Roger Access Control System

RKD32 Operating Manual

Product version: 1.0

Firmware version: 1.0.2

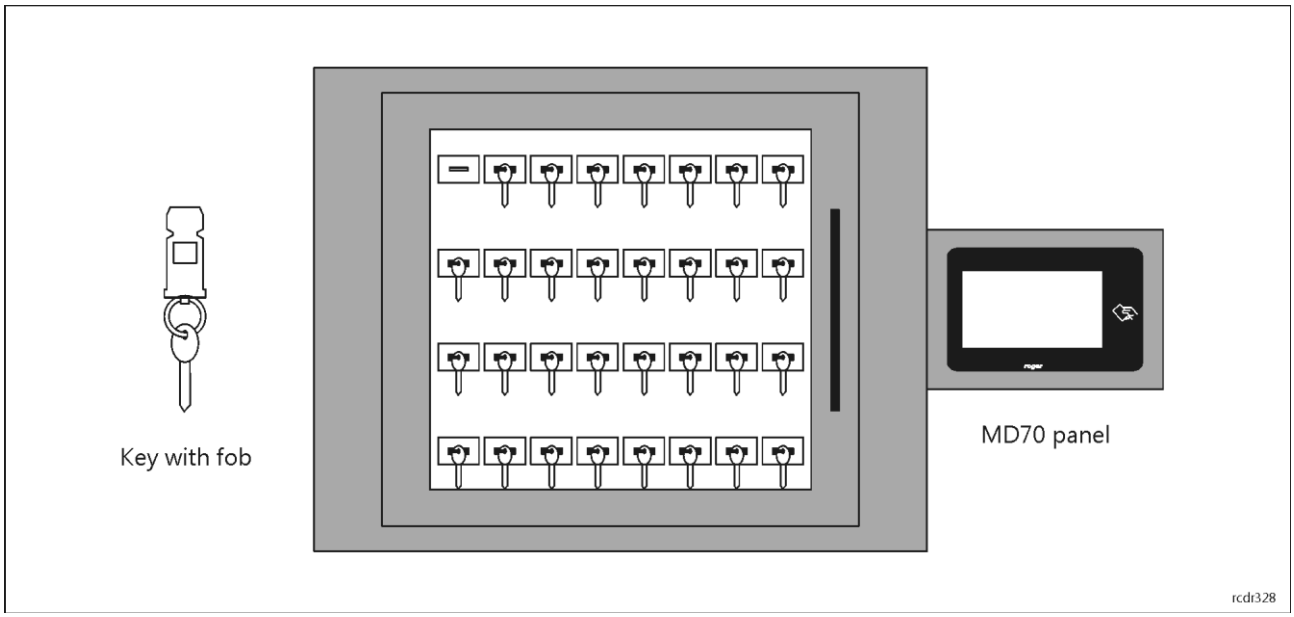
Document version: Rev. B

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 and the control of cabinet are performed with MD70 panel which is equipped with graphic touchscreen and Mifare card reader. 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. User can be identified at the panel with Mifare proximity card or PIN. 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.



Characteristics

- Electronic cabinet for 32 keys
- Up to 4 cabinets operated as single system
- Firm attachment of key to fob by user
- Additional seals or protections for attachment of key to fob are possible
- Mechanical locking of key inside the cabinet
- RFID fob attached to key
- Access to keys limited by schedule
- Registration of key collecting and returning
- Free access to keys in office mode
- Key reservations
- Key status information
- Control with 7” touchscreen panel
- Metal enclosure with glass door
- Emergency key collecting after cabinet opening
- Standalone or networked operation in RACS 5 system
- 12VDC power supply

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. 2). Battery cannot be directly connected to RKD32 so the emergency supply (battery, UPS) must be ensured on the level of buffer power supply unit. In case of lack of power supply, the RKD32 can be emergency supplied from powerbank connected to USB

cable which is connected to RKD board in order to offer emergency open of cabinet door and key locks inside cabinet.

Cabinet

RKD32 cabinet is made of stainless metal sheet which is powder painted in RAL7016 (anthracite grey). Cabinet's door is equipped tempered glass. The dimensions are given in fig. 2.

RFID fobs

The RKD32 include RFID fobs which are attached to keys or other supervised items. When a key is placed on a ring and the ring is manually inserted into a fob without any specialized tool 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 wheel so that only the oval part is visible. After joining, verify the correctness of the mechanism latch by attempting to pull the key from the key fob.

