

Roger Access Control System

RKD24CT-SE Installation Manual

Product version: 1.0

App version: 1.7.x

Document version: Rev. A

Contents:

1.	Design and application	3
2.	Characteristics	3
3.	Power supply	4
4.	Cabinet	5
5.	RFID fobs.....	5
6.	Control panel	6
7.	Identification.....	6
8.	Other proximity cards and biometrics	7
9.	Connection with the alarm control panel	7
10.	Release all keys from external system	7
11.	Installation.....	7
12.	Support for optional function.....	11
13.	RAACA app	11
14.	Configuration in standalone mode	18
15.	Configuration via web browser	19
16.	Configuration in network mode	20
17.	Management and general issues	20
18.	Troubleshooting	22
19.	Specification	23
20.	Ordering information	23
21.	Product history	23

This document is subject to the Terms of Use in the current version published on the website www.roger.pl. The manufacturer reserves the right to make changes to the product without prior notice. The product communicates only with another network device using a non-Internet-compatible communication protocol.

1. Design and application

The RKD24CT-SE electronic key cabinet enables the management of keys and other elements such as, for example, cards, remote controls devices, fobs, etc. The configuration in standalone mode is performed manually with control panel which is equipped with graphic touchscreen or remotely via web browser. The initial configuration in network mode is performed with control panel while further configuration in regard of users and authorization is performed in computer network on the level of VISO management software (RACS 5 system). Up to 3 cabinets can be operated from a single panel. In such a system, the RKD24CT-EXT or RKD32EXT cabinets are connected to the RKD24CT-SE electronic key cabinet. Prior to placing keys inside cabinet, they must be firmly attached to included RFID fobs. It is possible to assign users with authorization for particular keys. Typically, users are identified with PIN codes or Mifare proximity cards. When the key is retrieved, the appropriate container is released and the frame around the slot where the key is placed is highlighted in green.

RKD24CT-SE cabinet is delivered as a complete set with internal connections, and its installation requires only connection of power supply and wall mounting inside premises.

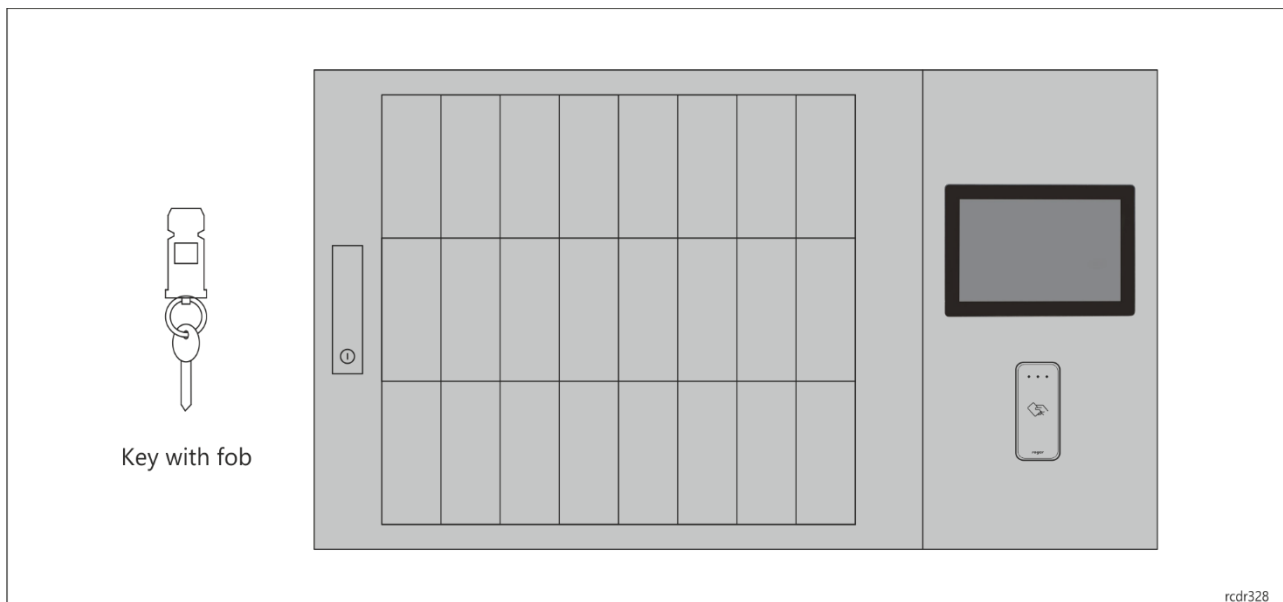


Fig. 1 RKD24CT-SE overview

2. Characteristics

- Operates standalone or as a part of RACS 5 access control system
- Local management from a touch panel
- Remote management from web browser
- Remote management from the RACS 5 access control system software (VISO application)
- Graphic panel with a 10" touch screen
- Built-in ISO/IEC 14443A MIFARE® Ultralight, Classic, Plus and DESFire EV1, EV2, EV3 card reader
- Support for secure Mifare sectors
- Possibility to connect an external reader with Wiegand interface
- Possibility to connect an external reader with a Roger RS485 interface
- 24 keys in the RKD24CT-SE main (Master) depositor
- 24 keys in the RKD24CT-EXT extension (Slave) depositor
- 32 keys in the RKD32EXT extension (Slave) depositor

- Possibility to connect 3 RKD24CT-EXT or RKD32EXT expansion depositors to the RKD24CT-SE 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
- Key containers blocked mechanically
- Contactless identification and key presence control via Mifare® proximity identifier
- Time dependent 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
- Key absentee to long indication
- Quick key return mode
- Fixed key position mode
- Light indication of slot with key
- Reservation of keys
- User activities reports
- Key usage reports
- Emergency unlocking of all keys via an external signal (e.g., from the fire protection system)
- Emergency unlocking of the keys
- Cabinet extension on site
- Cabinet door opening detection
- Cabinet enclosure opening detection
- RAL7016 color metal enclosure
- RKD24CT-SE dimensions: 600 x 969 x 182 mm
- RKD24CT-EXT dimensions: 600 x 677 x 182 mm
- Internal dimensions of key container: 55 x 115 x 73mm
- Weight RKD24CT-SE: 48,5kg
- Weight RKD24CT-EXT: 39kg
- MK option: Key to unlock the case in the Master Key system
- SDK
- Built-in 230VAC buffer power supply
- Space for 18Ah battery
- Post-warranty service
- No obligatory warranty maintenance required

3. Power supply

Control panel is equipped with power supply module, connection module and offers place for a 17Ah battery. For proper operation of the key cabinet system it is obligatory to install battery. A missing battery or its poor technical condition may cause disruptions in the operation of the device. To connect the power supply, unscrew the screw covered his housing and connect the 230VAC power cables and the protective conductor. After installation is complete inform the end user how to disconnect the mains power supply from the device.

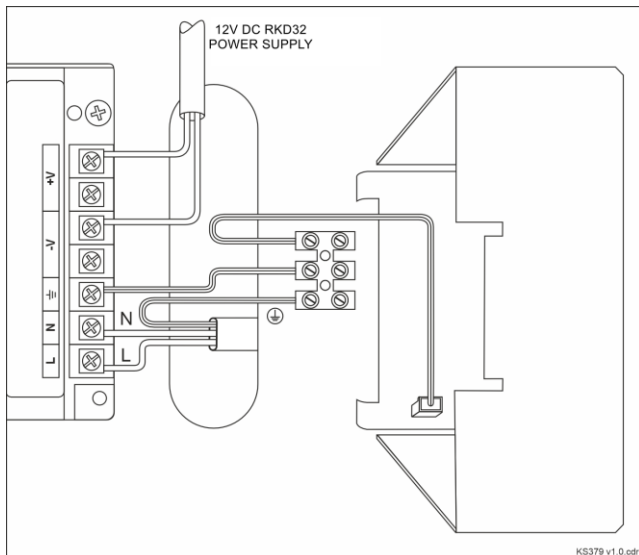


Fig. 2 Connection of 230VAC mains power to the terminal block.

