*Roger Access Control System*

# RKD32 Installation Manual

*Product version: 1.1*

*App version: 1.4.4*

*Document version: Rev. E*

CE

roger

# 1. DESIGN AND APPLICATION

RKD32 electronic key cabinet enables management of keys or other items e.g. cards, remote control devices, fobs, etc. The configuration in standalone mode is performed manually with MD70 panel which is equipped with graphic touchscreen and card reader (Mifare and EM125kHz) or remotely via web browser. The initial configuration in network mode is performed with MD70 panel while further configuration in regard of users and authorisation is performed in computer network on the level of VISO management software (RACS 5 system).
Up to four cabinets can be operated with single panel. In such scenario RKD32EXT cabinets are connected to RKD32 cabinet. Prior to placing keys inside cabinet, they must be firmly attached to included RFID fobs. RKD32 can recognize fobs so keys can be returned to any unoccupied slot in the cabinet. It is possible to assign users with authorizations for particular keys. Typically users are identified at the panel with Mifare or EM125kHz proximity cards, or PINs. When key is collected then both door lock and fob lock are released and frame around the key is highlighted in green.
RKD32 cabinet is internally connected in factory and its installation requires only connection of power supply and wall mounting inside premises.

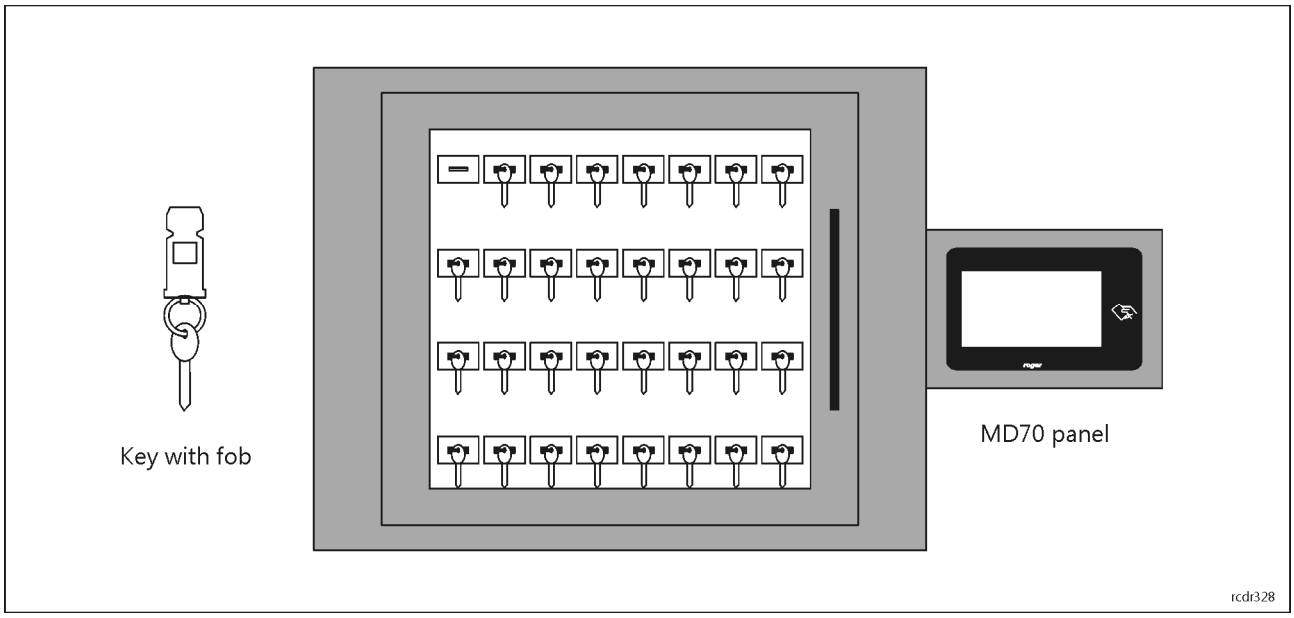



Fig. 1 RKD32 overview

## Characteristics

- Operates standalone or as a part of RACS 5 access control system
- Local management from a control panel
- Remote management from an embedded web browser
- Remote management from the RACS 5 access control system software (VISO application)
- Graphic control panel with a 7" touch screen
- Built-in Mifare® and EM 125 kHz cards reader
- Support for Secure Mifare Sectors
- Optional identification on external reader with Wiegand interface
- Optional identification on external reader with RS485 EPSO 3 (Roger) interface
- One-time PINs
- User photo upon key take/return
- 32 keys in the RKD32 main depositor
- 32 keys in the RKD32EXT extension depositor
- Possibility to connect 3 RKD32EXT expansion depositors to the RKD32 main depositor
- Permanent connection of the key with the fob without the use of seals
- Possibility of using seals connecting the key with the fob
- Keys blocked mechanically in slots
- Contactless identification and key presence control via Mifare® proximity key fob

- Time dependant access rights to keys
- Limitation of the number of keys taken by the user
- Internal and external group of keys
- Two user option for keys
- Card + PIN authorization option
- Alert signalisation when key not returned within predefined time
- Email notifications upon alarm events
- Free access to all keys when operating in Office Mode
- Option to return keys without user identification (Quick Key Return Mode)
- Fixed or variable key position mode
- Light indication of slot with selected key
- Reservation of keys
- Key status comments
- User activities reports
- Key usage reports
- Generating and sending reports
- Voice prompts
- Emergency unlocking of all keys via an external signal (e.g. from the fire protection system)
- Emergency unlocking of the keys
- Door opening detection
- Enclosure opening detection
- Metal enclosure in RAL7016 colour
- RKD32 dimensions: 535 x 935 x 183 mm
- RKD32EXT dimensions: 535 x 675 x 183 mm
- SG option: P2 class anti-burglary glass
- RP option: Control panel for wall mounting
- SH option: Electric roller shutter instead of depository door
- MK option: Key to unlock the case in the Master Key system
- ND option: Cabinet without door
- CL option: Special lock cylinder
- SDK
- External 12V power supply
- 10 years of post-warranty service\
- No warranty service required

## Power supply

RKD32 requires 12VDC/2A buffer power supply. The power supply must be connected to connection block which is wired to +12V and GND screw terminals at RKD board (fig. 4). Battery cannot be directly connected to RKD32 so the emergency supply (battery, UPS) must be ensured on the level of buffer power supply unit (e.g. HPSB2512B PSU from Pulsar company). The required emergency operational time of key cabinet(s) must be considered when battery or UPS is selected.
In case of complete power supply loss, the RKD32 can be supplied from powerbank (min. 2A rated output) connected to USB cable which is connected to RKD board (fig. 4).

## Cabinet

RKD32 cabinet is made of stainless metal sheet which is powder painted in RAL7016 (anthracite grey).
As standard, the RKD32 is equipped with a door with a tempered glass panel. Depending on the option, the cabinet can be equipped with an P2 class anti-burglary glass panel, full door or without a door. There is also a variant with an electrically raised and lowered shutter. Cabinet can be equipped with mechanical locks in the Master Key system. The cabinet dimensions in standard version are given in fig. 4.

## RFID fobs

The RKD32 includes 32 RFID fobs which are attached to keys or other supervised items. A key can be attached to the fob manually without any specialized tools. When a key is placed on a ring and the ring is inserted into a fob then it is not possible to detach the key from the fob without damaging it. This prevents possible tampering with keys and fobs.

In order to join a key (or other object) with an identification fob, place the key on the metal ring, and then press the ring so that only the oval part is visible. After joining, verify the correctness of the latch mechanism by attempting to pull the key from the key fob. Optionally when secured element cannot be applied on the ring then it can be attached to hole in the fob using wire and seal.

