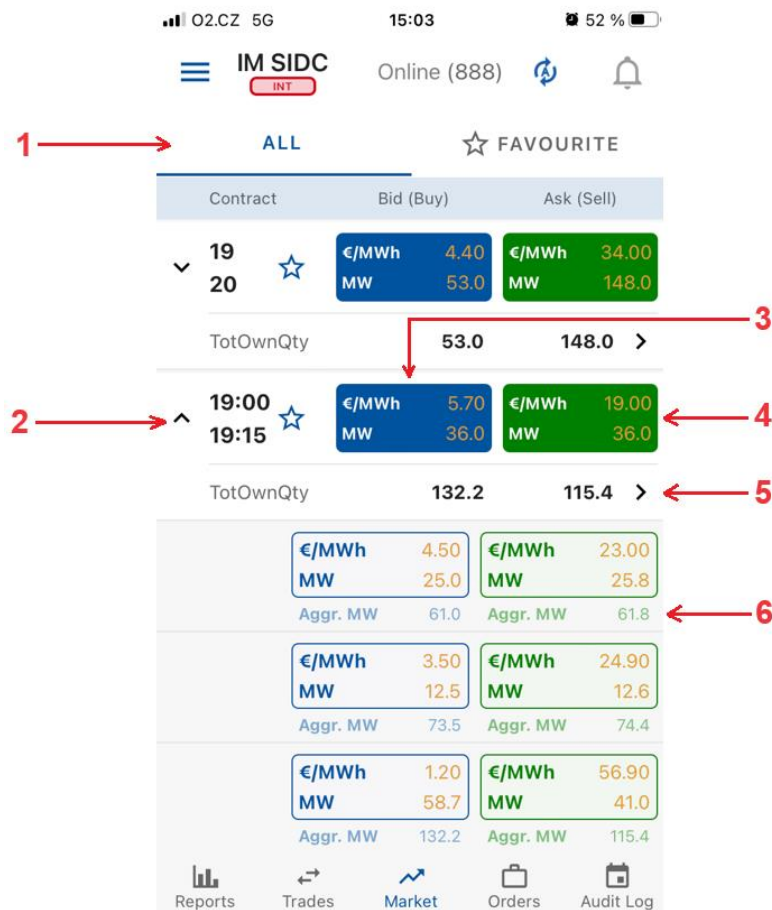


Fig. 33 – Market screen

- 1 Filtering between all and favorites contracts
- 2 The name of the contract with the possibility of opening/closing of the market depth (after clicking)
- 3 Best order to buy – after clicking user is forwarded to the *Create Order screen* – create order Sell / Quick Accept
- 4 Best order to sell - after clicking user is forwarded to the *Create Order screen* – create order Buy / Quick Accept
- 5 Total Own Quantity – after clicking user is forwarded to *Orders by contract* screen
- 6 Aggregated quantity (MW)

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

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.