RKD24CT-SE key containers can be released when there is power failure. In such case connect powerbank (min. 2A rated output) to USB port (under the emergency opening flap located on the left side of the housing) and release key containers pressing ROW-1/2/3/4 buttons on emergency board. The procedure must be done for each cabinet individually.

4. Cabinet

The electronic key cabinet is made of powder coated steel sheet in RAL7016 (anthracite grey). As standard, the cabinet is equipped with 24 containers, there are also reduced variants (8, 16 containers), which, if necessary, can be expanded to the full variant. The cabinet can be equipped with mechanical locks in the Master Key system. The dimensions of the depositor in the basic variant are given in fig. 6.

5. RFID fobs

The RKD24CT-SE includes 24 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 mounted on the ring then it can be attached to hole in the fob using wire and seal.

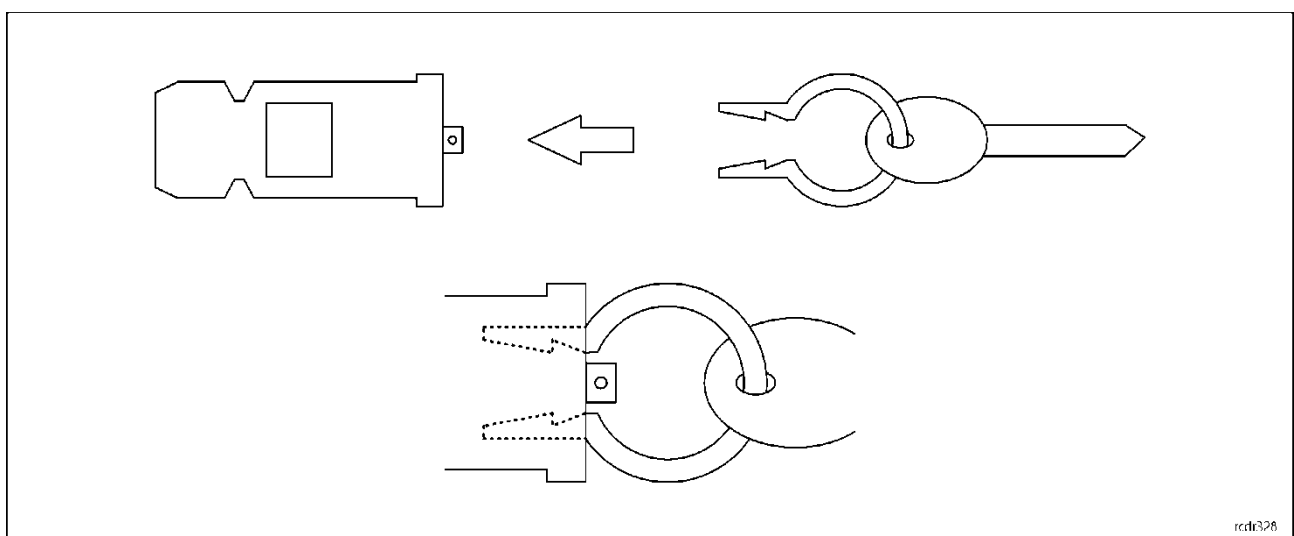


Fig. 3 RFID fob

6. Control panel

The electronic key cabinet is equipped with a 10" touchscreen. After connecting the power supply, the control panel will launch the RAACA application. Upon first launch, you will be prompted to create a default Master user with the password 9999. You can log in to the application using the password 9999# (if created) or the administrator password 12345*. The administrator account is intended for the installer or system manager, i.e., for maintenance and service purposes. Daily operation and changes to the controller configuration should be performed using a user account with the appropriate permissions.

Note: Both default passwords must be changed to your own passwords as described in section 7.

7. Identification

Following user identification methods are offered by the panel:

- MIFARE Ultralight/Classic/Plus/DESFire
- 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.

Note: Advanced configuration of the MCT terminal requires the RUD-1 interface and the RogerVDM application. If the card reading mode is changed to something other than the default, it will not be able to read the key fob when adding a key to the system or during a quick key return.

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 reader to open the door and return the key to unoccupied slot. The recommended orientation for fob reading at the reader and fob reading at RUD-3 reader is shown below.

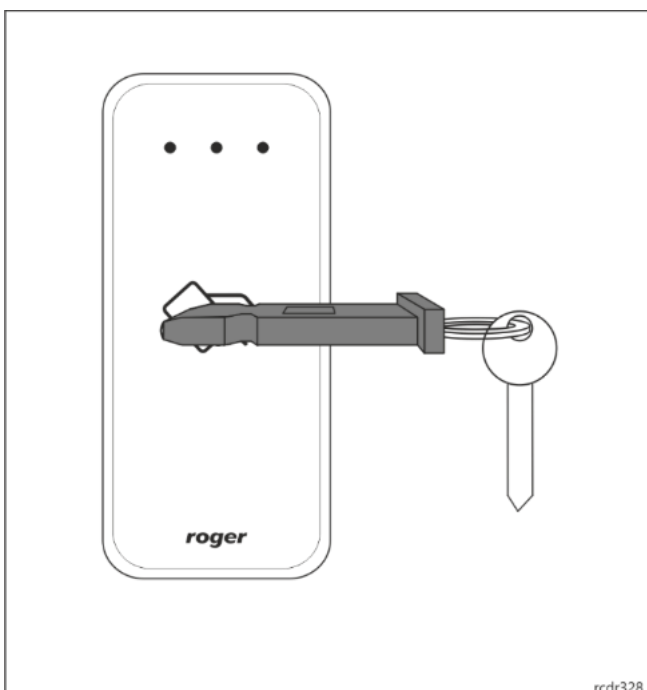


Fig. 4 Reading the key fob on the MCT reader.

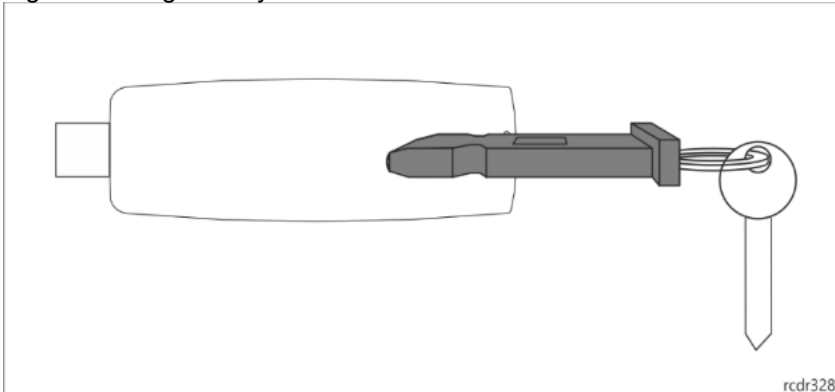


Fig. 5 RFID fob reading at RUD-3 reader.