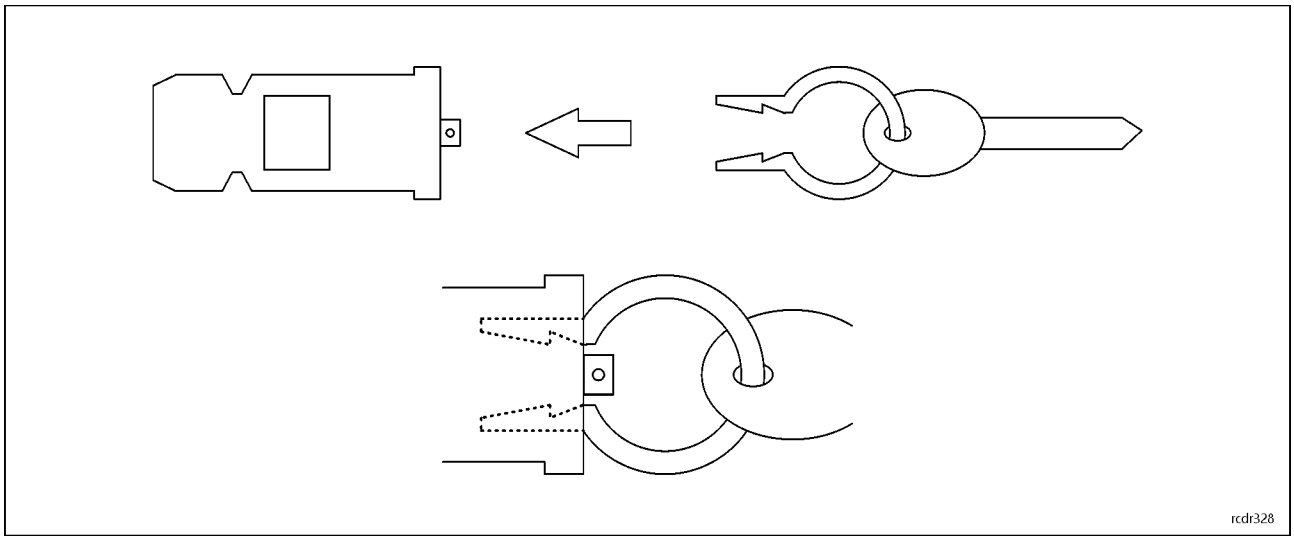



Fig. 2 RFID fob

# MD70 panel

Management of RKD32 is performed by means of MD70 panel. Single panel can be used to control up to 4 cabinets, each with 32 slots for RFID fobs and keys. The next cabinets (RKD32EXT) are connected to the main cabinet (RKD32) using RJ45 sockets on RKD boards (fig. 7). Connections can be ensured with U/UTP cat. 5 cable but the maximal cable length cannot exceed 5m. MD70 panel is equipped with graphic touch screen, sounder and Mifare/EM 125kHz card reader. More information on the panel is given in its Operating Manual which is available at www.roger.pl.

# Identification

Following user identification methods are offered by the panel:

- MIFARE Ultralight/Classic/Plus/DESFire and EM125kHz proximity cards
- PINs
- RFID fobs

**MIFARE cards**
By default the panel reads serial numbers (CSN) of MIFARE cards but it is possible to program cards with own numbers (PCN) in selected and encrypted sectors of card memory. The use of PCN prevents card cloning and consequently it significantly increases security in the system. More information on MIFARE cards with PCN is given in section 7 and in AN024 application note which is available at www.roger.pl.

**EM 125kHz cards**
By default, the panel also reads the serial number of EM 125kHz cards. The EM 125kHz card reader works in parallel with the reading of Mifare cards. In the MD70 device settings it is possible to limit card reading to one of two standards.

**PINs**
The panel accepts variable length PINs (by default 4-16 digits). PIN entered with keypad must be concluded with # or OK key.

**RFID fobs**
If the option *Quick key return mode* is enabled (table 2) then key fob can be used for identification at MD70 panel to open the door and return the key to unoccupied slot. The recommended method of fob reading at the panel is shown below.

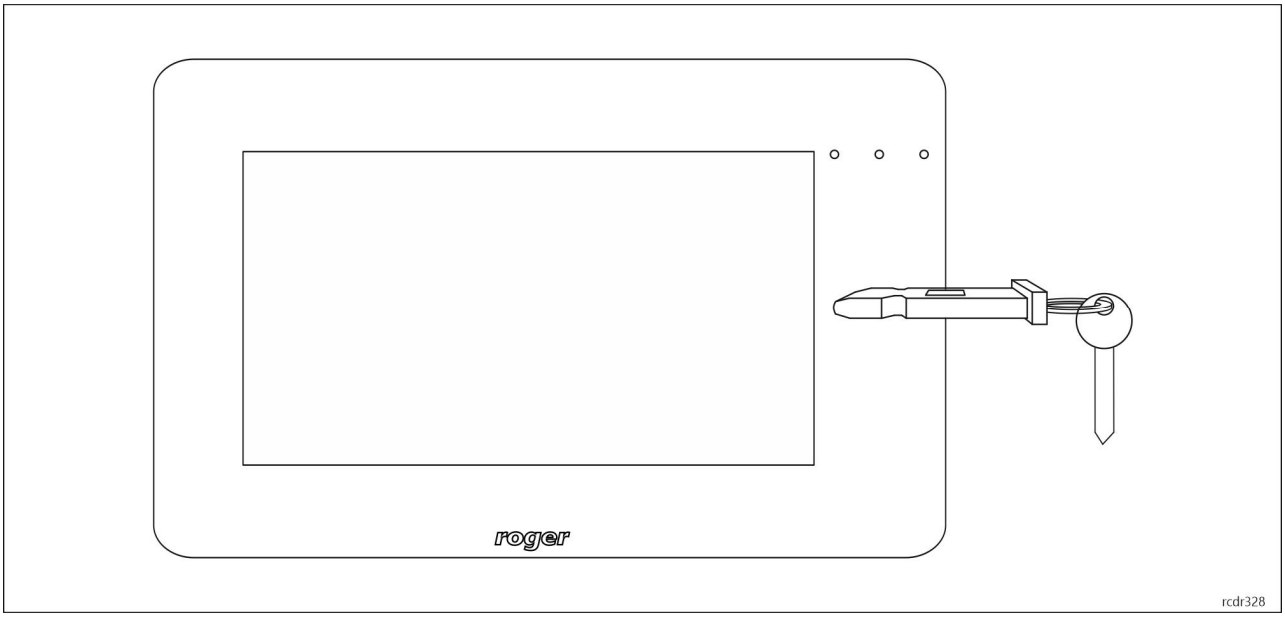



Fig. 3 RFID fob reading at MD70 panel

## Other proximity cards and biometrics

User can be identified at MD70 panel with other methods if additional external reader is connected. Any MCT series reader or RFT1000 fingerprint reader can be used for that. Such reader must be configured with ID=915 address and connected to RS485 A and RS485 B screw terminals of MCX4D module.
If it is necessary to apply identification method which is not offered by Roger then external reader with Wiegand interface can be connected. In such scenario an additional MCX102 expander with ID=915 address must be installed inside the cabinet. Wiegand reader can be connected to IN1 (D0 line) and IN2 (D1 line) screw terminals of the expander while the expander is connected to RS485 A and RS485 B screw terminals of the MCX4D module.

## Connection with intruder alarm system

RKD32 is equipped with tamper detectors which enable detection of cabinet enclosure opening. Additionally tamper detector is located inside MD70 panel. Opening of RKD32 or MD70 enclosure is signalled on LCK4 transistor output of MCX4D board (fig. 8). Door ajar warning is signalled when user becomes logged out (manually or automatically) to the panel's starting screen. The warning is generated acoustically by MD70 panel for the time specified by the parameter *Door open too long prealert time* (table 2). If the door remains opened when time elapses then BELL4 output of MCX4D board is activated for 3 minutes or till door closing. BELL4 output is activated immediately also when door is opened by force. Both LCK4 and BELL4 outputs can be connected to intruder alarm system, siren or other alarm device.

## Connection with fire alarm system

In case of fire alarm detection or any other emergency situation, the RKD32 can release all locks to enable key collecting by any person without authorisation. Such release requires connection of fire alarm system output to DR3 screw terminal of MCX4D board. As long as output line is activated, door lock and key fob locks are released. In such scenario the option *Fire alarm support (fobs released)* (table 2) must also be enabled.

# 2. INSTALLATION

Two people are required for the installation of RKD32. Before installation, turn both locks shown in fig. 4 simultaneously to detach back cover. Connect and lead all cables through cable hole in back cover and then mount the cover on wall according to fig. 6 using holes shown in fig. 5. When RKD32 is mounted on back cover as in fig. 6 then both locks will latch automatically. The communication with RKD32 in network mode and via web browser can be provided through Ethernet or Wi-Fi connection (more information on configuration of MD70 network parameters is given in its manual). appropriate authorization.

Caution: After changing the number of cabinets (e.g. adding RKD32-EXT), start device scanning (Settings / Configuration / Detect devices, in order to properly handle all slots.