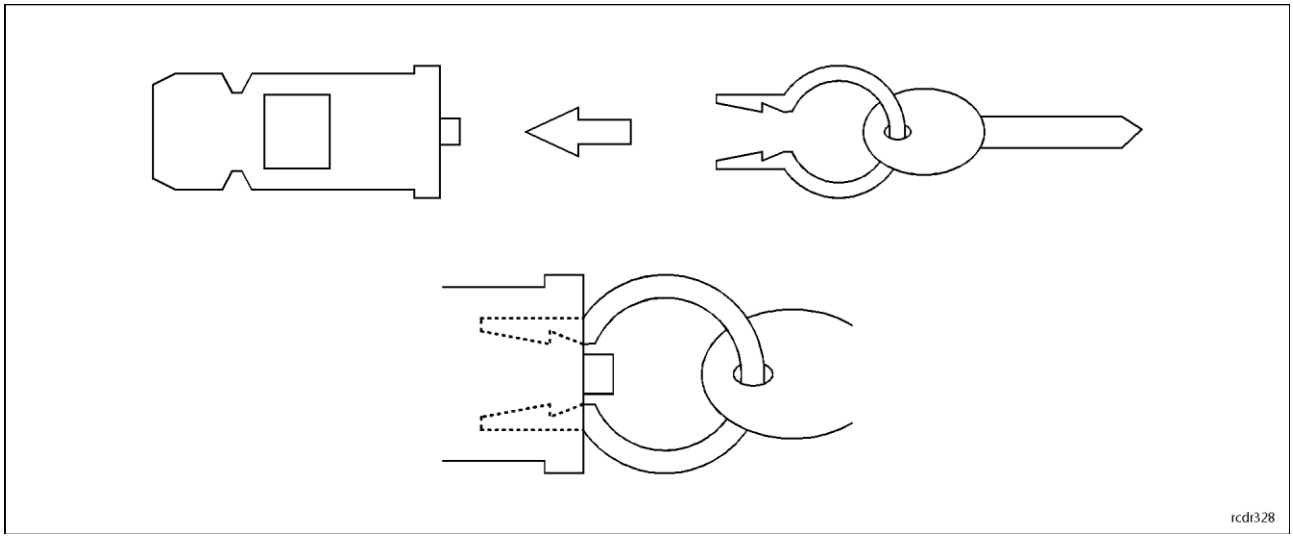


Fig. 1 RFID fob and key

MD70 panel

Management and configuration of RKD32 are performed with 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 main cabinet (RKD32) using RJ45 sockets on RKD boards (fig. 5). Connections can be ensured with U/UTP cat 5 cable but the maximal cable length cannot exceed 3m. MD70 panel is equipped with graphic touch screen, sounder and Mifare 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 proximity cards
- PINs

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 4 and in AN024 application note which is available at www.roger.pl.

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

External reader

User identification is possible not only with MD70 reader but also with additional external reader with Wiegand interface. In such scenario the MCX102 expander with ID=915 address should be mounted on DIN rail inside the cabinet. The reader must be connected to IN1 and IN2 terminals of the expander while the MCX102 expander must be connected to RS485 A and RS485 B terminals of MCX4D expander.
It's also possible to use MCT or RFT series readers, which enables the use of other standard of proximity cards or biometric authentication (RFT1000).

Tamper detectors and door alarms

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 output of MCX4D board (fig. 6). 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.

2. INSTALLATION

Two people are required for the installation of RKD32. Before installation, turn both locks shown in fig. 1 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. 4 using holes shown in fig. 3. When RKD32 is mounted on back cover as in fig. 4 then both locks will latch automatically. The communication with RKD32 (in RACS5 mode) can be ensured by Ethernet cable of Wi-Fi connection (more information in MD70 user manual).

