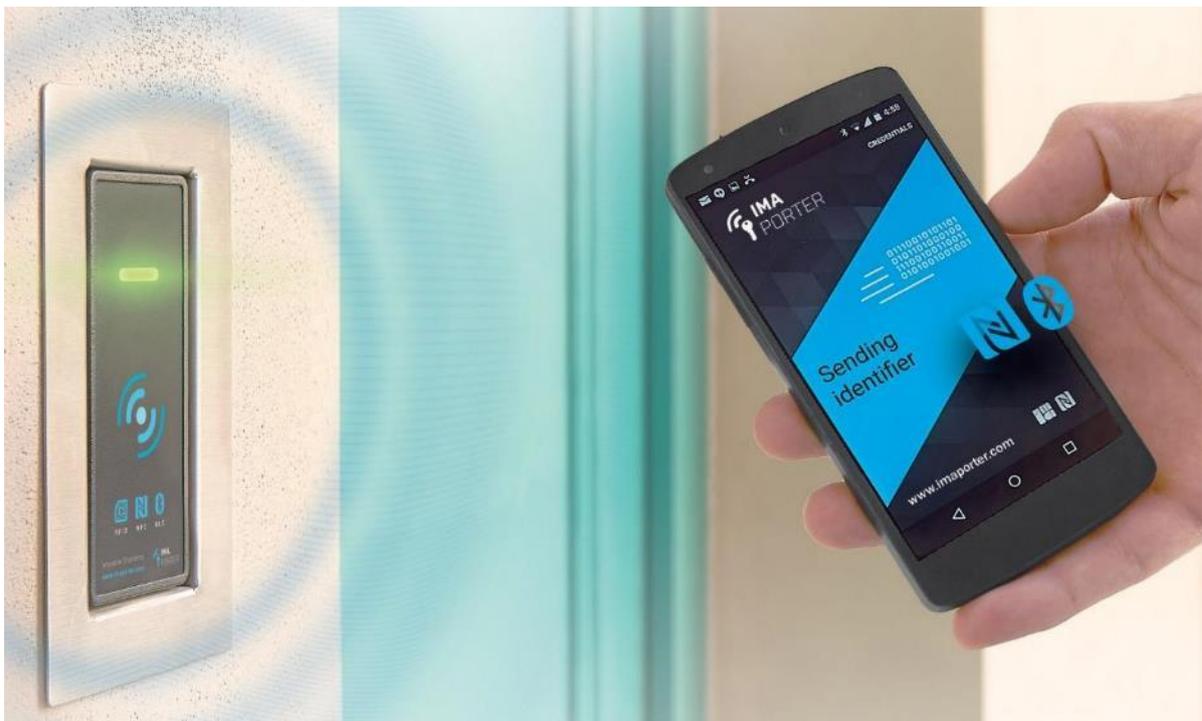


IMAporter Mobile Key

Mobile Key app for IMAporter MobileAccess Readers
with NFC and BLE communication
Android and iOS version



User manual

DOCUMENT HISTORY

Revision	Date	Author	Description
v0.1	7. 8. 2015	Karel Kalivoda	First draft of document
v1.0	15. 2. 2016	Karel Kalivoda	Final version for Android
v1.1	11. 4. 2018	Karel Kalivoda	Added manual for iOS
v1.2	12. 12. 2018	Karel Kalivoda	Added reader download from IDcloud

TABLE OF CONTENTS

1	Introduction to Mobile Key functions	3
1.1	Receiving the Mobile Key from the IDcloud.....	3
2	Mobile Key app for Android	5
2.1	Enrolment of a Mobile Key using an activation code.....	6
2.2	Adding the Mobile Key manually	8
2.3	Identification via NFC	10
2.4	Identification via Bluetooth 4.0+.....	11
2.5	Pairing Bluetooth readers and simplified identification settings.....	12
2.5.1	Admin pairing (IDcloud)	13
2.5.2	Manual pairing (by user)	14
3	Mobile Key app for iOS.....	16
3.1	Enrolment of a Mobile Key using an activation code.....	17
3.2	Adding the Mobile Key manually	20
3.3	Identification via Bluetooth 4.0+.....	22
3.4	Pairing Bluetooth readers and simplified identification settings.....	23
3.4.1	Admin pairing (IDcloud)	24
3.4.2	Manual pairing (by user)	25
4	Troubleshooting and error messages	26
4.1	Simplified identification malfunctions on Android	26
4.2	Reader not responding / blinking red LED	27
4.3	App deleted all my data	28
4.4	Unknown System ID	28
4.5	Unknown System Key.....	29
5	Necessary app permissions and why we need them	30
6	Downloading the app (Android and iOS)	31

1 Introduction to Mobile Key functions

IMAporter Mobile Key is a user app enabling communication between the mobile device and MobileAccess reader to identify the user.

The app is available for **Android** and **iOS** mobile platforms. Please find download links for both platforms on the last page of this guide.

Mobile Key app enables these types of identification:

- NFC light up the display and tap the reader with your mobile device (app running in the background; device can stay locked) – **Android only**
- BLE (inside the app) the most secure option; necessary to open the app and choose an available door/reader – **Android and iOS**
- BLE (notification bar) click on the **Open door** button on the notification bar / widget; the mobile device scans for 5 seconds and then establishes communication with a known reader in range – **Android, widget for iOS to be ready in Q2/2019**
- BLE (automatic) automatic identification based on just lighting up the display; the same process as with the notification bar / widget – **Android only**

After installing the app, it is necessary to introduce the mobile key. This key can be either downloaded automatically from the IMAporter IDcloud or it can be added manually (*described in chapter 2.2 Adding the Mobile Key manually (Android) or 3.2 Adding the Mobile Key manually (iOS)*).

Loading it automatically from the IDcloud is the more comfortable option.

The procedures for each operating system differ a bit and are fully described in the respective chapters of this manual:

- [2. Mobile Key app for Android](#) page 5
- [3. Mobile Key app for iOS](#) page 16

1.1 Receiving the Mobile Key from the IDcloud

In larger systems such as company premises and apartment buildings, the Mobile Key is often created by the system admin and sent to users using **e-mail / SMS / QR code**.

The user receives a message (either email or SMS) with an *activation code, link* for downloading the Mobile Key app (with automatic platform recognition) and *simple description*.

Enrolment of a prepared key is very intuitive, and the app will guide the user through the process. The procedure is fully described in the respective chapters of this manual:

- Android: [2.1 Enrolment of a Mobile Key using an activation code \(page 6\)](#)
- iOS: [3.1 Enrolment of a Mobile Key using an activation code \(page 17\)](#)

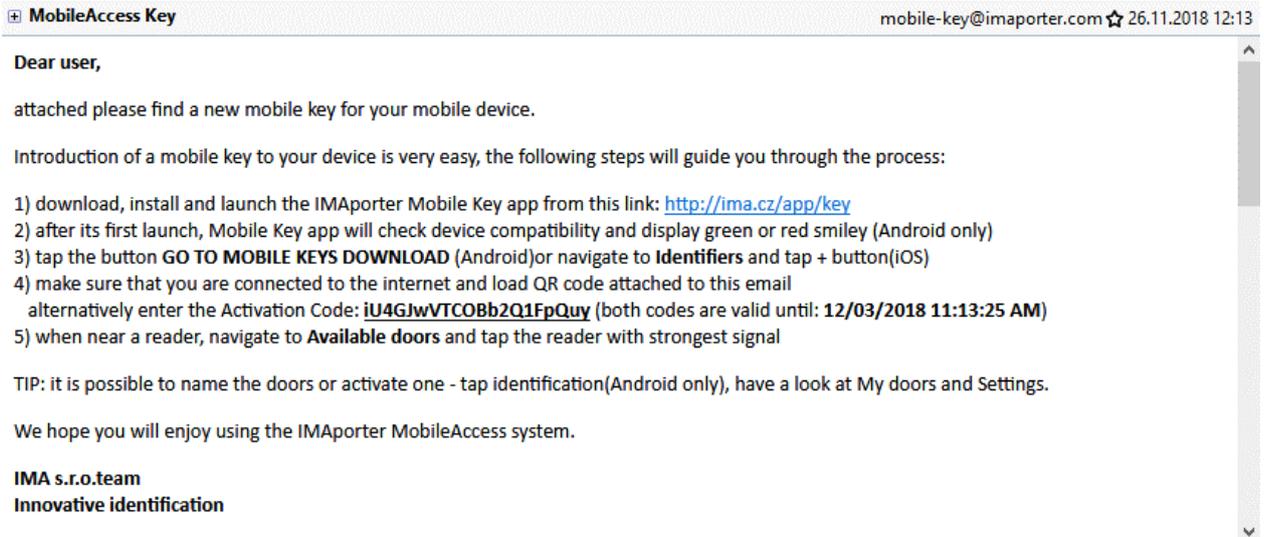


Figure 1 - Email informing user about a prepared Mobile Key and its activation code