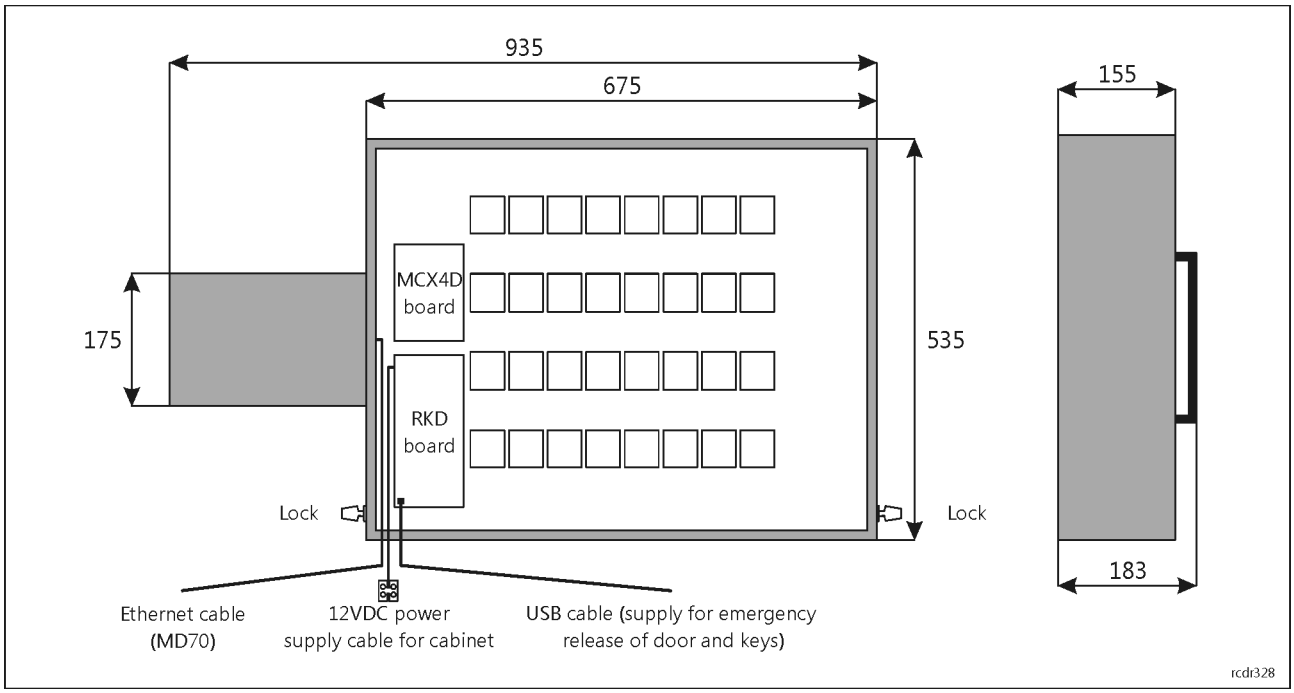



Fig. 4 Inside RKD32 with back cover removed

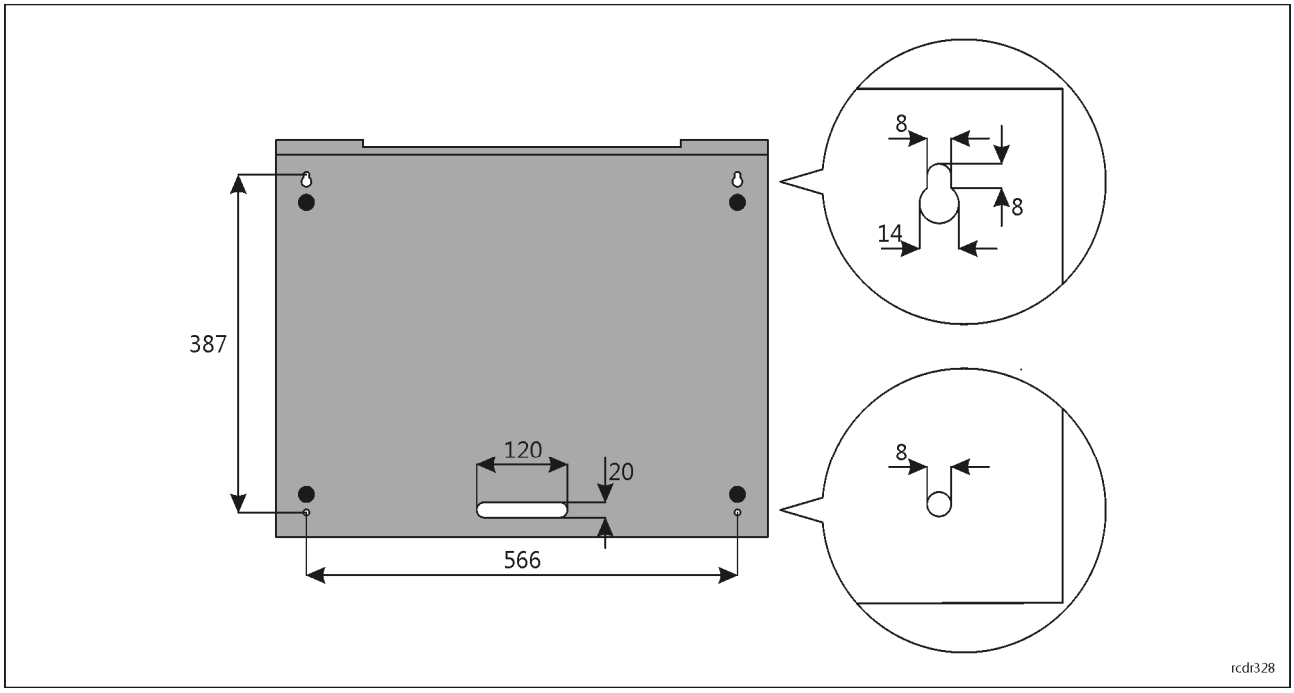



Fig. 5 Back cover

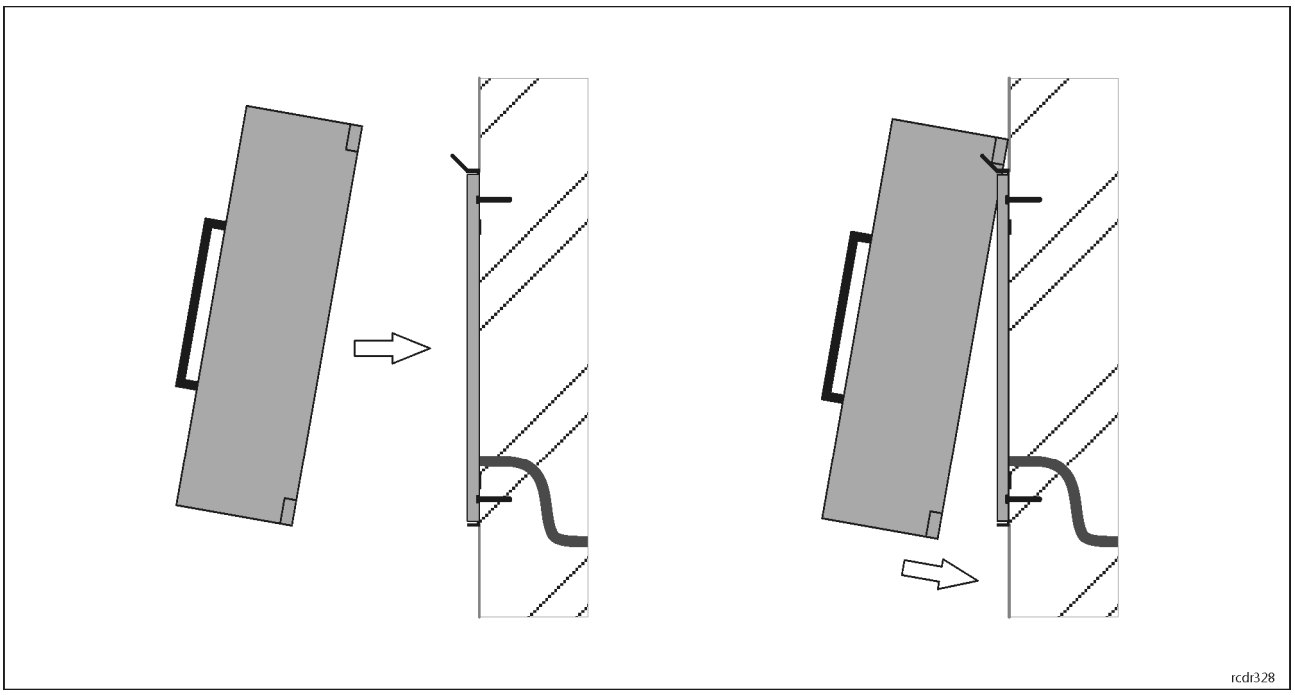



Fig. 6 Wall mounting

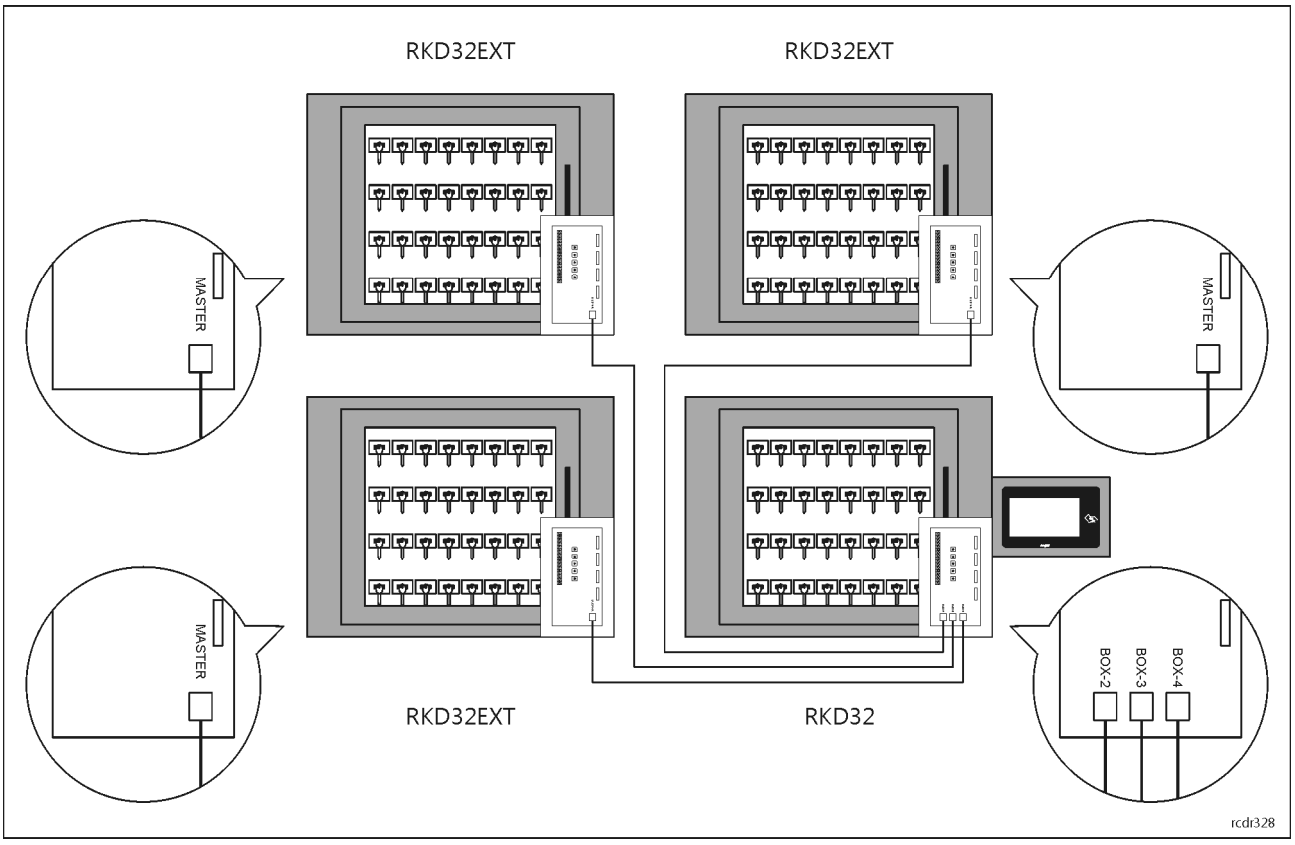



Fig. 7 Connection of additional cabinets (RKD32EXT) to main cabinet (RKD32)

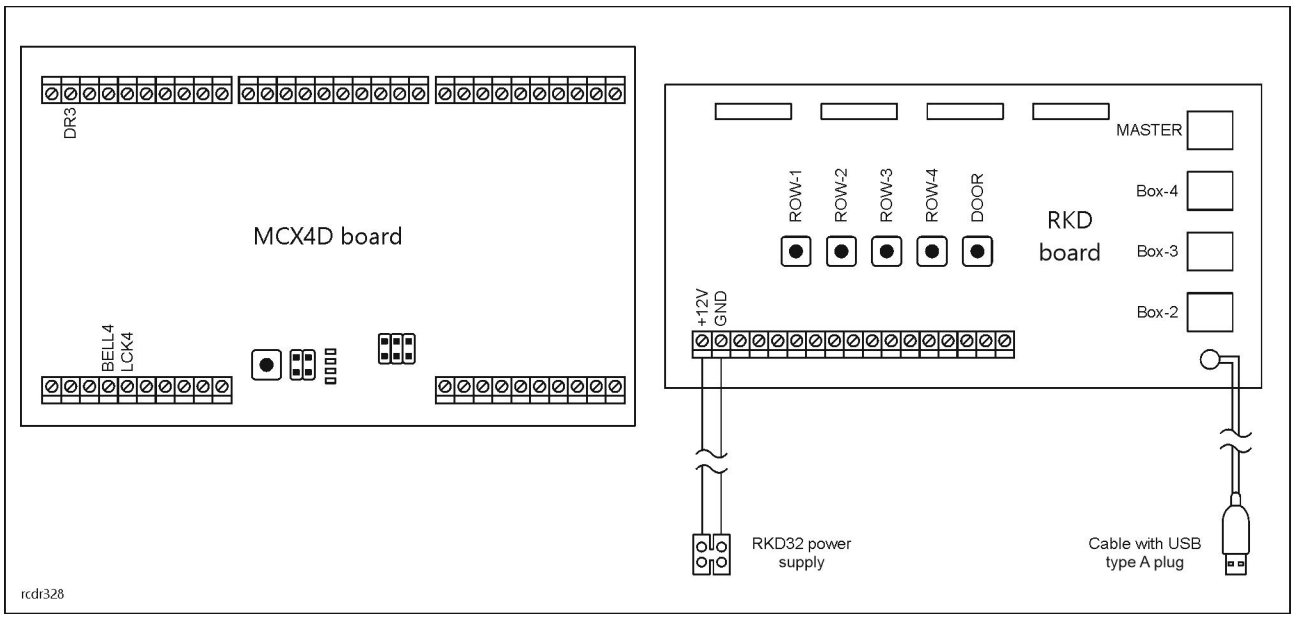



Fig. 8 RKD and MCX4D boards

| **Table 1. Screw terminals and sockets** | |
|---|---|
| Terminal/ socket | Description |
| +12V | 12VDC power supply |
| GND | Ground |
| BELL4 | 15VDC/1A output line for door alarms |
| LCK4 | 15VDC/1A output line for tamper alarms |
| DR3 | Input line for connection of fire alarm system (emergency release of door and key locks) |
| MASTER | RKD32: USB type A socket for connection of pendrive*<br>RKD32EXT: RJ45 socket for communication with RKD32 |
| BOX-2 | RJ45 socket for connection of second module (RKD32EXT), only at RKD32 |
| BOX-3 | RJ45 socket for connection of third module (RKD32EXT), only at RKD32 |
| BOX-4 | RJ45 socket for connection of fourth module (RKD32EXT), only at RKD32 |

USB socket designed to connect of flash memory (for backup or write a reports) is available inside key chamber after door opening in the right bottom corner (fig. 9).