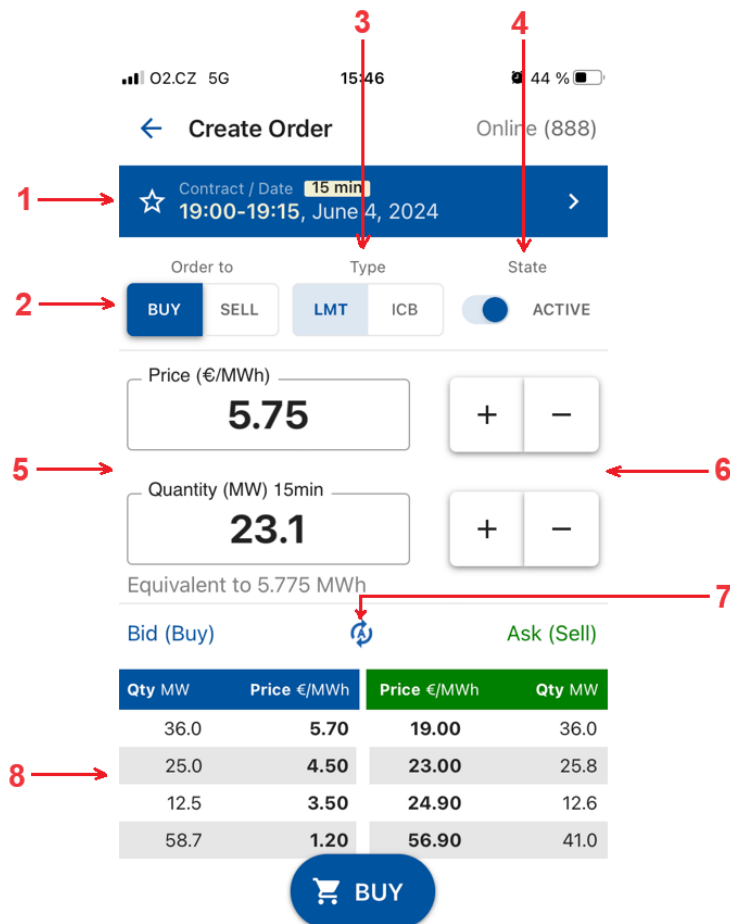


Fig. 34 – Create Order screen

- 1 Date and name of the contract – possibility of contract selection
- 2 Order to – switch button to select the buy/ sell operation
- 3 Type – display of order type and its restriction (LMT/ICB)
- 4 State – switch button for setting the active / inactive order
- 5 Quantity / price setting field using the keypad
- 6 Quantity / price setting buttons
- 7 Update content manually
- 8 View of a maximum five best orders to buy and sell

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

1.6 Reports Screen

Provides list of all reports in the mobile app.

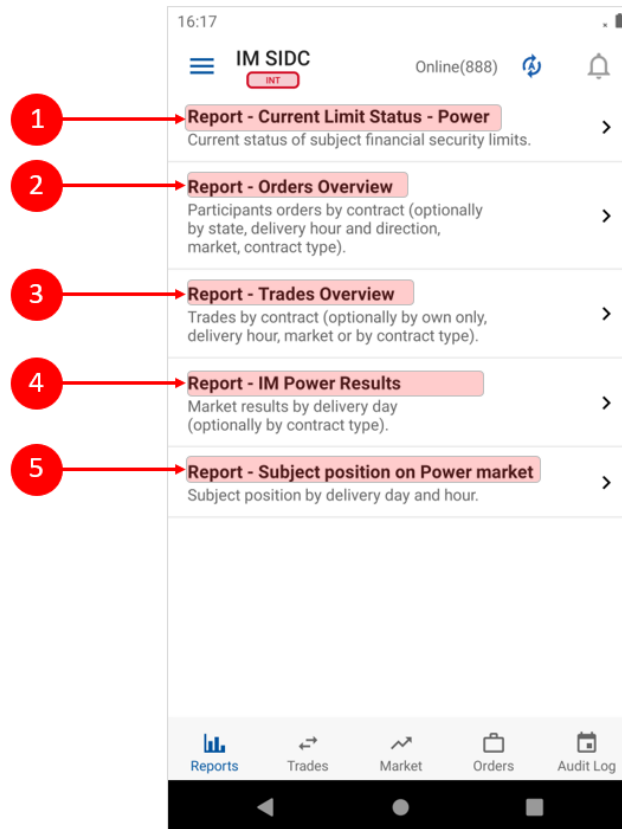


Fig. 35 – Reports screen

- 1 Report – Current Limit Status – Power – displays an overview of the current BRP limits
- 2 Report – Orders Overview – displays the order data related to the selected contract
- 3 Report – Trades Overview – displays trades data
- 4 Report – IM Power Results – displays the summary results of the intraday power market
- 5 Report – Subject position on Power market – displays the current position of BRP

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

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, Period selection, Order Status, Order Direction, Product Type and Market. Some parameters are used only in certain reports.