Figure 2 - Activation code in form of a QR code for easy scanning

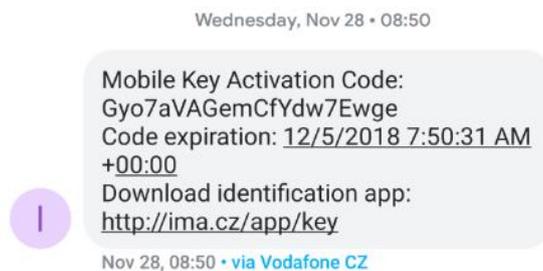


Figure 3 - Text message (SMS) informing user about a prepared Mobile Key and its activation code

2 Mobile Key app for Android

After the first start of the app, you will see a start-up screen informing you of device compatibility with the individual technologies (NFC/BLE).

Compatibility is represented by a green or red emoticon and text description.

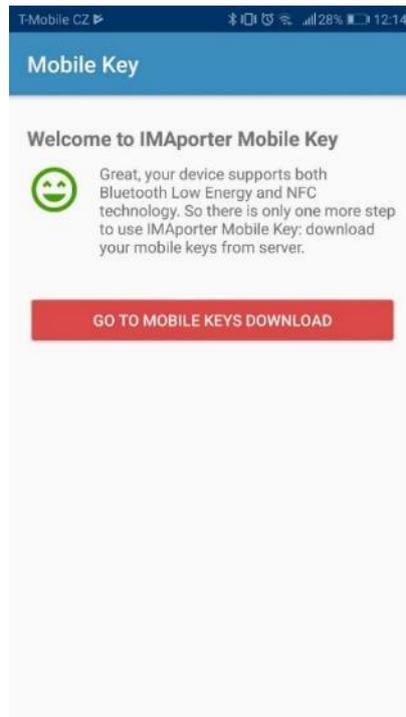


Figure 4 - start-up screen with compatibility info

If the device is compatible with at least one of the identification technologies, you may continue with the button **GO TO MOBILE KEYS DOWNLOAD**

2.1 Enrolment of a Mobile Key using an activation code

If you have received an **email** or **SMS** notification about a prepared Mobile Key as described in [chapter 1.1 Receiving the Mobile Key from the IDcloud \(page 3\)](#), you may navigate to **Mobile Key download**.

Newly installed app

Users with newly installed app are automatically redirected to the **Mobile Key download screen** ([Figure 7 - Mobile key download screen](#)) by tapping the **GO TO MOBILE KEYS DOWNLOAD** button on the start-up screen.

Users adding another key

Users who are already using the **Mobile Key app** for some time or are adding another Mobile Key must navigate to the **My Keys** tab in the app menu ([Figure 5 - My keys menu](#)) and tap the **red + icon** ([Figure 6 - My keys tab with red + icon](#)).

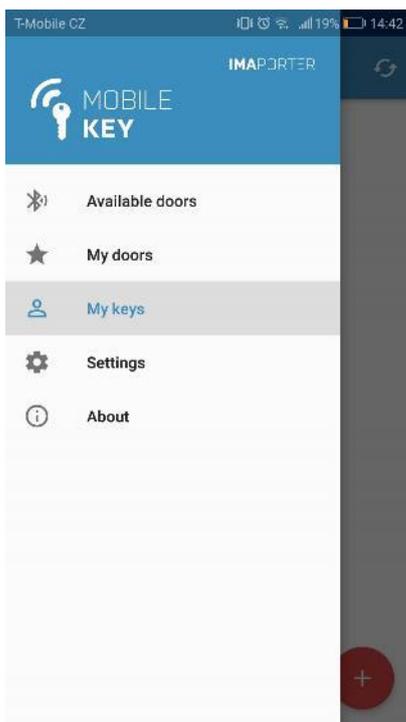


Figure 5 - My keys menu

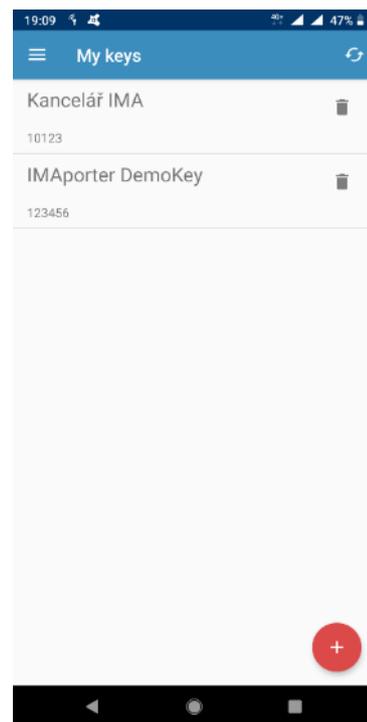


Figure 6 - My keys tab with red + icon

When on the Mobile keys download screen, the app allows user to enter the Mobile Key activation code in one of the following ways:

- 1) Enter it manually (or copy/paste) to **Activation code** field
- 2) Scan QR code using camera
- 3) Load activation code from text message (SMS)

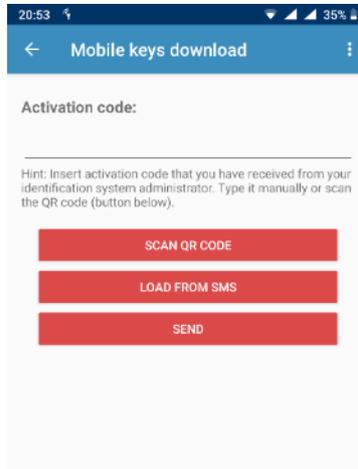


Figure 7 - Mobile key download screen

After entering the activation code, scanning the QR code or loading it from SMS, the new Mobile Key will be downloaded automatically.

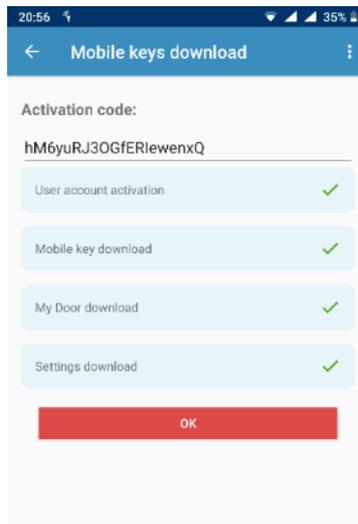


Figure 8 - After a Mobile Key has been successfully downloaded, all ticks display green

Note: Both the activation code and the attached QR code are time-restricted and available for one use only. Please express caution during the process of registration. When a code expires or in case of an error, the system admin needs to create a new Mobile Key.

2.2 Adding the Mobile Key manually

To add the Mobile Key manually, it is essential to enter a unique **User ID** into the system (e.g.: using the IMAporter Mobile Admin app or PC Admin SW) together with the following records that should be provided by the system admin:

- **System ID**
- **System Key**

To add the Mobile Key manually, navigate to **New mobile key** screen.

Newly installed app

Users with newly installed app are automatically redirected to the **Mobile Key download screen** by tapping the **GO TO MOBILE KEYS DOWNLOAD** button on the start-up screen. There, they must tap menu in top right corner and select **Add manually** (Figure 11 - From the top right menu (three dots) select Add manually)

Users adding another key

Users who are already using the **Mobile Key app** for some time or are adding another Mobile Key must navigate to the **My Keys** tab in the app menu (Figure 9 - My keys menu) and tap the **red + icon** (Figure 10 - My keys tab with red + icon) and on the following screen tap the top right corner menu and select **Add manually** (Figure 11 - From the top right menu (three dots) select Add manually).

