IMAporter Reader

Contactless card reader with MobileAccess function

RSW.04 reader with NFC support
RSW.04-B reader with NFC and Bluetooth LE support

Installation guide

Version: 1.4	Karel Kalivoda	Date: 1. 3. 2019

1 Table of contents

2 Product description

The IMAporter Reader is a white-label OEM reader with universal communication interface. It is designed for easy integration into third party identification solutions and widening their features with MobileAccess for Android and iOS devices.

Features

- universal smart solution for mobile identification
- supports RFID, NFC and BLE communication
- supports Android (v4.4+) and iOS (v7+) devices
- “on-tap” or “on-approach” identification
- white-label solution
- easy integration
- add-on ID management platform

The solution is based on the RSW.04 intelligent reader allowing user identification using a mobile device equipped with NFC or Bluetooth Low Energy (Bluetooth LE or BLE) technologies.
The reader supports identification media of ISO14443 standard (e.g.: MIFARE DESFire, MIFARE Classic, MIFARE Plus, PayPass etc.), communication with NFC devices in Peer-to-Peer, Reader / Writer and Card Emulation modes and communication with devices supporting Bluetooth LE.
The reader can be equipped with optional SAM module for advanced secure authentication. It also allows communication with NFC SIM cards of Mobile Network Operators. This function is not standard and requires additional configuration by the manufacturer.

Reader variants:

Order code	Features	Range	Identification	Platforms
RSW.04	RFID + NFC	up to 7 cm (2.8”)	on tap	Android
RSW.04-B	RFID + NFC + BLE	up to 10 m (33 ft.)	on approach	Android + iOS

3 Technical specification

3.1 Reader characteristics

Frequency: **NFC**: 13,56 MHz
BLE: 2,4 GHz

Standard: **NFC**: ISO / IEC 14443
BLE: IEEE 802.15.4

Identification Media: **NFC media ISO14443**: (Mifare 1k, DESFire EV1, Ultralight, NTAG20x, NTAG21x, PayPass, etc.)
NFC devices: Android 4.4+
BLE devices: Android 4.4+, iOS 7+

Identification distance: **NFC media ISO14443A**: up to 70 mm (2.8”)
NFC devices: up to 50 mm (2.0”)
BLE devices: 50 mm (2.0”) to 10 m (32.8 ft.)

Communication interface: Wiegand / RS232

Indication: LED (green/red), beep

Protection: tamper contact

Power supply / max. consumption: 12 – 15 VDC / 200 mA
IP Rating: IP 65
Housing: plastic (ABS)
Color: black with exchangeable front sticker
Temperature range: -25°C to +60°C (-13°F to 140°F)
Wiring: 2x power, 2x communication, 1-3x indication, 2x tamper contact
Cable: Pigtail, cable LiYCY 12x0, 14 mm^2, 3m
Cable Distance: **Wiegand:** 150 m (500 ft.), **RS232:** 30 m (100 ft.)

Reader dimensions:

	Height	**Width**	**Depth**
Standard housing	11,7 cm (4.6“)	5,0 cm (2.0”)	2,0 cm (0.8“)
Only PCB	8,5 cm - 10,5 cm (0.0”)	4,5 cm (0.0”)	1,1 cm (0.0”)

Antenna dimensions:

Height	**Width**
6,0 cm (2.36”)	4.5 cm (1.77”)

3.2 Configuration options

Reader configuration is carried out using a configuration card. Configuration steps are described in chapter *4. Configuration, reconfiguration and getting into operation*.

Communication interface: only Wiegand / only serial line RS232 / both (different wires)

Wiegand settings: 26bit* / 32bit / 56 bit / (other can be ordered)
Wiegand 26 is 24 bit + parity bit on the beginning and at the end
Wiegand 32 and 56 is without parity

** Wiegand 26bit is not suitable for systems reading UID from RFID cards as duplicated may occur (card UID required a longer Wiegand transfer).*

RS232 output:
Broadcast length: 32 bits / 64 bits
Baud rate: 9600 / 19200 / 15200 (8bits without parity)
Format: ASCII / HEX

Reading options: **standard** (number is broadcasted as read from card)
reverse (number is broadcasted in reverse order by bytes)

Reading signalization: **LED blinking**: on / off
Beeper: on / off

LED control: **two-wire** (green and red LED are controlled separately)
one-wire (green LED is controlled, red LED shines continuously)

Accepted ID media:
MIFARE Classic: UID / sector
MIFARE DESFire: UID / file
NFC media: UID
NFC device: PIN: yes / no
Bluetooth LE device: PIN: yes / no

3.3 Reader connection – wiring scheme

Signal	Color	Function
+12V	red	power supply
GND	black	power supply
Data0	green	Wiegand data
Data1	white	Wiegand data
LEDG	pink	green LED
LEDR	brown	red LED
BEEPER	blue	beeper
T1	purple	tamper contact
T2	grey	tamper contact
RxD2	red-blue	RS232 data
TxD2	grey-purple	RS232 data

Used pigtail cable is LiYCY 12 x 0.14. Cable shielding can be connected to GND terminal of the control unit power supply.
Length of the connection cable is 3 m. It can be extended up to 150 m (500 ft.) (if used with Wiegand protocol), using a shielded cable with corresponding wire thickness for +12V and GND (for 150 m minimum of 0,5 mm^2).