8. Other proximity cards and biometrics

User can be identified at electronic key cabinet 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=101 address and connected to the RS485 A and RS485 B terminals of the readers' communication bus. If it is necessary to use other 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=101 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 connected to the RS485 A and RS485 B terminals of the readers' communication bus.



9. Connection with the alarm control panel

RKD24CT-SE is equipped with tamper detectors which enable detection of cabinet enclosure opening. Opening of RKD24CT-SE or touch panel enclosure is signaled on LCK4 transistor output of MCX4D (cabinet 1) board (fig. 11). Door ajar warning is signaled when user becomes logged out (manually or automatically) to the panel's starting screen. The warning is generated acoustically by touch 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 (cabinet 1) board is activated for 3 minutes or till door closing. BELL4 output is activated immediately when door is opened by force. Both LCK4 and BELL4 outputs can be connected to intruder alarm system, siren, or other alarm device.

10. Release all keys from external system

In case of fire alarm detection or any other emergency, the RKD24CT-SE can release all locks to enable key collecting by any person without authorization. Such release requires connection of fire alarm system output to DR3 screw terminal of MCX4D (cabinet 1) 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.

11. Installation

 Warnings 
<p>The installation can be done by qualified person only who poses all necessary certificates concerning connection/maintenance of 230VAC and low voltage networks.</p>
<p>The network circuit supplying the device must be equipped with an installation switch with a nominal current of 6A. Before servicing the device, disconnect it from the 230VAC network.</p>
<p>System earthing must be performed carefully, properly and effectively. It is forbidden to use device without properly performed and fully operated protective earthing.</p>

Follow the instructions included in the equipment to be installed in enclosure. Failure to do so may result in equipment damage, electric shock, fire, injury, or other consequences.

The electronic modules located internally in the cabinet enclosure are sensitive to electrostatic discharge (ESD). Before performing any work on the modules, ensure you are free of electrostatic charge e.g. by touching a grounded metal object with your bare hand.

Two people are required for installation of RKD24CT-SE. Before installation, turn locks shown in fig. 6 simultaneously to detach both back covers. 230V power supply with a protective wire should be connected to the control panel housing and connected to the power supply located under the cover secured with a screw. The protective conductor must be connected to the connection block. Behind the electronic modules there is a space for the one battery (up to 18Ah). The battery should be connected to the MCX4D module using the cables included in the set.

Between each depository cabinet and the control panel enclosures, the following should be carried out:

- 12V power cables (min. 1mm²) by connecting them to the appropriate 12V, GND terminals of the connection module,
- RJ45 cable (unshielded twisted pair cat.5) connecting to the appropriate BOX1-6 socket, the maximum length of the cable is 3m,

After making the connections, the enclosure should be attached to the base mounted on the wall as shown in fig. 9, while closing the enclosure locks will self-latch. Communication with the key cabinet (in network mode) and via a web browser can be realized via Ethernet (RJ45 socket on the control panel). Connect green plug to the socket on the connection panel and optionally connect the Ethernet cable and mount the housing on the base screwed to the wall.

Note: After changing the number of cabinets (e.g. adding RKD24CT-EXT), start device scanning (after logging in by a user with configuration rights to the Settings / Configuration / Detect devices) in order to properly handle all slots. RKD24CT-EXT must first be connected with the RJ45 cable to the connection module in the control panel housing, and then the power supply should be connected.