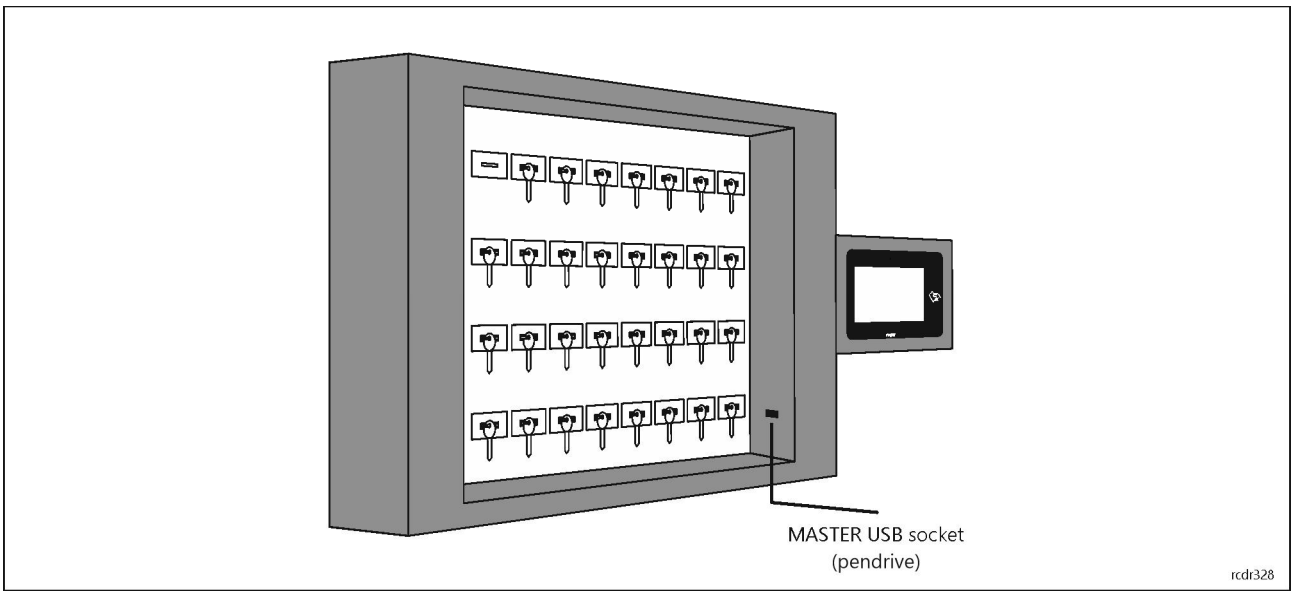



Fig. 9 USB MASTER socket

# 3. RAACA APP

After connection of power supply, the MD70 panel will start RAACA app. When started for the first time the panel will offer to create default Master user with 9999 password. You must also select the operating mode of the device:

- Any fob position: keys can be returned to any socket
- Fixed fob position: each key is assigned a socket to return it to

Additionally, for the *SH* option, select the "Depository equipped with a shutter" option, and for the *ND* option, "Depository without door". If items other than keys are stored in the cabinet, after selecting the "Cabinet with general purpose assets" option, the text phrases "key" in the device interface will be replaced with "asset".
Then app can be accessed with 9999# password (if created) or with 12345* administrator password. The administrator account is intended for the installer or the person who manages the system i.e. for maintenance and service purposes. Daily service and configuration of RKD32 should be done by means of user account with the appropriate authorization.

Caution: Both default passwords should be changed to your own passwords as described in section 7.