4 Configuration, reconfiguration and getting into operation

This chapter describes the procedure of reader configuration for cases when the reader has not yet been configured, is missing part of its configuration or needs to be reconfigured with new settings.

To erase current configuration or **change system settings of MobileAccess function**, it is necessary to proceed with factory reset of the reader according to chapter *4.1 Restoring factory settings (factory reset)*.

4.1 Restoring factory settings (factory reset)

Sometimes it is necessary to restore factory settings of a reader. Such circumstances may occur when we need to change system settings (system ID / Porter key) or after FW upgrade. Factory reset deletes all configuration and data stored in the reader.

Resetting IMAporter Reader (RSW.04 or RSW.04-B)

1. Power the reader OFF
2. Short **black, pink, brown** and blue wires (ground the signalization wires)
3. Power the reader ON
4. The reader will start blinking red LED in 1sec interval and will not accept any ID media or communicate with mobile devices, Bluetooth signal will not be visible
5. Disconnect the wires and reconnect to the control unit
6. Continue with reader configuration using a configuration card

NOTE: If the wires remain shortened, the reader will factory reset each time the power goes down!

4.2 Reconfiguration using a configuration card

A configuration card is used for setting the basic parameters of communication protocols, accepted identification media, indication options etc. according to chapter *3.2 Configuration options*.

4.2.1 Delivery and preparation of configuration cards

Configuration card with configuration agreed upon with the customer is usually supplied together with the IMAporter Reader. Configuration cards are prepared and supplied by the system manufacturer or authorized distributors.

4.2.2 Demo configuration cards for reader testing

For initial testing of the IMAporter Reader, it is possible to order a reader with a set of 3pcs DEMO Configuration Cards prepared with various communication protocols and 2pcs of identification cards for testing the correct system functions.

NOTE: DEMO configuration cards can be used only to configure readers ordered as a DEMO reader. These cards cannot be used with ordinary readers and at the same time a DEMO reader cannot be set using common configuration cards. For more information about reconfiguration of a DEMO reader, please contact the supplier or manufacturer.

Demo Configuration Cards:

- Wiegand 26bit + RS232
- Wiegand 32bit + RS232
- Wiegand 56bit + RS232

Demo Access Cards:

- MIFARE Classic 1k (UID reading)
- MIFARE DESFire (File: 0; No: 65534; Key: 12345678901234567890123456789012)

Mobile devices:

- Android 4.4+ NFC / BLE devices with IMAporter Mobile Key app installed (link on last page of this manual)
- iOS 7+ BLE devices with IMAporter Mobile Key app installed (link on last page of this manual)

All configuration cards are set to use the following settings:

- Wiegand output according to card description:
  - Wiegand 26: 1 bit parity, 24 data bit, 1 bit parity
  - Wiegand 32: without parity
  - Wiegand 56: without parity
- RS232 output:
  - Broadcast length: 32 bits
  - Baud rate: 9600, 8bits without parity
  - Format: ASCII
- Accepted ID media:
  - MIFARE Classic 1K - UID reading
  - MIFARE DESFire - File reading (according to specification above)
  - NFC media – UID reading
  - NFC devices - needs to be set using ***IMAporter Reader Config*** app
  - BLE devices (if supported by HW) - needs to be set using ***IMAporter Reader Config*** app

4.2.3 Reader configuration using a configuration card

Connect the reader to the control unit and power it up according to chapter *3.3 - Reader connection – wiring scheme*.

New or Factory reset reader

If you are configuring a new or a recently reset reader, it will start blinking red LED in 1sec interval. Apply a configuration card and hold it at the reader for 5sec. During configuration download, the reader shines green LED for about 3sec. After that it shortly blinks red LED. In case that identification using mobile devices (NFC or BLE) was not allowed, the reader switches to normal operating state in which it behaves according to the settings of the master control unit.

In case that NFC or BLE identification was allowed by the configuration card, the reader continues to blink red LED in 1sec interval and waits for setting up using the IMAporter Reader Config app (described in chapter *4.3 Setting up using IMAporter Reader Config*).

Reconfiguration of a working reader

To change configuration of an already configured and operated reader, factory reset is not necessary. To reload the reader with a different configuration, restart the power (switch the reader OFF and ON again) and apply a new configuration card in the first 10sec after start-up. Hold the card at the reader for 5sec.

During configuration download, the reader shines green LED for about 3sec. After that it shortly blinks red LED and switches to normal operating state in which it behaves according to the settings of the master control unit.
When reconfiguring a reader, the MobileAccess system settings do not get deleted and therefore cannot be changed. If you need to change these settings, it is necessary to reset the reader into factory settings and configure it again.