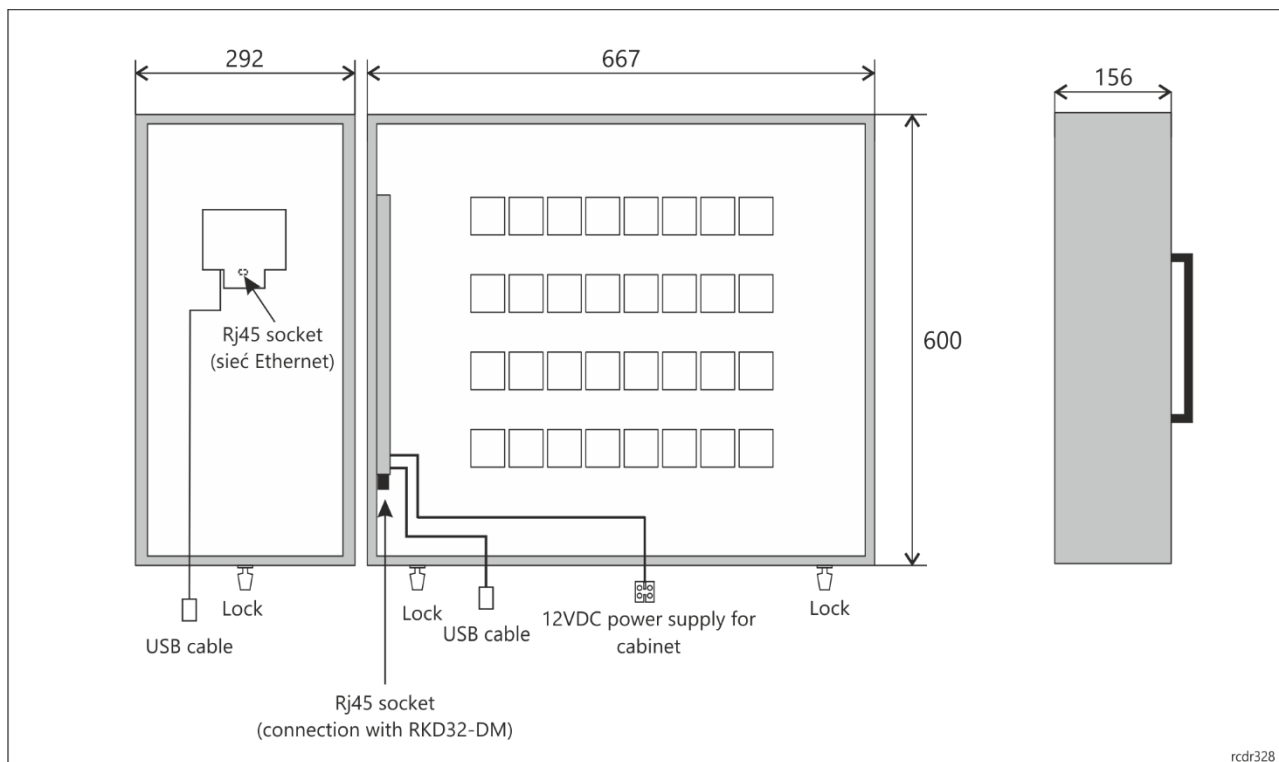


Fig. 6 Inside RKD24CT-SE with back cover removed

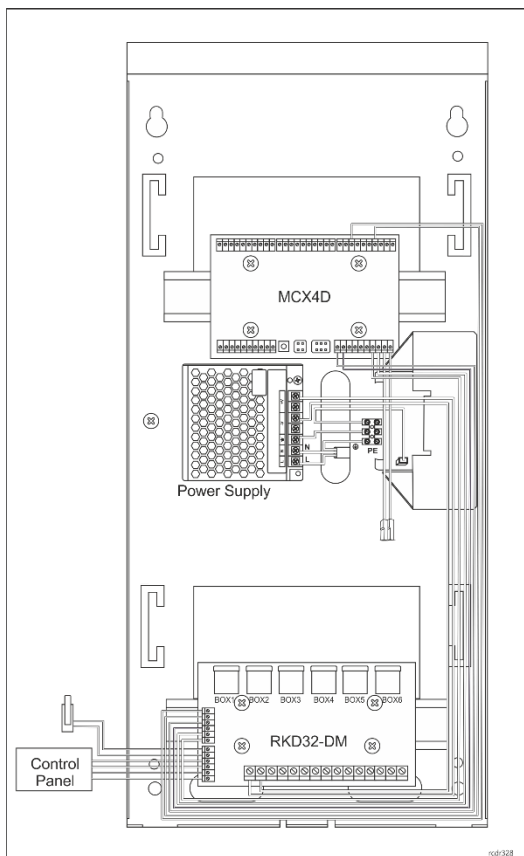


Fig. 7 Base of the control panel housing

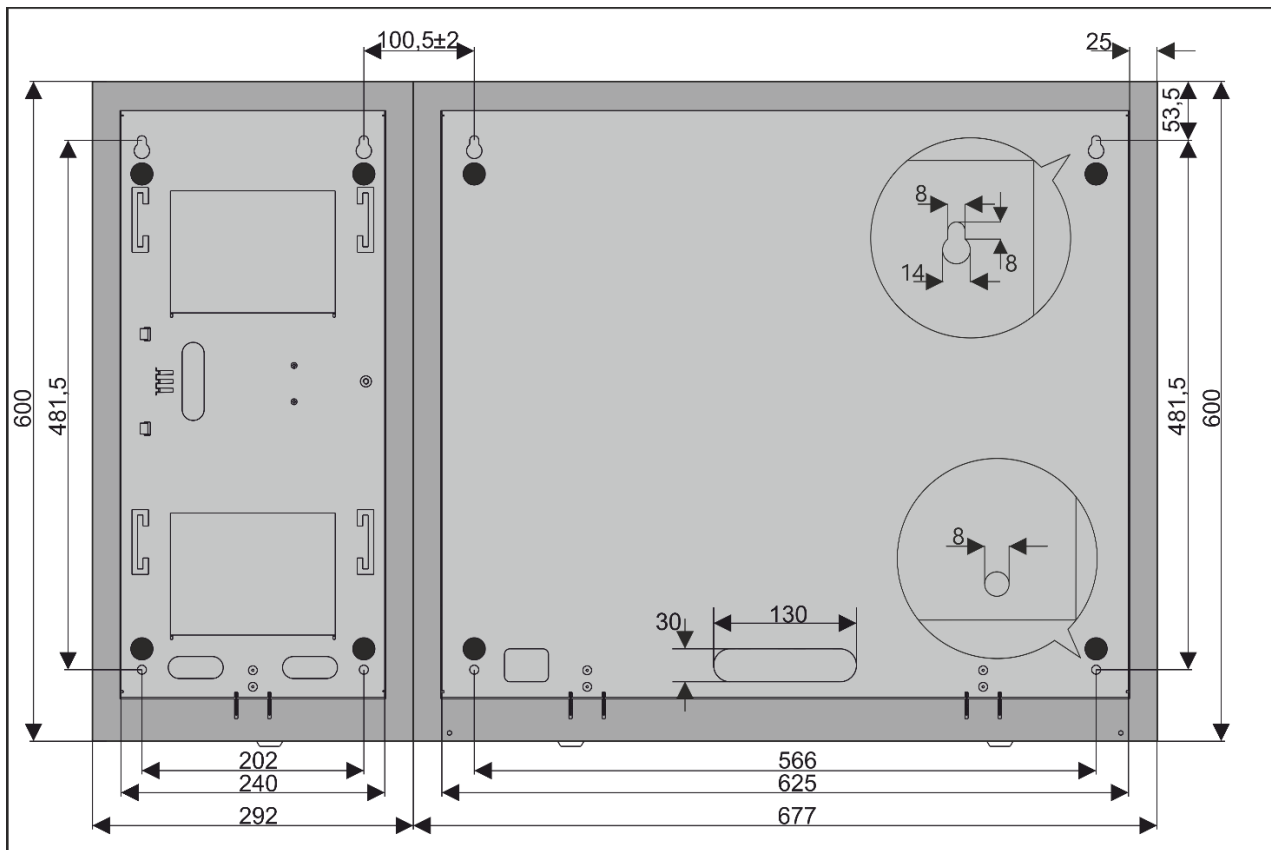


Fig. 8 Back cover

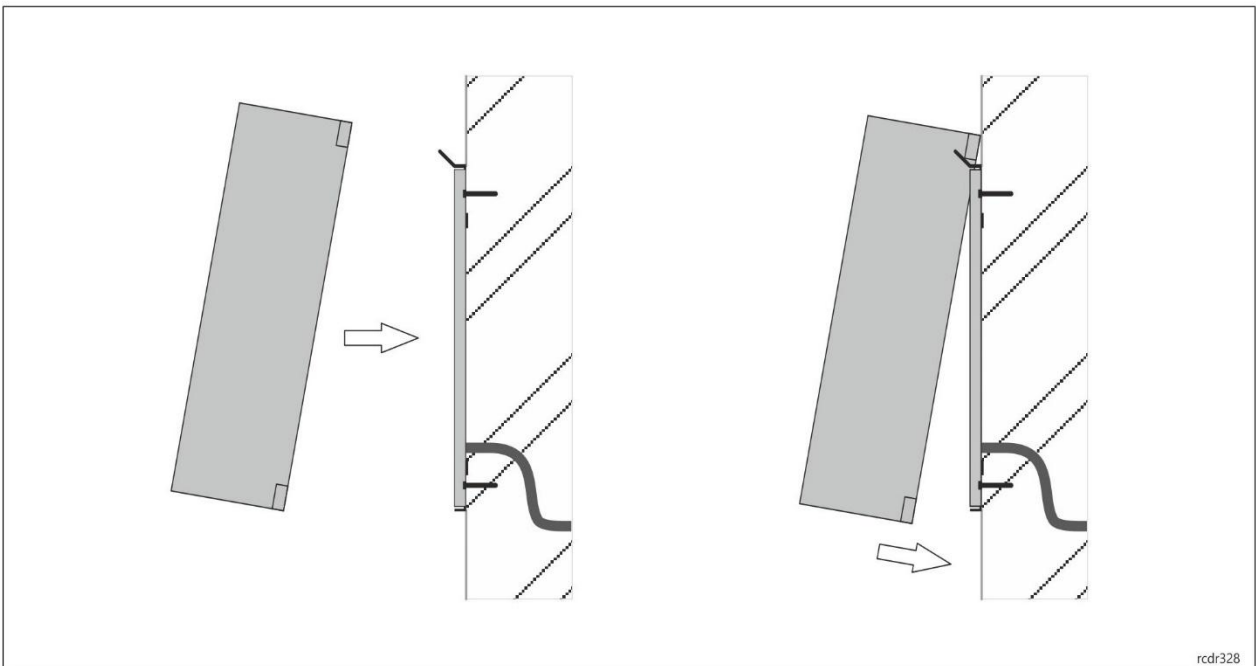


Fig. 9 Wall mounting

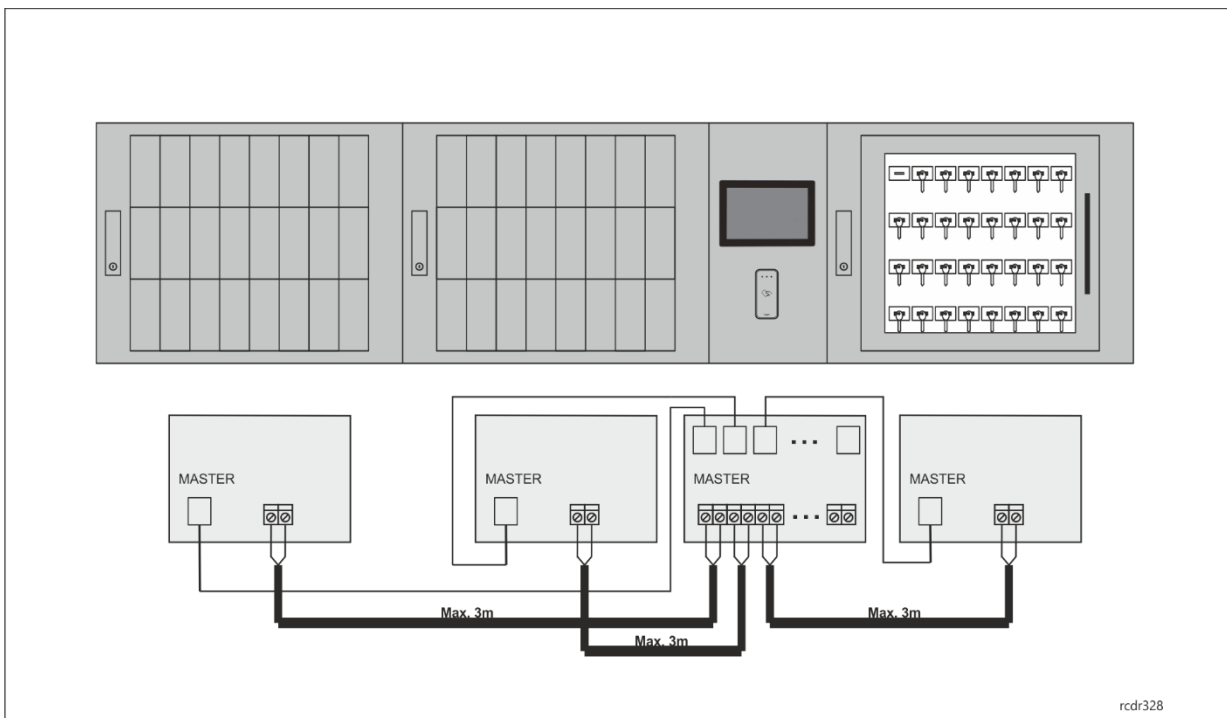


Fig. 10 Connection of additional cabinets (RKD24CT-EXT, RKD32EXT) to main cabinet (RKD24CT-SE)

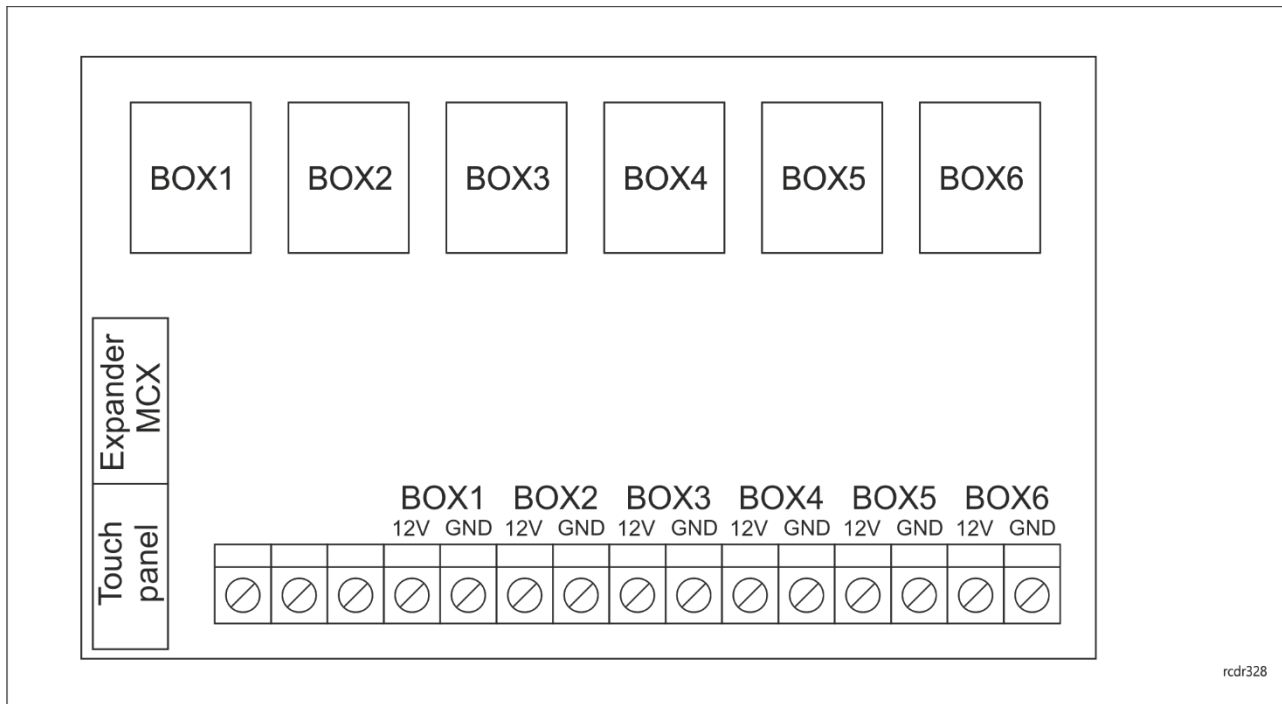


Fig. 11 Connection module in control panel housing

12. Support for optional function

In order to support additional functionalities, it is possible to connect executive elements (e.g. an alarm siren) to the outputs of the MCX4D expander located in cabinet no. 1. Additionally, the DR3 input line is dedicated to remote release of all keys (e.g. control from the fire protection system). The functions of the accessory I / O zones of the MCX4D expander are described in the table below, while the electrical parameters of the zones are available in the expander user's manual. In order to provide easy access to the terminal blocks, remove the cover of expander cables, and then unscrew the device fixing plate in order to slide the entire assembly out of the housing. After making the connections, install in reverse order.

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 to release all keys
MASTER	RJ45 socket for communication with connection module

13. RAACA app

After connection of power supply, the control 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 (**Note: not for use in RKD24CT**)
- Fixed fob position: each key is assigned a socket to return it to

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 RKD24CT-SE should be done by means of user account with the appropriate authorization.

Note: Both default passwords should be changed to your own passwords as described in section 17.