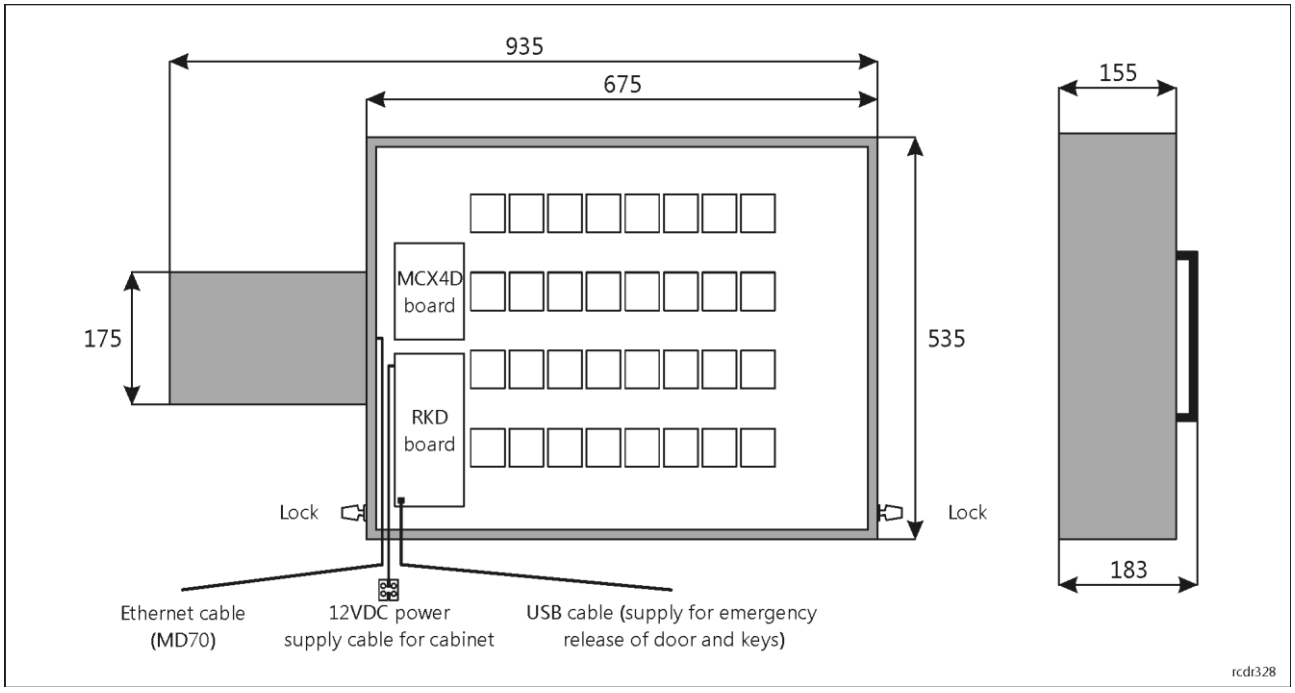


Fig. 2 Inside RKD32 with back cover removed

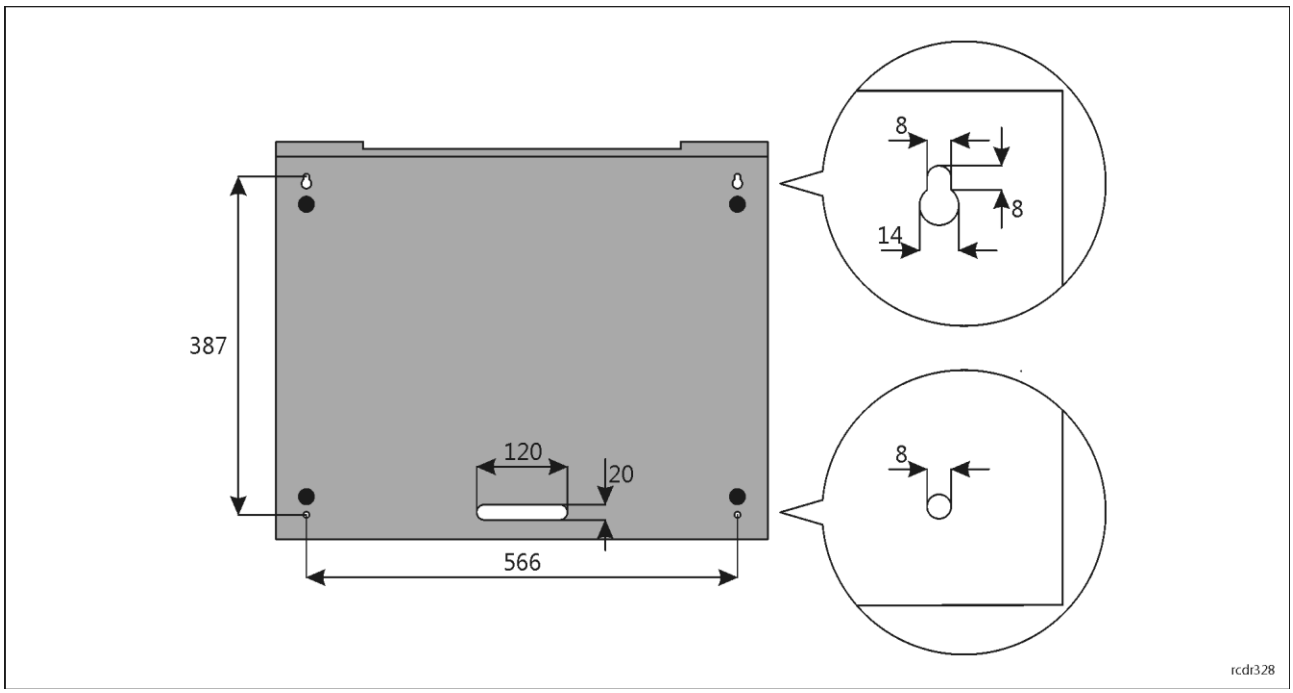


Fig. 3 Back cover

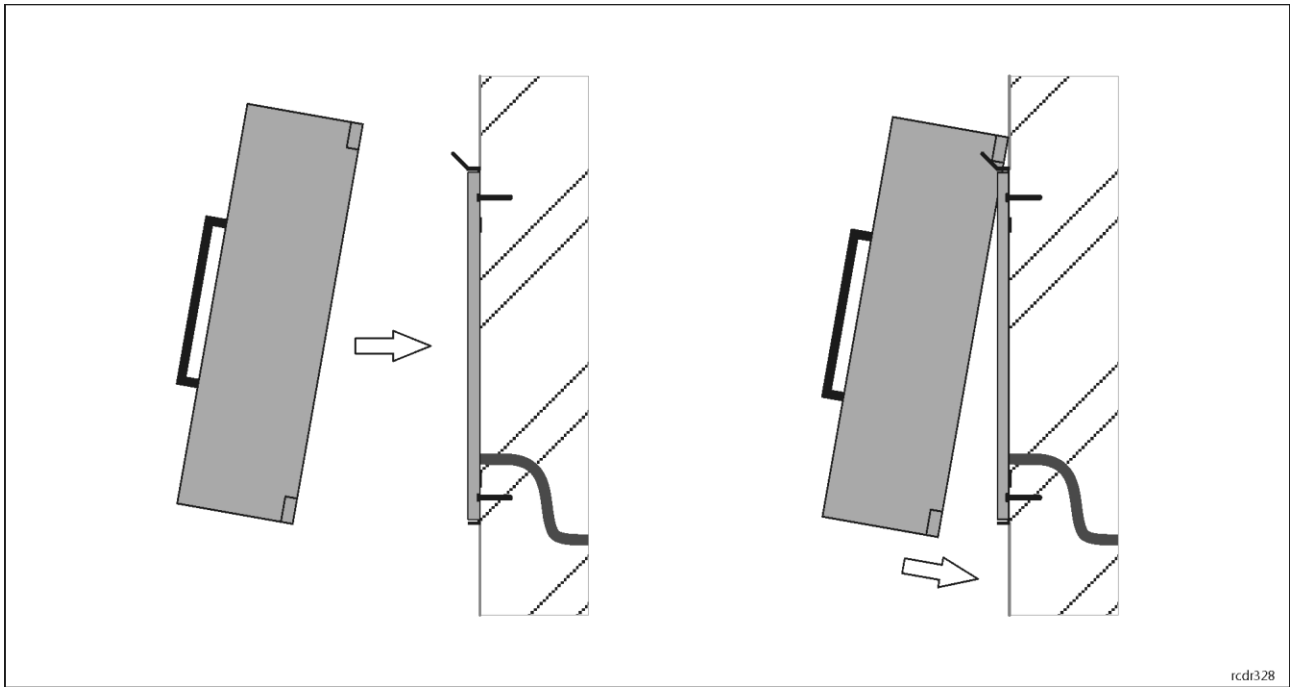


Fig. 4 Wall mounting

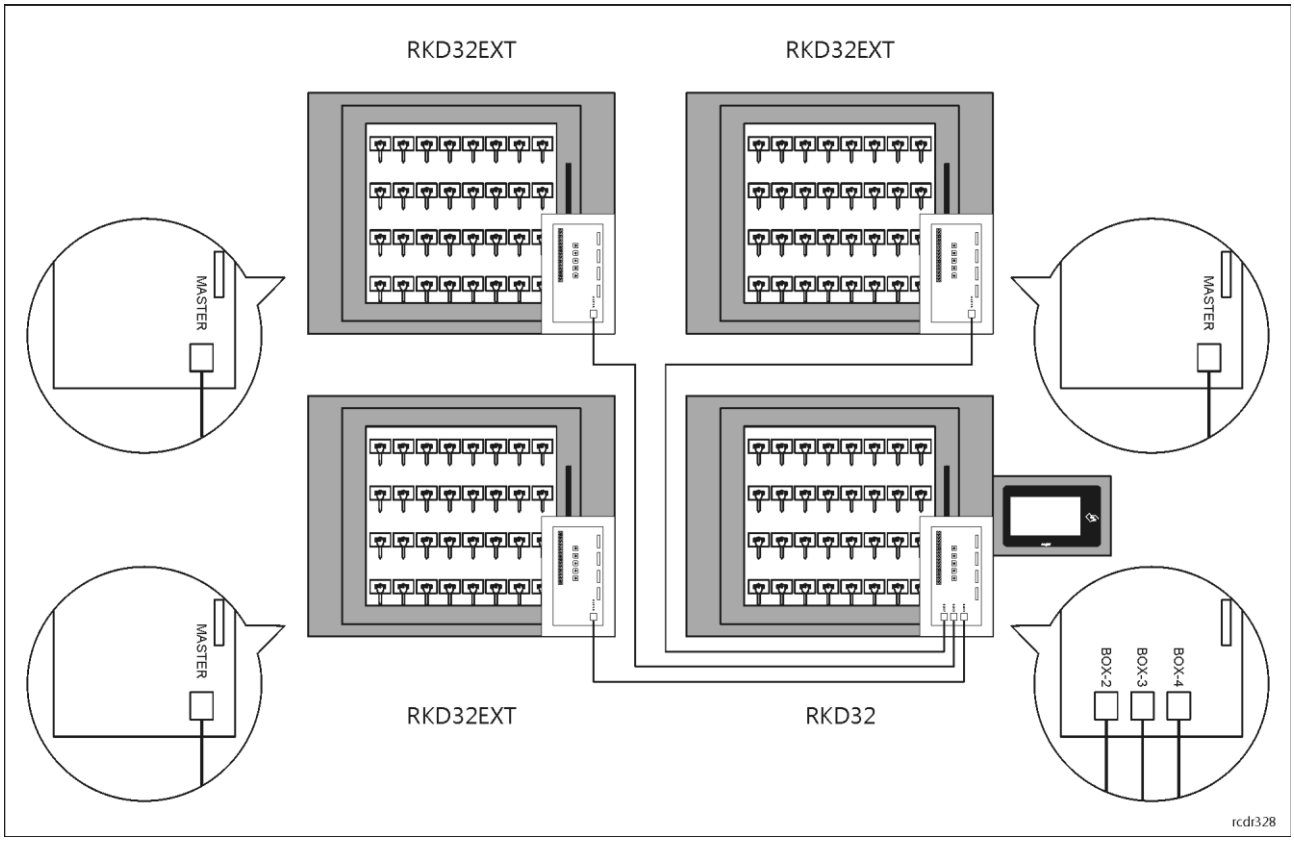