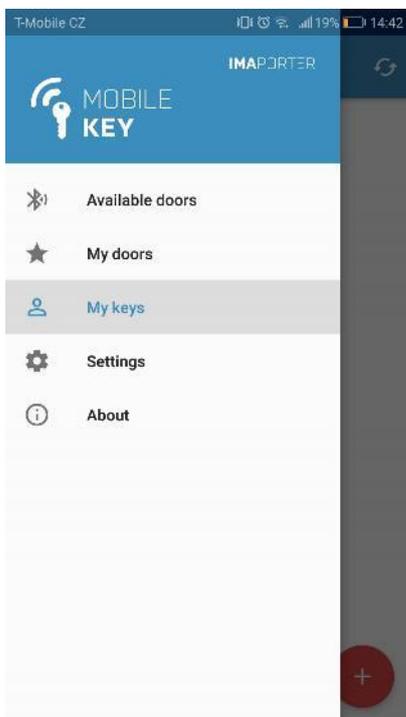


Figure 9 - My keys menu

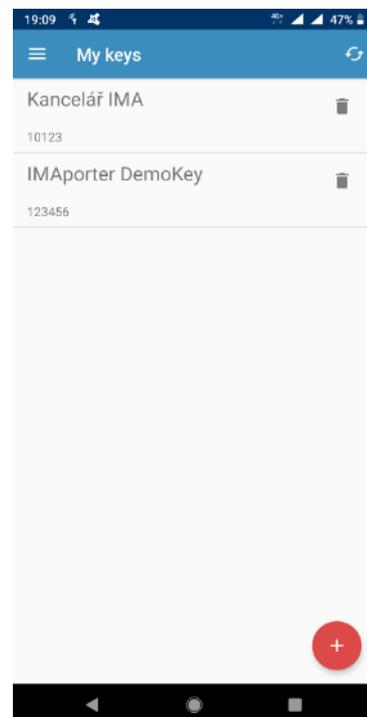


Figure 10 - My keys tab with red + icon

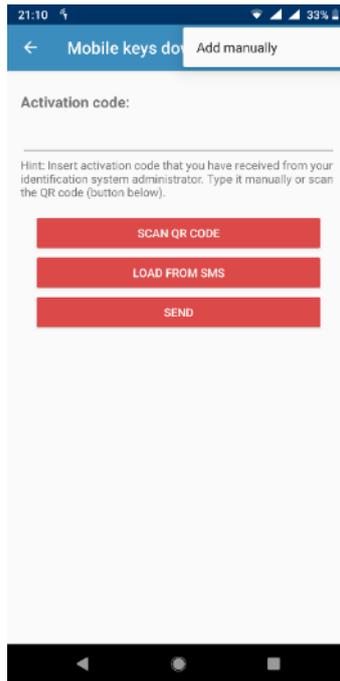


Figure 11 - From the top right menu (three dots) select Add manually

On the following screen a New mobile key form is shown.



Figure 12 - New mobile key form with entered demo data

- **Mobile key name** = “Office” (or any description)
- **System ID** = “SystemID” (identification of the ACS configured using the ACS Config app by the admin)
- **System Key** = “Secret password” (encryption key configured using the ACS Config app)
- **User ID** = “123456” (max. 8-character long unique ID number of the user, based on which the user is recognized in the ACS)
- **User PIN** = “1234” (optional figure designed for higher level of security, can be enabled by a configuration card or using the ACS Config app)

2.3 Identification via NFC

Once the Mobile Keys are downloaded, it is possible to test the identification.

Android mobile devices equipped with NFC technology enable easy identification just by tapping the reader with the device.

Make sure that NFC is switched on, light up the display and tap the reader with your mobile device.

For identification using the NFC, only lighting up the display is needed. Your device can stay locked and no clicking on the app is necessary.

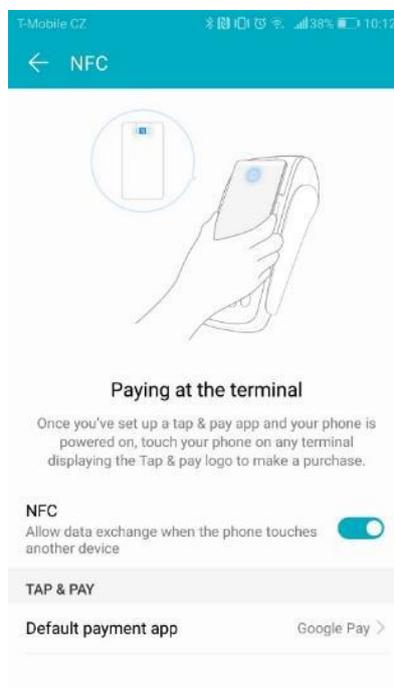


Figure 13 - Make sure that NFC on your device is switched ON

Note: For a flawless and quick identification, it helps if you know the location of the NFC antenna in your device. Most models have differently placed antenna with different signal strength, so it takes a few tries to find to ideal spot. For most devices, is the antenna located on the back side or around the camera lens.

2.4 Identification via Bluetooth 4.0+

Note: This section applies only to systems with RSW.04-B or RSW.04-PB (BLE-based) readers

To test the Bluetooth identification function, click on the **Available doors** in the app menu. The app scans available readers for ID and signal strength. Higher the signal strength, the closer the reader usually is.

By clicking on the reader, the Mobile Key is sent. A communication window will be displayed for about 1 second. Following the communication, the reader will beep and indicate either a green or red LED depending on the user's access rights set in the ACS.



Figure 14 - List of available readers in range

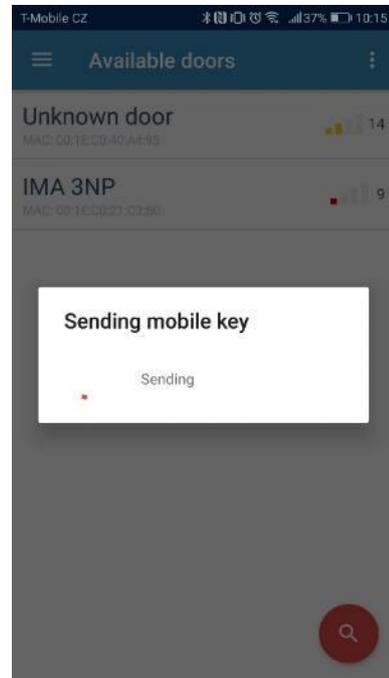


Figure 15 - Communication with a reader

2.5 Pairing Bluetooth readers and simplified identification settings

In order to use simplified identification for Bluetooth readers (such as identification by lighting up the display or from notification bar) or to recognize them by names, the readers must be paired in advance.

The IMAporter MobileAccess system allows two options how to pair a Bluetooth reader:

- Admin pairing (IDcloud)
- Manual pairing (by user)

In the following chapters, we will describe the differences and procedures to assign or update reader settings.

To pair new readers or alter the settings of the existing ones, navigate to the **My doors** tab in the app menu.

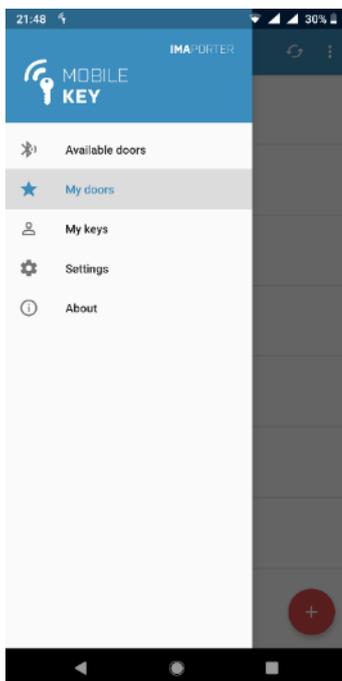


Figure 16 - Select My doors from menu

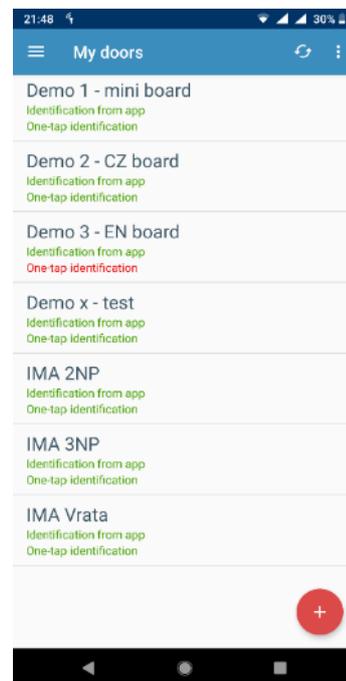


Figure 17 - List of already paired readers

2.5.1 Admin pairing (IDcloud)

This option is automatically available to users enrolling Mobile Keys from the IDcloud. System admin can prepare a list of readers in the IDcloud management platform and assign them with names and settings.