Fig. 12 Default starting screen

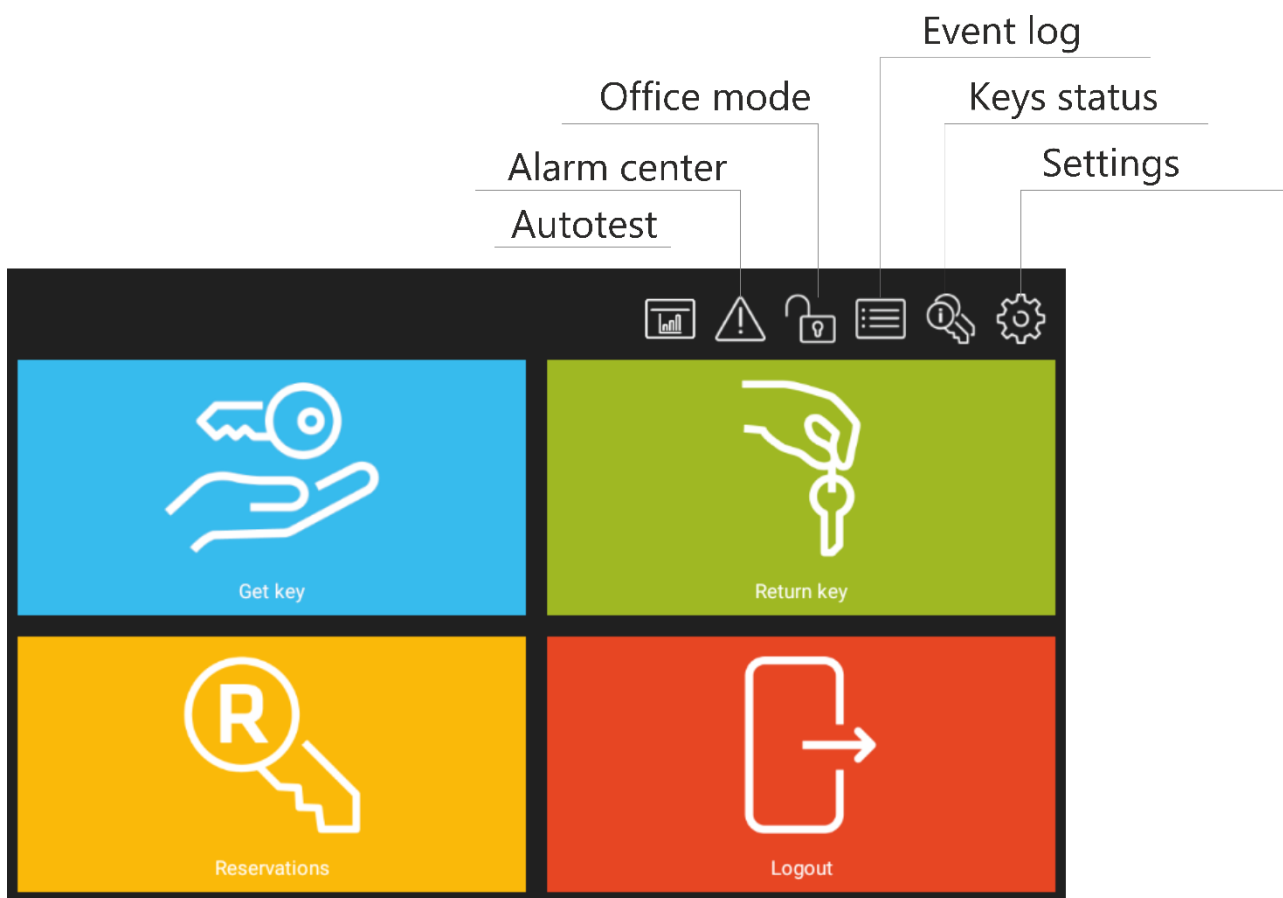






Fig. 13 Main menu

When  in the top right corner is selected then Alarm Center is started. It shows all alarm events (forced opening, tamper, etc.) registered by RKD24CT-SE in selected time range. The color 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 (depend of configuration) 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. 15) and assigned with the command *Office Mode schedule* (table 3).

Note: The office mode only applies to the RKD32EXT cabinets.

When  is selected then Report Center is started as in fig. 14. 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 RKD24CT-SE. Key Report and User Report enable us to display respectively events related to particular key and events related to particular user. In both cases events can be exported. The statistics allow you to check the times of renting keys in a given period of time. Events in Report Centre can be exported to pendrive connected to USB port, exported to internal memory or sent by email according to settings in *Configuration* window (table 2). Available formats are XLS (Excel) and PDF.

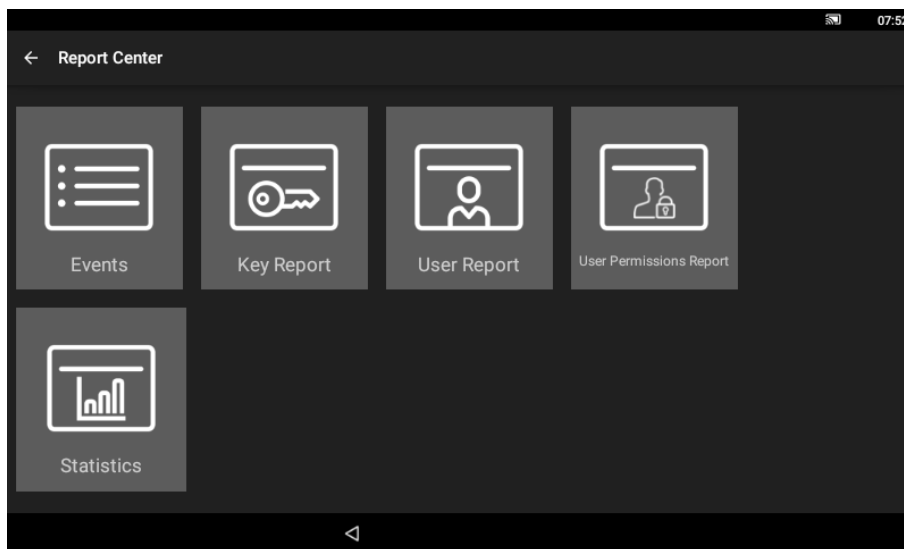




Fig. 14 Report Center

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

When  is selected then settings window is displayed as in fig. 15.

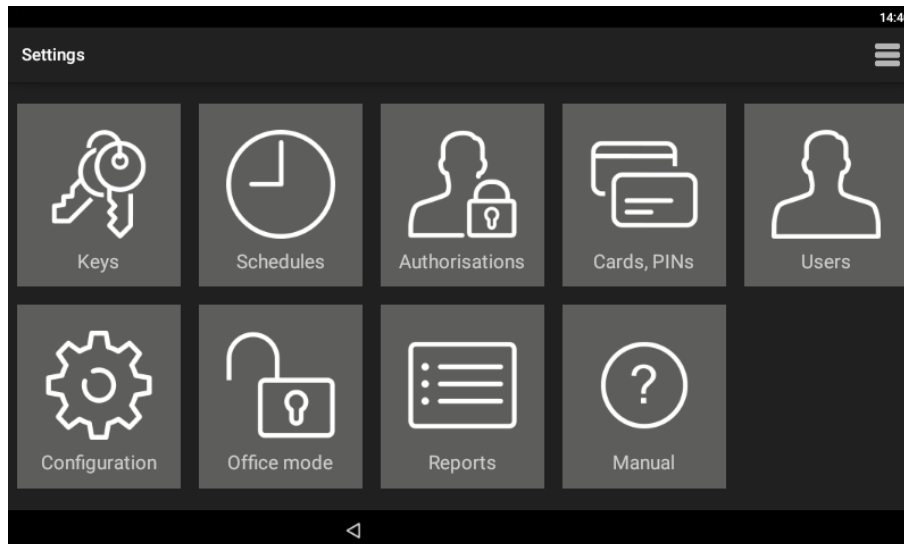


Fig. 15 Settings window

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 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 collect 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 collect a key, the application will ask you to read the card or enter the PIN, depending on the type of medium that was initially 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 authorizations and to manage office mode.

Authorizations

When selected then list of authorizations is displayed. New authorization is defined by selection of *Add* command. Editing and deleting can be done by long clicking of an object on the list. Authorization may concern access to keys, settings, event log, key status and may enable key reservation override. Authorizations 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 reader. Adding, editing and deleting is possible on the list. During card enrolment its number can be read at reader.