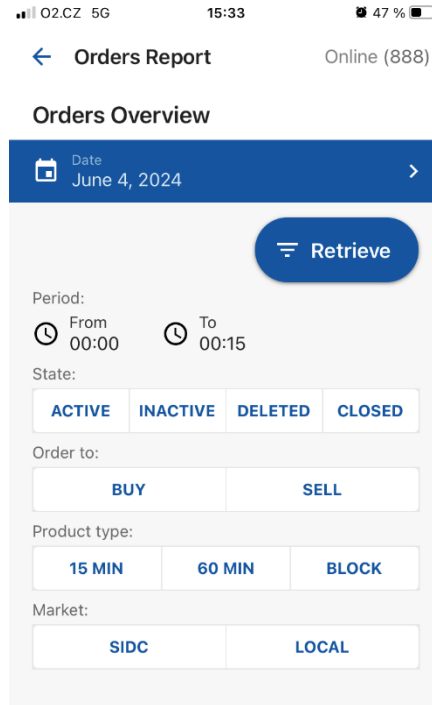


Fig. 36 – Report Orders Overview - header

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.

Contract	Last trade	TotalQty	OwnQty
19	☆ €/MWh	34.00	S 13.7
20	☆ MW	3.7	B 5.6
19:00	☆ €/MWh	7.25	S —
19:15	☆ MW	5.6	B 5.6
19:15	☆ €/MWh	7.25	S —
19:30	☆ MW	5.6	B 5.6
19:30	☆ €/MWh	7.25	S —
19:45	☆ MW	5.6	B 5.6
19:45	☆ €/MWh	7.29	S —
20:00	☆ MW	5.7	B 5.7
20	☆ €/MWh	1.00	S —
21	☆ MW	19.1	B 5.7
20:00	☆ €/MWh	7.29	S —
20:15	☆ MW	5.7	B 5.7
20:15	☆ €/MWh	7.29	S —
20:30	☆ MW	5.7	B 5.7

Fig. 37 – Trades screen

- 1 TotalQty – quantity of all trades created during the session in MW
- 2 OwnQty – 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 MW.
 - 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 MW.
- 3 Click the contract for displaying the Trading History screen

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

1.8 Trading History screen

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



Fig. 38 – Trading History

- 1 Best order to buy - after clicking user is forwarded to the *Create Order* screen – create order Sell / Quick Accept
- 2 Best order to sell - after clicking user is forwarded to the *Create Order* screen – create order Buy / Quick Accept
- 3 Last price (€/MWh) – price of the last trade in EUR/MWh with trend indication
- 4 Last quantity (MW) - quantity of the most recent trade in MW
- 5 Total quantity (MW) - quantity of all trades created during the session in MW
- 6 Own quantity (MW) – displays:
 - Total quantity sold, calculated as the sum of all trades for a given contract where the participant acts on the sales side in MW.
 - 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 MW.

Confidential

- 7 Graph – used for displaying progress of the prices and traded quantities of the selected contract in time
 - Points curve – price progression
 - Columns – quantity progression
- 8 Timeframe – time span of graph, 2D (2 days), 1D (1 day), 4H (4 hours), 1H (1 hour), 15M (15 minutes)
- 9 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 (MW) - The quantity of the created trade in MW
 - Realized – Time stamp of trade creation
 - OwnQty – The cumulative **own** quantity at a time point in MW – 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 MW.

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

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.