After user downloads a Mobile Key from IDcloud, this list is automatically downloaded with it.

Readers paired by the admin have special features:

- They are **automatically downloaded** from the server when downloading Mobile Key
- In case of a change, they **get automatically updated**
- **No need to pair** the readers manually
- Readers downloaded from IDcloud **cannot be deleted** or renamed by the user
- Settings of such readers can be **adapted only in the range allowed** by the admin as can be seen on the below screenshots.

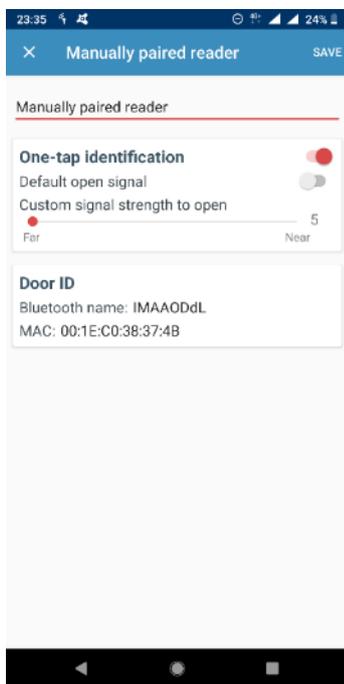


Figure 18 - Manually paired reader - user can change its name, identification settings and open signal strength or delete the reader

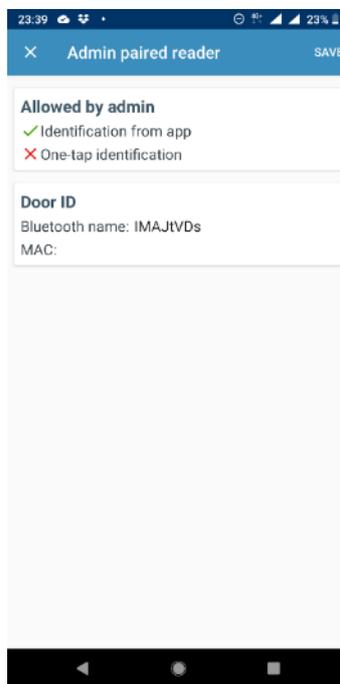


Figure 19 - Admin paired reader with disabled one-tap identification

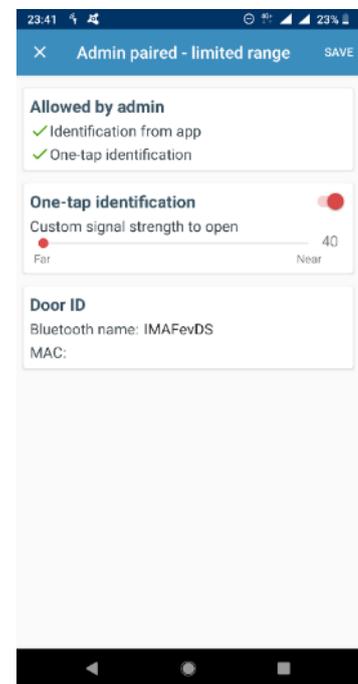


Figure 20 - Admin paired reader with allowed one-tap identification and limited range (signal 40-50, i.e. 1m-5cm range)

As shown on the screenshots above, the admin can restrict the features of the readers. Whereas standard signal range for simplified identification is from 5 (furthest away; approx. 10m) to 50 (closest to reader; approx. 5cm) as can be seen on [Figure 18](#), the admin can restrict that to for example only 40-50 ([Figure 20](#)) or even set an exact range or completely disable simplified identification for the specific reader ([Figure 19](#)).

If necessary (and allowed by the admin), the user can alter the reader settings in the predefined range or turn off some of the allowed features. It is therefore always possible to turn OFF simplified identification for readers which have this function allowed or limit its range.

2.5.2 Manual pairing (by user)

Users who are enrolling Mobile Keys manually or IDcloud users whose admin did not prepare a list of readers to be downloaded from IDcloud may need to pair the readers manually.

In order to do that navigate to **My doors** tab (*Figure 17 - List of already paired readers*) a tap the **red + button** to scan for available BLE readers (*Figure 21 - Readers in range available for pairing*).

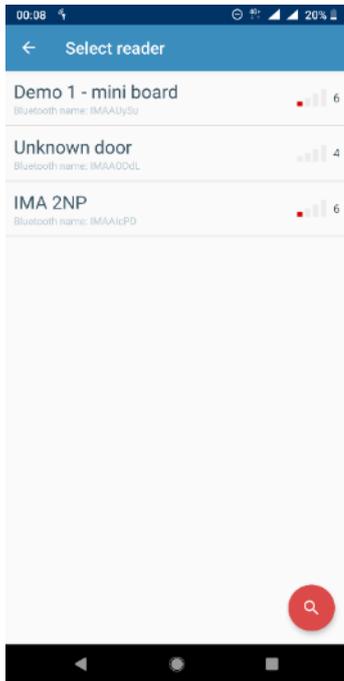


Figure 21 - Readers in range available for pairing

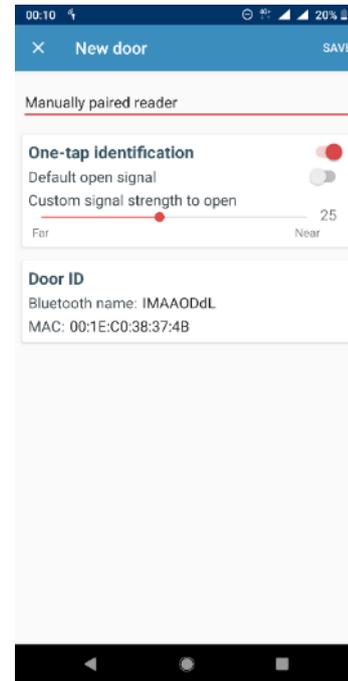


Figure 22 - Newly paired reader

Explanation of terms:

- Bluetooth name – unique identifier of the reader
- MAC address – alternative unique identifier of the reader
- Name = „Manually paired reader” (user defined name of the reader)
- One-tap identification – enables / disables simplified identification
- Default open signal – enables simplified identification using a global signal strength set in app settings
- Custom signal strength to open – enables setting reader-specific signal strength

Now proceed to the **Settings** tab to enable either **One-tap identification** (from the notification bar) or **Automatic identification** (by lighting up the display).

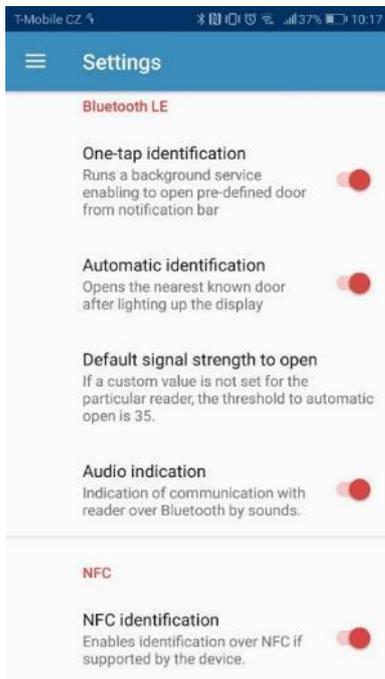


Figure 23 - Settings tab

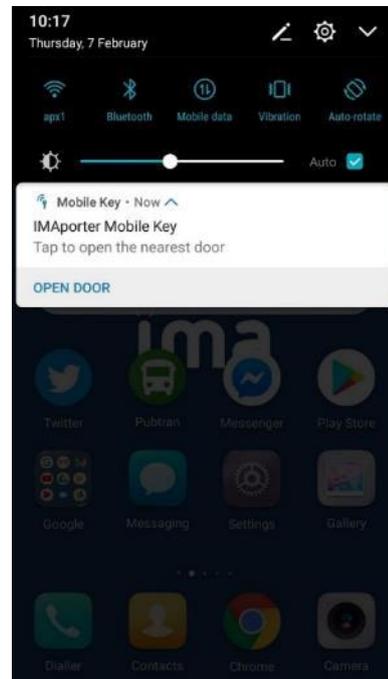


Figure 24 - Mobile Key service in notification bar

For the simplified Bluetooth identification from the notification bar or by lighting up the display, it is necessary to enable this feature both in the global application settings and in the configuration of each individual reader (through the **My Doors** tab).