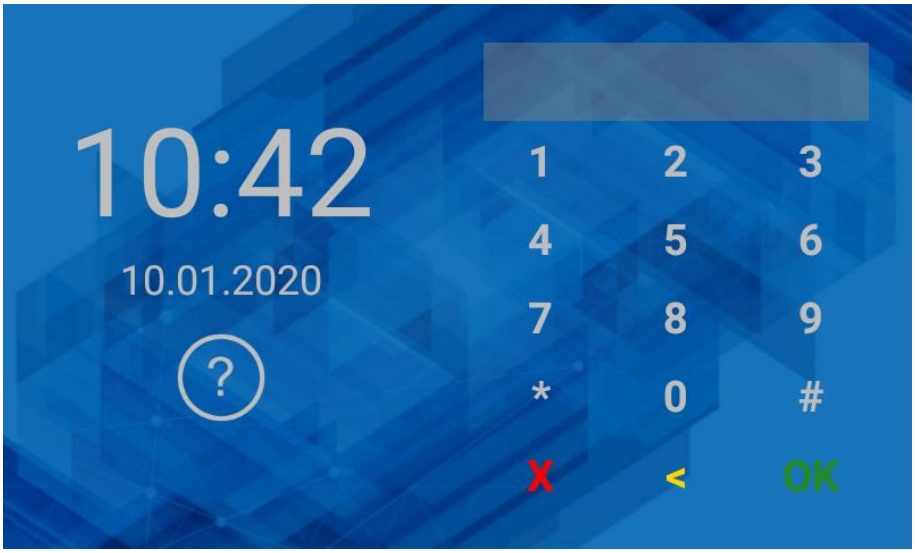



Fig. 10 Default starting screen

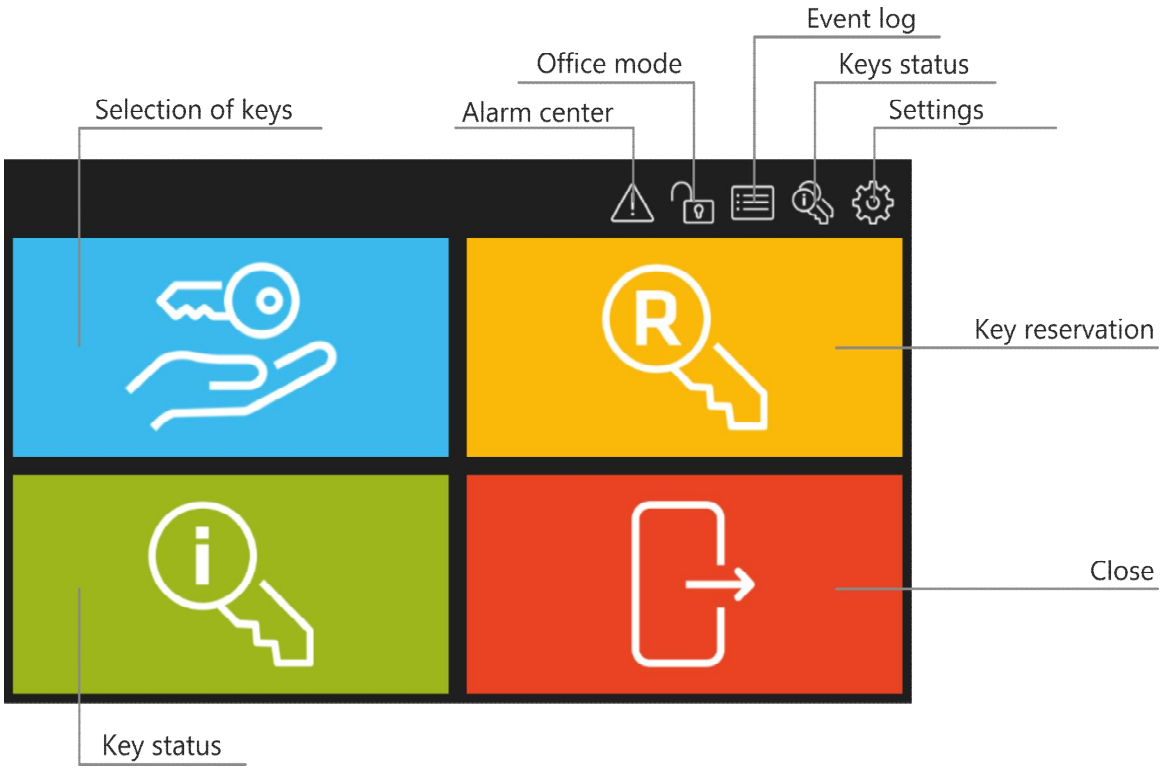



Fig. 11 Main menu

When ⚠ in the top right corner is selected then Alarm Center is started. It shows all alarm events (forced opening, tamper, etc.) registered by RKD32 in selected time range. The colour of icon corresponds to following statuses:

- White: No unconfirmed alarms.
- Orange: Alarm(s) from the past is/are in the memory of device.
- Red: At least one unconfirmed alarm is still on.

When 🔓 is selected then office mode will be started after returning to the starting screen. In office mode door lock and key locks are released indefinitely but keys which are reserved with blocking will not be released. Office mode can also be automatically started and finished by schedule which can be defined in *Settings* window (fig. 13) and assigned with the command *Office Mode schedule* (table 3).

When ☰ is selected then Report Center is started as in fig. 12. After selection of Events tile it is possible to browse, events (e.g. user login, key collecting, etc.) and after selection of ☰ in the same window it is possible to delete and export events registered by RDK32. Key Report and User Report enable to display respectively events related to particular key and events related to particular user. In both cases events can be exported. Database Report displays list of users with their cards and PINs and their Authorisations. Events in Report Centre can be exported to pendrive connected to MASTER USB socket (fig. 9), exported to internal memory or sent by email according to settings in *Configuration* window (table 2). Available formats are Excel (XLS) and PDF.

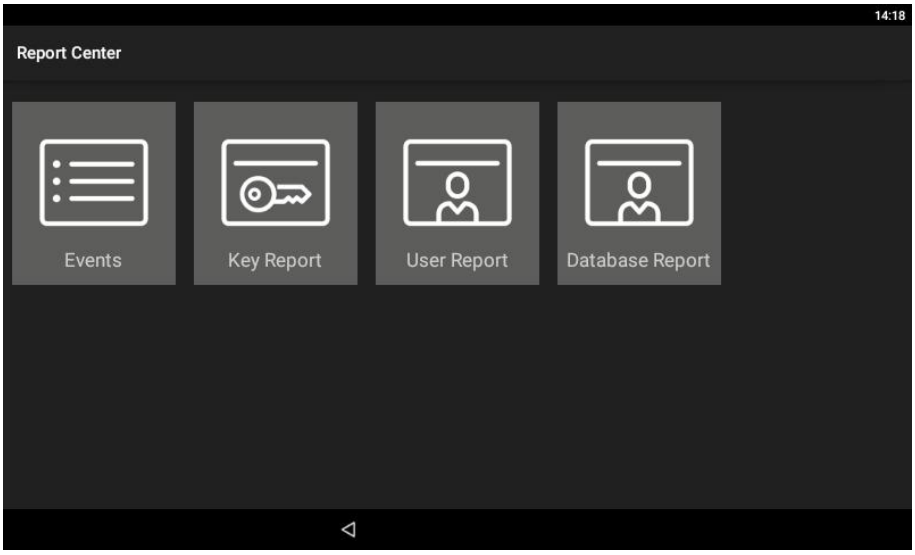



Fig. 12 Report Centre

When is selected in top right corner of the main menu then statuses of keys in the system are displayed. It informs what keys are collected, by whom and which keys are reserved.

When is selected then settings window is displayed as in fig. 13.

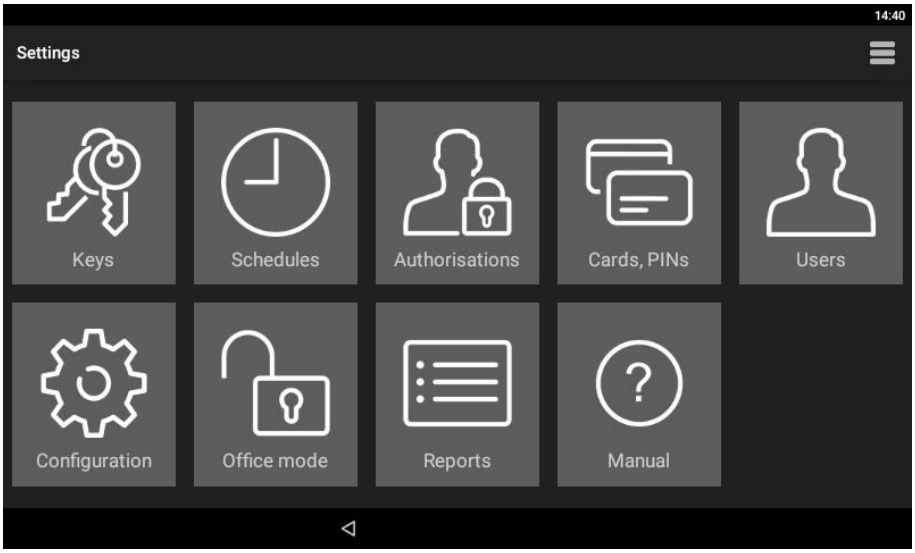



Fig. 13 Settings window

**Keys**

When selected then the list of keys enrolled in the system is displayed. New key can be enrolled by selection of *Add* command and then by reading fob at MD70 reader or inserting the fob into one of unoccupied slots. Editing and deleting can be done by long clicking of an object on the list.