Fig. 5 Connection of additional cabinets (RKD32EXT) to main cabinet (RKD32)

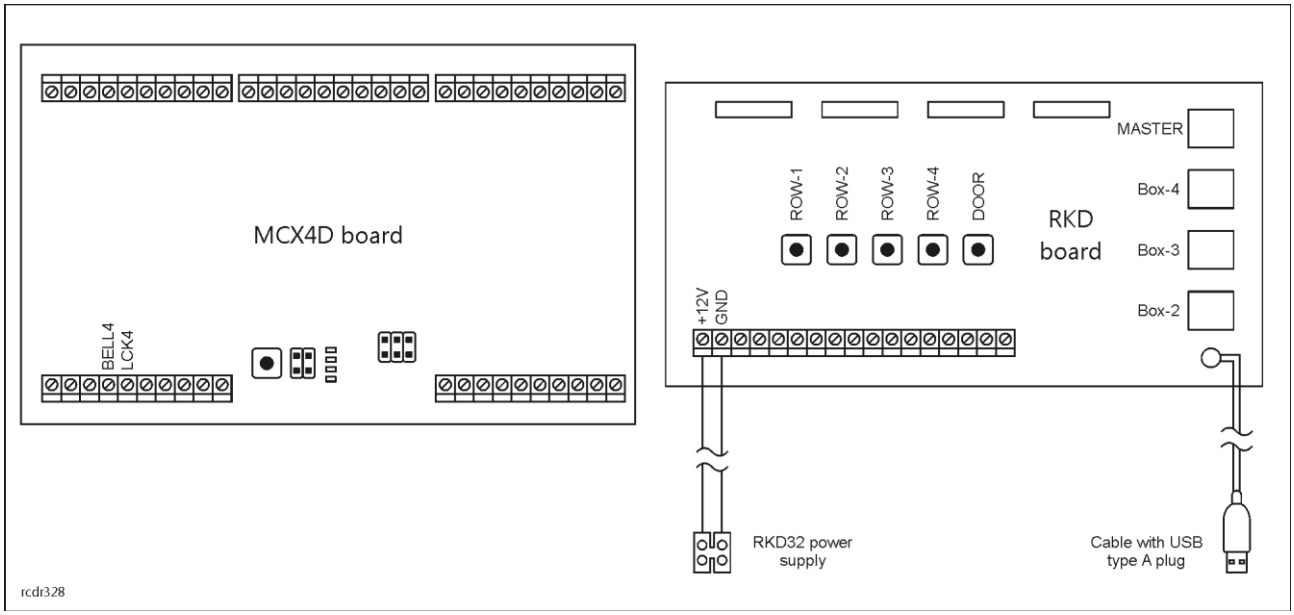


Fig. 6 RKD and MCX4D boards

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
MASTER	RKD32: USB type A socket for connection of pendrive RKD32EXT: RJ45 socket for communication with RKD32
BOX-2	RJ45 socket for connection second module (RKD32EXT), only at RKD32
BOX-3	RJ45 socket for connection third module (RKD32EXT), only at RKD32
BOX-4	RJ45 socket for connection fourth module (RKD32EXT), only at RKD32