For Admin paired readers, this setting may be enabled automatically.

After taping the **Open Door** button in the notification bar or after **lighting up the display**, the phone scans for available readers for approx. 5 seconds.

If, during this time, it finds a reader that is authorized to open and this reader indicates sufficient signal strength (depending on the custom signal strength setting on the **My Door** tab of each individual reader), communication is established and the reader unlocks after about 1 second.

3 Mobile Key app for iOS

After the first start of the app, you will be asked to allow IMAporter Mobile Key to send notifications. If not allowed, the app will not function properly and will not be able to receive Mobile Keys.

In the next step we kindly ask you to agree with our license agreement and privacy policy.

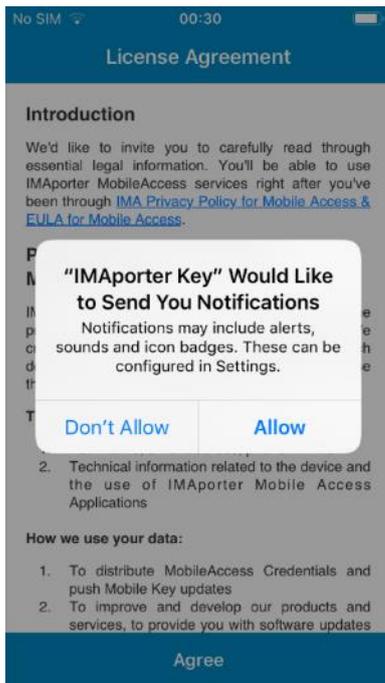


Figure 25 - Request to allow notifications in order to be able to receive a Mobile Key

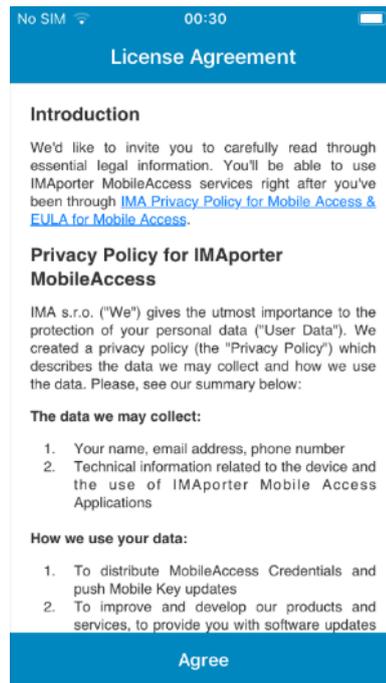


Figure 26 - License agreement

3.1 Enrolment of a Mobile Key using an activation code

If you have received an **email** or **SMS** notification about a prepared Mobile Key as described in [chapter 1.1 Receiving the Mobile Key from the IDcloud \(page 3\)](#), you may navigate to **Device registration**.

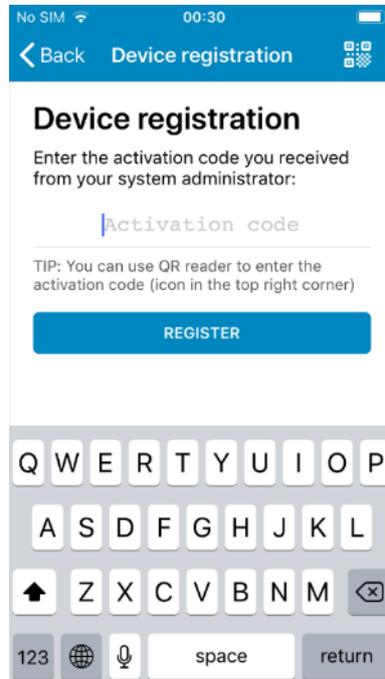


Figure 27 – Device registration screen

Newly installed app

Users with newly installed app are automatically redirected to the **Device registration screen** ([Figure 27 – Device registration screen](#)) after agreeing to the License and Privacy Policy Agreement ([Figure 26 - License agreement](#)).

Users adding another key

Users who are already using the **Mobile Key app** for some time or are adding another Mobile Key must navigate to the **My identifiers** tab in the app menu (*Figure 28 - My keys menu*) and tap the **+ icon** in the top right corner (*Figure 29 - My keys tab with red + icon*).

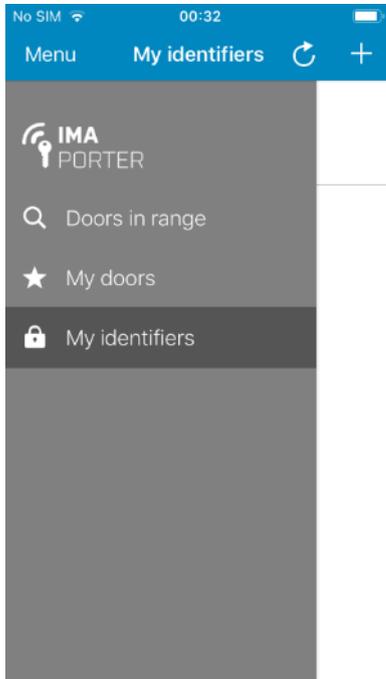


Figure 28 - My keys menu



Figure 29 - My keys tab with red + icon

A menu appears asking for the type of identifier to be added. Select **Synchronize with IDcloud**.

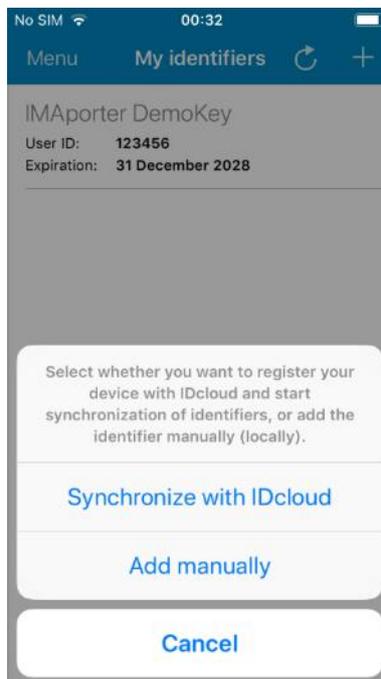


Figure 30 – From the menu select Synchronize with IDcloud

When on the **Device registration** screen, the app allows user to enter the Mobile Key activation code in one of the following ways:

- 1) Enter it manually (or copy/paste) to **Activation code** field
- 2) Scan QR code using camera

After entering the activation code or scanning the QR code, the new Mobile Key will be downloaded automatically.

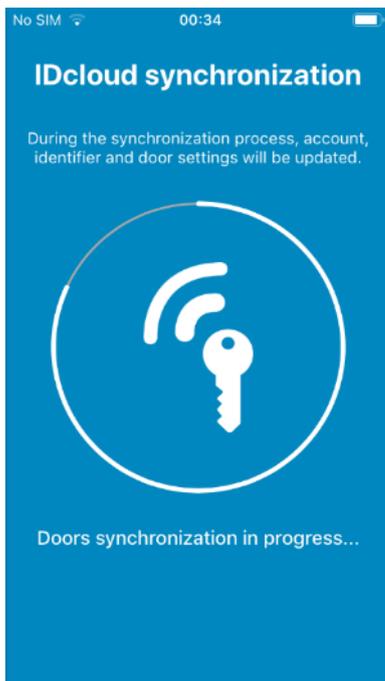


Figure 31 - After a Mobile Key has entered/scanned, data is being synced with the IDcloud

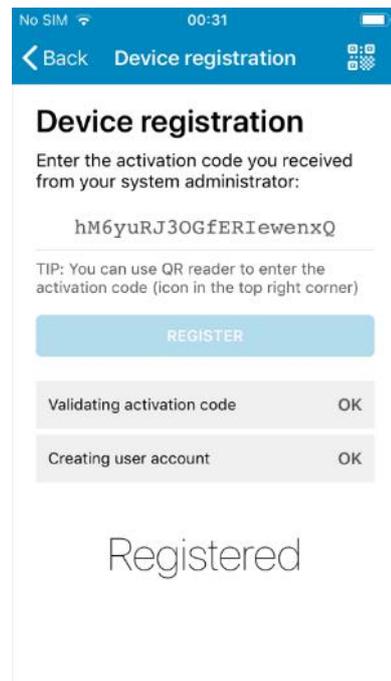


Figure 32 - Device successfully registered by entering the Mobile Key activation code

Note: Both the activation code and the attached QR code are time-restricted and available for one use only. Please express caution during the process of registration. When a code expires or in case of an error, the system admin needs to create a new Mobile Key.