Users


When selected then list of users is displayed. Users can be assigned with cards, PINs and authorizations. The *Fob limit* option allows you to specify the total number of keys that the user can collect at the same time.

Value 0 means no limit. Additionally, *Quick key get mode* and *Master exemption* can be enabled. The first option enables to release authorized keys automatically when user is logged at control 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 authorizations 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 control 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 <i>Automatic logout time</i> 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 control 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.
Keys	
Quick key return mode	Parameter enables quick key returning after identification at the control 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 collecting 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 control 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.
Predefined comment content (1)	After you enter your text, it will appear as an option to check when reporting a comment.
Predefined comment content (2)	After you enter your text, it will appear as an option to check when reporting a comment.
Predefined 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, e.g. after entering the text "Mileage [km]", the user may enter the car's odometer reading when returning the key. 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: ON.
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 control panel. Custom wallpaper is indicated by <i>Select wallpaper</i> command in  menu. Range: ON, OFF. Default value: OFF.
Font colour	Parameter specifies colour of the font used on control panel starting screen. Range: Light, Dark, Orange. Default value: Light.
Voice prompts	Enabling the option activates playback of the voice messages. Default value: OFF.
Automatic reports	
Sending automatic email reports	The parameter allows you to send automatic event reports to an e-mail address. Default value: OFF.
Reports every 12 hours	The parameter allows you to send an event report twice a day. Default value: OFF.
Sending time	The parameter determines the report sending time within 24 hours. Default value: 18
RACS 5 settings	
RACS 5 mode	Parameter enables RKD32-SE 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
Device name (comment)	Parameter specifies the name of RKD32-SE which is then used in reports and logs.


MAC	Info box with MAC address.
WWW settings	
Web access enable	Parameter enables RKD24CT-SE 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 RKD-SE.
Login	Email account login for email sending by RKD24CT-SE.
Password	Email account password for email sending by RKD24CT-SE.
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.
Alarm notification	The parameter allows you to send email notifications about electronic key cabinet alarm events. Default value: OFF.

Table 3. Commands in  menu in Configuration window	
Select wallpaper	Command enables indication of custom wallpaper (800x480px, *.jpg format) for control panel starting screen. Additionally, the parameter <i>Custom wallpaper</i> (table 2) must be enabled.
Detect devices	Command starts the view of the list of devices in the RKD32-SE 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 <i>Schedules</i> in <i>Configuration</i> 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-SE 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 17.
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 17.

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. 13).

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. 13).



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 an abridged app manual is displayed on control panel screen.



Menu  in Settings window

Menu  in window shown in fig. 15 includes additional commands that are not available in the menu  displayed in *Configuration* window.


Show launcher	Command enables to exit app and start Android environment. Default password is admin.
System settings	Command enables configuration of Android system settings.
Files	Command starts app that enables file navigation at control panel.
About	Command displays change log.
License	Command displays license agreement for Roger software.
License file	Command displays information on uploaded RKD24CT-SE licenses in regard of network mode and management via web browser.
Third-party software licenses	The command displays information about the rules for using components or modules from another, external supplier.
Export database	Command enables to make backup of RKD24CT-SE settings on pendrive as explained in section 17.
Import database	Command enables to import RKD24CT-SE settings from file on pendrive as explained in section 17.
Show system buttons	The command shows the Android system buttons.
Hide system buttons	The command hides Android system buttons.
Remote support	Command enables to establish remote connection with control panel in computer network for the purpose of technical support by specialist as explained in section 17.

14. 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 reader  (fig. 4) or insert fob into one of free slots.
5. You can set other key options as needed.
6. Add 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 authorizations and office mode.


Authorizations

1. Log in at the panel (default PIN: 9999#), select  and then *Authorizations*.
2. In the opened window select *Add*.
3. In the next window name the authorization and click *Location* to indicate keys which can be collected by user with this authorization.
4. Optionally click *Schedule* and assign previously created schedule to limit the authorization to specified time periods.
5. Additionally, you can select if the authorization 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 reader. Similarly, as in case of fob, card number can be read at 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 control panel. Click *Authorizations* to assign previously created authorizations 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 authorized 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 authorizations 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 RKD 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 USB port (fig. 6).
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. 13) 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 authorized for the key and then such collecting is only accompanied by warning on ongoing reservation. User who is assigned with authorization which has the option *Key reservation override authorization* can collect reserved keys without limits including keys which were reserved with blocking.

15. Configuration via web browser

RKD24CT-SE 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 control panel can be in Ethernet network. Network parameters should be configured in the Android system settings. To do this,

exit the RAACA application using the System Settings command (table 4). Prior to establishing connection with the RKD24CT-SE 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 RKD24CT-SE has the proper license selecting *License file* command (table 4).

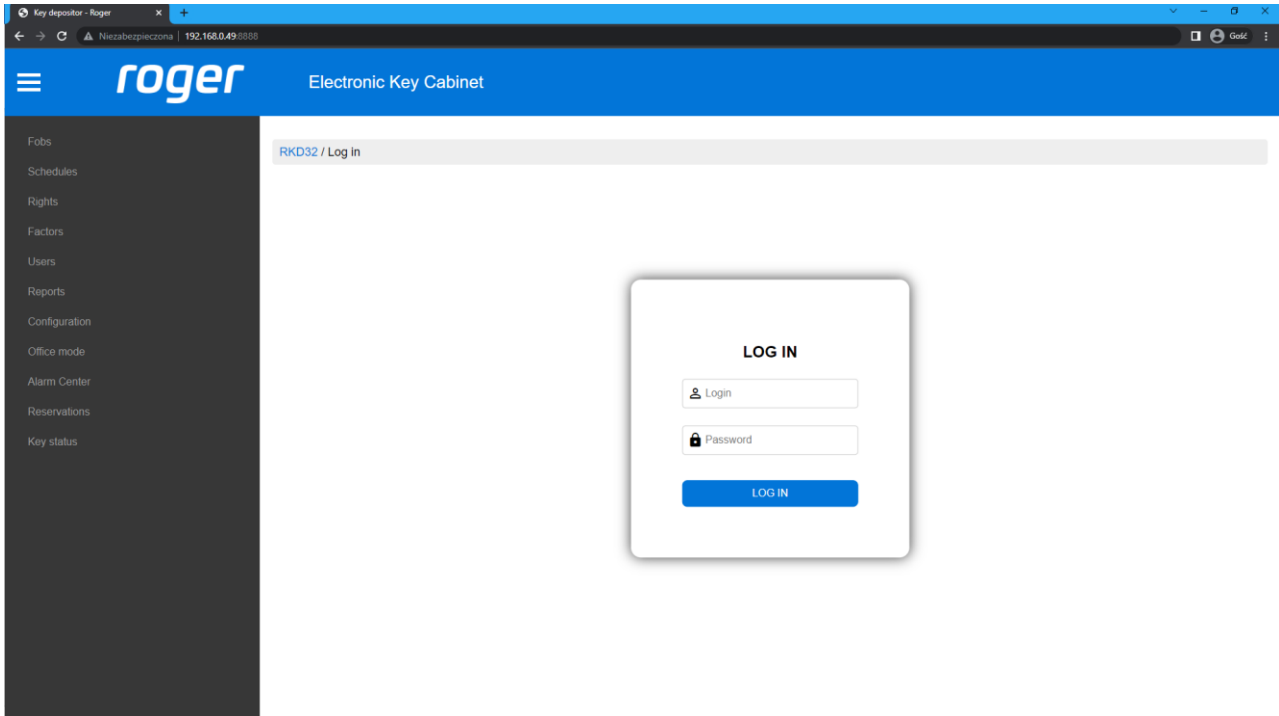


Fig. 16 RKD24CT-SE web app

16. Configuration in network mode

RKD24CT-SE 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 RKD24CT-SE 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: Remote management from the RACS 5 requires license purchase. You can verify if your RKD24CT-SE has the proper license selecting *License file* command (table 4).