3. RKD32 APP

After connection of power supply, the MD70 panel will start RDK32 app. When started for the first time the panel will offer to create default Master user with 9999 password. Then app can be accessed with 9999# password (if created) or with 12345* administrator password. Both default passwords should be changed in the next steps as explained further in the manual.
The administrator account is intended for the installer or the person who manages the system for maintenance and service purposes; daily service and change of the depository configuration should be done by means of a user with the appropriate authorization.

Caution: Both default passwords should be changed to your own passwords as described later in this manual.

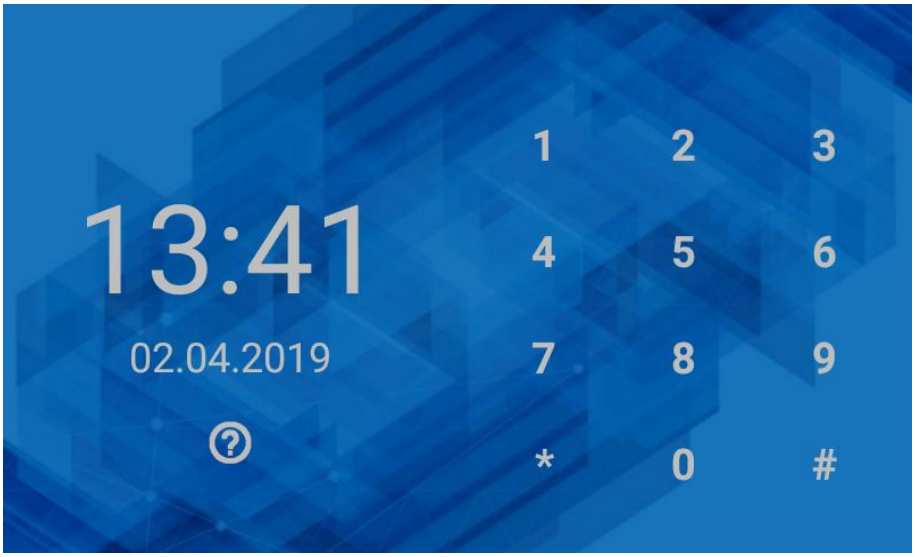


Fig. 7 Default starting screen

When in top right corner is selected then office mode is started after returning to starting screen. In office mode door lock and key locks are indefinitely released.
When is selected then events registered in a system are displayed, including history of key collected and returns.
When is selected in top right corner then statuses of keys in the system are displayed.
When is selected then settings window is displayed as in fig. 9.