4.3 Setting up using IMAporter Reader Config

Setting up the reader identifiers is carried out using the **IMAporter Reader Config** for Android, which can be downloaded here:

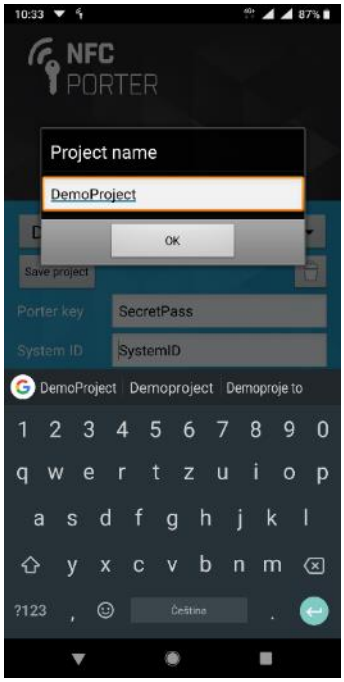
http://ima.cz/app/setup

Note: Setting up using the **IMAporter Reader Config** app is not required, if the MobileAccess (NFC, nor BLE) function was not allowed in the configuration card.

4.3.1 Configuration app IMAporter Reader Config

The configuration app **IMAporter Reader Config** is designed for initial setup of identification settings and communication encryption keys.

After starting the app, a screen is shown asking to input ***Porter key*** and ***System ID***.



Porter key (System Key):
This Key is a secret shared password authorizing the user device to communicate with the reader / set of readers and enciphering the communication between the reader and the mobile device.
The system admin is able to change the ***Key*** using the ***IMAporter Reader Config*** app at any time if needed. He must however make sure that all authorized users have the correct ***Key*** entered in the **IMAporter Mobile Key** apps, otherwise they would not be allowed to identify themselves at the reader.

The ***Key*** must not be disposed to third parties as it could result in lowering the system security level.

System ID:
Identifier used by the user identification app for distinguishing between individual systems. The **IMAporter Mobile Key** user identification app allows saving credential sets for multiple access systems used in different premises. These premises are recognized according to the ***System ID***.
A System is a specific set of readers, where the user is authorized to access using the his unique ***User ID*** and which are connected to the same identification system. The same ***System ID*** may therefore be used in the headquarters of a company and on all of its branches. In case of remote offices, the readers in each office can have a different ***System ID***.

All settings can be saved within the app as a project.

Setting up the reader:
By pressing the ***Setup reader*** button, a setup screen is launched. Now all that needs to be done is to tap the mobile device onto the red-blinking reader (a reader in factory setup, that loaded only with initial configuration using a configuration card).

After taping the reader with the mobile device, a short communication dialog appears on the display. If set correctly, the reader stops blinking red LED and begins to follow the behavior set in the ID system Control Unit.

4.3.2 Communication with ID system (control unit)

A set reader is ready to be put into operation. After this step has been finished, it is necessary to install and set the user identification app according to chapter *5. IMAporter Mobile Key identification* app.

The identification app requires entering the ***User ID*** together with the system settings described in the previous chapter. After the user's mobile device had been tapped at the reader, the reader validates the ***Key*** authentication key and decodes the ***User ID***. The ***User ID*** is sent to control unit in the preset format.

5 IMAporter Mobile Key identification app

IMAporter MobileKey is a user identification app designed to process communication between the mobile device and the IMAporter MobileAccess Reader in order to transfer user identification data.
The app is available for mobile devices running Android or iOS operating systems. Links for downloading the corresponding apps can be found on the last page of this manual.

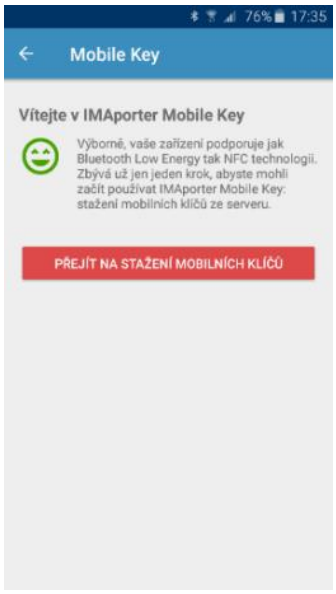
NOTE: This manual is a shortened version limited to the Android platform. The complete manual for Android and iOS apps including description of all system features and remote distribution of Mobile Keys is available for download from the product website.

The app allows the following identification options:

NFC	just light up the display and tap the reader (app is running in the background and the device can remain locked during user identification)
BLE (from app)	most secure identification option, to initiate the identification process it is necessary to run the app and select the available reader
BLE (notification area)	identification process is initiated by taping a button in the notification bar. The device scans for 5sec and when it detects a paired reader nearby, it starts communication.
BLE (fully automatic)	identification process is initiated by lighting up the display, the scanning and communication procedure is the same as in the previous step.

After installation of the IMAporter MobileKey app, it is necessary to configure the app for communication with the system. For this, the corresponding identifiers and authorization keys need to be set according to the following procedure.

When running the app for the first time, a screen informing about compatible technologies will be displayed.



For mobile access using the RSW.04 reader, it is necessary for the mobile device to support NFC; while for RSW.04-B readers, the mobile device can support either or both NFC and BLE.

If your mobile device supports the required identification technologies, click Go to Mobile Keys Download to continue. For applications already in use, go to My Keys in the application menu and press the red '+' button to add a new mobile key.