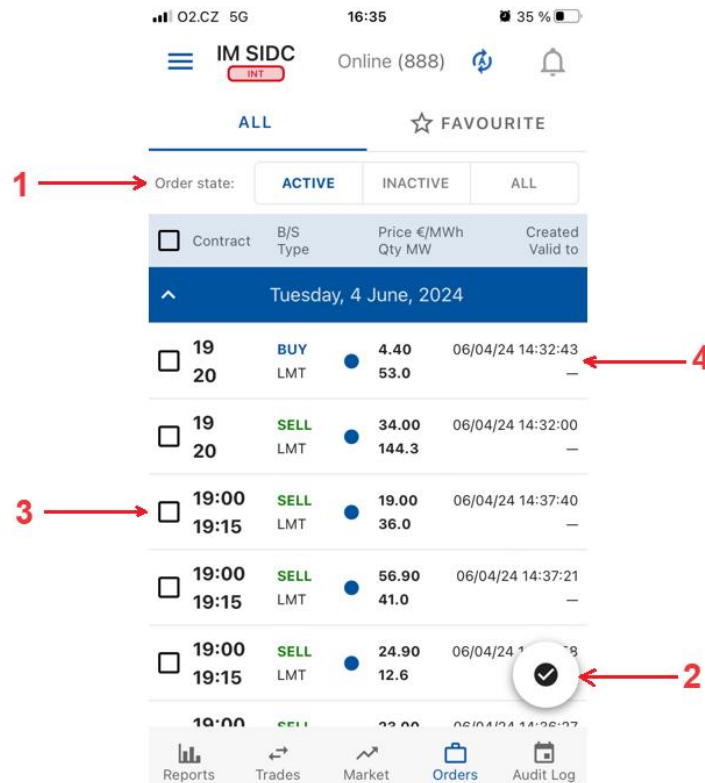


Fig. 39 – Orders screen

- 1 Filters orders according to whether they are active/inactive or both
- 2 Floating action button
- 3 Selection of order/orders for their activation/deactivation/delete -> after selection, the confirmation buttons for these operations are displayed
- 4 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 and Iceberg modification allows the user for changing only following attributes:

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

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

Block 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.

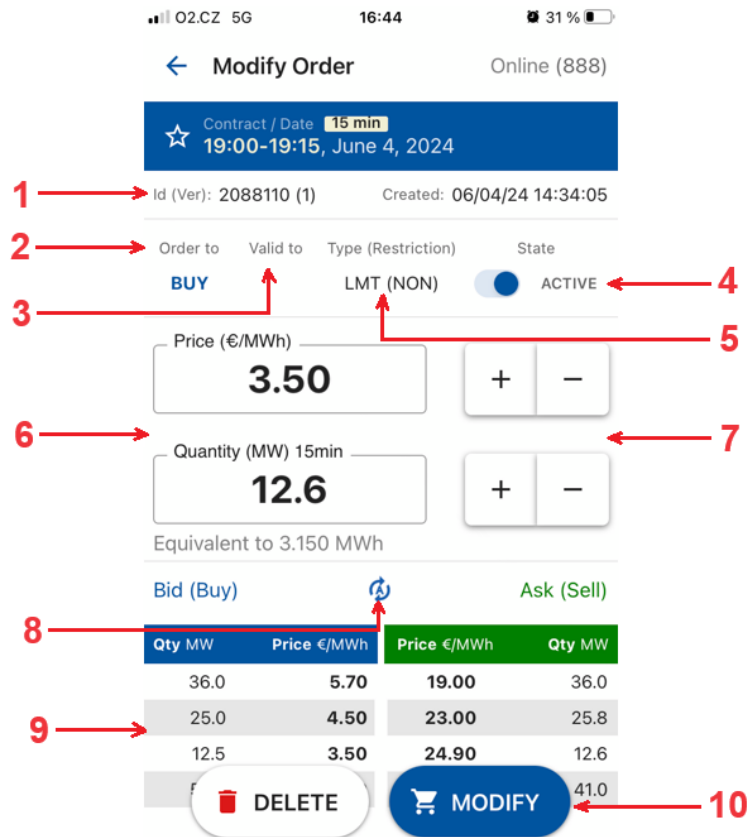


Fig. 40 – Modify Order screen

- 1 The identification number, version, date and time of the created order that the user wants to modify
- 2 Order to – information about the order direction (Buy / Sell)
- 3 Valid to – time period of order validity for trading (time restriction)
- 4 State – switch button for setting the active / inactive order
- 5 Type Restriction – type of order and its restriction (LMT (NON) / ICB (NON) / BLM (AON))
- 6 Quantity / price setting field using the keypad
- 7 Quantity / price setting buttons
- 8 Update content of the best orders table (Automatic or Manual)
- 9 View of a maximum five best orders to buy and sell
- 10 Buttons for delete order or its modification

Confidential

2024 OTE, a.s.

Date of revision:
5.6.2024

Document name:
IM Power Mobile Application manual

1.10 Audit log screen

Informs user of the following events for the currently active market:

- 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
- Change of market settings
- Acceptance/cancelation of VIP news

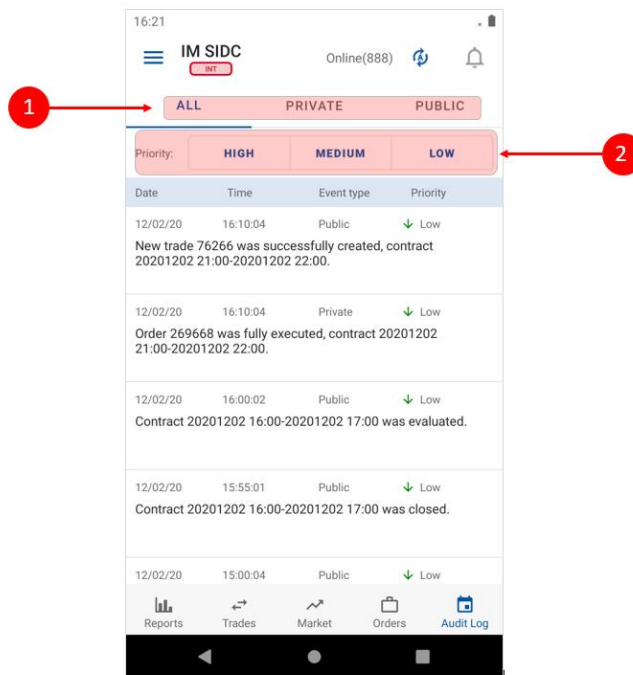


Fig. 41 – Screen Audit log

- 1 Filter by message type – ALL/PRIVATE/PUBLIC
- 2 Filter by message priority – HIGH, MEDIUM, LOW

1.11 Changes when Backup IM is active

When the local Backup IM is active, the change in the header and color coding of contracts will be reflected in all top-level screens. The report screen is not affected by market switching, as it always contains information from both markets. Only records related to the Backup IM are displayed on the event screen.

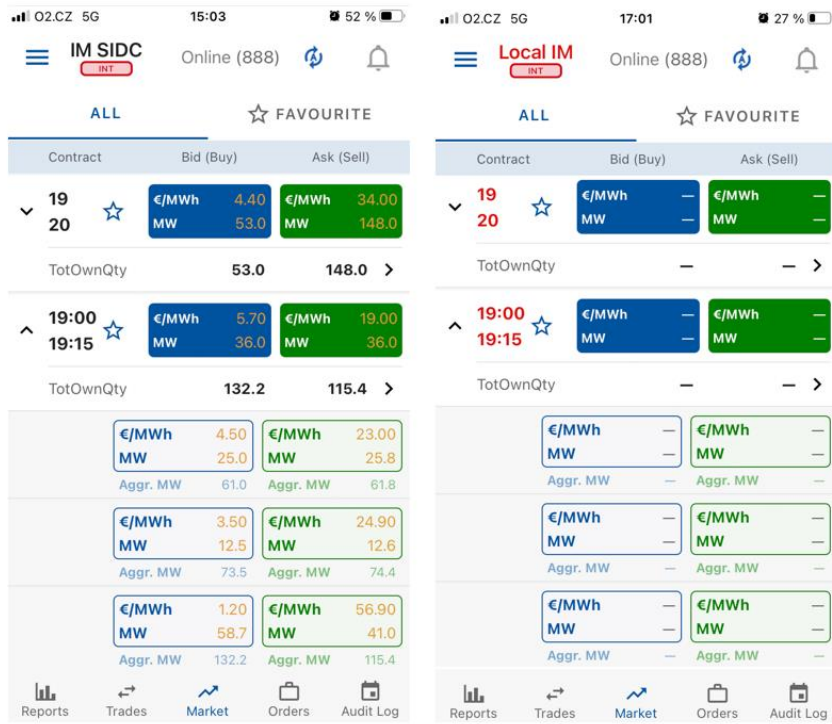


Fig. 42 – Difference between SIDC and local Backup IM