3.2 Adding the Mobile Key manually

To add the Mobile Key manually, it is essential to enter a unique **User ID** into the system (g.g.: using the IMAporter Mobile Admin app or PC Admin SW) together with the following records that should be provided by the system admin:

- **System ID**
- **System Key**

To add the Mobile Key manually, navigate to **New mobile key** screen.

Newly installed app

Users with newly installed app are automatically redirected to the **Device registration screen** (*Figure 27 – Device registration screen*) after agreeing to the License and Privacy Policy Agreement (*Figure 26 - License agreement*).

Note: In order to add Mobile Key manually, they must tap the **Back** button and proceed according to the procedure for **Users adding another key**

Users adding another key

Users who are already using the **Mobile Key app** for some time or are adding another Mobile Key must navigate to the **My identifiers** tab in the app menu (*Figure 33 - My keys menu*) and tap the **+ icon** in the top right corner (*Figure 34 - My keys tab with red + icon*).

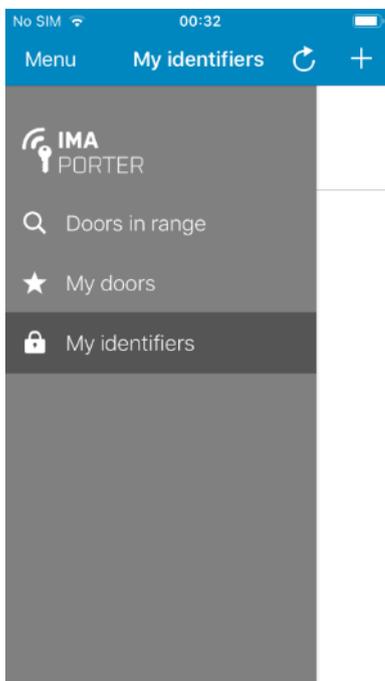


Figure 33 - My keys menu



Figure 34 - My keys tab with red + icon

A menu appears asking for the type of identifier to be added. Tap the **Add manually** button

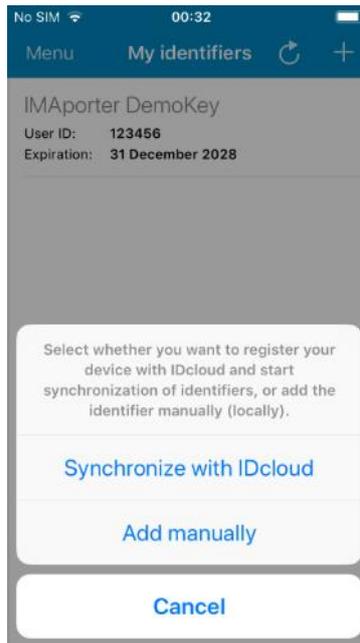


Figure 35 – From the menu dialog select Add manually

On the following screen a New mobile key form is shown.

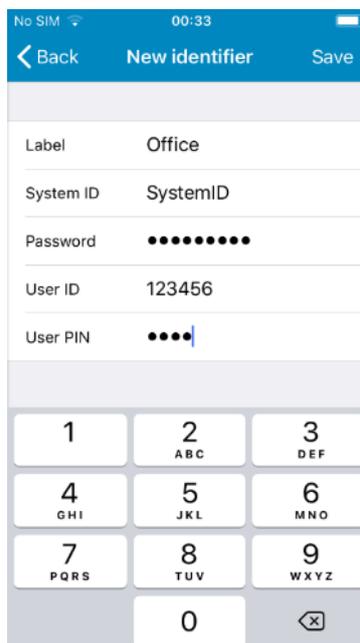


Figure 36 - New mobile key form with entered demo data

- **Label** = “Office” (or any description)
- **System ID** = “SystemID” (identification of the ACS configured using the ACS Config app by the admin)
- **Password (System Key)** = “Secret password” (encryption key configured using the ACS Config app)
- **User ID** = “123456” (max. 8-character long unique ID number of the user, based on which the user is recognized in the ACS)
- **User PIN** = “1234” (optional figure designed for higher level of security, can be enabled by a configuration card or using the ACS Config app)

3.3 Identification via Bluetooth 4.0+

Note: iOS devices support only identification using Bluetooth (NFC is not supported by Apple). To be able to use iOS device for identification, make sure that you are using RSW.04-B or RSW.04-PB (BLE-based) readers.

To test the Bluetooth identification function, click on the **Doors in range** in the app menu. The app scans available readers for ID and signal strength. Higher the signal strength, the closer the reader usually is.

By clicking on the reader, the Mobile Key is sent. A communication window will be displayed for about 1 second. Following the communication, the reader will beep and indicate either a green or red LED depending on the user's access rights set in the ACS.

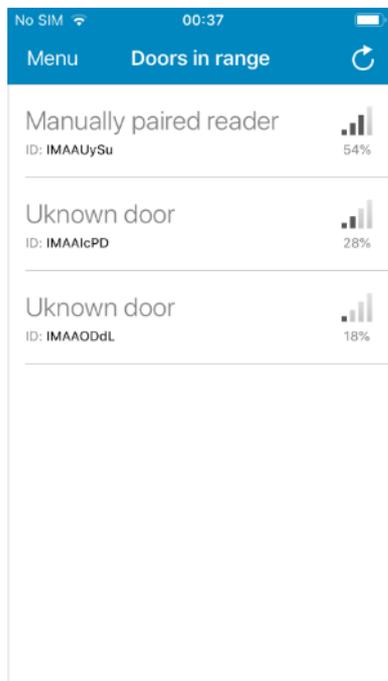


Figure 37 - List of available readers in range

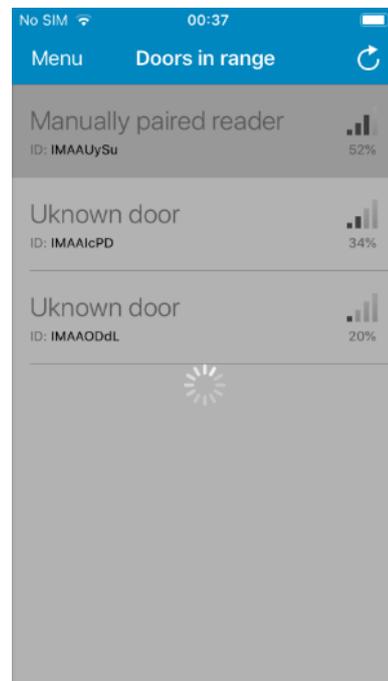


Figure 38 - Communication with a reader

3.4 Pairing Bluetooth readers and simplified identification settings

Note: this feature is available only in beta testing and will be opened in Q2/2019

In order to use simplified identification using a lock screen widget or to recognize them by names, the readers must be paired in advance.

The IMAporter MobileAccess system allows two options how to pair a Bluetooth reader:

- Admin pairing (IDcloud)
- Manual pairing (by user)

In the following chapters, we will describe the differences and procedures to assign or update reader settings.

To pair new readers or alter the settings of the existing ones, navigate to the **My doors** tab in the app menu.

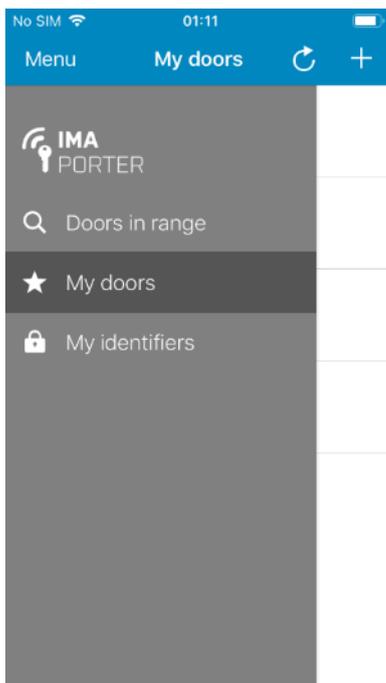


Figure 39 - Select My doors from menu

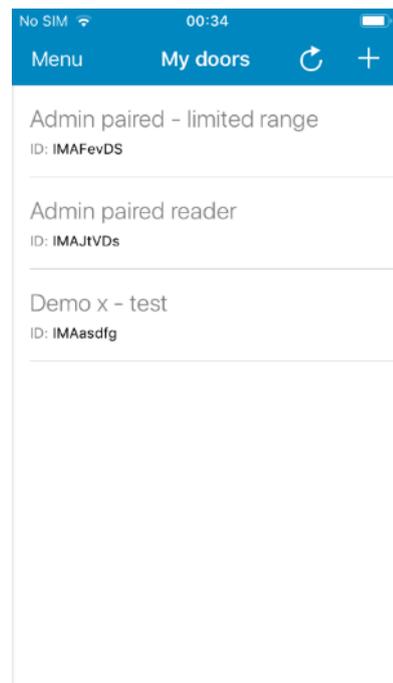


Figure 40 - List of already paired readers

3.4.1 Admin pairing (IDcloud)

This option is automatically available to users enrolling Mobile Keys from the IDcloud. System admin can prepare a list of readers in the IDcloud management platform and assign them with names and settings.