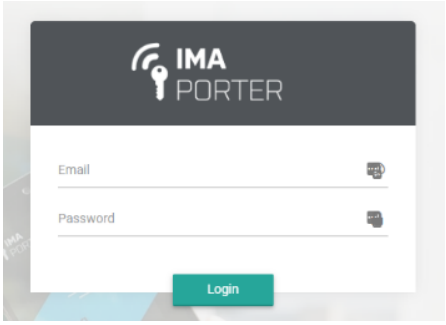
5.1 Adding the Mobile Key using IDcloud platform

IMAporter IDcloud is a web service designed for easy and secure remote key distribution.
Because of IDcloud utilization, there is no need to manually rewrite identifiers and keys to user phones, and the keys can be comfortably managed through an intuitive web interface.
The service will be appreciated by users and administrators of both private and public ACS with a higher number of users and increased demands on central management of all system components, as well as residential and family home administrators thanks to a user-friendly and intuitive UI.

The IDcloud system offers also advanced configuration options, including centralized reader settings and user identification. These advanced settings are described in the relevant IDcloud manual.

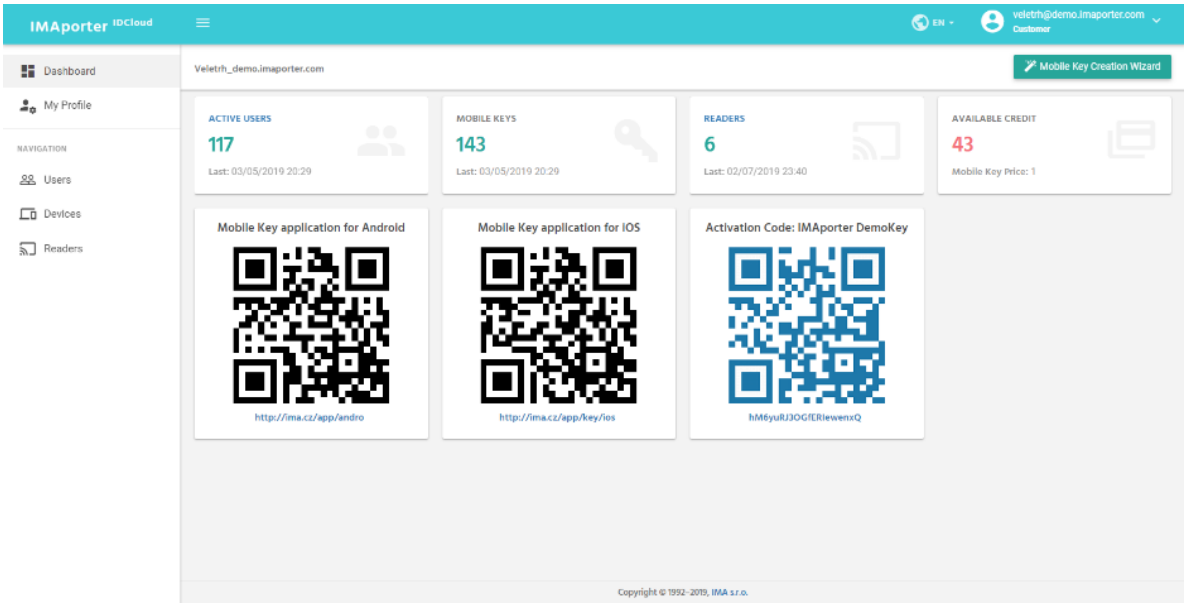
The operation of the IDcloud system is free of charge, only the newly created mobile keys are being charged.
Each new account is provided with five free demo credits for mobile keys creation and distribution. Additional credit can be purchased from the system vendor.

To create a new mobile key, go to http://my.imaporter.com and log in using the parameters described on the last page of this brochure:

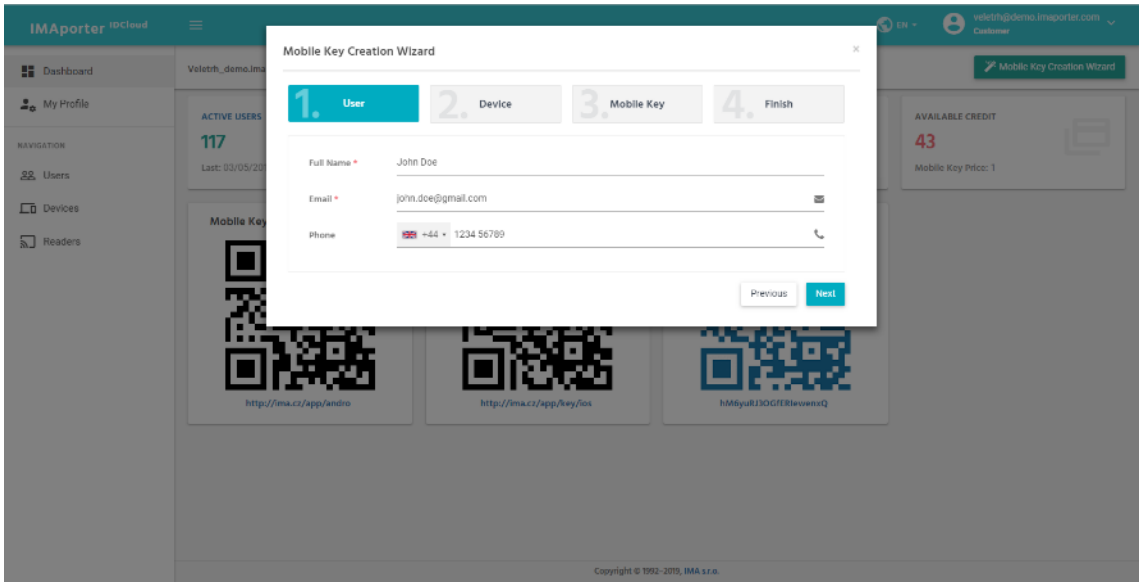


In case you have not received your IDcloud login parameters, contact your system vendor.