Assigning the key to the Inner zone allows the implementation of key anti-passback function. The user can collect a key from another zone only when he returns all keys belonging to inner zone. The inner zone is intended for keys that should stay as short as possible outside the cabinet (e.g. record office, confidential office).

The option *Required return time* allows to control the return of a key on time. After exceeding the indicated time, a related event is generated and can be displayed in the Alarm Center.

Commission get mode - after selecting this option, when trying to download a key, authorization is required by another user who has rights to the given key.

Card + PIN mode - to get the key, you must identify it with both the card and the PIN. When trying to download the key, the application will ask you to read the card or enter the PIN, depending on the type of medium that was used when logging in.

If both of the above options are selected, the card must be read and the PIN code entered to confirm the commission collection.
Group option allows you to easily identify the key's position on the list of available assets. After selecting specific group, the key will be marked with the appropriate color on the list.

**Schedules**
When selected then list with predefined *Always* and *Never* schedule is displayed. New schedule can be defined by selection of *Add* command and then *Add range*. Editing and deleting can be done by long clicking of an object on the list. Schedule consists of time periods which are specified for days of a week. Schedules can be used to limit authorisations and to manage office mode.

**Authorisations**
When selected then list of authorisations is displayed. New authorisation is defined by selection of *Add* command. Editing and deleting can be done by long clicking of an object on the list. Authorisation may concern access to keys, settings, event log, key status and may enable key reservation override. Authorisations are assigned to users in the next steps of configuration.

**Cards, PINs**
When selected then list of cards and PINs is displayed. Cards and PINs are used for identification of users at MD70 panel. Adding, editing and deleting is possible on the list. During card enrolment its number can be read at MD70 reader.

**Users**
When selected then list of users is displayed. Users can be assigned with cards, PINs and authorisations. The *Fob limit* option allows you to specify the number of keys that the user can have simultaneously downloaded. Value "0" means no limit. Additionally, *Quick key get mode* and *Master exemption* can be enabled. The first option enables to release authorised keys automatically when user is logged at MD70 panel so the manual selection of key from the list is not necessary. For this mode the option *Quick key get mode* (table 2) must be enabled. The *Master exemption* option assigns unlimited authorisations in the system for a user.

**Configuration**
When selected then list of parameters given in table 2 is displayed.

| **Table 2. Parameter list in Configuration window** | |
|---|---|
| **General** | |
| Admin password | Administrator password. In case of login at MD70 panel the admin password is concluded with * key. Range: 4-10 digits. Default value: 12345. |
| Logout when door closed | Parameter enables automatic user logout and reverting to starting screen when door is closed. Range: ON, OFF. Default value: ON. |
| Automatic logout time [s] | Parameter defines time after which user is automatically logged out and panel reverts to starting screen if no actions are performed by user in the main menu of the panel. Range: 0-99. Default value: 60. |
| Automatic logout | Parameter enables automatic user logout and reverting to starting screen when *Automatic logout time* elapses. Range: ON, OFF. Default value: ON. |
| Alarm signalling time [min] | Parameter defines time for tamper alarm signalling on output LCK4. Range: 0-99. Default value: 3. |
| Door open too long prealert time [s] | Parameter defines time for acoustic warning at MD70 panel when door is opened and user is logged out. Range: 0-99. Default value: 60. |
| Fire alarm support (fobs release) | Parameter enables emergency release of door and key locks as long as the input DR3 is triggered by external system e.g. fire alarm system. Range: ON, OFF. Default value: OFF. |
| Office mode: cabinet door only | After selecting this option, while in office mode, the lock of the |

| | |
|---|---|
| | depository door is released and the keys remain locked. Default value: OFF. |
| Selective cabinet's opening | After selecting this option, only the cabinets where available keys are located (after logging in for quick key get mode or after indicating the key to be collect) and those cabinets from which the keys were collected by the user will be opened. |
| Fast relogin | After activating the option, it is possible to change the logged in user without logging out (only by reading the card). |
| Events with photos | After selecting this option, photos will be taken when users log in. |
| **Keys** | |
| Quick key return mode | Parameter enables quick key returning after identification at the MD70 panel with key fob. In such scenario, user card or PIN are not required to open cabinet door and return a key. This can be used for example by temporary worker after finishing his job in a room. Range: ON, OFF. Default value: ON. |
| Show absent key on list | Parameter enables to display collected keys both in key selection window and keys status window. Range: ON, OFF. Default value: ON. |
| Fast get: show absent key info | Parameter enables to display message on keys which are currently not available for quick getting by user. The message is displayed when user logs at the panel. Range: ON, OFF. Default value: OFF. |
| Function: identify key | After selecting this option, it is possible to identify the key. In order to identify, read the key on the MD70 panel reader after logging in. |
| Shortcut to getting key | Automatic display of the list of keys after logging in. Note - active only for the activated "Disable reservation" option and the mode of any key position, and for the user who has no access to the application settings. Default value: OFF. |
| Shortcut: logout after get single key | The parameter activates automatic logout after getting one key and reduces the idle time in the get key activity to 10s. Note - the parameter works only for the " Shortcut to getting key" option. Default value: OFF. |
| Email notification | Enabling the parameter starts sending e-mail notifications about alarm events and when return time exceeded. |
| **Comments** | |
| Reporting a comment about the equipment status | After activating the option, a dialog box will be displayed during the key retrieval and return, where it is possible to add a comment regarding the key status or other request for the system administrator |
| Comments on demand | This option enables the possibility of entering a comment at any time. Note: this option replaces the key reservations icon. |
| Predefinied comment content (1) | After you enter your text, it will appear as an option to check when reporting a comment. |
| Predefinied comment content (2) | After you enter your text, it will appear as an option to check when reporting a comment. |
| Predefinied comment content (3) | After you enter text, it will appear as an option while typing your comment. The predefined content may be completed by the user, eg after entering the text "Mileage [km]", the user may enter the car's odometer reading when returning the key.<br>Note: when none of the 3 texts is defined, only the option to enter your own comment will be available when entering a comment. |
| **Reservation** | |

| | |
|---|---|
| Disable reservations | The parameter blocks the possibility of defining a key reservation. Default value: OFF. |
| Block reserved key | Parameter enables key blocking by default when key is reserved. Range: ON, OFF. Default value: OFF. |
| Maximum reservation time [h] | Parameter defines maximal period for reservation of key by user. Range: 0 – 99. Default value: 30. |
| **Display** | |
| Custom wallpaper | Parameter enables switching between default and custom wallpaper for MD70 panel. Custom wallpaper is indicated by *Select wallpaper* command in ☰ menu. Range: ON, OFF. Default value: OFF. |
| Font color | Parameter specifies colour of the font used on MD70 starting screen. Range: Light, Dark, Orange. Default value: Light. |
| Voice prompts | Enabling the option activates playback of the voice messages. Default value: OFF. |
| **RACS 5 settings** | |
| RACS 5 mode | Parameter enables RKD32 operation in network mode and management by means of VISO software from RACS 5 system. |
| Server address | Parameter defines IP address of server with virtual controller. |
| Communication port | Parameter defines communication port of server with virtual controller. Default value: 9788. |
| Login | Parameter defines login for communication with virtual controller. |
| Communication password | Parameter defines password for communication with virtual controller. |
| TLS | When checked, TLS encryption of communication is activated |
| MAC | Info box with MD70 MAC address. |
| Device name (comment) | Parameter specifies the name of RKD32 which is then used in reports and logs. |
| **WWW settings** | |
| Web access enable | Parameter enables RKD32 configuration and management via web browser. |
| Port | Parameter defines communication port for web browser access. Due to security reasons the port cannot be below 1024. Default value: 8888. |
| Login | Parameter defines login for web browser access. |
| Password | Parameter defines password for web browser access. |
| **Email account** | |
| Address | Email account which is used for sending messages and reports from RKD32. |
| Login | Email account login for email sending by RKD32. |
| Password | Email account password for email sending by RKD32. |
| SMTP port | Email port. Default value: 587. |
| Host | Email host address. |
| SSL | Parameter enables SSL encryption for email sending. Range: ON, OFF. Default value: OFF. |
| Address 1 | Recipient email address. |

| | |
|---|---|
| Address 2 | Recipient additional email address. |

| **Table 3. Commands in ☰ menu in Configuration window** | |
|---|---|
| Select wallpaper | Command enables indication of custom wallpaper (800x480px, *.jpg format) for MD70 starting screen. Additionally the parameter *Custom wallpaper* (table 2) must be enabled. |
| Detect devices | Command starts the view of the list of devices in the RKD32 system. After adding another depositor cabinet, run a scan to detect new devices. |
| Office Mode schedule | Command enables assignment of schedule to office mode. The schedule can be defined after selection of *Schedules* in *Configuration* window. |
| Key slot settings | Command enables to adjust the light level of key slots. |
| Check for update | Command enables to check and download updates. In such case the RKD32 must be connected to computer network. |
| Install update | Command enables installation of downloaded update. |
| Import users from PRMaster | Command enables to import users from PR Master software of RACS 4 system as explained in section 7. |
| Configuration export | This command allows you to export configuration settings for transfer to another depositor or for backup |
| Configuration import | The command restores the previously saved device configuration |
| Factory reset | Command enables to restore factory settings as explained in section 7. |

**Office mode**

When selected then office mode is started in the same way as in case of previously described icon which is located in the top right corner of main menu (fig. 11).