After user downloads a Mobile Key from IDcloud, this list is automatically downloaded with it.

Readers paired by the admin have special features:

- They are **automatically downloaded** from the server when downloading Mobile Key
- In case of a change, they **get automatically updated**
- **No need to pair** the readers manually
- Readers downloaded from IDcloud **cannot be deleted** or renamed by the user
- Settings of such readers can be **adapted only in the range allowed** by the admin as can be seen on the below screenshots.

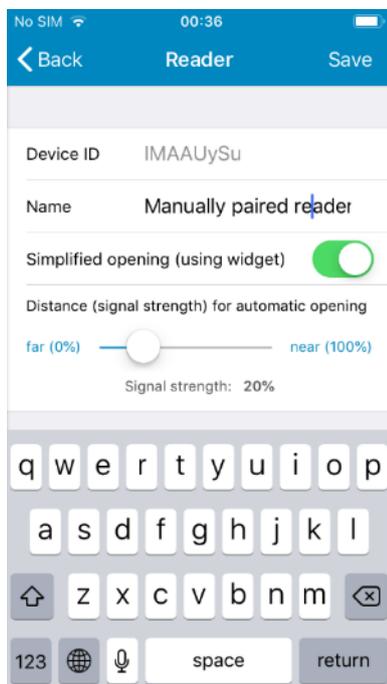


Figure 41 - Manually paired reader - user can change its name, identification settings and open signal strength or delete the reader

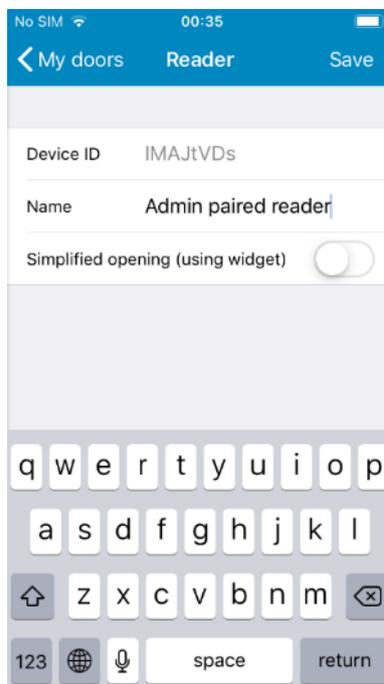


Figure 42 - Admin paired reader with disabled one-tap identification

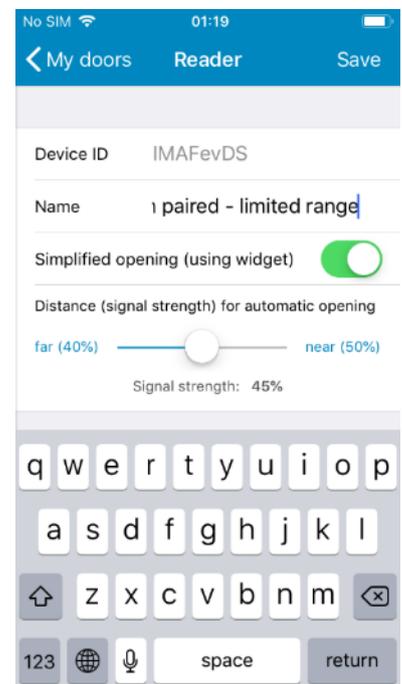


Figure 43 - Admin paired reader with allowed one-tap identification and limited range (signal 40-50, i.e. 1m-5cm range)

As shown on the screenshots above, the admin can restrict the features of the readers. Whereas standard signal range for simplified identification is from 5 (furthest away; approx. 10m) to 50 (closest to reader; approx. 5cm) as can be seen on [Figure 18](#), the admin can restrict that to for example only 40-50 ([Figure 20](#)) or even set an exact range or completely disable simplified identification for the specific reader ([Figure 19](#)).

If necessary (and allowed by the admin), the user can alter the reader settings in the predefined range or turn off some of the allowed features. It is therefore always possible to turn OFF simplified identification for readers which have this function allowed or limit its range.

3.4.2 Manual pairing (by user)

Users who are enrolling Mobile Keys manually or IDcloud users whose admin did not prepare a list of readers to be downloaded from IDcloud may need to pair the readers manually.

In order to do that navigate to **My doors** tab (*Figure 40 - List of already paired readers*) a tap the **+ button** in the top right corner to scan for available BLE readers (*Figure 44 - Readers in range available for pairing*).

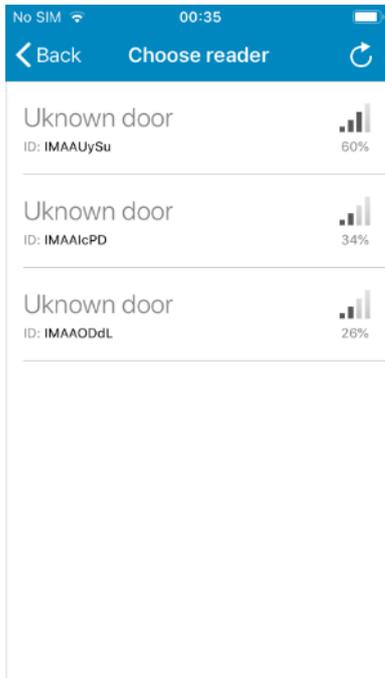


Figure 44 - Readers in range available for pairing

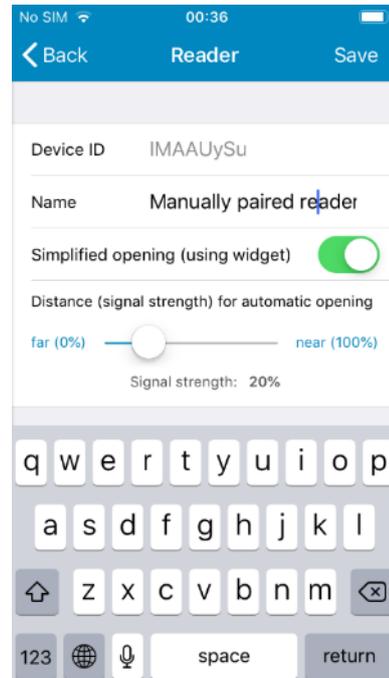


Figure 45 - Newly paired reader

Explanation of terms:

- Device ID – unique identifier of the reader
- UUID – alternative unique identifier of the reader
- Name = „Manually paired reader” (user defined name of the reader)
- Simplified opening – enables / disables simplified identification using iOS widget (not yet available)
- Distance (signal strength) for automatic opening – enables setting reader-specific signal strength

4 Troubleshooting and error messages

4.1 Simplified identification malfunctions on Android

Problem: One-tap and/or Automatic identification stops working after not using it for some time.

Solution: This is caused by energy saving algorithms on mobile phones. Some brands and models are more aggressive than others and each new version of Android tries to save more and more energy.

In order to provide the One-tap identification and Automatic identification functions, we need to have our IMAporter Mobile Key service up and running (is represented by key app in notification area). If this system does not run, the mentioned functions do not work.