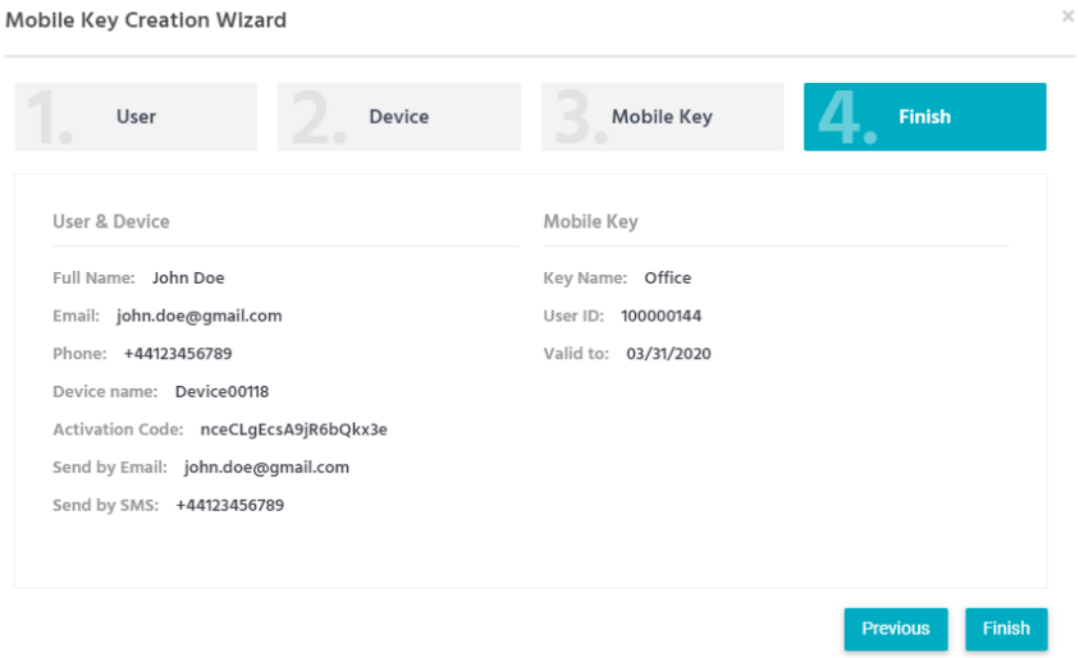
On the homepage you will find an overview of the issued mobile keys, active users and QR codes to download the IMAporter Mobile Key mobile app.



Launch an intuitive guide by clicking on the **Mobile Key Creation Wizard**.
You only need to enter a person's name/title/description and email or telephone contact to send the activation code. Everything else is done automatically - the system generates a unique ID and sends the mobile key to the user via email or SMS.
Alternatively, you can change the user ID to an ID of your choosing, set its validity, and other settings.



Once you have filled in the parameters, the system will show a recap. By clicking on **Finish**, the system will the activation code to the new user.



The new user will receive their mobile key via email, SMS or printed in the form of a QR code, depending on the chosen form of sending:

Dear user,

attached please find a new mobile key for your mobile device.

Introduction of a mobile key to your device is very easy, the following steps will guide you through the process:

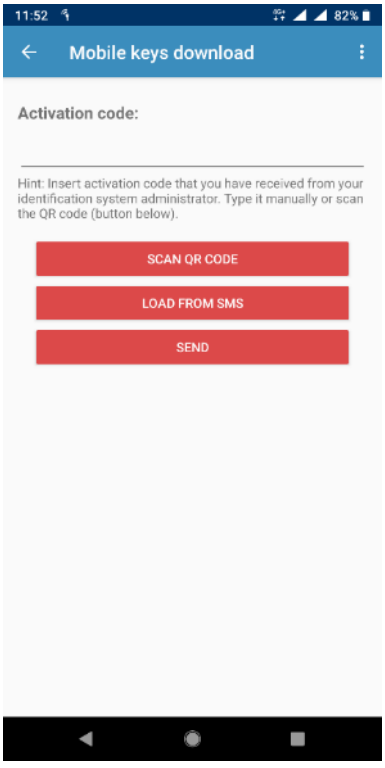
1) download, install and launch the IMAporter Mobile Key app from this link: http://ima.cz/app/key
2) after its first launch, Mobile Key app will check device compatibility and display green or red smiley (Android only)
3) tap the button **GO TO MOBILE KEYS DOWNLOAD** (Android)or navigate to **Identifiers** and tap + button(iOS)
4) make sure that you are connected to the internet and load QR code attached to this email
   alternatively enter the Activation Code: **X6yyFdQhbflETnUv0oPa** (both codes are valid until: **02/26/2019 11:55:53 PM**)
5) when near a reader, navigate to **Available doors** and tap the reader with strongest signal

TIP: it is possible to name the doors or activate one - tap identification(Android only), have a look at My doors and Settings.