**Events**

When selected then Report Centre is started in the same way as in case of previously described icon which is located in the top right corner of main menu (fig. 11).

**Key report**

When selected then history of particular key is displayed. Events can be deleted, exported to external memory i.e. pendrive connected to MASTER socket at RKD board (fig. 6) or send by email according to settings in *Configuration* window.

**Manual**

When selected then app abridged manual is displayed on MD70 screen.

**Menu ☰ in Settings window**

Menu ☰ in window shown in fig. 13 includes additional commands that are not available in the menu ☰ displayed in *Configuration* window.

| **Table 4. Commands in ☰ menu in Settings windows** | |
|---|---|
| Show launcher | Command enables to exit RKD32 app and start Android environment. Default password is admin. |
| System settings | Command enables configuration of Android system settings. More information is given in MD70 manual. |

| | |
|---|---|
| MD70 settings | Command enables configuration of MD70 parameters. More information is given in MD70 manual. |
| Files | Command starts app that enables file navigation at MD70 panel. |
| About | Command displays change log. |
| License | Command displays license agreement for Roger software. |
| License file | Command displays information on uploaded RKD32 licenses in regard of network mode and management via web browser. |
| Export database | Command enables to make backup of RKD32 settings on pendrive as explained in section 7. |
| Import database | Command enables to import RKD32 settings from file on pendrive as explained in section 7. |
| Remote support | Command enables to establish remote connection with MD70 panel in computer network for the purpose of technical support by specialist as explained in section 7. |

# 4. CONFIGURATION IN STANDALONE MODE

## Keys

1. Attach keys to RFID fobs.
2. Log in at the panel (default PIN: 9999#), select ⚙ and then *Keys*.
3. In the opened window select *Add*.
4. In the next window name the key (e.g. Room 101), click *Value* and read fob at MD70 reader ☜ (fig. 2) or insert fob into one of free slots.
5. You can set other key options as needed.
6. Enrol remaining fobs with keys into system.

## Schedules (optional)

1. Log in at the panel (default PIN: 9999#), select ⚙ and then *Schedules*.
2. In the opened window select *Add*.
3. In the next window name the schedule and click *Add range*.
4. Specify periods for days of week. Schedules can be applied for authorisations and office mode.

## Authorisations

1. Log in at the panel (default PIN: 9999#), select ⚙ and then *Authorisations*.
2. In the opened window select *Add*.
3. In the next window name the authorisation and click *Location* to indicate keys which can be collected by user with this authorisation.
4. Optionally click *Schedule* and assign previously created schedule to limit the authorisation to specified time periods.
5. Additionally you can select if the authorisation gives access to settings, event log and keys status as well as enables to override blocking of reserved keys.

## Card, PINs

1. Log in at the panel (default PIN: 9999#), select ⚙ and then *Cards, PINs*.
2. In the opened window select *Add card* or *Add PIN* in order to specify factor(s) that can be used to identify user at MD70 panel. Similarly as in case of fob, card number can be read at MD70 reader ☜ after clicking *Card code*.

## Users

1. Log in at the panel (default PIN: 9999#), select ⚙ and then *Users*.

2. In the opened window select *Add*.
3. In the next window name the user (e.g. first and last name). Click *Cards, PINs* to assign previously defined factors that can be used to identify user at MD70 panel. Click *Authorisations* to assign previously created authorisations which will specify keys that can be collected by user in particular time periods (schedules).
4. Additionally and optionally, quick get key mode can be enabled so authorised keys could be released automatically after user logging without need for selection of key(s) from the list and Master exemption can be enabled to assign unlimited authorisations to a user. Master exemption is usually assigned to system operator. Setting a value other than zero for the *fob limit* allows you to limit the number of keys a user can retrieve.

Note: Editing and deleting requires long clicking of an object (e.g. user) on the list.

## User importing from PR Master (RACS 4)

Users who were defined in PR Master software of RACS 4 system can be imported to avoid another manual enrolment of the same data on the level of RKD32 key cabinet.

1. Start PR Master program, select *Users* and then *Export* in order to export users with their card numbers and PINs to PRM.CSV file.
2. If it is necessary to preserve non-latin characters then open PRM.CSV file in Windows notepad and save with UTF-8 coding.
3. Copy PRM.CSV file on pendrive.
4. Connect the pendrive to MASTER USB socket (fig. 9).
5. Log in at the panel (default PIN: 9999#), select ⚙ and then *Configuration*
6. In the opened window select ☰ and then *Import users from PR Master*.

## Reservation

Key can be reserved by selection of ® area in the main menu (fig. 11) and then *Add* command. In the next window a time range must be specified and the option *Block key during reservation* can be selected. If the global option *Block reserved key* option is enabled (table 2) then all keys are blocked by default during reservation. Key which is reserved without blocking can be collected during reservation by any user who is authorised for the key and then such collecting is only accompanied by warning on ongoing reservation. User who is assigned with authorisation which has the option *Key reservation override authorisation* can collect reserved keys without limits including keys which were reserved with blocking.

# 5. CONFIGURATION VIA WEB BROWSER

RKD32 key cabinet can be remotely configured and managed via web browser. In such scenario it is necessary to define parameters in section WWW settings (table 2). The communication with MD70 panel can be in Ethernet network or Wi-fi network. The IP address of the panel in LAN/WAN is configured by means of Ethernet app after exiting RAACA app with the command *Show launcher* (table 4). Prior to establishing connection with the RKD32 it is necessary to enter IP address and communication port (8888 by default). The port may require unblocking in firewall and/or antivirus software.

Note: Configuration via web browser requires license purchase. You can verify if your RKD32 has the proper license selecting *License file* command (table 4).

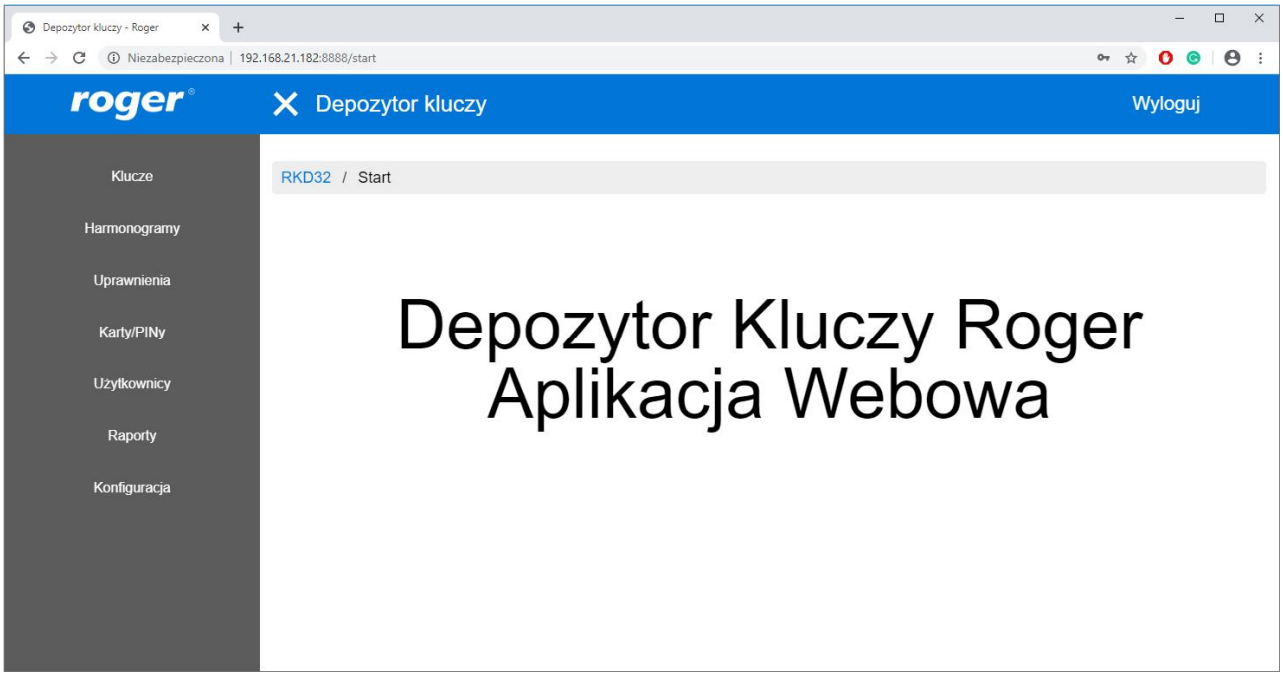



Fig. 14 RKD32 web app

# 6. CONFIGURATION IN NETWORK MODE

RKD32 key cabinet can be remotely operated in network mode. In such scenario, the configuration and management of keys and users is performed on the level of VISO software from RACS 5 system and RKD32 users can use the same factors (e.g. Mifare cards, PINs) as in access control system.
Prior to connection with RACS 5 system the key cabinet must be configured in regard of parameters given in section *RACS 5 settings* (table 2). Further configuration and management of key cabinet is explained in AN042 application note which is available at www.roger.pl

Note: Configuration via web browser requires license purchase. You can verify if your RKD32 has the proper license selecting *License file* command (table 4).