If you are facing issues of this kind, you may need to go to the battery settings of your phone and switch off battery optimization for **IMAporter Mobile Key**:

- 1) Open Mobile Key app and tap Android switch app button (square), then hold the app icon to show the app options menu (*Figure 46 - App options menu in "switch app" view*). Note that it may be a bit different on each version of Android and phone brand.
- 2) Open battery settings from the app info settings screen (*Figure 47 - App info settings of a specific app*)
- 3) Navigate to Battery optimization settings (*Figure 48 - Battery usage settings of Mobile Key app*)
- 4) Open battery settings and select All apps (*Figure 50 - List of battery optimized apps*)
- 5) Find the Mobile Key app and select Don't optimize (*Figure 49 - Battery optimization options for specific app*)

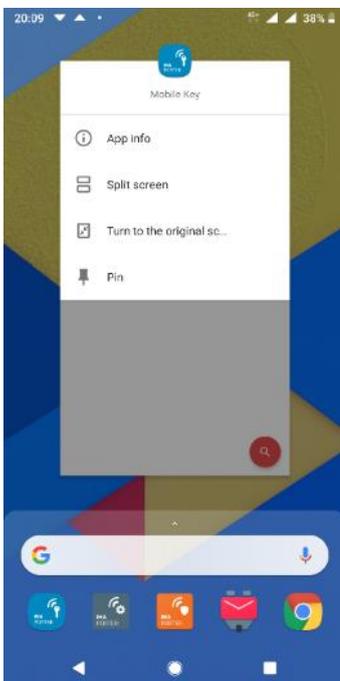


Figure 46 - App options menu in "switch app" view

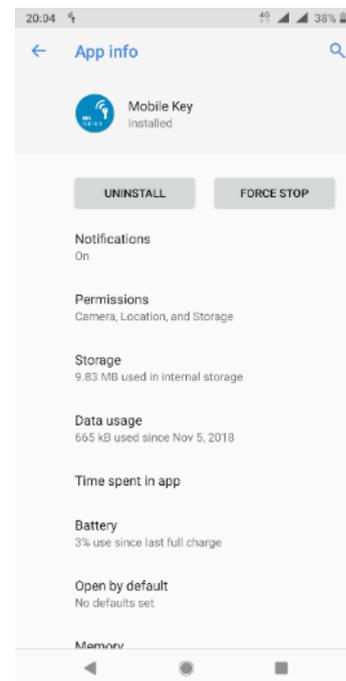


Figure 47 - App info settings of a specific app

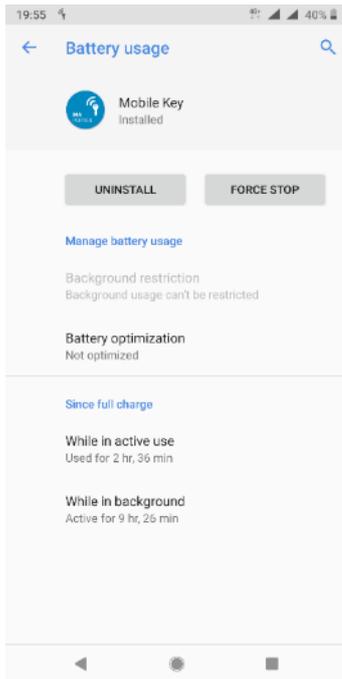


Figure 48 - Battery usage settings of Mobile Key app

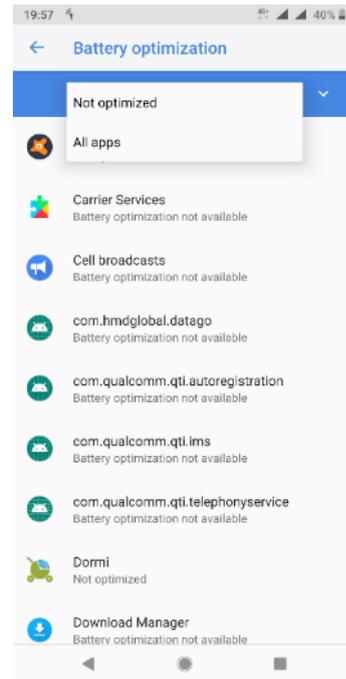


Figure 50 - List of battery optimized apps

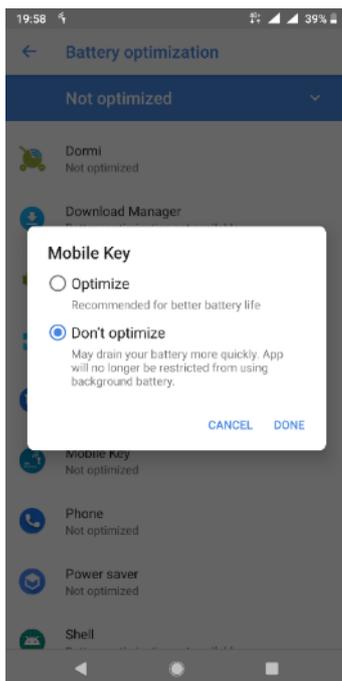


Figure 49 - Battery optimization options for specific app

4.2 Reader not responding / blinking red LED

Problem: The app indicates that the mobile key was successfully sent, but the reader does not respond / indicates red LED and does not unlock the door.

Solution: The user is not allowed to access the reader, his User ID is refused by the control unit. Most probably, because he does not have sufficient access rights.

4.3 App deleted all my data

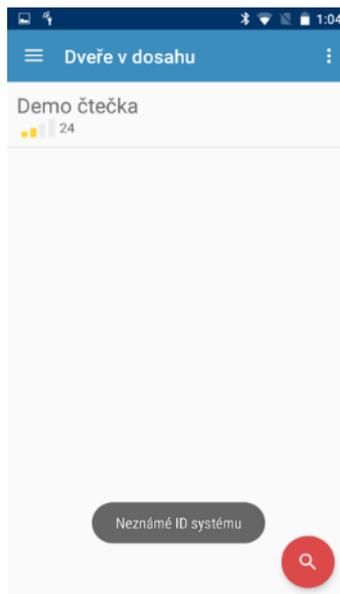
Problem: The app erased all my Mobile Keys and data and displays a screen informing me that my phone is not safe.

Solution: The IMAporter MobileAccess is by design a security system and as such, it must protect the secured property by every mean. We have therefore implemented number of security features to protect the integrity of all parts of the system. If the app erased all data, it has done so, because it evaluated your device as not being safe to operate the system. Please contact your admin or supplier in order to help you fix the issue.

4.4 Unknown System ID

Problem: While testing the BLE or NFC communication, the app indicates Unknown System ID message and the reader does not respond.

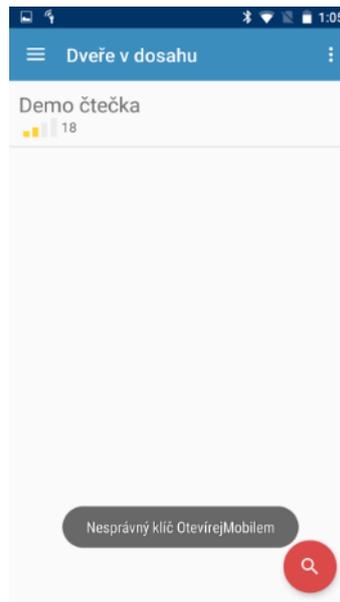
Solution: The Mobile Key is not authorized for this system. The reason may also be a typo in the System ID when manually adding the Mobile Key (or typo by admin when configuring the IDcloud).



4.5 Unknown System Key

Problem: While testing the BLE or NFC communication, the app indicates **Unknown System Key** message and the reader does not respond.

Solution: The Mobile Key is authorized for this system, but the System Key is wrong. The reason may be a typo in the System Key when manually adding the Mobile Key (or typo by admin when configuring the IDcloud).



5 Necessary app permissions and why we need them

The IMAporter Mobile Key app may ask the user for access to the following functions:

Camera

We need permission to use camera in order to be able to scan QR code.

Location

We need this permission in order to scan for Bluetooth readers in range. Without the permission to access Location, the device will not detect any readers.

Storage

We may need this permission if the user chooses to back up some of the apps settings to file.

Access internet

Internet access is necessary for us to be able to download your Mobile Keys from the IDcloud.

Access Bluetooth settings

Without access to Bluetooth settings and Bluetooth ON, identification using this technology would not work.

Access NFC settings

In order to use identification using NFC, we need to be able to check the state of NFC and write our identifier into the phones “inner NFC tag”.

Prevent phone from sleeping

This function is necessary for us to be able to provide simplified identification by lighting up the display and similar.

6 Downloading the app (Android and iOS)

Please scan desired QR code using your mobile device to download the IMAporter Mobile Key app.

Android



www.ima.cz/app/key/andro

iOS



www.ima.cz/app/key/ios