We hope you will enjoy using the IMAporter MobileAccess system.

IMA s.r.o.team
Innovative identification

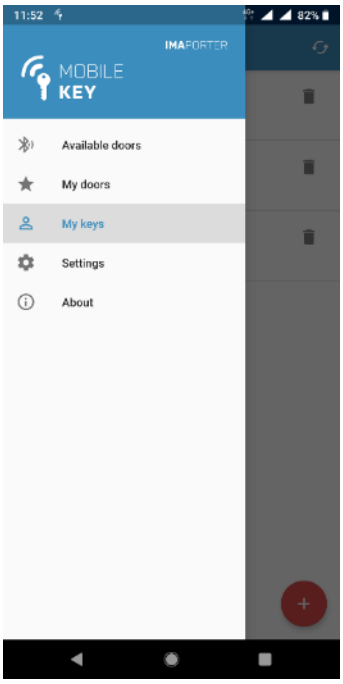
Now the user needs to only download the IMAporter Mobile Key app then on the **Mobile Keys Download** screen, enter or scan the received **activation code**. By sending the activation code, the system will authenticate the information from the server and automatically download chosen settings. Then the user can approach the reader and identify themselve.



NOTE: Each activation code can be used to activate only one mobile device.

5.2 Adding the Mobile Key manually

To input the Mobile Key manually using the in-app form, proceed according to the following instructions. On the ***Mobile Keys download*** screen tap the menu icon in the top right corner and select the ***Add manually*** item. Now enter the settings as described below.



- **Mobile key name** = „Office“ (or anything of your choice)
- **System ID** = “SystemID” (previously set using IMAporter Reader Config app or written on the last page of this manual)
- **System key** = “SecretPass” (previously configured using IMAporter Reader Config app or written on the last page of this manual)
- **User ID** = “123456” (max. 9 digit unique User ID that gets transmitted to the control unit
- **User PIN** = “1234” (optional feature, can be required for doors with higher security)

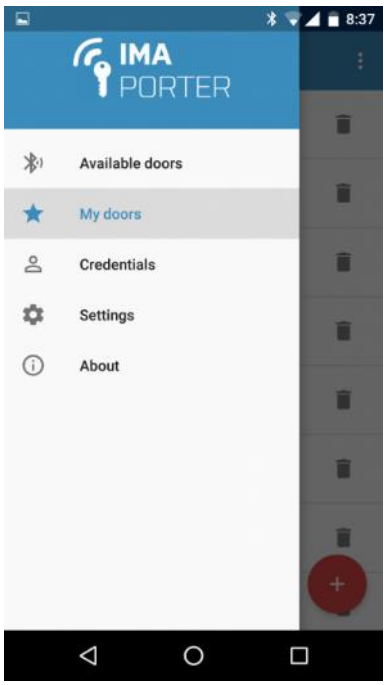
5.3 Testing user identification

5.3.1 Testing NFC identification

In case you have a device with NFC capabilities available, the easiest way to test the reader is as follows: Turn on the display and place the phone directly to the reader. The device may remain locked and there is no need to run any app. However, it is helpful to know the location of the NFC antenna of your mobile device, and to place it to the center of the reader.
To test the NFC identification, tap the reader with your mobile device.
To identify using NFC, the screen needs to be lit, but the IMAporter Mobile Key app does not need to be run.

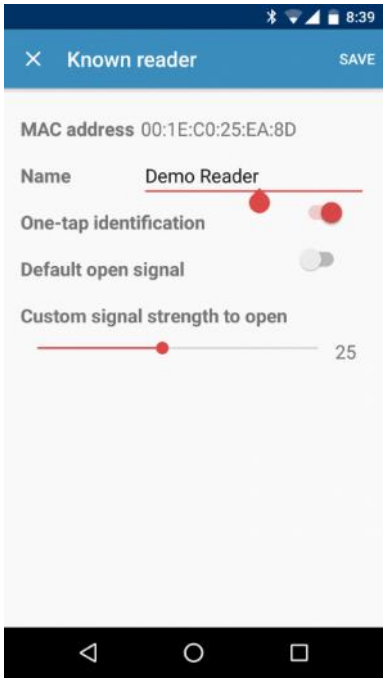
5.3.2 Testing Bluetooth identification

RSW.04-B only (reader with BLE): Navigate to ***My doors*** tab and tap the **+** button to search for a BLE reader in range.

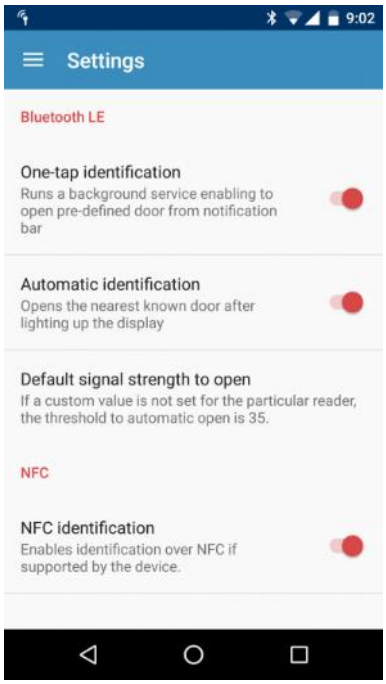


RSW.04-B only (reader with BLE): Tap on the reader to view a configuration form and fill it in