Note: Network parameters should be configured in the Android system settings. To do this, exit the RAACA application using the Show launcher command (table 4) and go to system settings.

17. 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 reader reads the serial numbers (CSN) of MIFARE cards used to identify users on the reader. However, it is possible to configure cards by programming custom numbers (PCN) in selected memory sectors, including encryption. Using PCN numbers prevents unauthorized duplication of cards and thus significantly increases system security. To configure a different card reading method, connect the terminal via the RUD-1 interface to the RogerVDM application and configure the device according to the AN24 note.



Note: If a card reading method other than the default one is set on the reader, it will not be possible to use the key fob reading when adding the key to the system and when quickly returning the key.

Note: 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

RKD24CT-SE 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 port (fig. 6).
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 port (fig. 6).
3. Log in at the panel (default PIN: 9999# or 12345*), select  and then .
4. Select the command *Import database*.

Emergency key release

RKD24CT-SE key containers can be released when there is power failure. In such case connect powerbank (min. 2A rated output) to USB port (under the emergency opening flap located on the left side of the housing) and release key containers pressing ROW-1/2/3/4 buttons on emergency board. The procedure must be done for each cabinet individually.

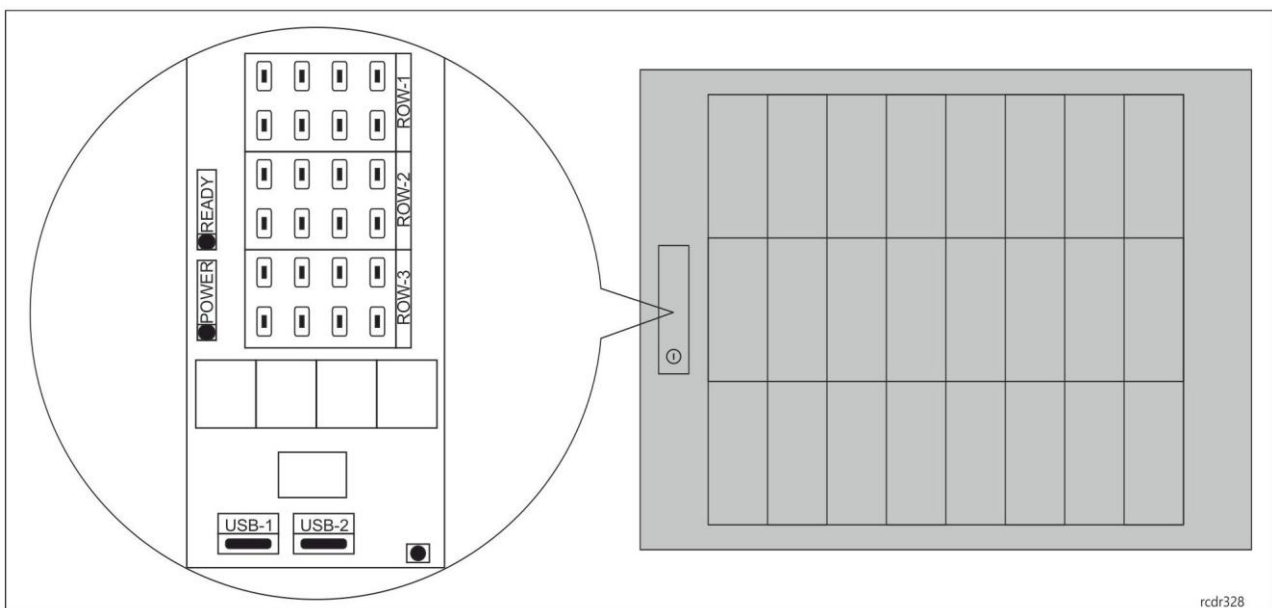




Fig. 17 Emergency opening module overview.

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

When using a web browser or the RACS5 system (VISO program - network mode), the electronic key cabinet must have the appropriate license installed. Current RKD licenses can be verified by selecting the License File command (Table 4). To install a license, place the license file on a USB drive or the root directory of the internal memory, then run the "RKDreceiver" application (available after exiting to the launcher) and import the license.

Remote technical support

Remote technical support by Roger specialist is available. In such scenario, key cabinet must be connected to Ethernet network 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 control panel.

18. Troubleshooting

Table 5. Troubleshooting	
Issue	Solution
Key is inserted into slot, but it is not on the list in RAACA app.	<ul style="list-style-type: none"> • Verify authorizations and schedules of current user. • Verify if user with <i>Master exemption</i> can see the key on the list.
No power supply, cannot collect a key.	<ul style="list-style-type: none"> • See Emergency key release in section 17.
Cannot read key fob at reader.	<ul style="list-style-type: none"> • Key fob reading range is limited due to its size. Read the fob as in fig. 3.
Starting screen is not displayed on control panel.	<ul style="list-style-type: none"> • Restart control panel by switching power supply off and on or press the button as in fig. 18. • Start RAACA app manually.
control panel is not reacting for touching.	<ul style="list-style-type: none"> • Verify power supply. • Restart control panel by switching power supply off and on or press the button as in fig. 18.



Fig. 18 Control panel reset button

19. Specification

Table 6. Technical information	
Nominal supply voltage	230VAC
Nominal current consumption	100mA (max. 150mA)
12VDC power output	Max 8.5A
Battery charging current	Configurable: ~0.3A/0.6A/0.9A
Tamper protection	Back cover opening and control panel opening are signaled 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 3 meters cable distance between RKD24CT-SE power unit and RKD24CT-EXT
Environment	Indoor general conditions, temperature: +5°C to +40°C, relative humidity: 10 to 75% (no condensation)
Dimensions H x W x D	RKD24CT: 600 x 969 x 182 mm RKD24CT-EXT: 600 x 677 x 182 mm
Weight	RKD24CT: 48,5 kg RKD24CT-EXT: 39 kg
Compliance	CE, RoHS

Note: Due to the production technology, minor variations in color, shape of cabinet and technical construction between production batches are permissible.

20. Ordering information

Table 7. Ordering information	
RKD24CT-SE	Electronic key cabinet with individual key containers and 7" touch control panel; 24 RFID ID fobs; key fobs attached to keys by user; 230 VAC power supply
RKD24CT-EXT	Electronic key cabinet with individual key containers without control panel; 24 RFID ID fobs; key fobs attached to keys by user; connection to the RKD32 or RKD24CT key cabinet is required
RKD32EXT	Electronic key cabinet without control panel; 32 RFID fobs attached to keys by user; glazed door; external 12V power supply; operates as an extension unit connected to RKD32 main key cabinet
RKD32KF	RFID keyfob; 5 pcs in set

21. Product history

Table 8. Product history		
Version	Date	Description
RKD24CT	01/2022	The first commercial version of product
RKD24CT-SE	01/2026	Modification of the RKD32-CP control panel



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: support@roger.pl

Web: www.roger.pl