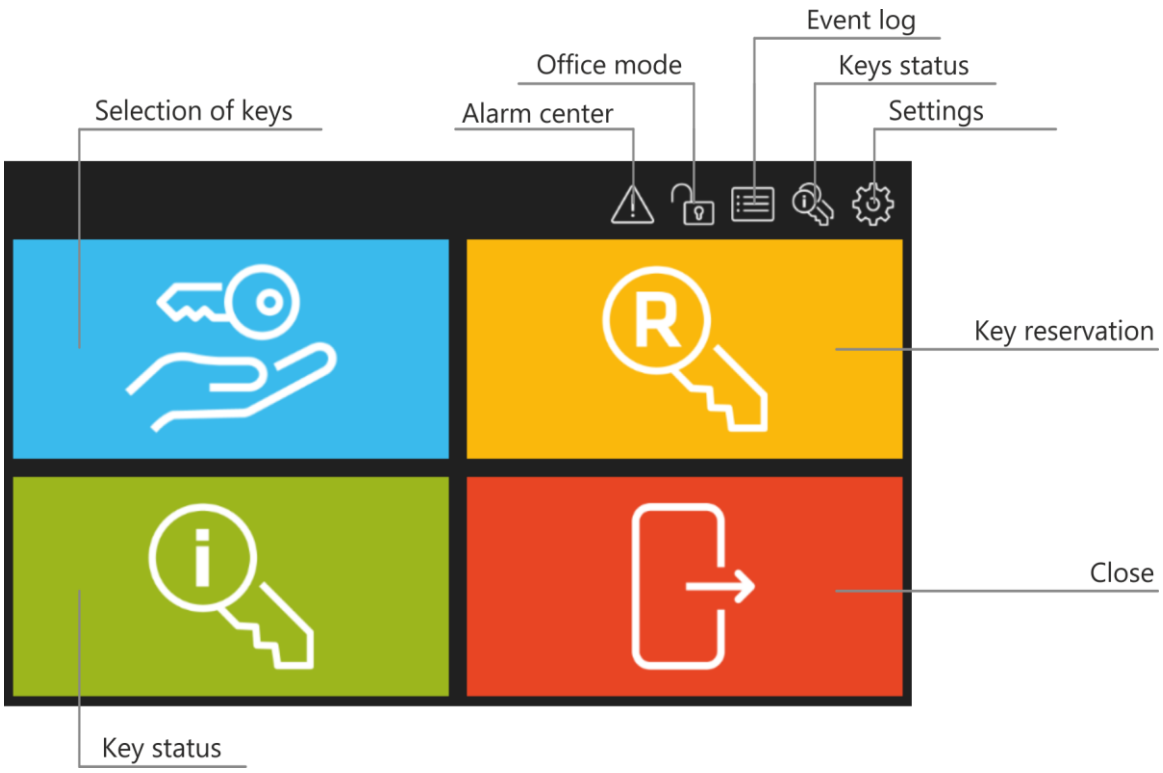


Fig. 8 Main menu

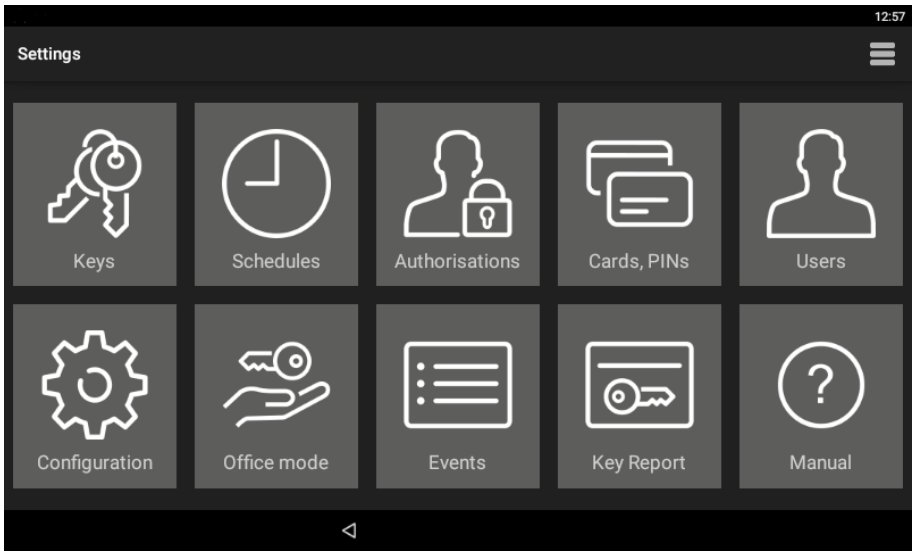


Fig. 9 Settings window

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 Internal zone allows the implementation of the *key anti-passback* function. The user can get a key from another zone only when he returns all keys. The internal zone is intended for keys that should stay as short as possible outside the cabinet (eg. archive).
Defining the key return time allows you to control the timely return of the key. After exceeding the indicated time, an "Invalid key return date" event is generated in the Alarm center.

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 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. When card is enrolled then 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. Additionally, quick key return mode and Master exemption i.e. all possible authorisations can be selected 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.
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 return a key. 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.
Reservation	
Block reserved key	Parameter enables automatic key blocking 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.
Owner	Parameter specifies owner/operator of the RKD32. The name is displayed in all reports.
RACS 5 settings	
These options are not supported in standalone operation of RKD32.	
Email account	
Address	Email account which is used for sending key reports events.
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.
Address 1	Recipient email address.
Address 2	Recipient additional email address.

Table 3. Commands in ☰ menu in Configuration window	
About	Command displays change log.
License	Command displays license agreement for Roger software.
Select wallpaper	Command enables indication of custom wallpaper (800x480px, *.jpg format) for MD70 starting screen. Additionally the parameter *Custom wallpaper* in *Configuration* window must be enabled.
Office Mode schedule	Command enables assignment of schedule to office mode. The schedule can be defined after selection of *Schedules* in *Settings* window.
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.
Factory reset	Command enables to restore factory settings.

Office mode
When selected then office mode is started after returning to starting screen. In office mode door lock and key locks are indefinitely released. Office mode can be automatically switched on and off by schedule, which can be defined by selection of *Schedules* in *Settings* window. The schedule is assigned to office mode by selection of *Office mode schedule* command in ☰ menu in *Configuration* window.