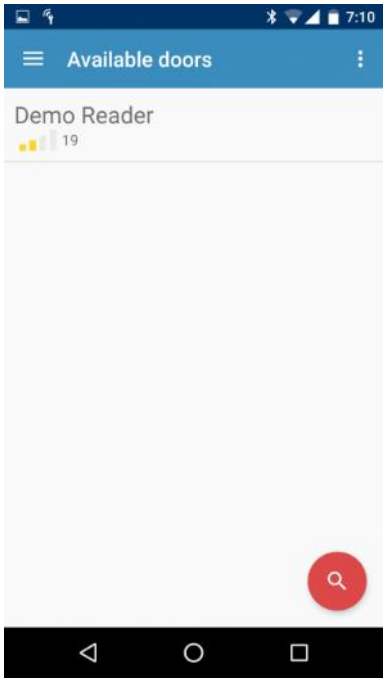
- MAC address - unique identifier of the reader
- Name = “Demo Reader” (your own name for the reader)
- Automatic open - enable/disable simplified opening service
- Default open signal - use individual or global signal strength for automatic opening
- Custom signal strength to open - set individual opening signal strength



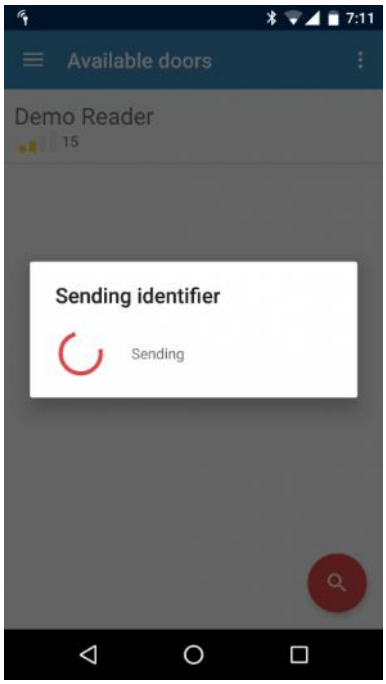
Navigate to **Settings** tab and enable NFC identification. BLE identification does not have to be enabled unless you want to use automatic opening from notification bar or by lighting up the display.



RSW.04-B only (reader with BLE): Navigate to the **Available doors** tab and click the available detected reader displaying with a predefined name.



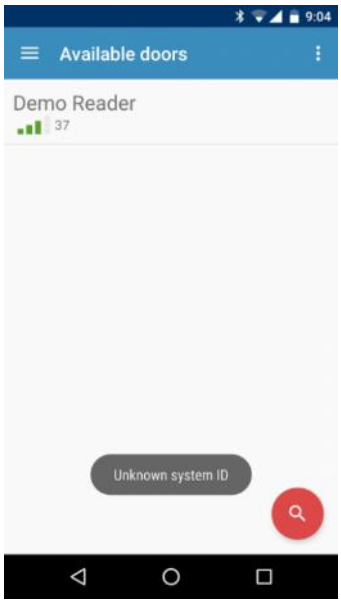
RSW.04-B only (reader with BLE): Communication window will pop up for a second and reader will beep and light green/red LED according to access rights settings in the connected control unit.



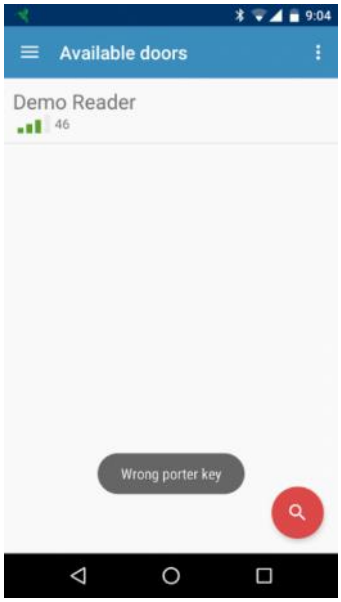
6 Support and Error Codes

6.1 IMAporter MobileKey identification app

During testing of BLE or NFC communication, the app says Unknown System ID and reader does not react.
You have a typo in the *System ID* field when entered to the IMAporter MobileKey app. Please check and rewrite if needed to match the record entered using the IMAporter Reader Config app.



During testing of BLE or NFC communication, the app says Wrong System Key and reader does not react.
You have a typo in the *System Key* field when entered to the IMAporter Mobile Key app or on IDcloud server. Please check and rewrite if needed to match the record entered using the IMAporter Reader Config app.