# 7. MANAGEMENT AND GENERAL ISSUES

## Admin password change

1. Log in at the panel (default PIN: 9999# or 12345*), select ⚙ and then *Configuration*.
2. Click *Admin password* and replace default 12345 password with your own.

## Default Master user password change (if available)

1. Log in at the panel (default PIN: 9999# or 12345*), select ⚙ and then *Cards, PINs.*
2. Select *Add PIN* in order to define new factor and return to *Settings* window.
3. Select *Users*.
4. Long click *USER_ADMIN* and then select *Edit*.
5. Click *Cards, PINs* deselect default *PIN_ADMIN* (i.e. 9999) and select your previously defined PIN.

## Programmable cards

By default the panel reads serial numbers (CSN) of MIFARE cards but it is possible to program cards with own numbers (PCN) in selected and encrypted sectors of card memory. The use of PCN prevents card cloning and consequently it significantly increases security in the system. In order to configure how the panel will read card numbers:

1. Log in at the panel (default PIN: 9999#) and select ⚙.
2. In the opened window select ☰ menu and then *MD70 settings* command.

3. In the next window click *Credentials settings*.

Note: If other than default card reading method is defined for MD70 panel then its reader cannot be used for fob enrolment and for quick fob return mode.

Mifare cards are programmed with RogerVDM software and RUD series reader (e.g. RUD-3-DES). Card programming is explained in AN024 application note which is available at www.roger.pl.

## Settings backup

RKD32 settings (including users) can be exported to file for the purpose of backup. Exporting and importing is also recommended in case of RAACA app update.

### Database export

1. Connect your pendrive to USB Master socket (fig. 9).
2. Log in at the panel (default PIN: 9999# or 12345*), select ⚙ and then ☰.
3. Select the command *Export database*.

### Database import

1. Rename previously exported database file into RKDdb.db and copy into pendrive..
2. Connect your pendrive to USB Master socket (fig. 9).
3. Log in at the panel (default PIN: 9999# or 12345*), select ⚙ and then ☰.
4. Select the command *Import database*.

## Emergency key release

RKD32 door and keys can be released when there is power supply shortage. In such case connect powerbank (min. 2A rated output) to USB cable (fig. 4 and 8) and release door and keys pressing DOOR and ROW-1/2/3/4 buttons on RKD board. The procedure must be done for each cabinet individually.

## Factory settings reset

In order to restore factory default settings:

1. Log in at the panel (default PIN: 9999# or 12345*), select ⚙ and then *Configuration*.
2. In the opened window select ☰ menu and then *Factory reset*.

## License upload

In case of RKD32 management via web browser or via VISO software (network mode) it is necessary to activate license on the level of key cabinet. You can verify your license selecting *License file* command (table 4). In order to upload purchased license place license file on USB disk or internal storage of device. Run “RKD receiver” app and import license.

## Remote technical support

Remote technical support by Roger specialist is available. In such scenario, key cabinet must be connected to Ethernet network or Wi-fi and it must be connected to Internet. After selection of *Remote support* command (table 4) Anydesk app is started. Reveal the number from the app to Roger technician so he could connect remotely. Then, accept the connection request from Roger technician on the RKD32 panel.

# 8. TROUBLESHOOTING

**Table 5. Troubleshooting**

| Issue | Solution |
|---|---|
| Key is inserted into slot but it is not on the list in RAACA app. | • Verify authorisations and schedules of current user.<br>• Verify if user with *Master exemption* can see the key on the list. |

| | |
|---|---|
| No power supply, cannot collect a key. | • See Emergency key release in section 7. |
| Cannot read key fob at MD70 panel. | • Key fob reading range is limited due to its size. Read the fob as in fig. 2. |
| Starting screen is not displayed on MD70 panel. | • Restart MD70 panel by switching power supply off and on or press the button as in fig. 13.<br>• Start RAACA app manually. |
| MD70 panel is not reacting for touching. | • Verify power supply.<br>• Restart MD70 panel by switching power supply off and on or press the button as in fig. 13. |

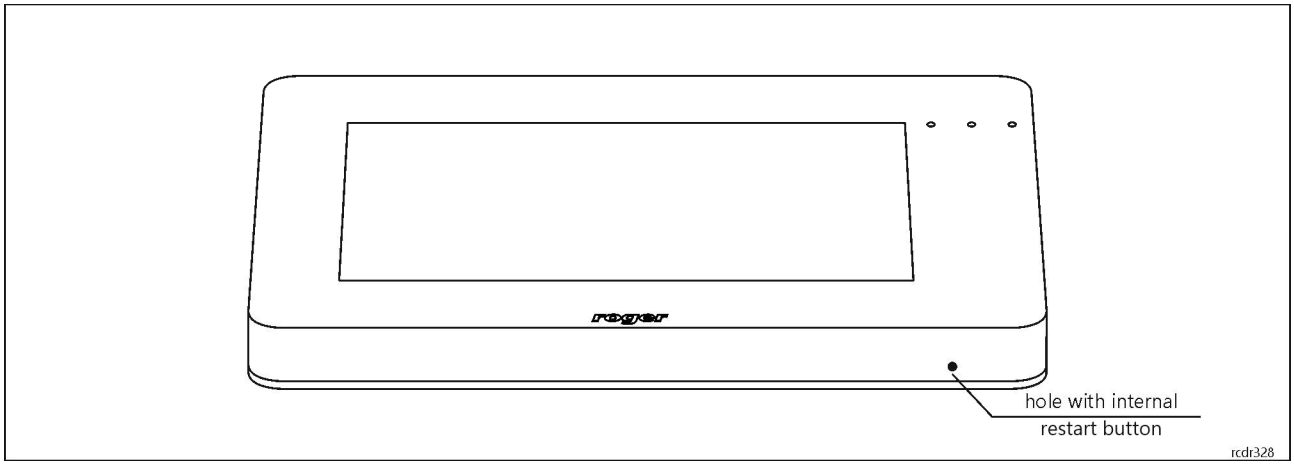



Fig. 15 MD70 restart button

# 9. SPECIFICATION

| **Table 6. Specification** | |
|---|---|
| Supply voltage | Nominal 12VDC, min./max. range 10-15VDC |
| Current consumption | 2.0A (1.1A average) |
| Tamper protection | Back cover opening and MD70 panel opening are signalled on 15VDC/1A output of MCX4D board |
| Identification methods | ISO/IEC14443A MIFARE Ultralight, Classic, Desfire EV1 and Plus proximity cards and PINs (4-16 digits) |
| Reading range | Up to 7 cm |
| Distances | Up to a 5 meters between RKD32 and RKD32EXT |
| IP Code | IP41 |
| Environmental class (acc. to EN 50133-1) | Class I, indoor general conditions, temperature: +5°C to +40°C, relative humidity: 10 to 95% (no condensation) |
| Dimensions H x W x D | RKD32: 535 x 935 x 183 mm<br>RKD32EXT: 535 x 675 x 183 mm |
| Weight | RKD32: 28 kg<br>RKD32EXT: 27,5 kg |
| Certificates | CE |

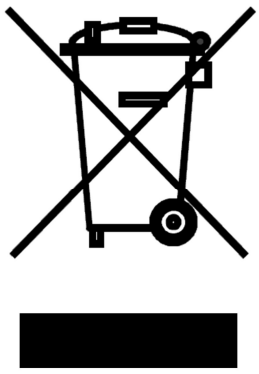
Note: Due to the production technology are permissible minor variations in the shade of the housing between production batches.

# 10. ORDERING INFORMATION

| Table 7. Ordering information | |
|---|---|
| RKD32 | RKD32: Electronic key cabinet with 7” touch control panel; 32 RFID fobs attached to keys by user; external 12V power supply; SG option for P2 class glass window; option RP for control panel installed separately on a wall |
| RKD32EXT | RKD32EXT: Electronic key cabinet without control panel; 32 RFID fobs attached to keys by user; external 12V power supply; SG option for P2 class glass window; operates as an extension unit connected to RKD32 main key cabinet |
| RKD32KF | RFID keyfob; 5 pcs in set |

# 11. PRODUCT HISTORY

| Table 8. Product history | | |
|---|---|---|
| Version | Date | Description |
| RKD32 | 05/2019 | The first commercial version of product |



This symbol placed on a product or packaging indicates that the product should not be disposed of with other wastes as this may have a negative impact on the environment and health. The user is obliged to deliver equipment to the designated collection points of electric and electronic waste. For detailed information on recycling, contact your local authorities, waste disposal company or point of purchase. Separate collection and recycling of this type of waste contributes to the protection of the natural resources and is safe to health and the environment. Weight of the equipment is specified in the document.

**Contact:**
**Roger sp. z o.o. sp.k.**
**82-400 Sztum**
**Gościszewo 59**
**Tel.: +48 55 272 0132**
**Fax: +48 55 272 0133**
**Tech. support: +48 55 267 0126**
**E-mail: biuro@roger.pl**
**Web: www.roger.pl**