Events
When selected then list of registered events is displayed including events related to key collecting and returning. The same window can be started by selection of icon in the main menu. 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.

Alarm center
When selected then list of alarm events from the selected time period is displayed. Clicking on the event confirms the alarm. In the main window, the color of the Alarm Center icon determines the status:

- White: no unconfirmed alerts,
- Orange: There are historical alarms in the device's memory,
- Red: At least one unconfirmed ongoing alarm.

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 RKD32 user manual is displayed on MD70 screen.

Menu ☰ in Settings window
Menu ☰ in window shown in fig. 9 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 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.
Export database	Command enables to make backup.
Remote support	Command enables to establish remote connection with MD70 panel in computer network.

4. CONFIGURATION AND MANAGEMENT

Quick configuration

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 ☜ or insert fob into one of occupied slots.
5. 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 key blocking override.

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 getting key and Master exemption i.e. all possible authorisations can be assigned to a user. Master exemption is usually assigned to system operator.

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

Admin password change

1. Log in at the panel (default PIN: 9999# or 12345*), select and then *Configuration*.
2. Long 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.

Management

Key getting

1. Log in at the panel and in the main menu (fig. 8) select blue field with the icon .
2. Select key for getting from the list. The list is limited to authorisations assigned to the user.
3. Selected keys will be released and highlighted in green.

By entering the name of the key at the top of the screen you can filter the list of keys to quickly find its location. In addition, it is possible to unlock all available keys.

Quick get key

If during the configuration of user the option *Quick get key* mode is enabled then in case of such user after login at the panel all keys resulting from authorisations will be automatically released and highlighted except for reserved keys which can be get manually by selection on the list if they are not blocked by their reservations.

Caution: In the quick get mode, it is not possible to retrieve keys from the internal zone..

Key returning

1. Log in at the panel with your card or PIN.
2. Insert key fob into any unoccupied slot.

Quick key returning

1. Log in at the panel with key fob.
2. Insert key fob into any unoccupied slot.

Quick key returning is available if the parameter *Quick key return mode* is enabled in *Configuration* window.

Key reservation

1. Log in at the panel and in the main menu (fig. 8) select yellow field with the icon .
2. In the opened window select *Add*.
3. In the next window select key, define time period and decide on key blocking during reservation.

By default, the maximal reservation time is 30h. The parameter can be changed in *Configuration* window. Additionally in the same window, default blocking of reserved keys can be enabled. User with Master exemption and user with the authorisation "Key reservation override authorization" can get blocked keys. In each case getting of reserved key is accompanied with the warning which must be confirmed on the panel.

Key status

1. Log in at the panel and in the main menu (fig. 8) select green field with the icon .
2. In the opened window select key to get information on its availability and possible reservation.

The access to key status is defined in the level of user's authorisation.

Office mode

In the office mode, door lock and key fobs are indefinitely released. Therefore keys can be taken without user identification on MD70 panel but key getting and returning are registered by the system. Office mode is activated by selection of icon in the top right corner of main menu or *Office mode* icon in *Settings* window. Office mode can also be switched on and off automatically by schedule.

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*.

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.

Emergency key release

RKD32 door and keys can be released when there is power supply shortage. In such case connect powerbank or charger to USB cable (fig. 6) and release door and keys pressing DOOR and ROW-1/2/3/4 buttons on RKD board (fig. 6). The procedure must be done for each cabinet individually.

5. SPECIFICATION

Table 5. Specification	
Supply voltage	Nominal 12VDC, min./max. range 10-15VDC
Current consumption	2,0A (1,1A average)

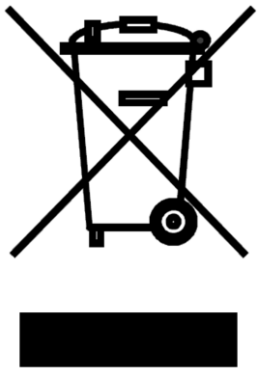
Tamper protection	Back cover opening and MD70 panel opening are signalled on 15VDC/1A output of MCX4D board
Identification methods	ISO/IEC14443A MIFARE Ultralight, Classic, Desfire EV1 and Plus proximity cards and PINs (4-16 digits)
Reading range	Up to 7 cm
Distances	Up to a few meter between RKD32 and 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 RKD32EXT: 535 x 675 x 183 mm
Weight	RKD32: 28 kg RKD32EXT: 27,5 kg
Certificates	CE

6. ORDERING INFORMATION

Table 6. Ordering information	
RKD32	Electronic key cabinet with control panel (32 keys)
RKD32EXT	Electronic key cabinet without control panel (32 keys)

7. PRODUCT HISTORY

Table 7. 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