Mobile device says that identifier has been successfully sent, but door does not open and reader does not react / shines with red LED

The user ID is not authorized to enter - it is not configured in the connected control unit

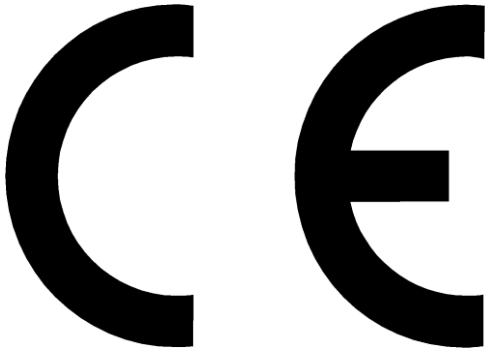
6.2 Reader state signaling – Error states

When turned ON, the reader blinks red LED in 1sec interval
The reader has either not yet been configured using the configuration card or it is missing the system settings that are to be set using the IMAporter Setup app.
Test if the reader is accepting RFID or NFC cards (e.g.: MIFARE Classic). If cards are accepted and the reader is still blinking red LED, it is only missing the system settings using IMAporter Setup app. If it does not accept cards at all, it is probably in default factory settings and needs to be configured.

Indication error during identification – the reader does not blink or beep
Check if the signalization wires are connected to the control unit and that the control unit is set properly. LED and BEEPER are controlled by grounding the specific wires. If the reader is behaves in a “strange” way, then the wires are probably not connected or controlled properly.

Identification using a mobile device is successful, but reader blinks red LED
The identifier assigned to the mobile device is probably not authorized to access. Please check settings in the control unit.

7 Declaration of Conformity



Manufacturer: **IMA s.r.o.**
Na Valentince 1003/1
15000 Prague
Czech Republic
VAT No.: CZ45277397

We declare under our sole responsibility that the product:

Name: **RSW.04 reader**
Variants: **RSW.04, RSW.04-B, RSW.04-P, RSW.04-PB, RSW.04-EM, RSW.04-L, RSW.04-DF**
Type of equipment: **Identification reader with RFID, NFC and BLE support**

to which this declaration relates is in conformity with the following Directives and Standards:

EMC Directive: 2004/108/EC
EN EMC Emission standard EN55022 class A
EN EMC Electromagnetic compatibility EN 50130-4:2011, EN 50130-5, EN 50131-1, EN 50131-2-2, EN 50133-1, EN 50133-2-1, EN 61000-4-2:2009, EN 61000-4-3:2006, EN 61000-4-4:2012, EN 61000-4-5:2006, EN 61000-4-6:2007, EN 60068-2-1, EN 60068-2-2, EN 60068-2-18, EN 60068-2-30, EN 60068-2-75, EN 60068-2-6

RSW.04 readers use low range wireless standard 13,56 MHz, work according to ISO/IEC 14443 protocol and are in conformity with the requirements of the related standards.

This product complies with the requirements of the following directives European Community Council Directives 89/336/EEC, 93/68/EEC and 73/23/EEC relating to electromagnetic compatibility and product safety respectively.

Place of issue: Prague, Czech Republic
Date of issue: August 20, 2015

Person responsible for RSW.04 product line

Jiří Bárta
Sales Director

7.1 Certification

Certificate of National Security Authority

The National Security Authority issued the NSA Certificate for RSW.04 on 3/12/2013 in accordance with Art. 46 of Act No. 412/2005 Coll., on the Protection of Classified Information and Security Clearance. This is a technology equipment certificate for the RSW.04 contactless smart card reader. It confirms the clearance of technology equipment of Type 2-4.

Certificate of Conformity

Accredited certification bureau TREZOR TEST s.r.o. issued on 24/10/2013 a certificate for the RSW.04 reader. It confirms the clearance of identification class of Type 2 and environment class of Type IV according to EN 50133-1:2001 and EN 50133-2-1:2001

Czech Product Certification

CZECH PRODUCT

The RSW.04 IMAporter Reader is licensed with the 'Czech Product' trademark.

IMA s.r.o. ISO Certificate

IMA s.r.o. obtained the ISO certificate based upon a certification audit carried out by TUV Rheinland in accordance with CSN EN ISO 9001:2009. The certificate was awarded after the entire company had undergone a preparatory process and increased supervision over its improved management system.

8 Delivery parameters

8.1 Type of reader:

☐ **RSW.04** **IMAporter Reader with NFC**
☐ **RSW.04-B** **IMAporter Reader with NFC and Bluetooth LE**

Reader settings:

- **Wiegand interface:** ☐ **26bit** ☐ **32bit** ☐ **56bit**
- **RS232 interface:** ☐ **9,6kbit** ☐ **19,2kbit** ☐ **115kbit**
- **indication:** ☐ **constant red LED** ☐ **separately controlled LEDs**
- **media:** ☐ **MIFARE Classic** ☐ **MIFARE DESFire** ☐ **NFC tags**
- **devices:** ☐ **NFC device** ☐ **BLE device**
- **other specification:**_____

8.2 System settings (for MobileAccess platform)

Security parameters:

System ID: _____

System Key: _____

IDcloud login (my.imaporter.com):

Username: _____

Password: _____

PLEASE NOTE: THESE CONFIGURATION PARAMETERS ARE CRUCIAL FOR SYSTEM SECURITY AND MUST NOT BE PROVIDED TO ANYONE.
Once typed into the IMAporter MobileKey identification app or to the IDcloud, the passwords remain hidden and cannot be accessed by the user.
For more information about individual settings and their meaning please read the system manual.

If lost or leaked to a third party, please contact the system supplier in order to restore or change the system settings.

To download the IMAporter MobileKey app scan the corresponding QR code with your mobile phone.

Android

www.ima.cz/app/key/andro

iOS

www.ima.cz/app/key/ios